Guida per l'utente

11.0

MDaemon Private Cloud
Guida per l'utente

MDaemon Private Cloud 11.0 | MDaemon 23.0.2 | luglio 2024

Sommario

Sezione

1 MDaemon Private Cloud 11.0

Introduzione

MDaemon Messaging Server di MDaemon Technologies è un server di posta basato su standard SMTP/POP3/IMAP che supporta Windows 7, Server 2008 R2 o versioni più recenti e offre un'ampia gamma di funzionalità di server di posta. Dotato di un'ampia suite di potenti strumenti integrati per la gestione di account di posta e dei vari formati di messaggistica, MDaemon è stato progettato per rispondere alle esigenze di posta elettronica di un numero illimitato di utenti. MDaemon include un server di posta scalabile per sessioni SMTP, POP3 e IMAP4, comprensivo di supporto LDAP e Active Directory, un client e-mail basato su browser, strumenti di filtro dei contenuti e della posta indesiderata (spam), avanzate funzioni di sicurezza e molto altro ancora.

Funzioni di MDaemon

Oltre alla gestione della posta SMTP, POP3 e IMAP4, MDaemon offre numerose altre funzionalità. Di seguito è riportato un elenco di alcune funzioni di MDaemon.

- Il supporto completo per la scansione antivirus e la protezione è disponibile come componente aggiuntivo per la licenza di MDaemon o MDaemon Private Cloud. Questo consente l'accesso alla Protezione attacchi 653 in tempo reale e a MDaemon AntiVirus 684. Consente infatti di eseguire la scansione dei messaggi e di ripulirli o eliminarli automaticamente prima che raggiungano i destinatari. Inoltre, è possibile configurare MDaemon per l'invio di un messaggio di notifica del virus all'amministratore, al mittente e al destinatario di un messaggio infetto.
- MDaemon offre una completa suite di servizi per la gestione delle liste di distribuzione e dei gruppi di posta elettronica e consente quindi di creare un numero illimitato di liste di distribuzione diverse, che possono contenere contatti locali e/o remoti. È possibile impostare i parametri delle liste di distribuzione in modo da consentire o rifiutare le richieste di iscrizione, definire il tipo di lista (pubblica o privata), inviare risposte sia alla lista sia al mittente del messaggio, ricevere i messaggi in formato riassunto e configurare una serie di altre funzioni.
- Un componente integrato di MDaemon è Webmail 325. Questa funzionalità consente agli utenti di accedere alle e-mail utilizzando il browser Web preferito invece di un client e-mail dipendente da una workstation. Questo strumento è

perfetto per il personale che viaggia spesso e per gli utenti che non dispongono di un dispositivo dedicato da cui accedere alla propria e-mail.

- MDaemon Webmail è dotato di una serie completa di funzionalità di client e-mail. È possibile: inviare e ricevere messaggi, eseguirne il controllo ortografico, gestire la posta elettronica in più cartelle personali, visualizzare l'interfaccia in 18 lingue, pianificare riunioni e appuntamenti nonché condividere il calendario e le attività con altri utenti, amministrare le impostazioni degli account (se utilizzato insieme a Remote Administration 359), gestire i contatti e molto altro ancora. Webmail dispone inoltre di MDaemon Instant Messenger (MDIM) 326, una piccola utilità che è possibile scaricare e installare sul computer locale dell'utente. Questa utilità consente di accedere facilmente a messaggi e a cartelle e di controllare la posta senza aprire il browser Web. Comprende inoltre un sistema di messaggistica istantanea che può essere utilizzato per rapide "chat" con altri utenti di MDaemon che utilizzano MDIM o un altro client XMPP 381 .
- MDaemon è dotato di numerose funzioni, ideate appositamente per rendere sicuro il sistema di posta elettronica. Spam Filter e DNS Le funzionalità della lista bloccati aiutano a porre fine alla maggior parte dei messaggi e-mail di "spam" che gli "spammer" cercano di indirizzare attraverso o verso il dominio controllato. Vaglio di IP e host e degli indirizzi Le liste bloccati consentono di filtrare e impedire a determinati indirizzi e domini di connettersi o inviare posta attraverso il sistema controllato. Queste funzioni, inoltre, permettono di collegarsi a determinati indirizzi IP controllando al contempo tutti gli altri.
- Grazie al supporto per il protocollo LDAP (Lightweight Directory Access Protocol), MDaemon consente di mantenere un server LDAP costantemente aggiornato su tutti gli account degli utenti. Questa funzione rende possibile la gestione di una rubrica di indirizzi LDAP aggiornata, alla quale possono accedere gli utenti che utilizzano client di e-mail compatibili con LDAP. Inoltre, è possibile utilizzare come database utenti di MDaemon Active Directory o un server LDAP anziché un database compatibile con ODBC o il sistema `USERLIST.DAT` locale. Questa possibilità consente di configurare più server MDaemon in più postazioni in modo da condividere il medesimo database utenti.
- Le complete funzionalità di analisi di MDaemon consentono di usufruire di un servizio di posta elettronica per un'intera LAN mediante un'unica casella postale POP3, con accesso remoto via ISP. In questo modo è possibile utilizzare un servizio di posta elettronica per un'intera rete, a un costo molto più contenuto rispetto a quello normalmente richiesto.
- Gli alias di indirizzo consentono di instradare i messaggi di posta elettronica indirizzati a caselle postali "fittizie" verso account o liste di distribuzione validi. Grazie a tale funzione, è possibile assegnare più indirizzi e-mail a un singolo account e a una singola lista presso uno o più domini.
- La funzione Gateway di dominio offre l'opportunità di impostare domini separati per gruppi o reparti diversi, sia locali all'interno della rete, sia esterni su Internet. Questa funzione fa sì che tutta la posta indirizzata verso un dominio per cui il server MDaemon funge da gateway venga inviata da MDaemon alla casella postale di quel dominio. In questo modo, è possibile raccogliere la posta dal server MDaemon o dal client di posta del dominio in questione e ridistribuirla fra gli utenti del dominio. Questa funzionalità può essere inoltre utilizzata per utilizzare MDaemon come server di posta di backup per altri domini.

- Amministrazione remota basata sul Web Il componente di MDaemon Remote Administration è integrato in MDaemon e Webmail e consente agli utenti di esaminare e modificare le impostazioni dei propri account attraverso il browser Web. È possibile definire le impostazioni che possono essere modificate direttamente dagli utenti, nonché assegnare un'autorizzazione di accesso per ogni account. Remote Administration può essere inoltre utilizzato dall'amministratore (e da un utente con pari privilegi) per controllare o modificare qualunque impostazione di MDaemon e qualsiasi file per cui sia stato autorizzato il controllo mediante il sistema Remote Administration.
- Un sistema interno di trasporto dei messaggi, noto come RAW, costituisce un semplice metodo per trasmettere i messaggi nel flusso della posta, semplificando notevolmente lo sviluppo di software di posta personalizzato. Grazie al sistema RAW è possibile disporre di un sistema completo di posta, utilizzando un semplice editor di testo e una coppia di file batch.
- Un sistema di filtro dei contenuti molto versatile consente di personalizzare il comportamento del server in base al contenuto dei messaggi e-mail in entrata e in uscita. È possibile inserire e aggiungere intestazioni di messaggio, aggiungere piè di pagina ai messaggi, rimuovere gli allegati, inoltrare copie ad altri utenti, attivare l'invio automatico di un messaggio istantaneo, eseguire programmi e altro ancora.

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) è un'edizione speciale di MDaemon Messaging Server sviluppata specificamente per i rivenditori e i fornitori di servizi IT che desiderano utilizzare il software MDaemon per fornire ai loro clienti dei servizi di posta elettronica su host. A differenza di MDaemon, che viene venduto per l'uso on-premise, MDPC è stato creato su una nuova base di licenze e codice progettati specificamente per l'uso in un ambiente basato su host. MDaemon Private Cloud include tutte le funzionalità di MDaemon e le seguenti funzionalità aggiuntive:

- Nuove licenze e fatturazione (per utente/al mese)
- Supporto per Outlook
- Controllo dei domini multipli migliorato
- Branding per dominio (etichetta bianca)
- Report per dominio
- Account di test utente non fatturabili (i conteggi non vengono inclusi nella fatturazione totale)
- Protezione attacchi, MDaemon AntiVirus e il motore antivirus ClamAV (opzionale, da pagare a parte)
- ActiveSync per MDaemon (opzionale da pagare a parte)

Requisiti di sistema

Per informazioni più aggiornate sui requisiti di sistema e sulle raccomandazioni di MDaemon, visitare la pagina Requisiti di sistema all'indirizzo mdaemon.com.

Marchi

Vedere:

Novità di MDaemon Private Cloud 11.0 15
Aggiornamento a MDaemon Private Cloud 11.0.0 65
Schermata principale di MDaemon 74
Guida 70

1.3 Novità di MDaemon Private Cloud 11.0

Novità di MDaemon Private Cloud 11.0.0

- MDaemon Private Cloud 11 comprende MDaemon 23.0.2 con MDaemon Connector 7.0.7.

MODIFICHE E NUOVE FUNZIONI

- [26947] Aggiornato MDaemon alla versione 23.0.2. Le novità relative a MDaemon 23.0.2 sono disponibili al seguente indirizzo: Note di rilascio di MDaemon 23.0.2.
- [26491] MDaemon disattiva l'aggiornamento automatico del client di MDaemon Connector nelle versioni precedenti alla 7.0.6, per risolvere un bug dell'aggiornamento automatico in quelle versioni.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 24.0.1.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 8.0.1.

Novità della versione 23.0 di MDaemon

Modifiche e nuove funzioni

Server MDaemon

- (23.0.2) Aggiunta un'opzione in Impostazioni | Impostazioni server | MultiPOP 146 per l'invio di un'e-mail di notifica in caso di più tentativi non riusciti durante la verifica di un account MultiPOP. Poiché i problemi temporanei non sono rari, è possibile scegliere il numero di tentativi non riusciti consecutivi che attivano la notifica. È inoltre presente un'opzione per stabilire quanti giorni devono passare

tra una notifica e l'altra, per evitare di inviarne troppe. Il contenuto e i destinatari delle e-mail di notifica possono essere personalizzati modificando \MDaemon\App\MPOPFailureNotice.dat. Per impostazione predefinita, le notifiche vengono inviate dopo 5 errori, non più di una volta ogni 7 giorni, al proprietario dell'account MultiPOP.

- È stata aggiunta una nuova pagina MultiPOP 146 sotto Impostazioni server. In questa pagina è possibile attivare/disattivare il server MultiPOP di MDaemon e utilizzare l'opzione "*MultiPOP elimina sempre la posta...*" (in precedenza disponibile nella pagina Raccolta MultiPOP 391) per ignorare l'impostazione dell'opzione *Lascia una copia del messaggio sul server POP* 754 per tutti gli utenti. Questa nuova pagina contiene anche le opzioni di supporto OAuth 2.0 per la raccolta di posta MultiPOP da Gmail e Office 365.

  Supporto MultiPOP OAuth 2.0 per la raccolta della posta da Gmail e Office 365 147: OAuth 2.0 è un metodo di autenticazione moderno, che questi servizi ora richiedono poiché stanno disabilitando il supporto per l'autenticazione tradizionale/di base.Affinché la funzione MultiPOP di MDaemon utilizzi OAuth 2.0 per raccogliere la posta da Gmail o Office 365 per conto degli utenti, è necessario registrare il server MDaemon con Google o Microsoft, rispettivamente, creando un'app OAuth 2.0 con la Google API Console o con Azure Active Directory di Microsoft. Questa procedura è simile a quella richiesta per l'utilizzo dell'integrazione con Dropbox 345 di MDaemon per gli utenti Webmail. Per ulteriori informazioni sulla configurazione del supporto di OAuth 2.0, vedere l'argomento della Guida in linea MultiPOP 147.

- Il server IMAP di MDaemon ora supporta i flag delle parole chiave. Questo consente ai client e-mail come Mozilla Thunderbird di memorizzare i tag dei messaggi sul server, in modo da consentire la visualizzazione dei tag impostati in un'istanza di un client da un'altra istanza del client.

- Migliorate le prestazioni del server IMAP quando si aprono cartelle di posta di grandi dimensioni.

Sicurezza

- (23.0.2) Aggiunto il supporto per Spamhaus Data Query Service (DQS) in Sicurezza | Spam Filter 691. Per ulteriori informazioni su Spamhaus DQS visitare il sito https://info.spamhaus.com/getting-started-with-dqs.

- È disponibile una nuova opzione *Blocca violazioni criteri di accesso* in Vaglio dinamico 623 che si può utilizzare per bloccare qualsiasi indirizzo IP che tenti di accedere senza utilizzare l'indirizzo e-mail completo. Questa opzione è disattivata per impostazione predefinita. Vedere la pagina Sistemi 501 per ulteriori informazioni sull'opzione corrispondente "*I server richiedono l'indirizzo e-mail completo per l'autenticazione*".

- È stata aggiunta un'opzione *Solo per gli account validi* per espandere l'opzione *Ignorare i tentativi di autenticazione che utilizzano password identiche* disponibile nella pagina Rilevamento errore di autenticazione 627. Attivare questa opzione per ignorare i tentativi di autenticazione con password duplicata solo quando i tentativi di accesso riguardano un account valido. Questo significa che se, ad esempio, un utente aggiorna la propria password in un client, ma un altro client è ancora in esecuzione con la vecchia password, i tentativi di accesso del vecchio client saranno comunque ignorati, poiché il nome di accesso del client è

corretto. Un bot che tentasse nomi di accesso casuali con una password simile non godrà dello stesso vantaggio e sarà bloccato non appena superata la soglia di errori di autenticazione. In tal modo sarà possibile sconfiggere i bot molto più rapidamente. Anche l'operazione DynamicScreen dell'API XML è stata aggiornata per l'implementazione di queste nuove funzionalità.

- Un'opzione Filtro contenuti » Allegati[672] è stata aggiunta a: "*Aggiungere un avviso all'inizio del corpo del messaggio se l'allegato è stato rimosso*". Quando rimuove un allegato da un messaggio, ad esempio perché è stato rilevato un virus, MDaemon aggiunge un di avviso all'inizio del corpo del messaggio. È inoltre disponibile un pulsante **Avviso** da utilizzare per rivedere o modificare il modello del messaggio di avviso. L'opzione è abilitata per impostazione predefinita.
- Aggiunta l'opzione *Escludi IP attendibili dalla scansione AntiVirus*[684].
- MDaemon invia un'e-mail di avviso agli amministratori quando i certificati SSL[585] configurati per l'uso con MDaemon[587], Webmail[590] o Remote Administration[594] stanno per scadere.
- MTA-STS[601] dispone ora di un elenco di esenzione, per cui i domini problematici possono essere esentati invece di dover disattivare MTA-STS quando gli errori influiscono sul recapito dei messaggi.
- Il componente ClamAV è stato aggiornato alla versione 0.105.2 (in MDaemon 23.0.1).

Webmail

- Integrazione con Google Drive[348]: Webmail ora può essere collegato all'account Google degli utenti per offrire loro la possibilità di salvare gli allegati dei messaggi direttamente nel proprio account di Google Drive e di modificare e lavorare con i documenti che archiviano. Per attivare questa funzionalità, sono necessari **chiave API**, **ID del client** e **segreto client**. Tutti questi dati si ottengono direttamente da Google creando un'app con la Google API Console e registrando il proprio MDaemon presso l'apposito servizio. Di questa app fa parte un componente di autenticazione OAuth 2.0, che consente agli utenti di accedere a Webmail e di autorizzare quindi l'accesso degli utenti ai rispettivi account Google Drive mediante MDaemon. Una volta autorizzati, gli utenti possono visualizzare le cartelle e i file archiviati su Google Drive. Inoltre, gli utenti possono caricare, scaricare, spostare, copiare, rinominare ed eliminare file, nonché copiare/spostare file da e verso le cartelle di documenti locali. Per modificare un documento, l'utente può fare clic sull'opzione per visualizzare il file in Google Drive e modificarlo in base alle autorizzazioni impostate in Google Drive. Il processo di configurazione di Google Drive è simile all'Integrazione Dropbox[345] di MDaemon e alle funzionalità di integrazione MultiPOP OAuth[146]. Vedere Integrazione con Google Drive[348] per ulteriori informazioni.
- Aggiunta un'opzione in tutti i temi, tranne Lite: "*Attiva trascinamento per spostare le cartelle*". La nuova opzione si trova in Webmail nella pagina **Cartelle** nel menu Opzioni ed è attivata per impostazione predefinita.
- Reso sicuro il cookie di sessione su HTTPS.
- La notifica di modifica della categoria ora viene inviata a MDaemon
- WorldClient non modifica più il file robots.txt all'avvio.

- Il server Web integrato impedisce il download di file .dll dalla directory HTML.
- Aggiunto un criterio alla lunghezza massima della nuova password, in modo da visualizzare il messaggio del requisito "Massimo 15 caratteri" non soddisfatto.
- È stato aggiunto un rapporto per i tentativi di accesso senza un indirizzo e-mail completo, a supporto della nuova opzione del Vaglio dinamico Blocca violazioni criteri di accesso 623.
- (23.0.2) L'opzione di annullamento della posposizione è stata resa più visibile con un'evidenziazione arancione.

Tema Pro

- Aggiunto il supporto per le ricevute di lettura.
- Aggiunta un'opzione per la disabilitazione del menu contestuale dell'editor HTML.
- Aggiunta la possibilità di ridimensionare l'elenco delle cartelle.

Remote Administration (MDRA)

23.0.2

- Aggiunta la casella di controllo a "Escludi IP accreditati dalla scansione AntiVirus 684"
- Aggiunta l'impostazione Non consentire l'autenticazione sulla porta SMTP 531
- Aggiunta un'opzione per il nome visualizzato di ActiveSync in Impostazioni | Cartelle pubbliche | Gestione cartelle pubbliche 317 | Modifica
- Aggiunte altre quattro opzioni di filtro per l'elenco degli utenti 726: Solo amministratori, Solo non amministratori, Solo amministratori globali e Solo amministratori di dominio
- Aggiunta la pagina DQS a Spam Filter 691 | Data Query Service. Per ulteriori informazioni su Spamhaus DQS visitare il sito https://info.spamhaus.com/getting-started-with-dqs.

23.0.0

- In Domain Manager ora è presente una nuova voce Impostazioni Webmail 354: "*Consenti agli utenti di ricevere i codici di verifica dell'autenticazione a due fattori via e-mail*", in modo che gli utenti possano ricevere il codice di verifica tramite un indirizzo e-mail alternativo anziché utilizzare l'app Google Authenticator. Questa opzione è attivata per impostazione predefinita.
- Modificate le autorizzazioni predefinite quando si aggiunge una nuova voce ACL a Lookup e Read.
- I pulsanti **Test** in: Spam Filter » DNS-BL » Host 718 e Impostazioni » Active Directory » Autenticazione 838 ora vengono disattivati durante la procedura.
- Il server Web integrato impedisce l'esecuzione e il download di file .dll nella directory Templates.
- Ora gli utenti possono personalizzare l'aspetto dell'interfaccia Web di Remote Administration facendo clic sul proprio nome utente (ad esempio, frank.thomas) nell'angolo superiore destro della finestra. Sono disponibili opzioni per impostare

l'interfaccia in Modalità scura, impostare la dimensione dei caratteri e scegliere la Lingua che si preferisce.

- La conferma dell'eliminazione dell'account è stata modificata per consentire l'utilizzo della funzione di conferma personalizzata.
- È stato aggiunto un rapporto del per i tentativi di accesso senza un indirizzo e-mail completo.

ActiveSync

- Aggiunta un'opzione Impostazioni client per *bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata* 430. Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.
- Ora è possibile disattivare il pulsante Cancellazione completa 470 per i client ActiveSync se necessario, in modo che non sia possibile eseguire una Cancellazione completa da remoto su un dispositivo ActiveSync senza prima disabilitare la nuova opzione Impedisci cancellazioni da ripristino impostazioni di fabbrica 430.
- I dati di BodyPreferences sono stati resi leggibili per facilitare la risoluzione dei problemi di sincronizzazione.
- Migliorate le prestazioni in arresto quando i client sincronizzano caselle di posta di grandi dimensioni.
- Aggiunta la possibilità di definire un nome di visualizzazione personalizzato per le cassette postali e le cartelle pubbliche.
- Migliorate le prestazioni in arresto.
- I client ActiveSync ora possono inviare alle liste di distribuzione personali nelle cartelle dei contatti.
- Modificato il layout della finestra di dialogo delle impostazioni del client nell'interfaccia grafica per ricavare spazio per le nuove impostazioni.

Altro

- (23.0.2) Filtro contenuti: è possibile utilizzare $LIST_ATTACHMENTS_REMOVED$ 677 nell'azione della regola (ad esempio, "invia nota", "aggiungi avviso...")
- Modificate nell'interfaccia grafica di MDaemon le autorizzazioni predefinite quando si aggiunge una nuova voce ACL a Lookup e Read.
- Aggiunta nell'interfaccia grafica di MDaemon un messaggio di avviso a comparsa che viene visualizzato quando si tenta di impostare le porte di Webmail, Remote Administration o Server BOSH XMPP con valori in conflitto.
- XMLAPI: aggiunta l'operazione Editor che si può utilizzare per modificare alcuni file INI di MDaemon
- Modificati alcuni plug-in per consentire l'esecuzione di versioni più recenti, in modo che i clienti possano testare eventuali versioni di hotfix/patch.

- LetsEncrypt: script aggiornato per il controllo degli ordini che sono pronti o validi.

Note di rilascio per il server MDaemon

Per un elenco completo delle funzionalità aggiunte, delle modifiche e delle correzioni incluse in MDaemon 23.0.2, vedere le Note di rilascio di MDaemon.

New in MDaemon Private Cloud 10.0.1

- MDaemon Private Cloud 10.0.1 includes MDaemon 22.0.4 with MDaemon Connector 7.0.7.

Informazioni Speciali

- Cyren Anti-Virus è stato sostituito da IKARUS Anti-Virus. Cyren di recente ha annunciato i suoi piani di interrompere le proprie attività con poco preavviso. Per questo motivo abbiamo dovuto cercare un nuovo partner anti-virus. A seguito di un'attenta valutazione, IKARUS si è distinto per l'eccellente velocità e tasso di rilevamento. IKARUS Anti-Virus aggiorna automaticamente le sue definizioni ogni 10 minuti. Scanning with IKARUS is disabled if your AntiVirus license is expired.
- La Protezione dagli attacchi di Cyren è stata rimossa. Cyren di recente ha annunciato i suoi piani di interrompere le proprie attività con poco preavviso. Stiamo attivamente facendo ricerche e considerando tecnologie antispam utilizzabili come aggiunte adatte ai meccanismi antispam già esistenti nei nostri prodotti software.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 22.0.4.

Novità di MDaemon Private Cloud 10.0.0

- MDaemon Private Cloud 9.5 comprende MDaemon 22.0.3 con MDaemon Connector 7.0.7.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 22.0.3.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 7.0.7.

Novità della versione 22.0 di MDaemon

Modifiche e nuove funzioni

Webmail

Tema Pro

- Durante la visualizzazione di un messaggio, è possibile posizionare il mouse sul nome del mittente per visualizzare una finestra a comparsa con le opzioni per aggiungere il mittente ai Contatti e alle cartelle dei mittenti consentiti o bloccati.
- Le viste Componi, Messaggio, Evento, Contatto, Attività e Nota ora si possono aprire in una nuova finestra.
- Ora è possibile aprire il messaggio non letto successivo dal riquadro di anteprima dei messaggi e dalla vista dei messaggi.
- Aggiunti i frammenti di messaggio all'elenco dei messaggi in modalità multilinea.
- Ora è possibile rendere disponibile un'opzione *Modifica nomi alias visualizzati* per gli utenti del tema Pro. Si trova in Impostazioni » Componi. L'opzione consente agli utenti di modificare il nome alias visualizzato associato al proprio account. Utilizzare "*Consenti agli utenti di modificare i nomi alias visualizzati*" nelle impostazioni Webmail 354 per consentire questa azione. **Nota:** L'opzione è disponibile solo nell'interfaccia Web di MDaemon Remote Administration (MDRA) 359.
- Le opzioni e i collegamenti che prima facevano riferimento a "lista bianca" o "lista nera" dei mittenti, ora fanno riferimento alle liste "consentiti" o "bloccati" dei mittenti. Inoltre, le cartelle Lista bianca e Lista nera ora sono denominate "Mittenti consentiti" e "Mittenti bloccati".
- L'elenco dei messaggi può essere ordinato in base alla colonna Flag.
- Nell'elenco Attività, le attività in ritardo ora sono evidenziate in rosso.
- Aggiornato il client XMPP alla versione 4.4.0.

Altro

- Quando sono richieste password complesse, ora è disponibile un elenco di requisiti per le password che viene visualizzato in verde e spuntato non appena l'utente soddisfa i requisiti. Aggiunti inoltre nuovi messaggi di errore più descrittivi per quanto riguarda l'errore di password non valida al momento dell'invio.
- Le opzioni di composizione ora comprendono le opzioni per la selezione dell'indirizzo "Da:" predefinito che verrà utilizzato quando si compone, si risponde o si inoltra un messaggio.
- È stata aggiunta l'impostazione "1 minuto" all'opzione Tempo di aggiornamento della lista, disponibile nella pagina Opzioni » Personalizza".
- Aggiunto il supporto per i CSRFTokens nella pagina di accesso di Webmail. Il supporto si attiva quando si abilita l'opzione "*Usa i token Cross-Site-Request-*

Forgery" nella pagina Impostazioni Webmail » Server Web[330]. Se si utilizzano modelli personalizzati per Webmail, aggiungere un input nascosto al modulo di accesso come segue: `<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />`

- Calendario pubblico: modificata la visualizzazione dell'elenco in modo che inizi dal giorno corrente e mostri i 30 giorni successivi.
- Aggiunta la conversione automatica degli URL in collegamenti ipertestuali nella visualizzazione dei messaggi.
- I nomi delle cartelle predefinite (Bozze, Posta inviata, ecc.) sono tradotti nella lingua dell'utente di Webmail, indipendentemente dalla lingua di MDaemon installata (in precedenza accadeva solo per MDaemon in inglese).
- Ora è disponibile un'opzione per inviare i codici di verifica dell'Autenticazione a due fattori a un indirizzo e-mail secondario.
- Temi LookOut e WorldClient: modificato il comportamento di visualizzazione di tutte le categorie dell'elenco in modo che corrispondano.
- Le cartelle Mittenti consentiti e Mittenti bloccati ora hanno icone diverse, a indicare che si tratta di cartelle speciali.

Remote Administration (MDRA)

- Aggiunta una pagina IP eccezioni autenticazione a due fattori MDRA, disponibile nel menu Principale. Gli utenti possono quindi accedere a Remote Admin o Webmail senza richiedere la 2FA quando si connettono da uno degli indirizzi IP specificati.
- La nuova opzione "*Consenti agli utenti di modificare i nomi alias visualizzati* è ora disponibile nelle Impostazioni Webmail[354] di MDRA. Attivare questa opzione per consentire agli utenti di modificare il nome alias visualizzato associato al proprio account. Per modificare il nome alias, gli utenti possono utilizzare l'opzione *Modifica nomi alias visualizzati*, disponibile nel tema Pro.
- Modificato autocomplete="off" in autocomplete="new-password" nei campo per le password per impedire a Firefox di compilare automaticamente le password fuori dalla pagina di accesso.
- Aggiunto l'editor dei messaggi di notifica alla pagina Notifiche[674] del filtro dei contenuti.
- Aggiunto il supporto per i CSRFTokens nella pagina di accesso. Il supporto si attiva quando si abilita l'opzione "*Usa i token Cross-Site-Request-Forgery*" nella schermata Impostazioni Remote Administration in MDRA.
- Le eventuali Code personalizzate[893] remote o locali create si possono gestire nella sezione Messaggi e code in MDRA.

Sicurezza

- MDaemon ora supporta TLS 1.3 sulle versioni più recenti di Windows. In Windows Server 2022 e Windows 11 TLS 1.3 è abilitato per impostazione predefinita. Le versioni di Windows 10 2004 (OS Build 19041) e successive

dispongono di un supporto TLS 1.3 sperimentale che si può abilitare per le connessioni in entrata impostando quanto segue nel Registro di sistema:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
    ders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- MDaemon registra la suite di cifratura (ad esempio, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) utilizzata dalle connessioni SSL/TLS.
- Aggiunta un'opzione Password 870 per la richiesta di inserimento di un carattere speciale nelle password complesse. La funzionalità è attivata per impostazione predefinita per le nuove installazioni, ma disattivata per impostazione predefinita per le installazioni già esistenti.
- Scanner AV per le cassette postali: quando viene rilevato un messaggio infetto durante la scansione della cassetta postale, il contatore di file infetti di MDaemon viene incrementato.
- AntiVirus: aggiornato ClamAV alla versione 0.104.3

ActiveSync

- Migliorate le prestazioni di FolderSync.
- La finestra di dialogo di monitoraggio delle connessioni di ActiveSync ora dispone di una nuova opzione nel menu contestuale che consente di terminare una sessione e bloccare un client.
- Aggiunta un'opzione alla finestra di dialogo Impostazioni client 470 per consentire a Outlook di inviare e-mail utilizzando un alias. Se l'intestazione "Reply-To" è impostata su un alias valido per l'account mittente, il messaggio sarà inviato con tale alias.
- Aggiunto il supporto per il comando Trova di EAS 16.1. Rimossa la restrizione del protocollo 442 che impediva a iOS di utilizzare EAS 16.1

Altro

- Filtro contenuti: aggiunto il supporto per le macro $CONTACT...$ nell'azione "Aggiungi una firma aziendale 661". Queste macro si possono utilizzare per personalizzare la firma con le informazioni del contatto del mittente nella rispettiva cartella dei contatti pubblici. Vedere: Macro firme 137 per un elenco completo delle macro supportate.
- Filtro contenuti: aggiunta un'azione per l'estrazione di allegati 661 e l'aggiunta di collegamenti ad allegati 373 nel messaggio.
- Le e-mail di riepilogo 890 per coda in sospeso, di quarantena e scartati ora possono contenere i collegamenti per rilasciare, riaccodare o eliminare ciascun messaggio. Questa nuova opzione "*Includi il collegamento dell'azione*" è abilitata per impostazione predefinita. Nota: L'URL di Remote Administration 361 deve essere impostato per generare i collegamenti.

- LetsEncrypt 605: aggiornato lo script per consentirne il funzionamento con PS 7.
- Aggiunta un'opzione Richiamo messaggio 124 del Recapito differito per sostituire l'intestazione "Date:" con la data e l'ora correnti al momento del rilascio del messaggio dalla Coda differita. Questa opzione è disabilitata per impostazione predefinita.
- MDaemon Connector 395 è stato aggiornato alla versione 7.0.7.
- XMLAPI: aggiunto il supporto per la pianificazione dell'inoltro.

Note di rilascio per il server MDaemon

Per un elenco completo delle funzionalità aggiunte, delle modifiche e delle correzioni incluse in MDaemon 22.0, vedere le Note di rilascio di MDaemon.

Novità di MDaemon Private Cloud 9.5.0

- MDaemon Private Cloud 9.5 comprende MDaemon 21.5.2 con MDaemon Connector 7.0.6.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 21.5.2.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 7.0.6.

Novità della versione 21.5 di MDaemon

Nuove funzioni principali

Password di applicazione 766

Le password di applicazione sono password molto sicure, generate in modo casuale, da utilizzare nei client e nelle applicazioni di posta elettronica, per contribuire a rendere più sicure le applicazioni di posta elettronica che non possono essere protette da autenticazione a due fattori 735 (2FA). La 2FA è un metodo sicuro che gli utenti possono utilizzare per accedere a Webmail o a MDaemon Remote Administration (MDRA), ma un'applicazione di posta elettronica non può utilizzarla, poiché deve essere in grado di accedere alla posta elettronica in background senza che l'utente debba inserire un codice dall'applicazione di autenticazione. Le funzionalità delle password di applicazione consente di creare password solide e sicure da utilizzare nelle applicazioni, mantenendo la password dell'account protetta da 2FA. Le password di applicazione si possono utilizzare solo nelle applicazioni di posta elettronica, non è possibile utilizzarle per accedere a Webmail o MDRA. Ne consegue che, anche se una password di applicazione venisse in qualche modo compromessa, l'utente non autorizzato non sarebbe comunque in grado di accedere all'account dell'utente legittimo e modificare la password o altre impostazioni, mentre l'utente legittimo sarà comunque in grado di accedere all'account con la password dell'account e la 2FA per eliminare la password dell'applicazione compromessa e crearne una nuova, se necessario.

Requisiti e raccomandazioni per la password di applicazione

- Per creare le password di applicazione, è necessario che la 2FA sia attivata per l'account (anche se si può eliminare questo requisito 870 se necessario).
- Le password di applicazione si possono utilizzare solo nelle applicazioni di posta elettronica, non è possibile utilizzarle per accedere a Webmail o MDRA.
- Ogni password di applicazione viene visualizzata solo una volta, al momento della creazione. Non sarà possibile recuperarla in un secondo momento, quindi gli utenti devono essere pronti a immettere la password nella propria applicazione quando questa viene creata.
- Gli utenti devono utilizzare una password di applicazione diversa per ogni applicazione di posta elettronica e devono revocare (eliminare) la password ogni volta che smettono di utilizzare un'applicazione o quando il dispositivo viene smarrito o rubato.
- Per ogni password di applicazione viene specificato il momento della creazione, quando è stata utilizzata per l'ultima volta e l'indirizzo IP da cui è stato effettuato l'ultimo accesso all'e-mail dell'account. Se un utente rileva qualcosa di sospetto nei dati relativi all'ultimo utilizzo o all'ultimo IP, deve revocare la password e crearne una nuova per la propria applicazione.
- Quando si cambia la password di un account, tutte le password di applicazione vengono eliminate automaticamente: l'utente non può continuare a usare le password di applicazione precedenti.

Richiesta di password di applicazione per SMTP, IMAP, ActiveSync e altro

Nella pagina di impostazioni di Account Editor 776 è disponibile un'opzione per gli account: "*Richiedi la password di applicazione per l'accesso a SMTP, IMAP, ActiveSync, ecc.*".

La richiesta di password di applicazione può aiutare a proteggere le password degli account da attacchi a dizionario e a forza bruta via SMTP, IMAP, ecc. La sicurezza è garantita dal fatto che, ove mai con un attacco di questo tipo si riuscisse a indovinare la password reale di un account, questa non funzionerebbe senza che l'aggressore possa accorgersene, perché MDaemon accetta solo una password di applicazione corretta. Inoltre, se gli account in MDaemon utilizzano l'autenticazione con Active Directory 835 e si è configurato Active Directory in modo da bloccare un account dopo un certo numero di tentativi non riusciti, questa opzione può aiutare a prevenire il blocco degli account, poiché MDaemon verifica solo le password di applicazione e non tenta l'autenticazione con Active Directory.

Altri miglioramenti e nuove funzionalità

Tema Pro

- Il tema Mobile ora è denominato **Pro**. È stato ampliato e migliorato per essere reattivo e adattabile all'uso su tipi di dispositivi e dimensioni dello schermo diversi, senza sacrificare le funzionalità.
- Sono stati aggiunti i token Cross-Site-Request-Forgery per garantire transazioni più sicure. La funzionalità è disabilitata per impostazione predefinita. Per

abilitarla da MDRA, passare a Principale | Impostazioni Webmail | Server Web 330 e selezionare "Usa token Cross-Site-Request-Forgery".

- Aggiunta un'opzione in Impostazioni | Personalizza per l'attivazione della modalità scura e la visualizzazione del tema Pro con uno sfondo scuro.
- Aggiunto un collegamento a "Traccia il mio pacco" nei messaggi aperti.
  - I numeri di tracciamento dei vettori che vengono controllati per impostazione predefinita sono: USPS, UPS, OnTrac, FedEx e DHL.
  - Il file di configurazione predefinito è memorizzato in: `\MDaemon\WorldClient\package_tracking.json`
  - Gli amministratori possono aggiungere altri vettori creando il file: `\MDaemon\WorldClient\package_tracking.custom.json`, con lo stesso formato del file `package_tracking.json` predefinito. Sono richiesti almeno un nome del servizio, un URL di tracciamento e un'espressione regolare valida. Includere i nomi dei servizi che potrebbero essere riportati in un messaggio per ridurre le probabilità di false corrispondenze positive.
- Aggiunta la finestra di dialogo Layout elenco messaggi al browser ridotto. Viene visualizzata solo l'impostazione Densità elenco messaggi.
- Aggiunto un misuratore della complessità della password.
- Aggiunta la funzione di presentazione delle immagini per la vista Messaggio.
- Aggiunta di una visualizzazione a schede per l'elenco Contatti.
- Spostato il pulsante "Nuova voce" dalla barra degli strumenti allo spazio sopra l'elenco delle cartelle in considerazione delle dimensioni del desktop.
- Aggiunta un'icona + (segno più) accanto a "Personale" per creare un nuovo calendario nella vista Calendario.
- Aggiunta una descrizione comandi dell'evento con le opzioni Modifica e l'opzione Invia un'e-mail a un partecipante.
- La barra di ricerca è sempre visibile per finestre del browser di larghezza pari o superiore a 1200 pixel.
- Aggiunta una finestra di dialogo per consentire agli utenti di rimuovere dalla Lista bloccati un contatto aggiunto alla Lista consentiti e viceversa.
- Aggiunto un messaggio che viene visualizzato quando si verifica un errore nella creazione o nella ridenominazione di una cartella.
- Aggiunto il supporto per le note HTML in Eventi, Contatti, Attività e Note.
- Sostituito l'attuale editor HTML (CKEditor) con Jodit.
- Modificata la visualizzazione dell'intestazione di base in modo da includere l'indirizzo e-mail riportato nel campo Da.
- Aggiunto il registratore vocale.

Altri miglioramenti di Webmail

- Aggiunto un collegamento Annulla iscrizione accanto all'indirizzo riportato in Da quando l'intestazione List-Unsubscribe è presente in un messaggio. Questa funzionalità si può disattivare in Webmail in Impostazioni | Personalizza.
- Aggiunta la possibilità di importare le e-mail nell'elenco messaggi corrente.
- Aggiornata l'integrazione Dropbox in modo che utilizzi il refresh_token fornito da Dropbox per la riconnessione degli utenti senza interazioni con la finestra di dialogo OAuth. Quando l'access_token scade, Webmail cercherà di utilizzare il refresh_token per ottenere un nuovo access_token. Le impostazioni non più necessarie sono state rimosse dalla pagina App Cloud. L'amministratore NON deve apportare alcuna modifica all'app Dropbox su Dropbox.com.
- Le richieste di Ricerca tutto/Sottocartelle non prevedono più la ricerca nelle cartelle non sottoscritte quando queste sono nascoste.
- Aggiunta una casella di controllo "Salta ricerca" per escludere cartelle specifiche dalle richieste Ricerca tutto/Sottocartelle.
- Aggiunta un'impostazione in Remote Admin che consente di nascondere la casella di controllo Ricordati di me dell'Autenticazione a due fattori.
- Aggiunto un effetto di sfocatura per lo sfondo quando la sessione utente è scaduta.
- Aggiunta una funzione Cc e Ccn automatica in Impostazioni | Componi.
- Aggiunta un'opzione in: `WorldClient\Domains.ini [Default:Settings] PreventComposeWithAlias` per impedire la composizione di messaggi con un alias. L'impostazione è disattivata per impostazione predefinita.
- Tema Lite: aggiunta la funzione di salvataggio automatico delle bozze di messaggio alla vista Componi.
- Aggiunta un'opzione nella vista Opzioni | Cartelle per consentire agli utenti di saltare le cartelle dei contatti nelle ricerche con compilazione automatica. Aggiunta l'opzione anche nel menu che si visualizza con il pulsante destro del mouse.
- Aggiunta una voce di registro di Webmail per lo User-Agent quando un utente effettua l'accesso.
- Aggiunta una notifica nella vista Componi che viene emessa quando un destinatario locale ha il risponditore automatico attivato.
- Tema WorldClient: aggiunta l'icona di una graffetta ai riquadri degli eventi con allegati.
- Le dimensioni massime degli allegati è impostata a 25 MB per le nuove installazioni.
- L'azione della cartella "Elimina tutto" è stata modificata in "Svuota cartella"
- Tema WorldClient: aggiunti i pulsanti "Modifica password" e "Modifica e-mail di ripristino" alla pagina Sicurezza

Remote Administration (MDRA)

- Aggiunta la possibilità di trascinare le regole di filtraggio dei contenuti. I pulsanti per copia, modifica ed eliminazione ora sono presenti in ogni regola.
- Sono stati aggiunti i token Cross-Site-Request-Forgery per garantire transazioni più sicure. Per impostazione predefinita questa funzionalità è attivata. Per disattivarla passare a: Principale | Impostazioni Remote Admin | Impostazioni e deselezionare "Usa token Cross-Site-Request-Forgery".
- Aggiunta un misuratore della complessità della password ad alcuni dei campi per le password.
- Aggiunta l'opzione: "Attiva Ricordati di me per l'Autenticazione a due fattori" a Impostazioni | Domain Manager | Modifica | Impostazioni Webmail 198 e Principale | Impostazioni Webmail | Impostazioni 354.
- Aggiunti i rapporti IP bloccati e IP rifiutati per il vaglio dinamico.
- Aggiunte le viste Gruppi 479 e Tipi client 486 in ActiveSync.
- Aggiornate le pagine Diagnostica 440 e Regolazione 427 di ActiveSync.
- Aggiunti un grafico e una tabella sull'utilizzo del browser in base al sistema operativo in Rapporti | Traffico | Statistiche di accesso a Webmail.
- Aggiunti i pulsanti per aprire una finestra a comparsa Sfoglia utenti e Sfoglia gruppi, per l'aggiunta alle liste di distribuzione: Principale | Liste di distribuzione | Modifica | Nuova 281. Solo gli amministratori di dominio o globali 773 possono accedere ai pulsanti.
- Aggiunte le opzioni Cancellazione solo account in Principale | Account personale | Client ActiveSync e in ActiveSync | Gestione client 470.
- È stata aggiunta la registrazione delle modifiche. Registrerà ogni modifica apportata mediante Remote Administration.
- Aggiornata la funzione Richiamo messaggio 124 per farla corrispondere all'interfaccia grafica di MDaemon.
- Aggiunta l'opzione "Estrai allegati da winmail.dat" a Sicurezza | Filtro contenuti | Compressione 681.
- Aggiunta la lingua slovena a MDaemon Remote Administration.

Altri miglioramenti di MDaemon

- Aggiunto il supporto di pipelining dei comandi SMTP (RFC 2920). MDaemon invierà i comandi MAIL, RCPT e DATA in batch invece che singolarmente, migliorando così le prestazioni sui collegamenti di rete a latenza elevata. Il pipelining SMTP viene sempre utilizzato per le connessioni in entrata. La funzionalità abilitata per impostazione predefinita per le connessioni in uscita, ma si può disabilitare in Impostazioni | Impostazioni server | Server e recapito | Server 94.
- Aggiunto il supporto per SMTP CHUNKING (RFC 3030). CHUNKING consente di trasferire messaggi non-line-oriented. La funzionalità è attivata per impostazione predefinita per le connessioni in entrata, ma disattivata per quelle in uscita. Gli avanzamenti riga semplici nei messaggi ricevuti vengono convertiti

in avanzamenti riga con ritorno a capo per impostazione predefinita. Queste impostazioni predefinite si possono modificare impostando `[Special] SMTPChunkingInbound=Yes/No`, `SMTPChunkingOutbound=Yes/No` e `SMTPChunkingAllowBareLF=Yes/No` in `\MDaemon\App\MDaemon.ini`.

- Filtro contenuti: aggiornato l'elenco di allegati con restrizioni[672] predefinito.
- Filtro contenuti: aggiunta l'azione della regola per aggiungere gli allegati al messaggio[661].
- Le voci di avvio/arresto del server ActiveSync vengono riportate nel Registro di sistema di MDaemon.
- Clustering: aggiunto il supporto per la sincronizzazione dei promemoria dai nodi secondari.
- Vaglio dinamico: aggiunta l'opzione Registra posizioni utilizzando i codici ISO-3166[623] per registrare i codici invece dei nomi.
- XMLAPI: aggiunto il supporto per l'impostazione AlwaysSendMeetingUpdates di ActiveSync.
- XMLAPI: aggiunto il supporto per la creazione del file Semaphore.
- XMLAPI: aggiunto il supporto per la segnalazione/modifica delle impostazioni da Impostazione/Impostazioni server/Registrazione.
- MDaemon Instant Messenger: la funzione di chat di gruppo è stata migliorata con l'aggiunta della possibilità di selezionare più amici di chat per la chat di gruppo. Aggiunta anche un'opzione per accettare in automatico le richieste di chat room.
- Screening posizione[582] contiene una nuova opzione che consente di controllare se l'intestazione `X-MDOrigin-Country` deve essere aggiunta o meno ai messaggi. L'opzione è abilitata per impostazione predefinita.
- Ora è disponibile un'impostazione degli account per consentire o meno agli utenti di accedere utilizzando gli alias, selezionabile in: Account | Impostazioni account | Alias | Impostazioni[849]. L'opzione è abilitata per impostazione predefinita.
- MDaemon Connector è stato aggiornato alla versione 7.5.0.
- Il testo predefinito del messaggio di conferma della consegna (in \MDaemonAppReceipt.dat) è stato modificato in modo da utilizzare la macro $HEADER:X-RCPT-TO$ invece di $RECIPIENT$ per evitare di rivelare l'indirizzo e-mail reale a cui fa riferimento un alias.

Note di rilascio per il server MDaemon

Per un elenco completo delle funzionalità aggiunte, delle modifiche e delle correzioni incluse in MDaemon 21.5, vedere le Note di rilascio di MDaemon.

Novità di MDaemon Private Cloud 9.0.0

- MDaemon Private Cloud 9.0 comprende MDaemon 21.0.2 con MDaemon Connector 7.0.4.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 21.0.2.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 7.0.4.

Novità della versione 21.0 di MDaemon

Nuove funzioni principali

Chat room persistenti

Il server XMPP di MDaemon ora supporta le chat room persistenti, che non devono quindi essere ricreate ogni volta che tutti gli utenti escono dalla chat room. È possibile configurarle in: Impostazioni | Web e servizi IM | XMPP.

Segnalazione di classificazioni di virus/spam errate

Nelle schermate delle code dei messaggi in quarantena, scartati o di Spam Trap dell'interfaccia utente grafica di MDaemon, è stata aggiunta un'opzione al menu di scelta rapida che consente di segnalare i messaggi a MDaemon.com come falsi positivi o falsi negativi. Opzioni simili sono state aggiunte a MDaemon Remote Administration. I messaggi segnalati saranno analizzati e inviati a fornitori terzi per le necessarie azioni correttive.

Interfaccia utente grafica di ActiveSync Migration Client (ASMC)

È stata creata un'interfaccia utente grafica per facilitare l'esecuzione di ASMC (`ASMCUI.exe` nella cartella `\app\` di MDaemon). L'interfaccia consente di archiviare le opzioni e richiamarle quindi in un secondo tempo. ASMC supporta la migrazione di posta, calendari, attività, note e contatti dai server ActiveSync che supportano la versione 14.1 del protocollo. La relativa documentazione è disponibile nella cartella Docs di MDaemon, in: `\MDaemon\Docs\ActiveSync Migration Client.html`.

Miglioramento del tema Mobile di Webmail

Il tema Mobile per gli utenti di Webmail è stato esteso e migliorato. Vedere il file `RelNotes.html` disponibile nella cartella `\Docs\` di MDaemon per conoscere l'elenco completo delle tante funzionalità che sono state aggiunte.

Miglioramenti del clustering

Sono stati apportati molti miglioramenti al Servizio cluster di MDaemon:

- È stato aggiunto un'opzione di instradamento della posta multinodo, quando le code della posta sono condivisi tra nodi del cluster diversi. L'elaborazione e il

recapito dei messaggi da parte di più macchine consente di suddividere il lavoro in modo più equilibrato ed evita che i messaggi restino bloccati nelle code di eventuali macchine non attive.

- I certificati SSL ora vengono replicati dal nodo primario ai secondari.
- Le code sui nodi secondari restano bloccate durante la replica iniziale dei dati, allo scopo di migliorare la reattività durante l'avvio.
- La replica viene sospesa non appena viene avviata la chiusura di MDaemon, eliminando così i ritardi nell'arresto dovuti al clustering.
- Altri nodi del cluster si possono aggiungere utilizzando i relativi indirizzi IP o nomi DNS.
- I percorsi di rete condivisi ora si possono gestire più facilmente dalla nuova schermata Percorsi di rete condivisi.
- Nella nuova schermata Diagnostica sono disponibili strumenti di registrazione e diagnostica.

Altre nuove funzionalità e modifiche

Remote Administration (MDRA)

Sono state aggiunte decine di opzioni all'interfaccia di MDaemon Remote Administration. Vedere il file `RelNotes.html` disponibile nella cartella `\Docs\` di MDaemon per un elenco completo delle opzioni aggiunte a MDRA e delle altre modifiche apportate.

Filtro contenuti

È stata aggiunta la possibilità di cercare file soggetti a limitazioni 672 all'interno dei file compressi 7-Zip.

Risposte automatiche 852

I risponditori automatici ora supportano Unicode (UTF-8), per consentire l'uso di qualsiasi lingua.

Filtri IMAP 751

Le regole del filtro IMAP ora consentono la ricerca di porzioni di testo nel corpo dei messaggi.

Webmail

- Ora è possibile allegare un evento a un nuovo messaggio e-mail facendo clic con il pulsante destro sull'evento e scegliendo l'opzione "Invia" nei temi LookOut e WorldClient e dall'anteprima dell'evento nel tema Mobile.
- Tutte le funzionalità di creazione di nuovi account sono state rimosse.
- Quando si pubblica un calendario (si condivide un collegamento Accesso pubblico), alcune nuove opzioni consentono di impostare la relativa vista predefinita del calendario (ad esempio, mese/settimana/giorno) e di pubblicare un collegamento Free/Busy al calendario.

- Aggiunta l'opzione per ignorare il controllo della persistenza dell'indirizzo IP per ogni singolo utente. In MDRA, modificare l'account di un utente, passare a Servizi Web e selezionare "Ignora controllo persistenza IP per sessioni Webmail".
- Aggiunta la possibilità di eseguire ricerche sul campo Cc nelle ricerche avanzate.
- Aggiunta l'opzione Numero massimo di messaggi inviati al giorno 746 alle quote visualizzate.

Interfaccia utente

- La finestra Impostazioni | Gestione dispositivi mobili è stata rimossa e sostituita dalla finestra di dialogo Gestione ActiveSync in Impostazioni | ActiveSync.
- La schermata Impostazioni client ActiveSync è stata rimossa. Sono disponibili impostazioni di personalizzazione del client nelle schermate Regolazione, Domini, Gruppi, Account e Client.
- Nella schermata Tipo client ActiveSync sono disponibili opzioni da menu che consento di inserire i tipi di clienti in lista bianca o lista nera.
- Sono state aggiunte le schermate Impostazioni | Indicizzazione dei messaggi che consentono di configurare la manutenzione in tempo reale e notturna degli indici di ricerca utilizzati da Webmail, ActiveSync e Remote Administration.
- Alcuni plugin ora condividono una schermata di configurazione Diagnostica comune.
- I sistemi di Guida in linea di MDRA e Webmail basati su browser sono stati aggiornati con un nuovo tempa più reattivo, per facilitarne l'uso su diversi tipi di dispositivi.

API XML

- L'aspetto del portale di documentazione dell'API XML può essere personalizzato sia in modo globale che per singolo dominio. Per ulteriori informazioni, consultare "Modifiche e note di sviluppo" sul portale della Guida in linea (http[s]://NomeServer[:PortaMDRA]/MdMgmtWS) o il file \MDaemon\Docs\API\XML API\Help_Readme.xml su disco con Internet Explorer. Una directory company.mail di esempio è disponibile in \MDaemon\Docs\API\XML API\Samples\Branding.
- Aggiunta l'operazione Alias per semplificare la gestione degli Alias, la risoluzione e la segnalazione degli alias.
- Aggiunta l'azione FolderOperation per la ricerca tra i messaggi.
- Aggiunto il supporto di Servizio cluster a QueryServiceState e ControlServiceState.

Archiviazione 132

- Quando un messaggio viene scambiato tra account locali, vengono create copie di archivio sia "in entrata" che "in uscita" quando sono attivate entrambe le opzioni "Archivia posta in entrata" e "Archivia posta in uscita".

- È stata reimplementata l'opzione di archiviazione dei messaggi di spam, che era stata rimossa nella versione 20.0.
- I messaggi di spam rilasciati da Spam Trap vengono archiviati.

Aggiornamento di componenti

- MDaemon Connector è stato aggiornato alla versione 7.0.0.
- Spam Filter: aggiornato a SpamAssassin 3.4.4 e rimosse le impostazioni obsolete in local.cf.
- Scheda AntiVirus ClamAV aggiornato alla versione 0.103.0 e motore di Cyren AV aggiornato alla versione 6.3.0.2.
- Server XMPP: backend del database aggiornato alla versione SQLite 3.33.0.

Per un elenco completo delle funzionalità aggiunte, delle modifiche e delle correzioni incluse in MDaemon 21.0, vedere le Note di rilascio di MDaemon.

Novità di MDaemon Private Cloud 8.0.0

- MDaemon Private Cloud 8.0 comprende MDaemon 20.0.2 con MDaemon Connector 6.5.2.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 20.0.2.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 6.5.2.

Novità della versione 20.0 di MDaemon

Servizio cluster di MDaemon 416

Il nuovo Servizio cluster di MDaemon è progettato per condividere la configurazione tra due o più server MDaemon sulla rete. Questo rende possibile utilizzare hardware o software di bilanciamento del carico per distribuire il carico dei messaggi di posta elettronica su più server MDaemon, aumentando in tal modo la velocità e l'efficienza e riducendo il sovraccarico e la congestione del traffico di rete per ottimizzare le risorse e-mail. Consente inoltre di garantire la ridondanza dei sistemi e-mail in caso di guasti dell'hardware o di errori del software. Vedere: Servizio cluster 416, per ulteriori informazioni sulla configurazione di un cluster di server MDaemon sulla rete.

Nuove estensioni SMTP

RequireTLS (RFC 8689) 601

Il lavoro per la funzione RequireTLS in IETF è stato finalmente completato ed è stato anche implementato il relativo supporto. RequireTLS consente di contrassegnare i messaggi che **devono** essere inviati usando TLS. Se l'invio tramite TLS non è possibile (o se i parametri dello scambio del certificato TLS sono inaccettabili) i

messaggi torneranno al mittente invece di essere consegnati in modo non sicuro. RequireTLS è attivato per impostazione predefinita, ma solo i messaggi contrassegnati in modo specifico con una regola creata usando una nuova azione ContentFilter[661], "*Contrassegna messaggi per REQUIRETLS...*", o i messaggi inviati a `<local-part>+requiretls@domain.tld` (ad esempio, `arvel+requiretls@mdaemon.com`) sono sottoponibili all'elaborazione RequireTLS. Tutti gli altri messaggi vengono trattati come se il servizio fosse disattivato. Inoltre vi sono diversi requisiti da soddisfare perché un messaggio possa essere inviato usando RequireTLS. In mancanza di alcuni di essi i messaggi non saranno inviati e torneranno al mittente invece di essere inviati in modo non sicuro. Per ulteriori informazioni su questi requisiti e su come configurare RequireTLS, vedere: Estensioni SMTP[601]. Per una descrizione completa di RequireTLS, vedere: RFC 8689: Opzione SMTP Richiedi TLS.

SMTP MTA-STS (RFC 8461) - Strict Transport Security[602]
Il lavoro per MTA-STS nell'IETF è terminato ed è stato anche implementato il relativo supporto. SMTP MTA Strict Transport Security (MTA-STS) è un meccanismo che consente ai fornitori di servizi di posta (SP) di dichiarare la propria idoneità a ricevere connessioni SMTP protette con Transport Layer Security (TLS) e di specificare se i server SMTP di invio si rifiuterebbero di recapitare posta a host MX che non offrono TLS con un certificato di server affidabile. Il supporto di MTA-STS è attivato per impostazione predefinita. Vedere: Estensioni SMTP[601] per ulteriori informazioni su come configurare questo supporto mentre la descrizione completa per MTA-STA è in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

Report TLS SMTP (RFC 8460)[603]
I report TLS consentono ai domini di che utilizzano MTA-STS di ricevere notifiche relative agli eventuali errori di recupero delle policy MTA-STS o di negoziazione di un canale sicuro che utilizzi STARTTLS. Quando i report sono abilitati, MDaemon invia un report giornaliero a ciascun dominio abilitato per STS a cui ha inviato (o tentato di inviare) posta durante la giornata. Sono disponibili diverse opzioni per configurare le informazioni che saranno contenute dai report. I report TLS sono disabilitati per impostazione predefinita e illustrati in RFC 8460: Report TLS SMTP.

Crittografia di MDPGP a livello di azienda/dominio con una chiave singola

MDPGP[641] supporta ora la crittografia dei messaggi tra domini con l'uso di una chiave singola per tutti gli utenti. Ad esempio, supponiamo che "Dominio A" e "Dominio B" desiderino crittografare tutti i messaggi e-mail scambiati reciprocamente, ma non desiderino configurare e controllare singole chiavi di crittografia per ogni account utente nel dominio. Questo può essere ottenuto nel modo seguente:

"Dominio A" e "Dominio B" si scambiano reciprocamente una chiave di crittografia pubblica nel modo desiderato. Ad esempio, possono inviarsi reciprocamente le chiavi via e-mail facendo clic con il pulsante destro del mouse su una chiave pubblica esistente nell'interfaccia utente MDPGP e selezionando "Esporta chiave &e-mail". Se desiderano creare nuove chiavi dedicate a questo scopo possono utilizzare il pulsante "Crea le chiavi per un utente specifico" e scegliere la voce "_Domain Key (domain.tld)_ <anybody@domain.tld>" inserita per questo scopo specifico (anche se qualsiasi chiave funzionerà). Una volta che ciascun lato abbia ricevuto la chiave dell'altro, dovranno fare clic sul pulsante "Importa chiave del dominio" nell'interfaccia utente di MDPGP e specificare il nome del dominio sul quale tutti i messaggi e-mail saranno crittografati

usando la chiave fornita. Il sistema non crea una chiave nell'elenco a discesa per ognuno dei domini. È possibile utilizzare la chiave fornita per tutti i domini oppure è possibile creare autonomamente chiavi specifiche del dominio se si desidera.

Se uno dei due lati ha una chiave pubblica che desidera utilizzare ed è già nel keyring, potrà fare clic con il pulsante destro del mouse nell'interfaccia utente di MDPGP e selezionare "Imposta come chiave del dominio". In ogni caso, non utilizzare una chiave per la quale si dispone anche della chiave privata corrispondente. Se la si utilizza, MDPGP crittograferà il messaggio e vedrà subito che la chiave di decrittografia è nota e quindi decrittograferà immediatamente lo stesso messaggio.

A questo punto MDPGP creerà una regola del filtro contenuti denominata "Crittografa tutta la posta inviata a <dominio>" che chiamerà l'operazione di crittografia su ogni messaggio e-mail inviato a tale dominio. Usare il filtro contenuti significa che è possibile controllare questo processo attivando o disattivando la regola del filtro contenuti. È anche possibile modificare la regola per ottimizzare i criteri che si desidera utilizzare prima che i messaggi vengano crittografati (ad esempio, si potrebbe voler fare questa stessa cosa ma per due domini o solo per specifici destinatari all'interno del dominio). Il filtro contenuti offre la flessibilità necessaria per questo tipo di operazioni.

Crittografia della posta in uscita in base a IP ricevente

MDPGP 641 ha una nuova casella di controllo e un nuovo pulsante Impostazioni che consentirà di associare indirizzi IP a specifiche chiavi di crittografia. Qualsiasi sessione SMTP in uscita per la consegna di un messaggio a uno di questi indirizzi IP dovrà prima crittografare il messaggio usando la chiave associata, immediatamente prima della trasmissione. Se il messaggio è già crittografato in base a una chiave diversa, non verrà eseguita alcuna operazione. Questo è utile ad esempio in situazioni in cui si desidera assicurarsi che tutti messaggi inviati a specifici partner, fornitori, consociate ecc., siano sempre crittografati.

Macro per i messaggi delle liste di distribuzione

La schermata Mailing List Editor » Instradamento 302 offre delle nuove opzioni che consentono l'uso delle macro all'interno del corpo del messaggio dei post delle liste. Questo consente ad esempio di personalizzare ciascun messaggio della lista. Le macro erano da tempo supportate nelle intestazioni e pie' di pagina delle liste di distribuzione ma mai nel corpo del messaggio fino a ora. Poiché le macro sono correlate a singoli membri della lista, questa opzione è compatibile solo con le liste configurate per "*Consegna singolarmente posta lista a ciascun membro*". Inoltre, a scopi di sicurezza è possibile impostare questa opzione per richiedere di specificare la password della lista per poter utilizzare le macro nel corpo del messaggio. Se si sceglie di non richiedere la password, qualsiasi membro della lista con l'autorizzazione per pubblicare sulla lista potrà utilizzarle. Vedere la schermata Instradamento lista di distribuzione 302 per ulteriori informazioni e per l'elenco di macro che è possibile utilizzare.

Sistema di rilevamento dei tentativi di hijack migliorato

Per il rilevamento dei tentativi di hijack 577 sono disponibili nuove opzioni per evitare che, mediante il furto della relativa password gli account vengano utilizzati per diffondere spam. Una caratteristica comune dei messaggi di spam è che vengono spesso inviati a un elevato numero di destinatari non validi, perché lo spammer tenta di inviarli a vecchi indirizzi e-mail oppure tenta di indovinare nuovi indirizzi. Per questo

motivo, se un account MDaemon inizia a inviare messaggi a un numero elevato di account non validi in un breve periodo di tempo, questa è una buona indicazione che l'account è stato sottoposto a hijack e viene utilizzato per l'invio di spam. Per evitarlo, MDaemon può ora tenere traccia di quante volte un utente autenticato tenta di inviare una e-mail a un destinatario non valido. Se si verificano troppi di questi errori in un intervallo di tempo troppo breve, si può fare in modo che MDaemon blocchi l'account (il postmaster riceverà una e-mail di avviso e potrà rispondere per riattivare l'account). Questo può essere d'aiuto per bloccare automaticamente un account sottoposto a hijack, prima che faccia troppi danni. **Nota:** Come parte dei miglioramenti di questa funzione, i comandi di modifica delle intestazioni From sono stati spostati in una pagina Scansione intestazione From 584 apposita per fare spazio ai nuovi comandi relativi al rilevamento di hijack.

Coda messaggi differiti e richiamo messaggi migliorato 124

Per migliorare l'efficienza del sistema di richiamo messaggi e dell'intestazione Deferred-Delivery, MDaemon ha ora una coda dedicata ai messaggi differiti. In precedenza, la coda In ingresso poteva essere bloccata da messaggi differiti che potevano rallentare la consegna della posta non differita. La nuova coda dei messaggi differiti consente di risolvere questo problema. I messaggi nella coda Differiti vengono inseriti lì dal sistema e hanno la data per la quale sono impostati per lasciare la coda codificata nel nome file. MDaemon controlla la coda una volta al minuto e quando è il momento che i messaggi lascino la coda, vengono spostati nella coda In ingresso e sono soggetti alle normali operazioni di elaborazione/recapito dei messaggi.

Inoltre, MDaemon ora traccia gli ID dei messaggi delle e-mail più recenti inviate da ciascun utente locale autenticato, il che significa che gli utenti possono richiamare l'ultimo messaggio inviato (ma solo l'ultimo) semplicemente inserendo RECALL (da solo) come oggetto in un messaggio inviato all'account mdaemon@system. Non è necessario cercare e incollare l'ID del messaggio che si desidera richiamare quando si tratta dell'ultimo messaggio inviato. Invece il richiamo di qualsiasi altro messaggio richiede ancora di includere l'ID del messaggio nel testo dell'oggetto o di allegare il messaggio originale dalla cartella INVIATI dell'utente alla richiesta di richiamo.

Oltre a ricordare i messaggi e-mail più recenti inviati da ciascun utente autenticato, MDaemon ricorda anche la posizione e gli ID dei messaggi degli ultimi 1000 messaggi e-mail inviati da tutti gli utenti autenticati. Questo ha reso possibile richiamare i messaggi anche dalle caselle postali degli utenti dopo che sono stati recapitati. Quindi i messaggi spariranno dai client di posta degli utenti e dai telefoni se vengono richiamati. **Nota:** questo naturalmente è possibile solo per i messaggi inviati ad altri utenti locali; una volta che MDaemon ha consegnato un messaggio a un altro server, il messaggio non sarà più sotto il controllo di MDaemon e non potrà pertanto essere richiamato.

Registro degli errori di autenticazione

È disponibile un nuovo file di registro degli errori di autenticazione che contiene una singola riga con i dettagli di ogni tentativo di accesso SMTP, IMAP e POP non riuscito. Le informazioni includono il protocollo utilizzato, l'ID sessione in modo che sia possibile cercare in altri registri, l'indirizzo IP dell'utente causa dell'errore, il valore di accesso raw che ha tentato di utilizzare (a volte si tratta di un alias) e l'account che corrisponde al tentativo di accesso (o "nessuno" se non esiste un account corrispondente).

Autenticazione durante l'inoltro o l'instradamento di e-mail

Sono disponibili diverse opzioni di inoltro in MDaemon nelle quali è ora possibile aggiungere credenziali di autenticazione. Questo significa che diversi file nella cartella \APP\ (ad es. `forward.dat`, `gateways.dat`, `MDaemon.ini` e tutti i file `.grp` delle liste di distribuzione) hanno ora la possibilità di contenere dati di accesso e password offuscati in uno stato di crittografia molto debole. Come sempre consigliato, utilizzare gli strumenti del sistema operativo ed eventuali altre misure per assicurare il computer e la struttura di directory di MDaemon contro l'accesso non autorizzato. Opzioni per le credenziali di autenticazione sono state aggiunte a: Posta sconosciuta 106, Instradamento lista di distribuzione 302, Gateway Editor » Inoltro 268, Gateway Editor » Annullamento dell'accodamento 269 e Account Editor » Inoltro 742.

Autenticazione host 127

Autenticazione host è una nuova schermata in cui è possibile configurare i valori relativi a porta, accesso e password per qualsiasi host. Quando MDaemon invia posta SMTP all'host verranno utilizzate le credenziali associate specificate in questa posizione. Si noti che queste credenziali sono un'alternativa e sono utilizzate solo quando altre credenziali più specifiche dell'attività non sono disponibili. Ad esempio, se si configura Accesso/Password AUTH usando le nuove opzioni Account Editor » Inoltro 742 o Gateway Manager » Annullamento dell'accodamento 269 verranno utilizzate le relative credenziali, andando a sovrascrivere quanto configurato in questa posizione. Questa funzione è utilizzabile solo con i nomi degli host e non con gli indirizzi IP.

Code personalizzate e instradamento dei messaggi migliorati 893

È ora possibile specificare host, dati di accesso, password, SMTP return-path e porta per qualsiasi coda remota. Se specificate, tutti i messaggi della coda sono consegnati usando queste nuove impostazioni. Tuttavia in base alla progettazione resta ancora possibile per i singoli messaggi nella coda avere i propri dati di recapito unici, che avranno priorità su queste nuove impostazioni. Inoltre è ora possibile impostare il numero di code remote desiderato, filtrare la posta usando il filtro contenuti in base ai criteri desiderati, assegnare a ciascuna coda una propria pianificazione di consegna e un instradamento completamente diverso in base alle specifiche necessità.

Condivisione dominio migliorata 117

Per qualche tempo la Condivisione dominio ha eseguito ricerche sui valori dei mittenti della posta SMTP MAIL in base alle necessità. Tuttavia i messaggi venivano spesso rifiutati con il messaggio "Autenticazione richiesta" anche se non è possibile che l'autorizzazione venga eseguita quando l'account mittente risiede su un server diverso. Questo problema è stato risolto e MDaemon può ora accettare posta da account esistenti su altri server senza richiedere l'autenticazione. Questo può essere disattivato con una nuova opzione di Security Manager in: Autenticazione mittente » Autenticazione SMTP 531. Se si preferisce non eseguire ricerche di condivisione dominio sul mittente di posta SMTP MAIL è possibile disattivarlo completamente con una nuova opzione di Condivisione dominio.

Condivisione dominio ha inoltre una nuova opzione che consente la condivisione delle liste di distribuzione. Quando arriva un messaggio per una lista di distribuzione viene creata una copia per ciascun host di Condivisione dominio che conserva anche una versione di tale lista (va fatta una query per controllare). Quando questi host ricevono

le loro copie, eseguiranno la consegna a tutti i membri della lista che servono. In questo modo le liste di distribuzione possono essere suddivise su più server senza alcuna perdita di funzionalità. Perché questo funzioni, ogni host di Condivisione dominio deve includere gli IP degli altri host nella configurazione degli IP attendibili 527.

Infine, Condivisione dominio ha un nuovo pulsante Avanzate che consente di aprire un file nel quale è possibile configurare i nomi dei domini ai quali è consentito utilizzare la Condivisione dominio. Se il file è vuoto (condizione predefinita), tutti domini possono utilizzare la Condivisione dominio. Per ulteriori informazioni, consultare le istruzioni nella parte superiore del file.

Controllo migliorato sull'inoltro dei messaggi

Preferenze » Varie 511 ha una nuova opzione che consente agli amministratori di impedire all'inoltro di posta dell'account di inviare messaggi e-mail al di fuori del dominio. Se un utente configura l'inoltro di posta per l'account in modo da inviare messaggi a un dominio esterno, i messaggi saranno spostati nella coda dei messaggi scartati. Questa impostazione si applica solo ai messaggi che sono inoltrati usando le opzioni di inoltro della posta dell'account.

Account Editor » Inoltro 742 ha un nuovo pulsante *Pianifica* che consentirà agli account di configurare una pianificazione relativa a quando avviare e interrompere l'inoltro. Questo pulsante è incluso anche nella corrispondente schermata Modelli account 823. Queste impostazioni configurano data e ora dell'avvio e dell'arresto dell'inoltro ma l'inoltro avverrà solo nei giorni della settimana selezionati.

Il campo Indirizzo inoltro nel modello Nuovo account 807 ora funziona con le macro relative agli account. Le uniche macro con dati al momento della creazione di un nuovo account sono comunque quelle correlate a nome completo, dominio, casella postale e password dell'account. Quindi se ad esempio si desidera che ogni nuovo account inoltri la posta allo stesso indirizzo e-mail ma in un dominio diverso, è possibile inserire questo nel campo Indirizzo inoltro: `$MAILBOX$@example.com`. Le macro possono essere utilizzate anche nei campi *Invia come*, *Accesso AUTH* e *Password AUTH*.

L'inoltro di un messaggio ora aggiorna l'ora dell'ultimo accesso dell'account. Questo significa che gli account che non fanno altro che inoltrare posta non vengono più potenzialmente eliminati per inattività. **Nota:** l'inoltro deve avvenire effettivamente e non essere impedito da altre opzioni di configurazione come limitazioni relative a dove può essere inoltrata la posta o la mancata aderenza alla pianificazione. Disporre semplicemente di un indirizzo di inoltro configurato non contrassegnerà automaticamente l'account come attivo.

Autenticazione SMTP migliorata

Autenticazione mittente » Autenticazione SMTP 531 offre due nuove opzioni. L'opzione "*Non consentire l'autenticazione sulla porta SMTP*" disattiverà completamente il supporto di AUTH sulla porta SMTP. AUTH non verrà offerto nella risposta EHLO e verrà considerato un comando sconosciuto se fornito dal client SMTP. L'altra opzione è di "*...aggiungere i relativi IP al Vaglio dinamico in caso di tentativi*". Questa opzione aggiungerà al Vaglio dinamico 638 l'indirizzo IP di qualsiasi client che tenta di eseguire l'autenticazione quando AUTH è disabilitato. Anche la connessione verrà interrotta immediatamente. Queste impostazioni sono utili in configurazioni in cui tutti gli account legittimi utilizzano MSA o un'altra porta per inviare la posta autenticata. In queste

configurazioni si presume che qualsiasi tentativo di autenticazione sulla porta SMTP avvenga da parte di malintenzionati.

Gestione degli account migliorata

Le opzioni di filtro di Account Manager sono state estese. È ora possibile selezionare gli account in base al fatto che siano o meno attivati, utilizzino MultiPOP, siano prossimi alla quota (70%) o alla quota (90%) o non stiano eseguendo l'inoltro. È anche possibile cercare nel campo della descrizione dell'account il testo desiderato e selezionare account in base a tale testo. Inoltre, il menu di scelta rapida di Account Manager ha due nuove opzioni che consentono di aggiungere o di rimuovere tutti gli account selezionati alle o dalle liste di distribuzione e gruppi. Presenta inoltre un'opzione che consente di copiare un account esistente per crearne uno nuovo. Tutte le impostazioni dell'account esistente vengono copiate nel nuovo account ad eccezione di nome completo, casella postale, password e cartella posta. Infine, la schermata Filtri IMAP 751 di Account Editor ha un nuovo pulsante denominato Pubblica che aggiunge la nuova regola all'account da modificare e a tutti gli altri account del dominio dell'account stesso. Questo consente di risparmiare tempo quando una regola è necessaria per tutti gli account.

Attivazione di "Non disturbare" per l'intero dominio 188

La schermata Nome e IP host 188 di Domain Manager ha una nuova impostazione che consente di attivare l'opzione "Non disturbare" per un dominio. Quando attiva, il dominio rifiuterà tutte le connessioni da parte di tutti gli utenti per tutti i servizi ma continuerà ad accettare messaggi dall'esterno. È inoltre possibile pianificare l'avvio e l'arresto del "Non disturbare". Se ad esempio si configura dal 1 maggio 2020 al 30 giugno 2020 dalle 17:00 alle 7:00, dal Lunedì al Venerdì, significa nessun servizio di posta sarà disponibile per gli utenti di quel dominio nei giorni della settimana specificati, a partire dalle 17:00 e i servizi riprenderanno alle 7:01 purché la data rientri tra il 1 maggio e il 30 giugno 2020. La cancellazione della data di inizio pianificata disattiverà la pianificazione, con l'effetto di **impostare l'opzione "Non disturbare" per il dominio per sempre**.

Archiviazione migliorata 132

Il semplice sistema di archiviazione di MDaemon è stato modificato in un sistema più efficiente e coerente. L'archiviazione ora funziona nel modo seguente: Quando un messaggio viene consegnato dalla coda locale alla cartella di posta di un utente, viene creata una copia di archiviazione a quell'ora (nella cartella della posta in arrivo del destinatario se così configurato). Quando un messaggio viene prelevato dalla coda remota per la consegna SMTP (che la consegna avvenga o meno) viene creata una copia di archiviazione a quell'ora (nella cartella di posta in uscita dell'utente, se così configurato). Si vedranno righe come "ARCHIVE message: pgp5001000000172.msg" oppure righe come "* Archived: (archives) \company.test\in\frank@company.test\arc5001000000023.msg" nel registro di instradamento quando viene elaborata la posta locale e remota. Inoltre, esiste ora una coda "ToArchive" come coda di sistema (non esposta nell'interfaccia utente). Questa coda viene controllata a intervalli regolari in relazione ai messaggi inseriti (manualmente, da un plug-in o in altro modo). Quando sono trovati dei messaggi in questa coda, questi vengono immediatamente archiviati ed eliminati. Se vengono trovati messaggi non idonei all'archiviazione, vengono semplicemente eliminati. Il nome della coda è \MDaemon\Queues\ToArchive\. La schermata o il registro Instradamento mostreranno i dettagli ogni volta che un messaggio viene archiviato correttamente. Inoltre,

l'archiviazione di messaggi crittografati viene ora gestita in modo più coerente. Per impostazione predefinita nell'archivio vengono memorizzate copie non crittografate dei messaggi crittografati. Se un messaggio non può essere decrittografato, verrà invece memorizzato il formato crittografato. Se si preferisce memorizzare le versioni crittografate, è possibile utilizzare l'opzione che lo consente. Inoltre è ora disponibile un'opzione, attivata per impostazione predefinita, per archiviare i messaggi inviati agli indirizzi di invio delle cartelle pubbliche. Infine, i tipi di messaggi riportati di seguito non sono mai archiviati: Traffico delle liste di distribuzione, spam (l'opzione che lo consentiva è diventata obsoleta ed è stata rimossa), messaggi con virus, messaggi a livello di sistema e risposte automatiche.

Registrazione più efficiente

MDaemon non crea più file di registro vuoti. Quando sono disattivati degli elementi nella schermata Impostazioni, il file di registro associato non verrà creato all'avvio. I file di registro già esistenti quando l'elemento viene disattivato restano dove sono (non vengono rimossi). Se un file di registro manca quando un elemento viene attivato, il file di registro necessario verrà creato immediatamente. Questa modifica si applica a tutti i file di registro gestiti dal motore core di MDaemon. I file di registro per Vaglio dinamico, Messaggistica istantanea, XMPP, WDaemon e WebMail sono eseguiti esternamente rispetto a MDaemon e non sono stati modificati. Altre modifiche correlate alla registrazione includono: come rendere corretti i registri della sessione ATRN, rendere tutti i registri coerenti riguardo ai colori e alla modalità di registrazione di ID sessione e ID secondari; il server MultiPOP non attiva e disattiva le sessioni per gli account che sono già superiori alla quota e pertanto non c'è più un'inutile registrazione in questi casi. Infine, il registro Router stava solo registrando l'analisi dei messaggi delle code in ingresso e locali. Ora registra anche l'analisi della coda remota quando sono eseguiti tentativi di consegna. In questo modo non è necessario cercare nel registro Router e nei registri SMTP per vedere quando un messaggio è stato elaborato.

Integrazione con Active Directory migliorata

È ora possibile configurare la funzione di integrazione di Active Directory di MDaemon per creare un account MDaemon quando si aggiunge qualcuno a un gruppo Active Directory, e quando si rimuove qualcuno da un gruppo Active Directory l'account MDaemon corrispondente verrà disattivato (ma non eliminato). Per utilizzare questa funzionalità, è necessario utilizzare un filtro di ricerca di Active Directory alternativo. Vedere: Active Directory » Autenticazione, per ulteriori informazioni.

Nella schermata Autenticazione di Active Directory è ora disponibile un'opzione "*Filtro ricerca contatti*" separata per le ricerche dei contatti. In precedenza, la ricerca dei contatti veniva effettuata usando il filtro di ricerca degli utenti. C'è anche un pulsante di test separato per il filtro di ricerca dei contatti. Le ricerche in Active Directory sono state ottimizzate in modo che quando i filtri di ricerca sono identici una singola query aggiorni tutti i dati. Quando i filtri di ricerca sono diversi, sono necessarie due query separate.

Sono stati aggiunti i seguenti campi ai modelli di file ActiveDS.dat in modo che siano inclusi nei record dei contatti quando il monitoraggio di Active Directory crea o aggiorna le rubriche: `abTitle=%personalTitle%`, `abMiddleName=%middleName%`, `abSuffix=%generationQualifier%`, `abBusPager=%pager%`, `abBusIPPhone=%ipPhone%` e `abBusFax=%FacsimileTelephoneNumber%`.

I contatti della cartella Pubblica saranno ora eliminati quando l'account associato viene eliminato da Active Directory. In ogni caso, i contatti vengono eliminati solo se creati dalla funzione di integrazione di Active Directory. L'impostazione per controllare questa funzione si trova nella schermata Monitoraggio di Active Directory 841.

Quando il sistema di monitoraggio di Active Directory crea o aggiorna un account e trova un valore di casella postale troppo lungo da correggere nello spazio limitato di MDaemon per il valore della casella postale, il valore verrà troncato come prima ma ora verrà anche creato un alias con il valore della casella postale completo (non troncato). Inoltre, quando si crea un account o un alias, la sezione della nota della schermata Ruoli amministrativi 773 dell'account viene aggiornata a scopo di auditing.

La schermata Active Directory 307 di Mailing List Manager ora consente di immettere un attributo di Active Directory nel campo nome completo dei membri della lista.

Le modifiche alle proprietà degli account in Active Directory possono causare la nuova creazione di un account in MDaemon anche quando l'account era stato eliminato in precedenza in MDaemon. Per evitare che gli account vengano nuovamente creati in questo modo, è stata aggiunta una nuova opzione a Monitoraggio di Active Directory 841 . Per impostazione predefinita, gli account non verranno creati nuovamente quando sono stati eliminati manualmente in MDaemon.

Scansione intestazione From migliorata 584

Le opzioni "*Modifica intestazione From*" sono state spostate dalla schermata di rilevamento dei tentativi di hijack a una schermata Scansione intestazione From 584 apposita alla quale sono state aggiunte anche nuove opzioni. Ad esempio, Scansione intestazione From può ora controllare nei nomi visualizzati delle intestazioni "From" stringhe che sembrano indirizzi e-mail. Se ne viene trovato uno e questo non corrisponde all'indirizzo e-mail effettivo del mittente, verrà sostituito con l'indirizzo e-mail effettivo. Ad esempio, se si sta usando questa funzione e l'intestazione "From:" riporta: "`From: 'Frank Thomas <friend@friend.test>' <enemy@enemy.test>`" verrà modificata in: "`From: 'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>`".

Controllo delle password compromesse 870

MDaemon può controllare le password di un utente in base a un elenco di password compromesse fornito da un servizio di terze parti. È in grado di eseguire questa operazione senza trasmettere le password al servizio e se la password di un utente è presente nell'elenco non significa che l'account è stato violato. Significa che qualcuno da qualche parte ha usato gli stessi caratteri di questa password in precedenza e la password è stata visualizzata in una violazione di dati. Le password pubblicate possono essere utilizzate dagli hacker negli attacchi con dizionario, ma le password univoche che non sono mai state utilizzate sono più sicure. Per ulteriori informazioni, vedere Password pwned.

Nella schermata Password 870 di Impostazioni di sicurezza, MDaemon ora ha un'opzione per impedire che la password di un account sia impostata su una delle password presenti nell'elenco di password compromesse. Può inoltre controllare la password dell'utente a intervalli predefiniti (giorni) al momento dell'accesso e inviare un messaggio e-mail di avviso all'utente e al postmaster nel caso in cui rilevi una password presente nei suddetti elenchi. Le e-mail di avviso possono essere personalizzate modificando i file di modello di messaggio nella cartella `\MDaemon\App`. Poiché le istruzioni per gli utenti su

come modificare la password possono dipendere da se l'account usa una password memorizzata in MDaemon o l'autenticazione di Active Directory, sono disponibili due file di modelli, `CompromisedPasswordMD.dat` e `CompromisedPasswordAD.dat`. È possibile utilizzare le macro per personalizzare il messaggio, modificare l'oggetto, il destinatario ecc.

Altre funzioni e miglioramenti apportati

Con più di 250 nuove funzioni e miglioramenti inclusi in MDaemon 20, molti non sono stati inclusi in questa sezione. Vedere `RelNotes.html` nella sottocartella `\Docs\` di MDaemon per un elenco completo di tutte le nuove funzioni, le modifiche e le correzioni incluse in questa versione.

Novità di MDaemon Private Cloud 7.5.0

- MDaemon Private Cloud 7.5 comprende MDaemon 19.5.3 con MDaemon Connector 6.5.1.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 19.5.3.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 6.5.1.

Novità della versione 19.5 di MDaemon

Nuovo tema Mobile di Webmail

Il tema Mobile di Webmail è stato sostituito da una GUI più moderna dotata di funzioni aggiuntive. L'elenco dei messaggi ora prevede funzionalità quali le categorie personalizzate, la posposizione dei messaggi, l'ordinamento in base a contrassegnati/non letti/posposti, le colonne di ordinamento e il richiamo dei messaggi. Il Calendario ora è dotato di funzionalità come l'importazione/esportazione di eventi come file csv o ics, l'aggiunta di calendari esterni, i collegamenti per l'accesso privato, la pubblicazione dei calendari e la visualizzazione simultanea di più calendari. Le funzionalità di composizione includono ora il recapito differito, le firme multiple, i messaggi in formato testo/html e i modelli di e-mail. Altre funzionalità comprendono il trascinamento dei filtri dei messaggi e-mail, l'editor di firme multiple, altre opzioni di gestione delle cartelle, notifiche, gestione delle colonne mediante trascinamento, gestione delle categorie mediante trascinamento e altro ancora. Se si esegue Webmail in IIS, è necessario eseguire ulteriori operazioni di configurazione per utilizzare il nuovo tema Mobile. Vedere l' articolo 1236 della Knowledge Base per ulteriori informazioni.

Gestione delle firme del client

È ora possibile configurare il push di una firma e-mail in Webmail e MDaemon Connector per gli utenti. .È possibile impostare una firma del client predefinita oppure impostare le firme in base al dominio nella schermata Firme client di Domain Manager. Per personalizzare le firme, è possibile utilizzare macro di firma come

$CONTACTFULLNAME$, $CONTACTEMAILADDRESS$, estraendo i dati dai contatti dell'utente archiviati nella cartella Contatti pubblici del dominio. Utilizzare la macro $ATTACH_INLINE:filename$ per le immagini in linea nella firma HTML. Dopo l'immissione del testo della firma, questa verrà visualizzata in Webmail come firma di sistema e diventerà la firma predefinita dell'utente. Può essere attivata o disattivata per impostazione predefinita per Webmail in Impostazioni Webmail 354, oppure per il dominio in Domain Manager 198. Per MDaemon Connector, il nome della firma e le impostazioni correlate possono essere configurate nella schermata Firma 413 di Impostazioni client MC. Questa funzionalità richiede MDaemon 6.5.0 o versione successiva.

Pagina Categorie 352

L'interfaccia di MDaemon Remote Administration (MDRA) ora ha una pagina Categorie 352 nelle opzioni di Webmail, per la configurazione delle categorie del dominio e delle categorie personali predefinite.

Altri miglioramenti di MDRA

Sono molte le opzioni che in precedenza potevano essere gestite solo tramite l'interfaccia dell'applicazione di MDaemon che sono state aggiunte a MDRA. Per un elenco complete, vedere le Note di rilascio.

Novità di MDaemon Private Cloud 7.0

- MDaemon Private Cloud 7.0 comprende MDaemon 19.0.2 con MDaemon Connector 6.0.1.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 19.0.2.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 6.0.1.

Novità della versione 19.0 di MDaemon

Supporto per TLS Server Name Identification (SNI) 587

MDaemon ora supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

API XML per la gestione di cartelle ed elementi

L'API XML è stata estesa per includere la possibilità di gestire le cartelle e gli elementi presenti all'interno delle cartelle postali. Le cartelle possono essere create, eliminate, rinominate e spostate utilizzando l'API. Le operazioni sugli elementi supportano e-mail,

calendario, contatti, attività e note. Gli elementi possono essere creati, eliminati e spostati utilizzando l'API. La documentazione completa è disponibile nella directory `MDaemon\Docs\API\XML-API\`.

Miglioramenti di Remote Administration

L'interfaccia Web di Remote Administration di MDaemon (MDRA) è stata estesa in modo da prevedere l'accesso a molte funzionalità che in precedenza si potevano amministrare solo utilizzando una Sessione di configurazione (ovvero, l'interfaccia dell'applicazione MDaemon), mentre ora alcune opzioni sono accessibili esclusivamente mediante MDRA. Ne consegue che, per le nuove installazioni di MDaemon, il menu di scelta rapida "Avvia MDaemon" ora apre un browser per impostazione predefinita al fine di utilizzare Remote Administration, anziché aprire una sessione di configurazione di MDaemon. Per cambiare questo comportamento, modificare il file `\MDaemon\App\MDaemon.ini` e impostare `[MDLaunch] OpenConfigSession=Yes/No` e `OpenRemoteAdmin=Yes/No`. Impostare "*URL Remote Administration*" su Impostazioni » Web e Servizi IM » Remote Administration » Server Web se l'URL generato automaticamente non funziona o se MDRA viene eseguito in un server Web esterno. Se non si riesce a determinare un URL funzionante, si aprirà invece una sessione di configurazione. Infine, nel menu Start di Windows, nel gruppo di programmi MDaemon, ora sono disponibili i collegamenti di scelta rapida *Apri MDaemon Configuration Session* e *Apri MDaemon Remote Administration*.

Miglioramenti di Webmail

- Agli utenti di Webmail che hanno l'opzione *Mostra cartelle ricerche salvate* abilitata (disponibile in Webmail in Opzioni » Cartelle) verrà ora chiesto se desiderano aggiungere una cartella di ricerca salvata "Tutti non letti" e "Tutti contrassegnati" all'elenco. La richiesta verrà presentata all'utente una sola volta, al primo accesso. Se sceglie "No", l'utente potrà creare facilmente in modo manuale tali ricerche salvate mediante i pulsanti *Crea ricerca salvata Tutti non letti* e *Crea ricerca salvata Tutti contrassegnati* (disponibili anche in Opzioni » Cartelle). Gli amministratori possono impedire a Webmail di chiedere agli utenti se desiderano creare tali ricerche aggiungendo `DefaultSavedSearchesCheck=Yes` sotto `[Default:UserDefaults]` nel file `MDaemon\WorldClient\Domains.ini`.
- Sono state modificate alcune icone del tema *WorldClient* per renderle più visibili.
- Aggiunto "(SCADUTA)" al titolo della scheda del browser quando la sessione scade. In tal modo, quando non è nella scheda di Webmail, l'utente può notare che la sessione è scaduta.
- Aggiunta un'icona Elimina per la rimozione dei contatti comuni dall'elenco di compilazione automatica.

Novità di MDaemon Private Cloud 6.5

- MDaemon Private Cloud 6.5 comprende MDaemon 18.5.1 con MDaemon Connector 5.6.0.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 18.5.1.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 5.6.0.

Novità della versione 18.5 di MDaemon

Macro firme 137

Le firme di MDaemon ora supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. `Ad esempio, $CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate nella pagina Firme predefinite 137.

Gli utenti possono inoltre controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e `$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Messaggistica istantanea MDaemon in Webmail

I temi WorldClient e LookOut ora dispongono di un client XMPP integrato nel browser che consente agli utenti di inviare messaggi istantanei senza dover eseguire l'applicazione desktop di messaggistica istantanea di MDaemon o altre applicazioni XMPP. Gli utenti possono attivarla dalla schermata Opzioni | Personalizza di Webmail, utilizzando l'opzione "Attiva la funzione di messaggistica istantanea di MDaemon nel browser". Gli amministratori possono attivare o disattivare la messaggistica istantanea per ogni dominio utilizzando il Domain Manager, per ogni account utilizzando l'Account Editor o per ogni gruppo utilizzando la Gestione gruppo.

MDaemon comprende un nuovo server BOSH per supportare la messaggistica istantanea in Webmail. Le relative impostazioni ora si possono configurare nella schermata XMPP 381 (**nuova in 18.5.1)**.

Escludere Webmail dal vaglio della posizione

Aggiunta un'opzione utente in Webmail per escludere gli accessi con autenticazione a due fattori dal vaglio della posizione. Se un utente ha `BypassLocationScreeningTFA=Yes` nella sezione `[User]` del file `User.ini` e l'autenticazione a due fattori è attivata, il vaglio della posizione viene aggirato. Questo consente agli utenti di effettuare l'accesso a Webmail in paesi che normalmente sarebbero bloccati dal vaglio della posizione.

Integrazione AD migliorata

Gli utenti con account impostati per utilizzare l'autenticazione Active Directory (AD) possono ora modificare la password AD in Webmail se l'impostazione "AllowADPasswordChange" è abilitata in \MDaemon\WorldClient\Domains.ini. Questa opzione è disabilitata per impostazione predefinita.

MDRA estesa

L'interfaccia Web di MDaemon Remote Administration (MDRA) è stata estesa in modo da prevedere l'accesso a molte funzionalità che in precedenza potevano essere gestite solo mediante l'interfaccia utente grafica di MDaemon.

Novità di MDaemon Private Cloud 6.0

- MDaemon Private Cloud 6.0 comprende MDaemon 18.0.2 con MDaemon Connector 5.5.2.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 18.0.2.

Per un elenco di tutte le modifiche apportate a MDaemon Connector, vedere le Note di rilascio di MDaemon Connector 5.5.2.

Novità della versione 18.0 di MDaemon

DNSSEC

La nuova opzione DNSSEC (DNS Security Extensions) consente a MDaemon di agire come risolutore stub non di convalida in grado di riconoscere la sicurezza, definito in RFC 4033 e 4035 come "una entità che invia query DNS, riceve risposte DNS ed è in grado di stabilire un canale protetto in modo appropriato a un server dei nomi ricorsivo in grado di riconoscere la sicurezza che fornirà questi servizi per conto del risolutore stub in grado di riconoscere la sicurezza". Con questo si intende che durante le query DNS di MDaemon possono richiedere il servizio DNSSEC dai server DNS utilizzati, impostando il bit AD (Authentic Data) nelle query e verificandolo nelle risposte. Questo può fornire un livello di sicurezza aggiuntivo durante il processo DNS per alcuni messaggi, anche se non per tutti, perché DNSSEC non è ancora supportato da tutti i server DNS o per tutti i domini di livello superiore.

Quando abilitato, il servizio DNSSEC viene applicato solo ai messaggi che soddisfano i criteri di selezione. Può essere richiesto o essere considerato obbligatorio nei termini e modalità selezionati dall'utente. È sufficiente specificare le combinazioni "`intestazione/valore`" selezionate nella schermata DNSSEC e MDaemon richiederà il servizio DNSSEC per i messaggi che corrispondono al criterio ogni volta che esegue una query DNS. Quando i risultati DNS non includono dati autenticati, non ne derivano conseguenze negative; MDaemon torna semplicemente al normale comportamento DNS. Se tuttavia si desidera *richiedere* DNSSEC per specifici messaggi, aggiungere "SECURE" alla combinazione intestazione/valore (ad es. `To *@esempio.net SECURE`). Per questi messaggi, quando i risultati DNS non includono dati autenticati, il messaggio sarà restituito al mittente. **Nota:** poiché le ricerche DNSSEC impiegano più tempo e risorse e dato che DNSSEC non è ancora supportato da tutti i server, MDaemon non è configurato per applicare DNSSEC a tutti i messaggi consegnati per impostazione predefinita. Tuttavia, se si desidera richiedere DNSSEC per tutti i messaggi, sarà necessario includere "`To *`" nei criteri.

Scansione cassetta postale AntiVirus

È disponibile una nuova opzione *Esegui scansione di tutti i messaggi ogni [n] giorni* in Sicurezza » AntiVirus 684 che può essere utilizzata per eseguire periodicamente la scansione di tutti i messaggi memorizzati, per rilevare eventuali messaggi infetti che possono essere passati attraverso il sistema prima che un aggiornamento delle definizioni dei virus fosse disponibile per rilevarli. I messaggi infetti vengono spostati nella cartella della quarantena con l'intestazione `X-MDBadQueue-Reason` , in modo da rendere evidente la spiegazione quando visualizzati in MDaemon. I messaggi che non possono essere sottoposti a scansione non vengono messi in quarantena. È inoltre disponibile un'opzione *Configura scansione cassette postali* che consente di specificare la frequenza di scansione dei messaggi e se si desidera sottoporre a scansione tutti i messaggi o solo quelli che hanno meno di un determinato numero di giorni. È anche possibile eseguire subito manualmente una scansione della cassetta postale.

Esclusione dei dispositivi ActiveSync noti dallo screening posizione

Abilitare la nuova opzione Escludi da screening posizione 470 nella schermata delle impostazioni di un client ActiveSync se si desidera escludere il dispositivo dallo screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione. Quando si esclude un dispositivo dallo screening posizione, è anche disponibile un'opzione per inserire nella lista bianca l'indirizzo IP remoto dal quale esegue la connessione. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Nuove funzionalità Webmail e MDRA

Ricordati di me

È ora possibile aggiungere una casella di controllo "Ricordati di me" alle pagine di accesso di MDaemon Webmail e MDaemon Remote Administration (MDRA), mediante le opzioni disponibili nella schermata Impostazioni 354 di Webmail e nella schermata Web Server 361 di MDRA, rispettivamente. Quando questa opzione è abilitata, gli utenti che accedono mediante la porta HTTPS vedranno la casella di controllo. Se gli utenti selezionano questa casella, le rispettive credenziali saranno ricordate per il dispositivo utilizzato. Quindi ogni volta che useranno quel dispositivo per connettersi a Webmail o a MDRA in futuro accederanno automaticamente fino a quando non eseguiranno la disconnessione manuale dall'account o il token di Ricordati di me scadrà. L'opzione*Ricordati di me* è disabilitata per impostazione predefinita e si applica a tutti i domini dell'utente. Per ignorare questa impostazione per domini Webmail specifici, utilizzare l'impostazione *Ricordati di me* che si trova nella schermata di Webmail 198 di Domain Manager nell'interfaccia desktop di MDaemon.

Per impostazione predefinita, le credenziali degli utenti saranno memorizzate per 30 giorni scaduti i quali sarà necessario eseguire di nuovo l'accesso specificando le credenziali, ma è possibile utilizzare l'opzione *Token scadenza Ricordati di me dopo questo numero di giorni* (in MDRA) per specificare un numero diverso di giorni se si

desidera. È possibile impostare questa opzione fino a 365 giorni. **Nota:** L'autenticazione a due fattori (2FA) ha una propria chiave per la scadenza di Ricordati di me (`TwoFactorAuthRememberUserExpiration=30`), che si trova nella sezione `[Default:Settings]` del file `Domains.ini` nella cartella `\MDaemon\WorldClient\`. Pertanto l'autenticazione 2FA sarà nuovamente richiesta all'accesso quando il token di Ricordati di me di 2FA scadrà, anche se il normale token è ancora valido.

In MDRA è inoltre disponibile un pulsante *Ripristina Ricordati di me* che è possibile utilizzare se si sospetta una violazione della sicurezza per un account. In tal modo si ripristinano i token Ricordati di me per tutti gli utenti, con la conseguente richiesta di eseguire di nuovo l'accesso.

Posporre i messaggi e-mail

In MDaemon Webmail è possibile posporre un messaggio e-mail nell'elenco messaggi. Un messaggio posposto sarà nascosto per il periodo di tempo indicato. Per posporre un messaggio, fare clic con il pulsante destro del mouse sul messaggio e scegliere l'opzione "Posponi per..." nel menu di scelta rapida. Scegliere quindi per quanto tempo si desidera posporre il messaggio. L'opzione "Scegli data e ora" è disponibile solo per i browser che supportano l'input di data e ora. I messaggi nascosti possono essere visualizzati nel tema LookOut facendo clic sull'icona "Visualizza messaggi posposti" nella barra degli strumenti e nel tema WorldClient selezionando "Visualizza posposti" dal menu a discesa nella barra degli strumenti. Questa funzione è attivata per impostazione predefinita. Per disattivarla selezionare Opzioni | Personalizza in Webmail e cercare Impostazioni Posta in arrivo. Deselezionare la casella "Abilita pospos. messaggi". Non sono disponibili comandi per posporre i messaggi nei temi Lite e Mobile, ma i messaggi posposti vengono comunque nascosti.

Calendari pubblici

In MDaemon Webmail gli utenti possono ora pubblicare un calendario in un collegamento accessibile pubblicamente ed è disponibile l'opzione per proteggere il calendario con una password. Per pubblicare un calendario, nei temi LookOut o WorldClient di Webmail selezionare Opzioni | Cartelle e fare clic sul pulsante "Condividi cartella" vicino al calendario che si desidera pubblicare. Quindi aprire la scheda Accesso pubblico e se si desidera, specificare il nome da visualizzare o richiedere una password, quindi fare clic sul pulsante "Pubblica calendario". Verrà visualizzata una finestra di dialogo di conferma e dopo aver fatto clic su OK verrà visualizzato un avviso con il nuovo URL al quale è disponibile il calendario. Sulla pagina verrà inoltre visualizzato un collegamento una volta pubblicato il calendario. Per annullare la pubblicazione del calendario, fare clic sul pulsante "Annulla pubblicazione calendario". Per modificare la password o il nome visualizzato, fare clic sul pulsante "Aggiorna".

Se si desidera disabilitare questa opzione a livello globale, modificare il valore della chiave `EnablePublicCalendars` su **No** nella sezione `[Default:Settings]` del file `Domains.ini`. Per disabilitarla in base all'utente, aggiungere `CanPublishCalendars=No` al file `User.ini` dell'utente.

Novità di MDaemon Private Cloud 5.5

- MDaemon Private Cloud 5.5 comprende MDaemon 17.5.2 e Outlook Connector 5.0.1.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 17.5.

Per un elenco di tutte le modifiche apportate a Outlook Connector, vedere le Note di rilascio di Outlook Connector 5.0.1.

Novità della versione 17.5 di MDaemon

Screening posizione 582

La funzione Screening posizione (o vaglio della posizione) è un sistema di blocco geografico che consente di bloccare connessioni SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP e Minger in ingresso da territori non autorizzati. MDaemon individua il paese associato all'indirizzo IP che si connette e blocca la connessione se questa proviene da un'area non autorizzata, aggiungendo quindi una riga al registro dello screening. Nel caso del SMTP, lo Screening posizione può bloccare solo le connessioni che utilizzano AUTH. La funzione è particolarmente utile, ad esempio, quando non esistono utenti che risiedono in determinato paese ma si desidera comunque ricevere posta da tale nazione. In questo modo si bloccano solo le persone che tentano di accedere al server.

La cartella `\MDaemon\Geo\` contiene i file del database utilizzato come database master degli IP nazionali. I file sono stati forniti da MaxMind (www.maxmind.com) ed è possibile scaricare gli aggiornamenti dal loro sito, se necessario.

Vaglio dinamico per tutti i protocolli e i servizi 623

Il sistema di vaglio dinamico di MDaemon è stato ampliato per funzionare con with SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP e Minger. Gli errori di autenticazione vengono controllati in tutti questi servizi ed è possibile bloccare gli indirizzi IP per tutti i servizi. Vaglio dinamico può essere configurato nella nuova finestra di dialogo dotata di più schede nel menu Sicurezza.

Allegati PIM

Gli elementi PIM (calendario, contatti, attività, note) ora supportano allegati. Gli allegati possono essere aggiunti a un elemento PIM tramite Webmail, Outlook Connector o CalDAV/CardDAV. Quando si pianifica una riunione, è possibile inviare eventuali allegati ai partecipanti alla riunione.

Scambio della chiave PGP durante SMTP 641

La finestra di dialogo MDPGP contiene una nuova opzione per abilitare la trasmissione automatica di chiavi pubbliche come parte del processo di invio di messaggi SMTP. A tal fine, il server SMTP di MDaemon riconoscerà il comando SMTP RKEY. Quando invia una

e-mail a un server che supporta RKEY, MDaemon offrirà di trasmettere la chiave pubblica preferita corrente del server all'altro host. L'host risponderà indicando che già ha la chiave ("250 2.7.0 Key already known") o che ha bisogno della chiave, nel qual caso la chiave viene trasferita immediatamente in formato ASCII armored ("354 Enter key, end with CRLF.CRLF") proprio come un messaggio e-mail. Le chiavi scadute o revocate non vengono trasmesse. Se MDaemon dispone di più chiavi per il mittente, invierà sempre la chiave correntemente contrassegnata come preferita. Se nessuna chiave è contrassegnata come preferita, sarà inviata la prima trovata. Se non sono disponibili chiavi valide, non verrà effettuata alcuna operazione. Vengono offerte solo chiavi pubbliche che appartengono agli utenti locali.

I trasferimenti di chiavi pubbliche avvengono come parte della sessione di posta SMTP che consegna il messaggio dell'utente. Perché le chiavi pubbliche trasmesse in questo modo vengano accettate, la chiave deve essere inviata insieme a un messaggio con firma DKIM 539 originata dal dominio del proprietario della chiave con il parametro i= impostato sull'indirizzo del proprietario della chiave, indirizzo che inoltre corrispondere esattamente all'indirizzo dell'intestazione From: univoco. Il "proprietario della chiave" viene estratto dalla chiave stessa. Inoltre, il messaggio deve arrivare da un host al percorso SPF 533 del mittente. Infine, il proprietario della chiave (o il relativo intero dominio grazie all'uso dei caratteri jolly) deve disporre dell'autorizzazione per RKEY con l'aggiunta di una voce al file di regole MDPGP (nel file di regole sono presenti istruzioni a questo scopo) che indica che il dominio può essere ritenuto affidabile per lo scambio delle chiavi. L'intero controllo viene eseguito automaticamente ma è necessario che DKIM 536 e la verifica SPF 533 siano abilitati o non sarà possibile effettuare alcuna operazione.

Il registro MDPGP mostra i risultati e i dettagli di tutte le chiavi importate o eliminate e anche il registro della sessione SMTP registra questa attività. Questo processo registra l'eliminazione delle chiavi esistenti e la selezione delle nuove chiavi preferite e aggiorna tutti i server che partecipano ai quali invia e-mail quando vengono effettuate modifiche in questo senso.

Gestione dei componenti aggiuntivi di Outlook per gli utenti di Outlook Connector 414

Nella nuova schermata Componenti aggiuntivi della finestra di dialogo Impostazioni client OC è possibile gestire lo stato dei componenti aggiuntivi di Outlook installati dagli utenti di Outlook Connector. È possibile autorizzare il normale utilizzo di alcuni o tutti i componenti aggiuntivi oppure si possono disattivare quelli che non si desidera vengano utilizzati. Questa funzionalità si dimostra particolarmente utile quando si è a conoscenza di conflitti generati da un componente aggiuntivo specifico nel client Outlook Connector, e consente quindi di disabilitare tale componente aggiuntivo per evitare problemi. La funzionalità Componenti aggiuntivi richiede Outlook Connector 5.0 o versione successiva.

Modifiche a Webmail

Importazione/esportazione di gruppi e liste di distribuzione

Nei temi LookOut e WorldClient è stata aggiunta l'opzione per esportare e importare gruppi/liste di distribuzione da e verso una cartella contatti in Webmail. Il formato è specifico per MDaemon Webmail, perché Outlook non supporta l'esportazione e l'importazione dei gruppi. Il formato è il seguente:

Colonne: **GUID gruppo**, **Nome del gruppo**, **GUID**, **Nome completo**, **E-mail**

Ogni riga che contiene un nome del gruppo o un GUID del gruppo è considerata l'inizio di un nuovo gruppo. GUID, nomi completi o indirizzi e-mail presenti sulla riga saranno considerati il primo membro del gruppo o della lista.

Esempio da Excel:

GUID gruppo	Nome del gruppo	GUID	Nome completo	E-mail
	The Jedis		Anakin Skywalker	ani@jedi.mail
			Leia Organa	leia.organa@jedi.mail
			Luke Skywalker	luke.skywalker@jedi.mail
			Yoda	yoda@jedi.mail
	The Siths		Darth Maul	darth.maul@sith.mail
			Darth Vader	darth.vader@sith.mail
			Emperor Palpatine	emperor.palpatine@sith.mail

Durante l'importazione, il GUID del gruppo viene sostituito con un GUID generato. Se non è incluso alcun nome del gruppo, il nome sarà visualizzato senza traduzione come "ImportedFromCSV_%GUID%", dove %GUID% viene sostituito con i primi cinque caratteri del GUID. Se si lasciano vuote le celle a destra del nome del gruppo, la riga successiva sarà il primo membro del gruppo o della lista. Il campo E-mail è richiesto per l'aggiunta di un membro.

Voice Recorder
La funzionalità di registrazione vocale Voice Recorder è stata aggiunta ai temi Lookout e WorldClient. Questa funzionalità richiede un microfono ed è disponibile solo in alcuni browser. Può essere disabilitata dall'amministratore o in base all'utente aggiungendo `EnableVoiceRecorder=No` al file User.ini. Il limite per gli utenti è cinque tracce di cinque minuti ciascuna. Se si tenta di registrare più di cinque tracce in una sessione di Voice Recorder la traccia selezionata o la prima traccia saranno sostituite dalla nuova registrazione (l'utente sarà avvisato). Una volta arrestata la registrazione (automaticamente o dall'utente), la traccia viene convertita in file mp3 e caricata sul server. Gli utenti hanno a disposizione quattro opzioni per ciascuna traccia:

- Salvataggio su desktop
- Salvataggio nella cartella documenti WorldClient predefinita
- Invio in un messaggio e-mail usando una finestra di invio rapido che include solo i campi A, CC, CCn, Oggetto e un corpo del messaggio di testo semplice

Solo il campo A è obbligatorio. Sono disponibili frasi generiche per l'oggetto e il corpo del messaggio utilizzabili quando l'utente non immette un oggetto o un corpo del messaggio.

- Apertura di una nuova vista di composizione con la traccia allegata

Gli utenti possono agire su una sola traccia per volta. Ad esempio, è possibile allegare una sola traccia a un messaggio. Se un utente desidera allegare a un messaggio più tracce, dovrà salvare ciascuna traccia nella cartella documenti predefinita e allegarli da lì.

Nuove funzionalità di gestione delle cartelle
I temi LookOut e WorldClient offrono nuove funzionalità di gestione delle cartelle nella vista Opzioni » Cartelle e nella vista dell'elenco cartelle principali.

Nella vista dell'elenco cartelle (riquadro a sinistra):

- Gli utenti possono trascinare le cartelle per spostarle da una cartella principale a un'altra.
- Gli utenti possono rinominare le cartelle e assegnare loro i nickname desiderati facendo clic su di esse una seconda volta (subito dopo la selezione della cartella)
- Il comando Mostra cartelle per tipo è ora disponibile nel tema LookOut
- Se esiste almeno una cartella preferita (perché i preferiti sono nascosti fino a quando ne viene aggiunto uno), gli utenti possono trascinare una cartella nei preferiti per aggiungerla (trascinare una cartella fuori dai preferiti non sortisce alcun effetto).
- Le finestre di dialogo Nuova cartella e Rinomina cartella sono state aggiunte al tema LookOut

Nella vista Opzioni » Cartelle, la struttura delle cartelle è ora comprimibile e la finestra di dialogo Nuova cartella è stata spostata in una finestra esterna come nel tema WorldClient.

Novità di MDaemon Private Cloud 5.0

- MDaemon Private Cloud 5.0 comprende MDaemon 17.0.2 e Outlook Connector 4.5.
- Aggiornamento a una versione più recente del motore dell'AV Cyren.
- Gli amministratori del dominio possono ora gestire i Servizi Web in Remote Administration per MDPC.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 17.0.2.

Per un elenco di tutte le modifiche apportate a Outlook Connector, vedere le Note di rilascio di Outlook Connector 4.5.0.

Novità della versione 17.0 di MDaemon

Supporto XMPP 381 per WorldClient Instant Messenger 326 (WCIM)

WCIM utilizza ora il protocollo XMPP per la messaggistica istantanea anziché il protocollo proprietario di WorldClient. Questo consente al client desktop di WCIM di comunicare non solo con altri client WCIM, ma anche con client XMPP di terze parti (inclusi client mobili) connessi al server XMPP di MDaemon. Inoltre WCIM offre ora due tipi di connessione: "WCMailCheck" e "WCIMXMPP." WCMailCheck consente la connessione a WorldClient per le notifiche di nuovi messaggi e-mail e conteggio messaggi. WCIMXMPP consente la connessione al server XMPP per la messaggistica istantanea. Di conseguenza, gli utenti di WCIM avranno ora una voce per ogni tipo di connessione elencata nella schermata Connessioni del client (ad es. "Esempio.com Mail" ed "Esempio.com WCIM"). Quando si esegue l'aggiornamento alla versione 17, WCIM creerà automaticamente una connessione WCIMXMPP da associare alla connessione WCMailCheck già esistente ed eseguirà la migrazione dei contatti IM dal sistema precedente a XMPP. L'aspetto del nuovo client WCIM è essenzialmente lo stesso, ma con qualche differenza, ad esempio nella gestione dei contatti e delle chat di gruppo. Per ulteriori informazioni su cosa è cambiato, vedere la Guida in linea del client WCIM.

Integrazione con Dropbox di WorldClient 345

WorldClient dispone ora di supporto diretto per Dropbox, che consente agli utenti di salvare allegati di file nei relativi account Dropbox e di inserire collegamenti diretti ai file Dropbox nei messaggi in uscita. Per fornire questa funzione agli utenti WorldClient, è necessario impostare WorldClient come app Dropbox sulla Guida degli sviluppatori della piattaforma Dropbox. Si tratta di un processo semplice che richiede solo di registrarsi a un account Dropbox, di creare un nome univoco per una app con l'accesso Dropbox completo, di specificare l'URI di reindirizzamento a WorldClient e di modificare un'impostazione predefinita. Si dovranno quindi copiare e incollare la Chiave app e il Segreto app di Dropbox nelle opzioni della schermata Dropbox in MDaemon. Dopodiché gli utenti saranno in grado di collegare gli account Dropbox a WorldClient quando accedono a WorldClient. Per le istruzioni dettagliate su come creare la app Dropbox e il collegamento a WordClient vedere: Creazione e collegamento alla app Dropbox 347.

Quando si crea la app Dropbox lo stato iniziale sarà "Sviluppo". Ciò consente a un massimo di 500 utenti WorldClient di collegare gli account Dropbox all'app. Secondo Dropbox, comunque, "dopo che l'app ha collegato 50 utenti Dropbox, per due settimane si potrà richiedere e ricevere l'approvazione allo stato Produzione prima che venga bloccata all'app la possibilità di collegare altri utenti Dropbox indipendentemente da quanti collegamenti compresi tra 0 e 500 abbia già eseguito". Ciò significa che finché non si riceve l'approvazione per la produzione, l'integrazione con Dropbox continuerà a funzionare ma nessun altro utente sarà in grado di collegare il proprio account. Dopo aver ricevuto l'approvazione per la produzione, sarà semplice accertarsi che l'app sia conforme alle linee guida e ai termini di servizio di Dropbox. Per ulteriori informazioni, vedere la sezione Approvazione per la produzione della Guida dello sviluppatore per piattaforma Dropbox.

Dopo aver creato e configurato correttamente la app WorldClient, ciascun utente WorldClient avrà la possibilità di connettere il proprio account all'account Dropbox quando accede a WorldClient. All'utente viene richiesto di accedere a Dropbox e di concedere alla app l'autorizzazione di accesso all'account Dropbox. A questo punto l'utente verrà reindirizzato a WorldClient tramite un URI trasferito a Dropbox durante il

processo di autenticazione. Per motivi di sicurezza all'URI dovrà corrisponda uno degli URI di reindirizzamento specificati nella pagina di informazioni dell'app all'indirizzo Dropbox.com. Infine, WorldClient e Dropbox si scambieranno un codice e un token di accesso, il che consentirà a WorldClient di connettersi all'account Dropbox dell'utente in modo che quest'ultimo possa salvare gli allegati in questa posizione. Il token di accesso scambiato scade ogni sette giorni, quindi l'utente periodicamente dovrà riautorizzare l'account all'uso di Dropbox. Inoltre gli utenti possono disconnettere manualmente i propri account da Dropbox o riautorizzarli se necessario, dalla schermata delle opzioni App Cloud in WorldClient.

Integrazione con Let's Encrypt 605 mediante script PowerShell

Per supportare SSL/TLS e HTTPS 585 per MDaemon 587, WorldClient 590 e Remote Administration 594, è necessario un certificato SSL/TLS. I certificati sono file di piccole dimensioni emessi da un'autorità di certificazione (CA) utilizzati per verificare che un client o un browser siano connessi al server previsto e che consentono a SSL/TLS/HTTPS di proteggere la connessione a un determinato server. Let's Encrypt è l'autorità di certificazione CA che fornisce certificati gratuiti mediante un processo automatizzato che intende eliminare il meccanismo complesso con cui attualmente si procede alla creazione, convalida, firma, installazione e rinnovo manuali di certificati per siti Web sicuri.

Per supportare la gestione di un certificato utilizzando il processo automatizzato di Let's Encrypt, MDaemon include uno script PowerShell nella cartella "`MDaemon\LetsEncrypt`". Il modulo ACMESharp v2, una dipendenza dello script, richiede PowerShell 5.1 e .Net Framework 4.7.2, il che significa che lo script non funzionerà in Windows 2003. Inoltre WorldClient deve essere in ascolto sulla porta 80 altrimenti non sarà possibile completare il test HTTP e lo script non funzionerà. Sarà necessario impostare correttamente il criterio di esecuzione per PowerShell prima di poter eseguire lo script. L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di WorldClient per completare il test http-01. Viene utilizzato il nome host SMTP 188 del dominio predefinito 185 come dominio per il certificato, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, WorldClient e Remote Administration.

Se esiste un'impostazione FQDN 188 per il dominio predefinito che non punta al server MDaemon, lo script non funzionerà. Se si desidera impostare nomi host alternativi nel certificato, è possibile trasferirli sulla riga di comando.

Esempio di utilizzo:

```
..\LetsEncrypt.ps1 -AlternateHostNames mail.domain.com,wc.domain.com -
   IISSiteName MySite -To "admin@dominiopersonale.com"
```

Non è necessario includere il valore FQDN del dominio predefinito nell'elenco `AlternateHostNames`. Ad esempio, si supponga che il dominio predefinito sia "`esempio.com`" configurato con un FQDN "`mail.esempio.com`" e si desideri utilizzare il nome host alternativo "`imap.esempio.com`". Quando si esegue lo script, come nome host alternativo, può essere trasferito solo "`imap.esempio.com`". Inoltre, se si trasferiscono nomi host alternativi, sarà necessario completare un test HTTP per ognuno. Se i test non vengono tutti completati il processo non si concluderà in modo corretto. Se non si desidera utilizzare alcun nome host alternativo, non includere il parametro `-AlternateHostNames` nella riga di comando.

Se si esegue WorldClient tramite IIS, non sarà necessario trasferire allo script il nome del sito utilizzando il parametro `-IISSiteName`. È necessario disporre degli strumenti di Web Scripting di Microsoft installati affinché il certificato venga impostato automaticamente in IIS.

Infine, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script. Il registro include la data e l'ora di inizio dello script ma non l'indicatore data/ora di ciascuna azione. Possono essere inoltre inviate notifiche via mail quando si verifica un errore. L'operazione si esegue tramite la variabile `$error` creata e impostata automaticamente da PowerShell. Se non si desidera ricevere notifiche via e-mail quando si verifica un errore, non includere il parametro `-To` nella riga di comando.

Opzione per memorizzare le password della casella postale utilizzando una crittografia non reversibile

È disponibile una nuova opzione Password 870 per memorizzare le password della casella postale utilizzando una crittografia non reversibile. In questo modo le password non possono essere decrittografate da MDaemon, dall'amministratore e da malintenzionati. Se è abilitata, MDaemon utilizza la funzione hashing delle passwordbcrypt che consente l'utilizzo di password più lunghe (fino a 72 caratteri), nonché di conservarle senza rivelarle durante l'importazione e l'esportazione di account. Alcune funzionalità, tuttavia, non sono compatibili con questa opzione, ad esempio il rilevamento di password non sicure e l'autenticazione APOP e CRAM-MD5, poiché queste dipendono dalla capacità di MDaemon di decrittografare le password. Le password irreversibili sono abilitate per impostazione predefinita.

Approvazione client ActiveSync

È disponibile una nuova impostazione ActiveSync che è possibile utilizzare per richiedere che i "I nuovi clienti devono essere autorizzati dall'amministratore prima della sincronizzazione" con un account. L'elenco Client 470 indica i client in attesa di autorizzazione da parte dell'amministratore che può concederla dalla stessa schermata. Questa opzione è disponibile nelle schermate di impostazioni client Globale 430 e Account 780. L'opzione globale è disattivata per impostazione predefinita mentre l'opzione account è impostata su "Eredita".

Notifiche di ActiveSync

Sono state aggiunte ad ActiveSync due tipi di notifiche amministrative: Notifiche di rollback della sincronizzazione e notifiche di messaggi corrotti.

Notifiche di rollback della sincronizzazione

Il servizio ActiveSync può ora inviare una notifica agli amministratori se un client invia ripetutamente o frequentemente chiavi di sincronizzazione scadute nelle operazioni di sincronizzazione.

Queste informano semplicemente l'amministratore che il server ha eseguito il rollback per una determinata raccolta perché un client ha fatto una richiesta di sincronizzazione con la chiave di sincronizzazione scaduta più di recente. L'oggetto riporta "Client ActiveSync che usa chiave di sincronizzazione scaduta". Questo può accadere a causa di errori di rete o del contenuto inviato in precedenza al client in

quella raccolta. In alcuni casi, sarà presente l'ID dell'elemento, a seconda se la precedente sincronizzazione sulla specifica raccolta abbia inviato elementi o meno.

Gli avvisi di rollback non significano che il client non è sincronizzato, ma che è possibile che il client non sia sincronizzato in futuro e che il sistema lo ha rilevato. Gli avvisi di rollback sono emessi per una raccolta una sola volta ogni 24 ore. È possibile modificare le chiavi seguenti nell'intestazione [System] del file `\MDaemon\Data\AirSync.ini`:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (L'impostazione predefinita è disabilitato)
- [System] RollbackNotificationThreshhold=[1-254] : Il numero di rollback che deve essere eseguito su una specifica raccolta prima che venga inviata una notifica all'amministratore. Si consiglia di utilizzare un valore di almeno 5 in questo campo, dato che eventuali problemi della rete possono avere un ruolo in questo. (L'impostazione predefinita è 10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Se inviare o meno una notifica in CC all'utente il cui client ha inviato la chiave di sincronizzazione scaduta. (L'impostazione predefinita è disabilitato)

Notifiche dei messaggi corrotti di ActiveSync

Il servizio ActiveSync può ora inviare una notifica all'amministratore se non è possibile elaborare uno specifico messaggio. Le notifiche sono inviate in tempo reale per informare l'amministratore di elementi di posta che non è stato possibile analizzare e sui quali non è possibile eseguire altre operazioni. L'oggetto riporta "Notifica di messaggio corrotto". Questi elementi, nelle versioni precedenti, potevano portare a un errore del sistema. Nella maggior parte dei casi, il contenuto del file msg non sarà costituito da dati MIME. Se si tratta di dati MIME, è probabile che sia corrotto. È possibile scegliere di inviare in CC tali notifiche all'utente interessato con la chiave CMNCCUser in modo che sia a conoscenza del fatto che è arrivato un messaggio e-mail non leggibile nella casella postale. L'azione appropriata in questi casi consiste nello spostare il msg designato dalla casella postale dell'utente e analizzarlo, per determinare il motivo per cui non è possibile eseguire il parse e come è giunto ad assumere lo stato in cui si trova. È possibile modificare le seguenti chiavi sotto l'intestazione [System] del file `\MDaemon\Data\AirSync.ini`:

- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False] (L'impostazione predefinita è abilitato)
- [System] CMNCCUser==[0|1|Yes|No|True|False] (L'impostazione predefinita è abilitato)

Novità di MDaemon Private Cloud 4.5

- MDaemon Private Cloud 4.5 comprende MDaemon 16.5.2 e Outlook Connector 4.0.1.
- Per il plug-in ClamAV è stata aggiunta l'opzione per mettere in quarantena i file che non possono essere sottoposti a scansione. Inoltre è stata aggiunta un'opzione per ammettere i file protetti da password che non si possono

sottoporre a scansione. Se vengono ammessi file che non è possibile sottoporre a scansione, i risultati dell'intestazione "X-CAV-Result:" potrebbero contenere "encrypted" (file protetto da password), "non-scan" (impossibile eseguire la scansione) o "scanning error" (errore durante la scansione).

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 16.5.

Per un elenco di tutte le modifiche apportate a Outlook Connector, vedere le Note di rilascio di Outlook Connector 4.0.1.

Novità della versione 16.5 di MDaemon

Miglioramenti a MDPGP

Supporto dei server delle chiavi

WorldClient

WorldClient può ora agire come server di chiavi pubbliche di base. Attivare la nuova opzione di MDPGP "*Invia chiavi pubbliche su HTTP (WorldClient)*" e WorldClient soddisferà le richieste di chiavi pubbliche degli utenti. Il formato dell'URL per sottoporre le richieste ha il seguente aspetto: "`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`". Dove `<WorldClient-URL>` è il percorso al server WorldClient (ad esempio, "`http://wc.esempio.com`") e `<Key-ID>` è l'ID chiave a sedici caratteri della chiave desiderata (ad esempio, "`0A1B3C4D5E6F7G8H`"). L'ID chiave è costituito dagli ultimi 8 byte del fingerprint della chiave: 16 caratteri in tutto.

DNS (PKA1)

Attivare la nuova opzione di MDPGP "*Raccogli chiavi pubbliche da DNS (pka1) e cache per [xx] ore*" se si desidera che MDPGP esegua una ricerca delle chiavi pubbliche su DNS del destinatario del messaggio mediante PKA1. Questo è utile perché automatizza il processo che consente di ottenere le chiavi pubbliche di alcuni destinatari, evitando la necessità di ottenerle e importarle manualmente per poter mandare messaggi crittografati. Quando vengono eseguite le query PKA1, tutti gli eventuali URI della chiave trovati vengono immediatamente raccolti, convalidati e aggiunti al keyring. Le chiavi raccolte e importate correttamente nel keyring mediante questo metodo scadranno automaticamente dopo il numero di ore specificato in questa opzione o in base al valore TTL del record PKA1 che vi fa riferimento, a seconda di quale valore è il maggiore.

Gestione delle chiavi

Registrazione delle chiavi

MDPGP ora traccia sempre le chiavi in base agli ID di chiave primaria anziché talvolta in base all'ID chiave e talvolta in base all'ID della chiave secondaria. Di conseguenza, nell'elenco di chiavi della finestra di dialogo di MDPGP sono state rimosse due colonne non più necessarie. Inoltre, MDPGP ora controlla in modo più severo il contenuto della cartella delle "esportazioni". Ne consegue che le copie esportate delle chiavi degli utenti

locali saranno sempre incluse in tale cartella. Anche se le chiavi private sono crittografate, per una ulteriore sicurezza è consigliabile utilizzare gli strumenti del sistema operativo per proteggere la cartella (anzi l'intera struttura di cartelle PEM) dall'accesso non autorizzato.

Chiavi preferite

In precedenza, quando nel keyring erano presenti più chiavi diverse per lo stesso indirizzo e-mail, MDPGP crittografava i messaggi utilizzando la prima chiave trovata. Ora è possibile fare clic con il pulsante destro del mouse su qualsiasi chiave e impostarla come preferita, in modo che MDPGP utilizzi tale chiave in presenza di più chiavi. Se non viene definita una chiave preferita, MDPGP utilizzerà la prima che trova. Durante la decrittografia di un messaggio MDaemon proverà con ciascuna chiave.

Chiavi disattivate

Le chiavi disattivate ed eliminate sono ora registrate in un nuovo file denominato `oldkeys.txt`. In precedenza le chiavi disattivate venivano registrate nel file `plugins.dat`.

Verifica della firma di MDPGP

MDPGP ora consente di verificare le firme incorporate all'interno dei messaggi non crittografati. In precedenza questo non era possibile, a meno che il messaggio non fosse sia crittografato che firmato. Quando si visualizza un messaggio con una firma verificata in WorldClient, viene visualizzata una nuova icona per indicare che è stato verificato. La verifica della firma è abilitata per impostazione predefinita per tutti gli utenti non locali. In alternativa è possibile specificare esattamente quali indirizzi e-mail possono o non possono utilizzare il servizio (vedere: "*Configura con precisione chi può e chi non può utilizzare i servizi MDPGP*" nella finestra di dialogo di MDPGP 641).

Server di messaggistica istantanea XMPP 381

MDaemon è ora dotato di un server XMPP (Extensible Messaging and Presence Protocol), talvolta definito server Jabber. Questo consente agli utenti di inviare e ricevere messaggi istantanei mediante client XMPP di terze parti, come Pidgin, Gajim, Swift e moti altri. I client sono disponibili per la maggior parte delle piattaforme dei dispositivi mobili e sistemi operativi. Il sistema di messaggistica istantanea XMPP è completamente indipendente dal sistema di chat corrente WorldClient Instant Messenger di MDaemon; i due sistemi non comunicano tra di loro e non condividono elenchi di amici.

Il server XMPP è installato come servizio Windows e le porte server predefinite sono la 5222 (SSL tramite STARTTLS) e 5223 (SSL dedicata). Il server XMPP utilizzerà la configurazione SLL di MDaemon se attivata in MDaemon. Inoltre, alcuni client XMPP utilizzano il record DNS SRV per il rilevamento automatico dei nomi host. Per ulteriori informazioni, visitare il sito http://wiki.xmpp.org/web/SRV_Records.

Gli utenti accedono attraverso il client XMPP preferito utilizzando indirizzo e-mail e password. Tuttavia alcuni client richiedono che l'indirizzo e-mail venga suddiviso in componenti separati per l'accesso. Ad esempio, anziché "`franco@esempio.com`", alcuni client richiedono "`franco`" come nome utente/accesso e "`esempio.com`" come dominio.

Per il servizio chat multiutente/gruppo, i client di solito mostrano "room" o "conference". Quando si desidera avviare una sessione chat di gruppo, creare una room/conference (assegnare un nome) e inviare gli altri utenti a tale chat room. Gran parte dei client non richiede di immettere una posizione server per la conferenza in quanto è sufficiente inserire un nome. Nel momento in cui viene richiesta questa operazione utilizzare comunque "`conference.<dominio>`" come posizione (ovvero. `conference.esempio.com`). Alcuni client richiedono di inserire il nome e la posizione insieme nel modulo: "`room@conference.<dominio>`" (ovvero `Room01@conference.esempio.com`).

Alcuni client (ad esempio Pidgin) supportano il servizio di ricerca utenti consentendo agli utenti la ricerca del server mediante nome o indirizzo e-mail, il che rende molto più semplice aggiungere i contatti. Di solito non è necessario fornire una posizione di ricerca, se tuttavia viene richiesto utilizzare "`search.<dominio>`" (ad es. `search.esempio.com`). Durante la ricerca, è possibile utilizzare il simbolo % come carattere jolly. Pertanto è possibile utilizzare "%@esempio.com" nel campo dell'indirizzo e-mail per visualizzare un elenco di tutti gli utenti il cui indirizzo e-mail termina con "@esempio.com."

Gestione centralizzata delle impostazioni del client OC

Utilizzare la finestra di dialogo Impostazioni client OC per gestire centralmente le impostazioni client degli utenti di Outlook Connector. Configurare ciascuna schermata con le impostazioni client desiderate; MDaemon le invierà alle schermate client corrispondenti secondo necessità ogni volta che un utente di Outlook Connector si connette al server. Le impostazioni del client OC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client. Se si è attivata l'opzione "*Consenti agli utenti OC di sostituire le impostazioni distribuite via push*", gli utenti possono ignorare le impostazioni inviate sui singoli client. Se invece è disattivata, tutte le schermate client sono bloccate e gli utenti di Outlook Connector non possono apportare alcuna modifica.

Per consentire la configurazione di impostazioni che devono essere diverse per ciascun utente o dominio, Impostazioni client OC supporta macro come `$USERNAME$`, `$EMAIL$` e `$DOMAIN$`. Quando si esegue il push delle impostazioni a un client, le macro vengono convertite in dati specifici per il singolo utente o dominio. Accertarsi che non vengano inseriti valori statici nei campi che devono contenere macro, ad esempio nomi propri come "Franco Tommaso" nel campo Nome. In questo caso tutti gli utenti di Outlook Connector che si connettono a MDaemon vedrebbero il proprio nome impostato su "Franco Tommaso". Per comodità dell'utente è disponibile un pulsante Riferimento macro nella schermata Generale in cui viene riportato un semplice elenco delle macro supportate.

Per chi utilizza MDPC (MDaemon Private Cloud), è disponibile un'altra finestra di dialogo Impostazioni client OC in Domain Manager per il controllo delle impostazioni client di Outlook Connector a livello di singolo dominio.

Questa funzione è disattivata per impostazione predefinita e funziona solo per chi utilizza il client Outlook Connector versione 4.0.0 o successiva.

Protezione/Modifica dell'intestazione From

Questa nuova funzione di sicurezza modifica l'intestazione "From:" dei messaggi in entrata in modo che la parte dell'intestazione che indica solo il nome, ora contenga sia il nome che l'indirizzo e-mail. Questo metodo serve a fronteggiare la tattica comunemente utilizzata nello spam e negli attacchi in cui il messaggio sembra provenire da altro destinatario. Quando si visualizza un elenco di messaggi, i client di posta elettronica in genere visualizzano solo il nome del mittente anziché nome e indirizzo e-mail. Per visualizzare l'indirizzo e-mail, il destinatario deve prima aprire il messaggio o eseguire altre azioni analoghe, ad esempio fare clic con il pulsante destro del mouse sulla voce, posizionare il puntatore sul nome o altro. Per questo motivo i responsabili degli attacchi di solito creano una e-mail in modo che un nome di persona o di azienda legittimi siano visualizzati nella parte visibile dell'intestazione "From:" mentre l'indirizzo e-mail non legittimo risulti nascosto. Ad esempio, l'intestazione "From:" di un messaggio dovrebbe effettivamente essere, `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, ma è possibile che il client visualizzi solo `"Honest Bank and Trust"` come mittente. Questa funzione consente di modificare la parte visibile dell'intestazione in modo da visualizzare entrambe le parti, di cui la prima è l'indirizzo e-mail. Nel suddetto esempio il mittente ora dovrebbe essere visualizzato come `"lightfingers.klepto@example.com -- Honest Bank and Trust,"` il che fornisce una chiara indicazione dell'illegittimità del messaggio. Questa opzione è valida solo per i messaggi inviati a utenti locali ed è disattivata per impostazione predefinita.

Vaglio IP migliorato

La schermata di Vaglio IP contiene ora un pulsante Importa che è possibile utilizzare per importare i dati dell'indirizzo IP da un file APF o .htaccess. Il supporto di questi file da parte di MDaemon attualmente è limitato a quanto segue:

- vengono supportati "deny from" e "allow from"
- vengono importati solo i valori IP (non i nomi di dominio)
- è possibile usare la notazione CIDR, ma non gli indirizzi IP parziali.
- Ogni riga può contenere un qualsiasi numero di indirizzi IP separati da spazi o virgole. Ad esempio, "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5" e simili.
- Le righe che iniziano per # vengono ignorate.

Installazione automatica di aggiornamenti dei prodotti

Grazie alle funzionalità di aggiornamento automatico, è possibile configurare MDaemon in modo da informare il postmaster ogni volta che si rende disponibile un aggiornamento per uno dei prodotti installati oppure scaricare e installare gli aggiornamenti automaticamente. I prodotti inclusi comprendono MDaemon, SecurityPlus e Outlook Connector. È possibile controllare l'installazione automatica degli aggiornamenti separatamente per ciascun prodotto. Ogni volta che si installa un aggiornamento, è necessario riavviare il server. I file di installazione vengono scaricati non appena viene rilevato l'aggiornamento, ma installazione e riavvio si possono eseguire nel momento che l'utente ritiene più opportuno. L'intera attività di installazione viene registrata nel registro di sistema di MDaemon, mentre il postmaster riceve una notifica dopo ogni aggiornamento. Per ulteriori informazioni, vedere la finestra di dialogo Aggiornamenti.

Modifiche apportate a WorldClient

Categorie

WorldClient supporta le categorie per i messaggi e-mail nei temi LookOut e WorldClient. Gli utenti possono aggiungere la colonna Categorie all'elenco messaggi in "Opzioni » Colonne" e selezionando "Categorie" nella sezione Elenco messaggi. Per scegliere le categorie per uno o più messaggi, selezionare i messaggi e fare clic con il pulsante destro del mouse su uno di questi. Per impostare la categoria utilizzare il menu contestuale.

- Gli amministratori possono creare categorie personalizzate. A questo scopo, sono stati creati due file: `DomainCategories.json` e `PersonalCategories.json`.
- Le categorie del dominio vengono abilitate in modo globale per impostazione predefinita. Per disattivarle aprire `MDaemon\WorldClient\Domains.ini` e nella sezione `[Default:Settings]` modificare il valore "`DomainCategoriesEnabled=`" da "`Yes`" in "`No`".
- Gli utenti possono aggiungere e modificare le proprie categorie per impostazione predefinita. Se si desidera disattivare questa opzione, l'operazione può essere eseguita per ciascun utente o globalmente modificando il valore "`CanEditPersonalCategories=`" da "`Yes`" in "`No`". L'opzione utente è disponibile nella sezione `[User]` del file `User.ini` mentre l'opzione globale si trova nel file `Domains.ini` nella sezione `[Default:UserDefaults]`.
- Se si abilitano le Categorie dominio e un utente non è autorizzato a modificare le categorie personali, l'utente visualizzerà solo le categorie riportate in `DomainCategories.json`.
- Se si disabilitano le Categorie dominio e un utente non è autorizzato a modificare le categorie personali, l'utente visualizzerà le categorie riportate in `PersonalCategories.json`.
- Il file `CustomCategoriesTranslations.json` viene utilizzato per supportare i nomi di categorie personalizzate in più lingue. Aggiungere le eventuali traduzioni delle categorie personalizzate a tale file in modo che WorldClient possa riconoscere una categoria salvata in un evento, in una nota o in un'attività in una lingua come categoria equivalente in un'altra lingua.

Per informazioni più dettagliate sui file qui menzionati, vedere: `MDaemon\WorldClient\CustomCategories.txt`.

Liste bianche e nere

È ora possibile nascondere le cartelle Lista bianca e Lista nera degli utenti WorldClient per impostazione predefinita. Per eseguire questa operazione, aprire `MDaemon\WorldClient\Domains.ini` e in `[Default:UserDefaults]` modificare il valore "`HideWhiteListFolder=`" o "`HideBlackListFolder=`" da"`No`" in "`Yes`". È possibile nascondere o mostrare queste cartelle a utenti specifici modificando quelle stesse chiavi nel file `User.ini` nella sezione `[User]`.

Controllo degli allegati

Nei temi LookOut e WorldClient è stata aggiunta un'opzione per il controllo degli allegati di un messaggio composto prima dell'invio, quando gli allegati sono menzionati nell'oggetto o nel corpo del messaggio. Questo può essere d'aiuto per evitare di inviare per errore un messaggio senza allegati mentre il messaggio dovrebbe includere degli allegati.

Autenticazione a due fattori 735

È ora possibile controllare se gli account possono utilizzare o richiedere di utilizzare l'autenticazione a due fattori (2FA). Sono disponibili due nuove opzioni nel modello Nuovi account 814 per il controllo delle impostazioni predefinite per i nuovi account, e sono disponibili opzioni corrispondenti nella schermata Servizi web 735 per il controllo 2FA per singoli account.

Novità di MDaemon Private Cloud 4.0

- MDaemon Private Cloud 4.0 comprende MDaemon 16.0.3 e Outlook Connector 3.5.2.
- Aggiornamento a una versione più recente del motore di Outbreak Protection.
- Motore ClamAV aggiornato alla versione 0.99.2.

Per un elenco di tutte le modifiche apportate a MDaemon, vedere le Note di rilascio di MDaemon 16.0.

Per un elenco di tutte le modifiche apportate a Outlook Connector, vedere le Note di rilascio di Outlook Connector 3.5.2.

Novità della versione 16.0 di MDaemon

Aggiornamento dell'interfaccia utente di MDaemon Remote Administration (MDRA)

L'interfaccia utente di MDRA non utilizza più i frame ed è stata aggiornata per l'uso di un Mobile First Responsive Design. Il supporto dei browser si limita a IE 10 o versione successiva, Firefox e Chrome più recenti e l'ultimo Safari su Mac e iOS. Il browser standard di Android causa problemi nello scorrimento, mentre Chrome sui dispositivi Android funziona bene.

Questo design è interamente basato sulle dimensioni della finestra in uso. A prescindere che si utilizzi un telefono, un tablet o un PC, a parità di dimensioni della finestra, l'aspetto sarà lo stesso. La variazione più importante riguarda il menu. Se la larghezza è inferiore ai 1024 pixel, il menu viene nascosto nel lato sinistro del browser. Per visualizzare il menu è possibile utilizzare due metodi. Con un dispositivo touch, se si fa scorrere il dito verso destra si visualizza il menu secondario. Indipendentemente da quale dispositivo sia in uso, è disponibile anche un pulsante "menu" nell'angolo superiore sinistro che consente di visualizzare il menu secondario. Se si tocca o si fa clic sul titolo

del menu con la freccia verso sinistra accanto alla parte superiore del menu, viene visualizzato il menu principale. Anche le opzioni di menu Guida, Informazioni su ed Esci nell'angolo superiore destro cambiano in base alla larghezza dello schermo. Oltre i 768 pixel vengono visualizzate le parole Guida, Informazioni su ed Esci. Da 481 a 767 pixel vengono visualizzate solo le icone e sotto i 480 pixel viene visualizzata l'icona dell'ingranaggio che, se cliccata o toccata, visualizza un menu a discesa con le opzioni Guida, Informazioni su ed Esci. Le viste dell'elenco con più colonne presentano pulsanti per attivare/disattivare le colonne a cui è possibile accedere facendo clic o toccando il pulsante con la freccia a destra grigia all'estrema destra del contenitore della barra degli strumenti. Le pagine delle impostazioni non sono più destinate a essere copie esatte della GUI MDaemon, bensì vengono ora riposizionate e ridimensionate in base a larghezza/altezza del browser.

Rilevamento spambot 580

Un nuova funzione denominata Rilevamento spambot tiene traccia degli indirizzi IP che ciascun valore SMTP MAIL (percorso restituzione) utilizza in un determinato periodo di tempo. Se lo stesso percorso restituzione viene utilizzato da un numero insolito di indirizzi IP in un breve periodo di tempo, è possibile che indichi una rete spambot. Anche se l'uso del sistema di posta è ancora consentito, ne è stata dimostrata la validità solo in alcuni casi al rilevamento di una rete spambot distribuita purché venga utilizzato per intero lo stesso percorso restituzione. Se viene rilevato uno spambot, la connessione corrente si interrompe immediatamente e il valore del percorso restituzione può essere inserito nella lista nera per un periodo di tempo specificato. Eventualmente è anche possibile aggiungere alla lista nera gli IP spambot conosciuti per un periodo definito dall'utente.

CardDAV 376

MDaemon ora supporta la sincronizzazione dei contatti tramite il protocollo CardDAV. Il server CardDAV consente a un client CardDAV autenticato di accedere alle informazioni di contatto memorizzate in MDaemon. I client CardDAV rilevanti sono i contatti Apple (inclusi in Mac OS X), Apple iOS (iPhone) e Mozilla Thunderbird tramite il plugin SOGO. Per ulteriori informazioni su CardDAV e configurazione dei relativi client, vedere: CalDAV e CardDAV 376.

Autenticazione a due fattori per WorldClient e Remote Administration

MDaemon ora supporta l'autenticazione a due fattori (ovvero la verifica in 2 fasi) per gli utenti che accedono a WorldClient o all'interfaccia Web Remote Administration di MDaemon. Qualsiasi utente che acceda a WorldClient tramite HTTPS può attivare l'autenticazione a due fattori per l'account nella schermata **Opzioni » Sicurezza**. Da quel momento l'utente quando accede a WorldClient o Remote Admnistration dovrà immettere un codice di verifica. Il codice viene fornito all'accesso da una app di autenticazione installata nel dispositivo mobile o tablet dell'utente. Questa funzione è progettata per i client che supportano Google Authenticator.

Client di migrazione del protocollo ActiveSync

MDaemon ora include un protocollo ActiveSync basato sul client di migrazione (`ASMC.exe`). Tale protocollo supporta migrazione della posta, calendari, attività, note e

contatti dai server ActiveSync che supportano il protocollo versione 14.1. La documentazione è reperibile nella cartella `\MDaemon\Docs`.

API XML per attività di gestione

MDaemon ora viene fornito con una API basata su XML su http(s). Ne consegue che i client di gestione di MDaemon possono essere scritti utilizzando qualsiasi linguaggio su qualsiasi piattaforma in grado di trasmettere richieste http(s):// al server. In MDaemon, questo è disponibile solo per gli amministratori di livello Globale ma in MDaemon Private Cloud un sottoinsieme delle operazioni disponibili è accessibile anche da parte degli amministratori di domini autenticati. L'API crea anche un sito web con documentazione sulle specifiche API. L'installazione predefinita è in `http://servername:RemoteAdminPort/MdMgmtWS/`, tuttavia è possibile eseguire l'impostazione su qualsiasi url per una maggiore sicurezza.

Le operazioni disponibili includono:

- Guida
- CreateDomain
- DeleteDomain
- GetDomainInfo
- UpdateDomain
- CreateUser
- DeleteUser
- GetUserInfo
- UpdateUser
- CreateList
- DeleteList
- GetListInfo
- UpdateList
- AddDomainAdministrator
- DeleteDomainUsers
- GetDomainList
- GetVersionInfo
- GetQueueState
- GetServiceState
- SetAddressRestriction
- GetAddressRestriction

Questa volta i client di gestione delle righe di comando sono stati scritti/testati in Javascript, Powershell, VBScript, C, C++ e Visual Basic. È stato utilizzato un semplice

sito di test HTML e Javascript come prova di concetto di una console di gestione basata su Web che funziona con diversi browser tra i più diffusi. Sebbene non ancora testata, si prevede che questa API funzioni bene dai server Web tramite PHP, Perl e altre piattaforme di sviluppo.

Per ulteriori informazioni, vedere:

Introduzione 12
Aggiornamento a MDaemon Private Cloud 11.0.0 65
Schermata principale di MDaemon 74

1.4 Aggiornamento a MDaemon Private Cloud 11.0.0

Di seguito è riportato un elenco di considerazioni e annotazioni speciali che possono essere utili per l'aggiornamento a MDaemon versione 23.0.2 da una versione precedente. Per un elenco completo delle funzionalità aggiunte, delle modifiche e delle correzioni incluse in MDaemon 23.0.2, vedere le Note di rilascio di MDaemon.

Versione 23.0.2

- La Protezione dagli attacchi (Outbreak Protection) è stato ripristinato in MDaemon 23.0.2.

Versione 23.0.1

- Cyren Anti-Virus è stato sostituito da IKARUS Anti-Virus. Cyren di recente ha annunciato i suoi piani di interrompere le proprie attività con poco preavviso. Per questo motivo abbiamo dovuto cercare un nuovo partner anti-virus. A seguito di un'attenta valutazione, IKARUS si è distinto per l'eccellente velocità e tasso di rilevamento. IKARUS Anti-Virus aggiorna automaticamente le sue definizioni ogni 10 minuti. Scanning with IKARUS is disabled if your AntiVirus license is expired.
- La Protezione dagli attacchi di Cyren è stata rimossa. Cyren di recente ha annunciato i suoi piani di interrompere le proprie attività con poco preavviso. Stiamo attivamente facendo ricerche e considerando tecnologie antispam utilizzabili come aggiunte adatte ai meccanismi antispam già esistenti nei nostri prodotti software.
- Il supporto dei flag delle parole chiave IMAP può ora essere attivato o disattivato mediante l'impostazione [Special] IMAPKeywordFlags=Yes/No in \MDaemon\App\MDaemon.ini. I flag delle parole chiave IMAP sono disattivati per impostazione predefinita durante l'aggiornamento di MDaemon da una versione precedente alla 23, per evitare la potenziale perdita di tag di messaggi nei client di posta Thunderbird. Quando Thunderbird si connette a un server IMAP che supporta i flag delle parole chiave, sovrascrive i tag dei messaggi locali con i tag letti dal server, che inizialmente sono vuoti. I flag delle parole chiave IMAP sono attivati per impostazione predefinita per le nuove installazioni e durante l'aggiornamento dalla versione 23.0.0.

Versione 23.0.0

- Per l'aggiornamento dalla versione 22.0.0 alla 23.0.0 non sono necessarie istruzioni particolari. Se si effettua l'aggiornamento da una versione precedente, consultare le note sulla versione riportate di seguito.

Versione 22.0.0

- MDaemon a 32 bit non è più supportato. MDaemon 22.0 e versioni successive saranno disponibili solo a 64 bit. Se attualmente si utilizza una versione a 32 bit su un sistema operativo a 64 bit supportato, è possibile installare la versione a 64 bit direttamente sull'installazione esistente.
- La lunghezza minima per le password complesse 870 è di almeno 8 caratteri. Se era impostata a meno di 8 caratteri prima dell'aggiornamento a MDaemon 22, la lunghezza minima verrà modificata a 8. La lunghezza minima predefinita per le password complesse nelle nuove installazioni è di 10 caratteri.
- MDaemon sta abbandonando l'uso dei termini "lista bianca" e "lista nera". In molti casi, ora si parla di "lista consentiti" e "lista bloccati". Le funzionalità che prevedevano una "lista bianca" per esentare IP, indirizzi e così via, ora prevedono un "elenco esenzioni". Le cartelle dei contatti di Spam Filter per i singoli utenti ora sono denominate "Mittenti consentiti" e "Mittenti bloccati". Le cartelle per tutti gli account verranno rinominate al primo avvio di MDaemon 22.

Versione 21.5.0

- L'intestazione `X-MDOrigin-Country`, che Screening posizione 582 può aggiungere ai messaggi, ora contiene i codici ISO 3166 a due lettere di paesi e continenti invece dei nomi completi. Aggiornare gli eventuali filtri che cercano valori particolari in questa intestazione.
- Con la ridenominazione del tema Webmail "Mobile" in "Pro", si è generato un possibile effetto collaterale per gli utenti che utilizzano il tema Mobile e hanno attivato l'opzione Ricordati di me. Per questi utenti potrebbe risultare impossibile aprire gli allegati. Per risolvere il problema, è sufficiente uscire dall'account di Webmail e riaccedere.

Versione 21.0.2

- Le impostazioni in Impostazioni » Preferenze » Varie per copiare tutte le notifiche del postmaster generate dal sistema per amministratori globali e amministratori di dominio ora vengono applicate a un maggior numero di notifiche, quali blocco e disattivazione dell'account, utente inesistente, errore del disco, spazio su disco quasi esaurito e scadenza beta e AV. Se non si desidera che gli amministratori ricevano queste notifiche, disattivare le impostazioni.

Versione 20.0.3

- MDaemon imposterà come commento la riga "`AlertExceedsMax yes`" nel file `clamd.conf` di ClamAV, poiché causa troppi errori di scansione AV "`Heuristics.Limits.Exceeded`".

Versione 20.0.1

- Nelle impostazioni di accesso alle risorse di rete nel menu Impostazioni | Preferenze | Servizio Windows ora è possibile configurare il servizio MDaemon (e i servizi Amministrazione remota e Server XMPP) per funzionare come account specificato, con la possibilità di eseguire processi e thread specifici. Il programma di installazione aggiornerà i servizi in modo da ottenere il funzionamento come account specificato con l'aggiornamento a questa versione.
- A causa delle modifiche e della dismissione di molte impostazioni in clamd.conf, il programma di installazione ora sovrascrive il file clamd.conf esistente. Se si è personalizzato il file clamd.conf, potrebbe essere necessario rivedere e modificare il file clamd.conf dopo l'installazione.

Versione 20.0.0

- Leggere con attenzione nelle note di rilascio complete la sezione indicata come attività [8930] poiché riguarda modifiche al sistema di integrazione di Active Directory e la risoluzione di problemi preesistenti ora corretti. Considerare le modifiche apportate in quell'area e leggere attentamente questa sezione delle note di rilascio.
- MDaemon 20.0 richiede Windows 7, Server 2008 R2 o versioni successive.
- Preferenze » Varie 511 ha due nuove caselle di controllo per indicare se le e-mail di notifica generate dal sistema inviate periodicamente all'alias Postmaster debbano essere inviate anche agli amministratori di livello Globale e Dominio. Per impostazione predefinita, queste opzioni sono entrambe attivate. Gli amministratori di livello Dominio possono ricevere solo le e-mail relative al proprio dominio e le Note di rilascio. Gli amministratori di livello Globale ricevono tutto, inclusi i rapporti di riepilogo code e quelli statistici, le Note di rilascio, le notifiche di "Utente inesistente" (per tutti i domini), di errori del disco, di blocco e disattivazione degli account per tutti i domini (che, come tutti gli amministratori del dominio, possono sbloccare e riattivare), avvertenze relative a licenze e versioni beta-test che stanno per scadere, rapporti di riepilogo su Spam e anche altri. Se non si desidera che gli amministratori ricevano queste notifiche, disattivare le impostazioni.
- È stato modificato il modo in cui sono memorizzati i risponditori automatici. Il testo per il risponditore automatico di un account è ora memorizzato come file `OOF.MRK` all'interno della cartella DATI dell'account che è una nuova sottocartella all'interno della cartella di posta radice dell'account. I file di script del risponditore automatico non vengono più conservati nella cartella APP e non sono condivisi tra gli account. Quando viene avviato per la prima volta, MDaemon esegue la migrazione di tutti i file e le impostazioni del risponditore automatico nelle posizioni corrette per ciascun account. Il file `AUTORESP.DAT` è

obsoleto e sarà eliminato con il file `.RSP` specifico di ciascun account (`OutOfOffice.RSP` e i file non specifici dell'account resteranno a scopo di riferimento e di esempio). Se si desidera assegnare rapidamente una singola configurazione del risponditore automatico a più account, è possibile utilizzare il nuovo pulsante Pubblica disponibile in Impostazioni account » Risponditore automatico 739. Il pulsante copierà il testo dello script del risponditore automatico esistente e tutte le impostazioni per l'account corrente negli altri account selezionati. È inoltre disponibile un pulsante Modifica file risponditore automatico 739 che consente di modificare lo script del risponditore automatico predefinito (`OutOfOffice.rsp`). Questo script predefinito viene copiato in un file `OOF.MRK` dell'account se il file `OOF.MRK` è mancante o è vuoto.

- È stato modificato il modo in cui sono memorizzati i file di firma degli account. I file di firma sono ora memorizzati come `SIGNATURE.MRK` all'interno della cartella DATI dell'account che è una nuova sottocartella all'interno della cartella di posta radice dell'account. Quando viene avviato per la prima volta, MDaemon esegue la migrazione di tutti i file di firma esistenti nelle posizioni corrette per ciascun account. La cartella Firme della cartella principale di MDaemon non conterrà più file di firma specifici dell'account ma continuerà ad essere presente perché potrebbe contenere elementi necessari a Remote Administration e al filtro contenuti di MDaemon. Il backup della cartella Firme originale veniva eseguito su `\Backup\20.0.0\Signatures\` prima della migrazione. Infine, il file `ADMINNOTES.MRK` di ciascun account è stato spostato dalla cartella radice dell'account alla nuova sottodirectory DATI.
- Il valore predefinito di Spam Filter » Lista bianca (automatica) 705 è stato modificato in disattivato per l'opzione "*...solo gli indirizzi in lista bianca che si autenticano con DKIM*". La relativa attivazione si è rivelata un po' restrittiva per molti e impedisce che l'inserimento nella lista bianca delle rubriche funzioni per la posta MultiPOP e DomainPOP. È possibile riattivare questa impostazione, se necessario.
- L'opzione di Preferenze » Interfaccia utente 497 per "*Centra tutte le finestre di dialogo dell'interfaccia utente*" è stata reimpostata sull'opzione predefinita "attivata" per tutti. Se si desidera, è possibile disattivarla. Questa opzione impedisce che le schermate vengano create parzialmente fuori dal campo visivo, ma rende anche più difficile, in alcuni casi, selezionare più schermate che si sovrappongono.
- Security Manager » Vaglio » Vaglio località 582 - L'impostazione predefinita per questa funzione è stata modificata da disattivata in attivata. Quando l'opzione Vaglio località è attivata, il paese o la regione che effettuano la connessione saranno sempre registrati (se conosciuti) anche quando il paese o la regione specifici non sono attivamente bloccati. Quindi anche se non si desidera bloccare alcun paese, è comunque possibile attivare l'opzione Vaglio località (senza selezionare alcun paese da bloccare) in modo che il paese o la regione possano essere visualizzati e bloccati. Poiché l'impostazione predefinita è stata modificata, chi esegue l'aggiornamento deve controllare la corretta configurazione dell'opzione Vaglio località. MDaemon inserirà l'intestazione "`X-MDOrigin-Country`" che elenca il paese e la regione per il filtro contenuti o per altri scopi.
- Il limite di dimensione fisso hard-coded di 2 MB per le scansioni dello Spam Filter è stato rimosso. Ora non c'è nessun limite teorico per le dimensioni dei messaggi

da sottoporre a scansione. È ancora possibile, tuttavia, configurare il proprio limite in caso questo sia un problema, ma configurare il limite su "0" (zero) ora significa nessun limite. Per accertarsi che questa opzione sia impostata sul valore desiderato, controllare la schermata Spam Filter » Impostazioni[715].

- Aggiunte le colonne "Dominio mittente" e "Dominio destinatario" alle schermate Code nell'interfaccia utente principale. Come risultato, è stato necessario eseguire un'unica reimpostazione della larghezza delle colonne salvate. Una volta impostata la larghezza delle colonne, le selezioni saranno memorizzate.
- Per impostazione predefinita ora il Vaglio host viene applicato alle connessioni MSA. Questa opzione è disponibile in: Security Manager » Vaglio » Vaglio host[573].
- Per impostazione predefinita i server IMAP, WebMail e ActiveSync di MDaemon non forniscono più l'accesso alle cartelle condivise degli account disattivati. È possibile modificare questa impostazione in Impostazioni server » Cartelle pubbliche e condivise[122].

Versione 19.5.2

- Le opzioni "*Comandi Max RSET consentiti*" in Impostazioni server » Server[94] sono state rimosse, poiché sono in effetti duplicati meno flessibili delle stesse funzionalità disponibili in nel Vaglio SMTP[575]. La versione Vaglio SMTP fa parte del sistema di vaglio dinamico che tiene conto di più fattori (vale a dire che utilizza una lista bianca, prende in considerazione lo stato di autenticazione e così via). I valori precedenti sono stati spostati in Vaglio SMTP. Controllare che i valori corrispondano a quelli previsti. I valori predefiniti corretti (e consigliati) per le opzioni sono: opzione *Blocca gli IP che inviano questo numero di comandi RSET* impostata su "**20**" e opzione *Chiudi sessione SMTP dopo blocco IP* impostata su **attivata/selezionata**.

Versione 19.5.1

- La funzionalità LetsEncrypt[605] è stata aggiornata per l'uso di ACME v2. Questo aggiornamento è richiesto perché LetsEncrypt interromperà il supporto per ACME v1. Sono ora richiesti PowerShell 5.1 e .Net Framework 4.7.2 per utilizzare LetsEncrypt.

Versione 19.5.0

- In preparazione per il supporto del clustering, alcune impostazioni (come le chiavi di registrazione) sono state spostate da `\MDaemon\App\MDaemon.ini` a `\MDaemon\LocalData\LocalData.ini`. Quando è necessario tornare a una versione precedente, le impostazioni non verranno trovate nelle nuove posizioni dai programmi di installazione precedenti, quindi questi richiederanno un codice di registrazione. Questo problema si può evitare copiando le impostazioni in `MDaemon.ini` o ripristinando il file `MDaemon.ini` di backup.

Versione 19.0.0

- L'interfaccia Web di Remote Administration di MDaemon (MDRA) è stata estesa in modo da prevedere l'accesso a molte funzionalità che in precedenza si

potevano amministrare solo utilizzando una Sessione di configurazione (ovvero, l'interfaccia dell'applicazione MDaemon), mentre ora alcune opzioni sono accessibili esclusivamente mediante MDRA. Ne consegue che, per le nuove installazioni di MDaemon, il menu di scelta rapida "Avvia MDaemon" ora apre un browser per impostazione predefinita al fine di utilizzare Remote Administration, anziché aprire una sessione di configurazione di MDaemon. Per cambiare questo comportamento, modificare il file `\MDaemon\App\MDaemon.ini` e impostare `[MDLaunch] OpenConfigSession=Yes/No` e `OpenRemoteAdmin=Yes/No`. Impostare "*URL Remote Administration*" su Impostazioni » Web e Servizi IM » Remote Administration » Server Web 361 se l'URL generato automaticamente non funziona o se MDRA viene eseguito in un server Web esterno. Se non si riesce a determinare un URL funzionante, si aprirà invece una sessione di configurazione. Infine, nel menu Start di Windows, nel gruppo di programmi MDaemon, ora sono disponibili i collegamenti di scelta rapida *Apri MDaemon Configuration Session* e *Apri MDaemon Remote Administration*.

- La funzionalità SyncML era obsoleta ed è stata rimossa.
- I calcoli dello spazio su disco di MDaemon erano incoerente in diversi punti del programma (ad esempio, per il calcolo di un kilobyte a volte venivano usati 1000, altre 1024 byte). Ora vengono utilizzati sempre 1024 byte. In alcuni casi la quota di spazio su disco degli utenti potrebbe quindi risultare leggermente diversa rispetto alla versione precedente. Controllare ed effettuare le eventuali regolazioni necessarie.
- L'opzione "Invia notifica di aggiornamento modifica solo se non riuscito 680" ora è attivata per impostazione predefinita. Quando si aggiorna alla versione MDaemon 19, l'opzione viene attivata al primo avvio di MDaemon.

Vedere:

Introduzione 12
Novità di MDaemon Private Cloud 11.0 15
Schermata principale di MDaemon 74

1.5 Assistenza

Opzioni di supporto

L'assistenza è una componente essenziale della interazione complessiva del cliente con MDaemon Technologies. Poiché desideriamo offrire al cliente il massimo rendimento dei prodotti per lungo tempo dopo l'acquisto e l'installazione iniziale, il nostro impegno è rivolto a garantire la risoluzione di eventuali problemi per consentire la massima soddisfazione. Per le informazioni relative al servizio clienti, alle opzioni di assistenza tecnica, alle risorse di supporto autonomo e ai prodotti, visitare la pagina dell'assistenza di MDaemon Technologies all'indirizzo: www.mdaemon.com/support/

Beta-test di MDaemon

MDaemon Technologies gestisce team di beta-test per i propri prodotti. Per informazioni su come unirsi ai beta-team di MDaemon, inviare un messaggio all'indirizzo MDaemonBeta@mdaemon.com.

Il beta-team è per coloro che desiderano acquisire aggiornamenti di MDaemon prima del rilascio generale e aiutare nel test di tali aggiornamenti. Non si tratta di un'alternativa all'assistenza tecnica. L'assistenza tecnica per MDaemon viene offerta solo con i metodi descritti alla pagina: www.mdaemon.com/support/.

Contatti

Orari
Lun. - ven. 8:30 - 17:30 (fuso orario degli Stati Uniti centrali)
esclusi weekend e festività statunitensi
Servizio clienti o vendite
Numero verde per gli Stati Uniti: Numero verde: 866-601-ALTN (2586)
Chiamate internazionali: 817-601-3222
sales@helpdesk.mdaemon.com

Assistenza tecnica
www.mdaemon.com/support/

Formazione
training@mdaemon.com

Sviluppo aziendale/collaborazioni
alliance@mdaemon.com

Media/Analisti
press@mdaemon.com

Richieste commerciali/rivenditori
Per ulteriori informazioni, consultare la pagina Channel Partner.

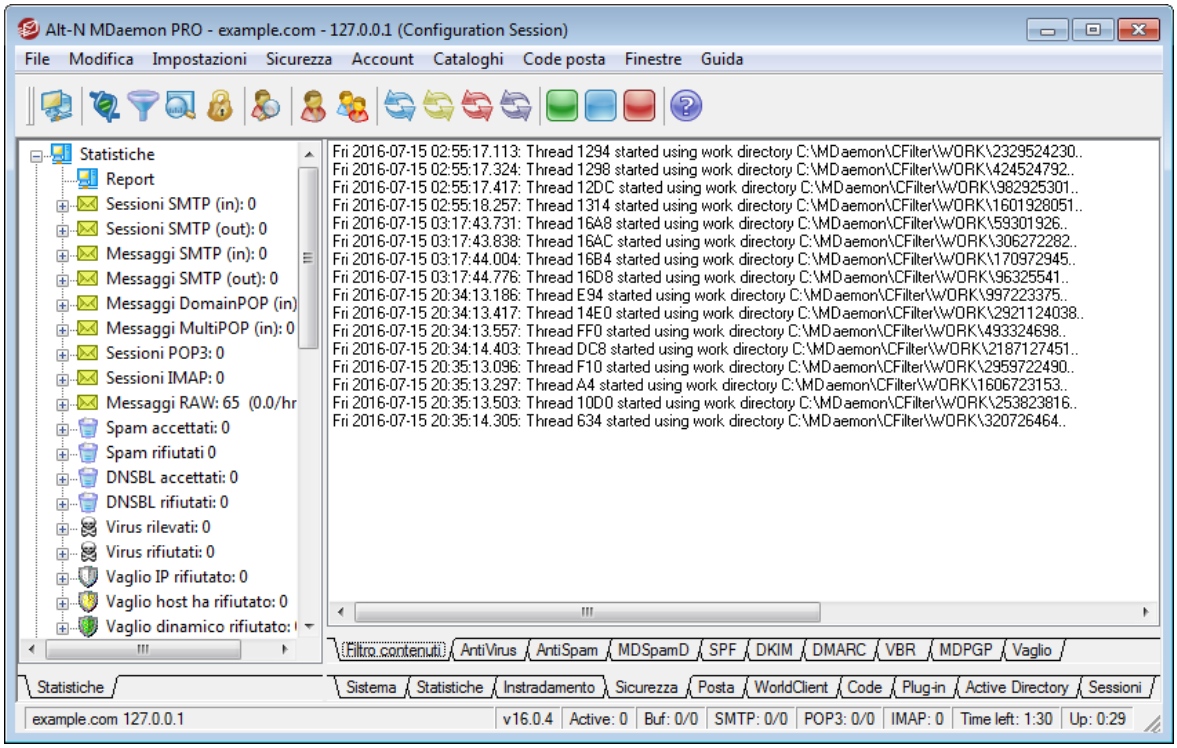
Sede centrale

MDaemon Technologies
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
Numero verde per gli Stati Uniti: Numero verde: 866-601-ALTN (2586)
Chiamate internazionali: 817-601-3222
Fax: 817-601-3223

Marchi

Sezione

2 Schermata principale di MDaemon



La GUI (interfaccia grafica utente) principale di MDaemon offre importanti informazioni su risorse, statistiche, sessioni attive e posta accodata in attesa di elaborazione. Sono inoltre presenti le opzioni per attivare/disattivare in modo semplice i vari server di MDaemon. I riquadri a schede della GUI forniscono informazioni aggiornate sulle prestazioni del server e sulle connessioni in entrata e in uscita.

Statistiche

Statistiche è il riquadro di sinistra predefinito dell'interfaccia principale di MDaemon. Comprende quattro sezioni: Statistiche, Account, Code e Server.

La sezione *Statistiche* contiene alcune statistiche relative al numero di messaggi inviati e ricevuti da MDaemon, oltre che alle sessioni POP e IMAP, ai messaggi spam accettati e rifiutati, ai virus e altro ancora. Le statistiche vengono conteggiate dall'avvio di MDaemon ed è possibile utilizzare un menu di scelta rapida per cancellare i contatori.

Quando si abilita l'opzione "Azzera contatori nodi principali", vengono resettati tutti i contatori e non solo quelli sui quali si è fatto clic con il pulsante destro del mouse. In Impostazioni » Preferenze » GUI è inoltre disponibile l'opzione "*Mantieni contatori posta nodo principale tra riavvii*." Se questa opzione non è abilitata, quando il server viene avviato i contatori vengono azzerati.

La sezione *Account* contiene voci per MDaemon, MDaemon Connector e ActiveSync. Ciascuna voce elenca il numero di account utilizzati e il numero di account rimanenti, in base alla licenza del prodotto.

La sezione *Code* include una voce per ogni coda di messaggi e il numero dei messaggi eventualmente contenuti nella coda. È possibile fare clic con il pulsante destro del mouse su ciascuna voce per aprire un menu di scelta rapida contenente una o più delle seguenti opzioni, a seconda della coda selezionata:

Visualizza coda. Consente di passare dal riquadro principale alla scheda Code posta e di visualizzare la coda selezionata. Verrà visualizzato un elenco di tutti i messaggi contenuti nella coda e sarà possibile fare clic con il pulsante destro del mouse su qualsiasi messaggio per aprire un menu di scelta rapida con numerose opzioni simili a quelle disponibili nell'applicazione di gestione delle code e delle statistiche, come Copia, Sposta, Modifica e così via.

Gestione delle code e delle statistiche. Consente di aprire la Pagina code di Gestione code e statistiche, con la visualizzazione della coda selezionata.

Elabora ora. Consente di "riaccodare" tutti i messaggi contenuti nella coda e di elaborarli normalmente per il recapito. Quando si tenta di elaborare la posta archiviata nella coda trattenuta o in quella dei messaggi scartati, è possibile che si ripetano gli stessi errori a seguito dei quali i messaggi erano stati inseriti in queste code e che i messaggi in questione vengano riposizionati nella stessa coda.

Sospendi/riprendi coda posta. Consente di sospendere temporaneamente l'elaborazione della coda selezionata o di riprenderla se attualmente sospesa.

Rilascia. Rilascia i messaggi della coda trattenuta. MDaemon tenterà di eseguirne la consegna ignorando eventuali errori. I messaggi non torneranno nella coda trattenuta anche se si verificano gli stessi errori che ne hanno causato originariamente l'inclusione.

Riaccoda. Questa funzione è disponibile per la coda trattenuta e svolge lo stesso ruolo descritto in precedenza per *Elabora ora*.

Abilita/disabilita coda. Consente di attivare o disattivare la coda trattenuta. In caso di disattivazione, i messaggi non verranno spostati nella coda trattenuta, a prescindere da eventuali errori.

Nella sezione *Server* è presente una voce associata a ogni server all'interno di MDaemon, che indica lo stato corrente del server, "Attivo" o "Inattivo". Sotto la voce relativa a ogni server, è presente una voce relativa al dominio (se applicabile) e la porta e l'indirizzo IP attualmente in uso per quel server o il dominio. Il menu di scelta rapida fornisce un comando che consente di attivare o disattivare ciascun server. Quando un server è inattivo, la relativa icona diventa rossa.

Monitoraggio e registrazione eventi

Il riquadro predefinito di destra dell'interfaccia principale comprende un gruppo di schede in cui vengono visualizzati lo stato e le azioni correnti dei vari server e delle varie risorse di MDaemon, costantemente aggiornate per riflettere le condizioni effettive del server. Ogni sessione attiva e ogni azione del server vengono registrate nella scheda appropriata al termine delle azioni. Se si è scelto di registrare tale attività, le

informazioni visualizzate in queste schede si riflettono nei file di registro conservati nella directory dei registri.

Nel riquadro principale della GUI di MDaemon sono incluse le schede seguenti:

Sistema. All'avvio del programma, in questa scheda viene visualizza la registrazione del processo di inizializzazione che segnala eventuali problemi relativi alla configurazione o allo stato di MDaemon. Sono inoltre mostrate altre attività, ad esempio l'avvio o l'arresto dei vari server di MDaemon.

Statistiche. In questa scheda viene visualizzato il report statistiche del server che corrisponde alle informazioni contenute nei diversi contatori relativi ai nodi principali della scheda Statistiche nel riquadro relativo alle statistiche e agli strumenti. Per modificare il tipo o la dimensione dei caratteri utilizzati per il report, modificare le seguenti impostazioni del file MDaemon.ini:

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

Ogni notte a mezzanotte, una copia del report verrà inviata via posta elettronica al Postmaster e a tutti gli indirizzi elencati nella schermata Destinatari 680 di Filtro contenuti. Si tratta dello stesso report generato con l'utilizzo del comando e-mail "Status" descritto in Comandi e-mail generali 915. Se non si desidera che il report venga inviato, disabilitare l'opzione "*Invia report statistiche al postmaster a mezzanotte*" della schermata Opzioni varie 511 di Preferenze.

Instradamento. Consente di visualizzare informazioni relative all'instradamento (To, From, Message-ID e così via) di ciascun messaggio analizzato da MDaemon.

Sicurezza. Facendo clic su questa scheda, verranno visualizzate le altre schede correlate alla sicurezza.

Filtro contenuti. In questa scheda vengono elencate le operazioni di Filtro contenuti 659. Quando un messaggio viene analizzato per la presenza di virus o risponde ai criteri di Filtro contenuti, le informazioni e le operazioni compiute in relazione al messaggio vengono registrate in questa scheda.

AntiVirus.In questa scheda vengono elencate le operazioni di AntiVirus 658. Quando un messaggio viene esaminato per rilevare l'eventuale presenza di virus, tutte le informazioni relative al messaggio e le operazioni eseguite al riguardo vengono registrate in questa scheda.

AntiSpam. Vengono visualizzate tutte le operazioni di Spam Filter 691 e le attività di prevenzione.

MDSpamD. Vengono visualizzate tutte le attività di MDaemon Spam Daemon 702.

SPF. Vengono visualizzate le attività di Sender Policy Framework 533.

DKIM. Vengono elencate tutte le attività relative a DomainKeys Identified Mail 536.

DMARC. Contiene tutte le attività DMARC 544.

VBR. In questa scheda vengono visualizzate le attività di Certificazione VBR 560.

MDPGP. In questa scheda vengono visualizzate le attività MDPGP 641.

Vaglio. In questa scheda vengono visualizzate le attività relative al tarpitting 614 e al vaglio dinamico 575.

Errori di autenticazione. Questa scheda (e il file di registro corrispondente) contengono una voce dettagliata per ogni tentativo di accesso SMTP, IMAP, e POP non riuscito. Le informazioni includono il protocollo utilizzato, l'ID sessione in modo che sia possibile cercare in altri registri, l'indirizzo IP dell'utente causa dell'errore, il valore di accesso raw che si è tentato di utilizzare (a volte si tratta di un alias) e l'account che corrisponde al tentativo di accesso (o "nessuno" se non esiste un account corrispondente). È possibile fare clic con il pulsante destro del mouse su una riga della scheda per aggiungere l'indirizzo IP causa dell'errore alle liste bloccati.

MTA-STS. visualizza tutte le attività correlate a SMTP MTA Strict Transport Security (MTA-STS).

Posta. Facendo clic su questa scheda, verranno visualizzate altre schede correlate al di sopra di essa.

SMTP (entrata). In questa scheda vengono visualizzate tutte le attività della sessione in entrata che utilizza il protocollo SMTP.

SMTP (uscita). In questa scheda vengono visualizzate tutte le attività della sessione in uscita che utilizza il protocollo SMPT.

IMAP. In questa scheda vengono registrate le sessioni di posta che utilizzano il protocollo IMAP.

POP3. In questa scheda vengono registrate le attività degli utenti che raccolgono la posta elettronica da MDaemon mediante il protocollo POP3.

MultiPOP. In questa scheda vengono visualizzate le attività di raccolta della posta MultiPOP di MDaemon.

DomainPOP. In questa scheda vengono visualizzate le attività DomainPOP di MDaemon.

LDAP. Vengono visualizzate le attività del server LDAP.

Minger. Mostra l'attività del server Minger 878.

RAW. In questa scheda vengono registrate le attività di posta RAW o generata dal sistema.

MDaemon Connector. Visualizza tutte le attività di MDaemon Connector 395.

Webmail

Webmail. Visualizza le attività correlate alla posta di MDaemon Webmail.

ActiveSync. In questa scheda viene visualizzata l'attività ActiveSync.

Code. Questa scheda consente di accedere a un altro insieme di schede sopra la scheda stessa, in cui ogni scheda corrisponde a una coda di messaggi, ad esempio locale, remota, trattenuta, quarantena, bayesiana e così via.

Plug-in. Vengono visualizzate tutte le attività correlate ai plug-in di MDaemon.

Active Directory. Vengono visualizzate tutte le attività correlate ad Active Directory.

Sessioni. Facendo clic su questa scheda, vengono visualizzate altre schede al di sopra di essa, in ciascuna delle quali viene visualizzata una voce per ogni connessione a MDaemon attiva. Che la connessione sia SMTP in ingresso o in uscita, POP in ingresso o in uscita, IMAP, Webmail o ActiveSync, in questa posizione vengono visualizzate informazioni su ciascuna sessione attiva. Facendo doppio clic su una sessione attiva, viene visualizzata la finestra Sessione 89, con la trascrizione dello stato di avanzamento della sessione SMTP.

Le informazioni visualizzate in queste schede non hanno alcun effetto sulla quantità di dati effettivamente memorizzata nei file registro. MDaemon è particolarmente flessibile per la quantità e il tipo di informazioni registrate in tali file. Per ulteriori informazioni sulle opzioni di registrazione, vedere la finestra di dialogo relativa alle opzioni di registrazione 169.

Menu di scelta rapida della finestra di monitoraggio degli eventi

Facendo clic con il pulsante destro del mouse in una qualsiasi delle schede del riquadro Monitoraggio eventi, si apre un menu di scelta rapida. Questo menu include diverse opzioni che consentono di selezionare, copiare, eliminare o salvare i contenuti di una determinata scheda. L'opzione *Stampa/Copia* del menu apre in Blocco note il testo selezionato consentendo così di stampare i dati o salvarli in un file. L'opzione *Elimina* consente di eliminare il testo selezionato. L'opzione *Ricerca* consente di aprire una finestra in cui è possibile specificare una parola o una frase da cercare nei file di registro. MDaemon eseguirà la ricerca della stringa di testo in tutti i file di registro. Successivamente, tutte le trascrizioni delle sessioni contenenti tale stringa saranno riunite in un singolo file e aperte in Blocco note per una verifica. Questa funzione si rivela utile, ad esempio, nel caso di una ricerca di una specifica intestazione Message-ID, fornendo la selezione, ricavata da tutti i file di registro, di tutte le trascrizioni delle sessioni che contengono tale Message-ID. In alcune schede sono disponibili anche opzioni per segnalare a MDaemon.com messaggi che sono stati erroneamente classificati come spam o infettati da virus oppure che avrebbero dovuto essere classificati come tali (vale a dire, falsi positivi o falsi negativi). I messaggi segnalati saranno analizzati e inviati a fornitori terzi per le necessarie azioni correttive.

Il layout dell'interfaccia grafica di MDaemon non si limita alle posizioni predefinite descritte in precedenza. Le posizioni possono essere modificate facendo clic su Finestre » Cambia riquadri nella barra dei menu.

Vista Registro misto

Nel menu Finestre della barra dei menu di MDaemon è presente l'opzione Vista Registro globale. Facendo clic su questa opzione, alla GUI verrà aggiunta una finestra in cui sono visualizzate congiuntamente le informazioni appartenenti a una o più schede del riquadro principale. Le opzioni della schermata Registro composito 171 della finestra di

dialogo Registrazione consentono di indicare le informazioni che verranno visualizzate in questa finestra.

Contatori delle prestazioni

MDaemon supporta i contatori di prestazioni di Windows, che consentono al software di monitorare lo stato di MDaemon in tempo reale. Si tratta di contatori relativi al numero di sessioni attive per i diversi protocolli, al numero di messaggi nelle code, agli stati attivo/inattivo dei server, ai tempi di attività di MDaemon e alle statistiche su sessioni e messaggi.

Per utilizzare i contatori delle prestazioni, avviare Monitor di sistema andando in Pannello di controllo | Strumenti di amministrazione | Prestazioni oppure eseguendo "perfmon". Si tratta di contatori a 32 bit, pertanto sulle macchine a 64 bit sarà necessario eseguire "mmc /32 perfmon.msc". Fare clic su Aggiungi contatori, selezionare l'oggetto delle prestazioni di MDaemon, quindi selezionare e aggiungere i contatori da visualizzare. Per visualizzare i contatori delle prestazioni da MDaemon in esecuzione su un'altra macchina, è necessario abilitare il servizio "Registro remoto" e accedere tramite i firewall.

Per ulteriori informazioni, vedere:

Finestra Sessione 89
Icona della barra delle applicazioni 87
Menu di scelta rapida 88
Registro composito 171

2. .1 Servizio AutoDiscovery

MDaemon supporta il servizio AutoDiscovery, che consente agli utenti di configurare i client di posta elettronica per connettersi ai propri account fornendo solo indirizzo e-mail e password, invece di dover conoscere altri dettagli di configurazione come i nomi e le porte dei server di posta. La maggior parte dei client supporta il servizio, anche se alcuni lo supportano solo limitatamente. Il servizio AutoDiscovery è attivato per impostazione predefinita, ma è possibile attivarlo o disattivarlo manualmente dall'interfaccia principale dell'applicazione di MDaemon. In **Server** nel riquadro Statistiche, fare clic con il pulsante destro del mouse su **Servizio AutoDiscovery**, quindi fare clic su **Attiva/Disattiva Servizio AutoDiscovery**.

I client in cui il servizio AutoDiscovery è pienamente supportato utilizzeranno il nome di dominio degli indirizzi e-mail degli utenti per eseguire una ricerca di record DNS (SRV) per il tipo di servizio _autodiscover._tcp e connettersi a tale server per ottenere ulteriori informazioni. Per supportare AutoDiscovery è quindi necessario creare i record DNS SRV per AutoDiscovery e i servizi che questo supporta. L'implementazione del servizio AutoDiscovery di MDaemon supporta: ActiveSync 425 (airsync), IMAP, POP, SMTP, DAV e XMPP.

```
_autodiscover._tcp  SRV 0 0 443 adsc.esempio.com.
_airsync._tcp       SRV 0 0 443 eas.esempio.com.
_imap._tcp          SRV 0 0 0   imap4.esempio.com.
_pop._tcp           SRV 0 0 0   pop3.esempio.com.
```

```
_smtp._tcp          SRV 0 0 0   msa.esempio.com.
_caldav._tcp        SRV 0 0 0   dav.esempio.com.
_carddav._tcp       SRV 0 0 0   dav.esempio.com.
_xmpp-client._tcp   SRV 0 0 0   chat.esempio.com.
```

Nota: alcuni client cercano sempre prima `autodiscover.{domain}.{tld}`. Quindi un record del servizio AutoDiscovery che punta a un server chiamato `autodiscover.{domain}.{tld}` può essere di aiuto in questi casi. Nell'esempio riportato di seguito, tuttavia, il server AutoDiscovery è `adsc.esempio.com`.

Esempio:

Nome del dominio: esempio.com

L'amministratore deve impostare un record di servizio _tcp per il tipo di servizio _autodiscover

```
_autodiscover._tcp SRV 0 0 443 adsc.esempio.com.
```

In questo caso, punta a `adsc.esempio.com`, che ha un record A che punta a `192.168.0.101`

Il client si connetterà quindi a tale server e chiederà informazioni sul punto di connessione per alcuni protocolli specifici: ActiveSync, IMAP, XMPP, SMTP, DAV, ecc...

Il servizio AutoDiscovery cercherà quindi i protocolli richiesti e restituirà i nomi dei server appropriati per tali protocolli. Ad esempio, per ActiveSync, restituirà il nome del server definito nel record del servizio _tcp _airsync, che in questo esempio è eas.{domain}.{tld}.

Se Outlook chiamasse AutoDiscovery, verrebbero restituiti i server IMAP e SMTP, rappresentati per i record di servizio _tcp di _imap e _msa, con il risultato che i server verrebbero restituiti come imap4.esempio.com e msa.esempio.com.

Ecco un esempio di impostazione corretta dei servizi AutoDiscovery. In questo si presuppone che si desideri utilizzare nomi univoci per ogni protocollo, ma l'esempio è facilmente adattabile all'uso di un nome comune, come mail.esempio.com.

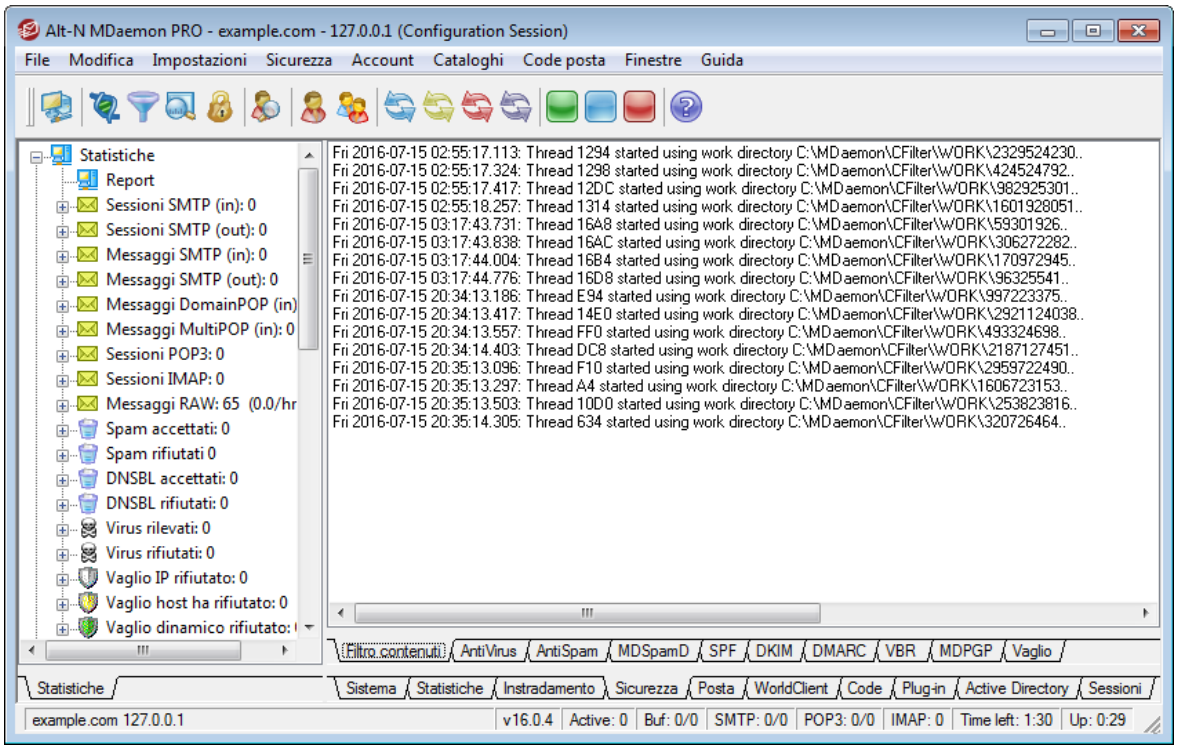
```
;
;  File di database esempio.com.dns per la zona esempio.com.
;

@ IN  SOA dns.mydnsprovider.org. hostmaster.mydnsprovider.org. (
        4            ; numero di serie
        900          ; aggiornamento
        600          ; retry
        86400        ; scadenza
        3600       ) ; TTL predefinita

;
;  Record NS zona
;

@       NS dns.mydnsprovider.org
```

```
;
;  Record zona
;

@             A 192.168.0.100
adsc                A 192.168.0.101
www                 A 192.168.0.102
imap4               A 192.168.0.103
pop3                A 192.168.0.104
msa                 A 192.168.0.105
eas                 A 192.168.0.106
api                 A 192.168.0.107
autodiscover        A 192.168.0.108
dav                 A 192.168.0.109
chat                A 192.168.0.110
inbound       A 192.168.0.111

              MX 10 inbound.esempio.com.
;
;  Record servizio
;

_autodiscover._tcp  SRV 0 0 443 adsc.esempio.com.
_airsync._tcp       SRV 0 0 443 eas.esempio.com.
_imap._tcp          SRV 0 0 0   imap4.esempio.com.
_pop._tcp           SRV 0 0 0   pop3.esempio.com.
_smtp._tcp          SRV 0 0 0   msa.esempio.com.
_caldav._tcp        SRV 0 0 0   dav.esempio.com.
_carddav._tcp       SRV 0 0 0   dav.esempio.com.
_xmpp-client._tcp   SRV 0 0 0   chat.esempio.com.
```

Vedere:

Per ulteriori informazioni generali su AutoDiscover, consultare il documento Microsoft: AutoDiscover per Exchange.

2.2 Monitoraggio e registrazione eventi



La GUI (interfaccia grafica utente) principale di MDaemon offre importanti informazioni su risorse, statistiche, sessioni attive e posta accodata in attesa di elaborazione. Sono inoltre presenti le opzioni per attivare/disattivare in modo semplice i vari server di MDaemon. I riquadri a schede della GUI forniscono informazioni aggiornate sulle prestazioni del server e sulle connessioni in entrata e in uscita.

Statistiche

Statistiche è il riquadro di sinistra predefinito dell'interfaccia principale di MDaemon. Comprende quattro sezioni: Statistiche, Account, Code e Server.

La sezione *Statistiche* contiene alcune statistiche relative al numero di messaggi inviati e ricevuti da MDaemon, oltre che alle sessioni POP e IMAP, ai messaggi spam accettati e rifiutati, ai virus e altro ancora. Le statistiche vengono conteggiate dall'avvio di MDaemon ed è possibile utilizzare un menu di scelta rapida per cancellare i contatori.

Quando si abilita l'opzione "Azzera contatori nodi principali", vengono resettati tutti i contatori e non solo quelli sui quali si è fatto clic con il pulsante destro del mouse. In Impostazioni » Preferenze » GUI è inoltre disponibile l'opzione "*Mantieni contatori posta nodo principale tra riavvii*." Se questa opzione non è abilitata, quando il server viene avviato i contatori vengono azzerati.

La sezione *Account* contiene voci per MDaemon, MDaemon Connector e ActiveSync. Ciascuna voce elenca il numero di account utilizzati e il numero di account rimanenti, in base alla licenza del prodotto.

La sezione *Code* include una voce per ogni coda di messaggi e il numero dei messaggi eventualmente contenuti nella coda. È possibile fare clic con il pulsante destro del mouse su ciascuna voce per aprire un menu di scelta rapida contenente una o più delle seguenti opzioni, a seconda della coda selezionata:

Visualizza coda. Consente di passare dal riquadro principale alla scheda Code posta e di visualizzare la coda selezionata. Verrà visualizzato un elenco di tutti i messaggi contenuti nella coda e sarà possibile fare clic con il pulsante destro del mouse su qualsiasi messaggio per aprire un menu di scelta rapida con numerose opzioni simili a quelle disponibili nell'applicazione di gestione delle code e delle statistiche, come Copia, Sposta, Modifica e così via.

Gestione delle code e delle statistiche. Consente di aprire la Pagina code di Gestione code e statistiche, con la visualizzazione della coda selezionata.

Elabora ora. Consente di "riaccodare" tutti i messaggi contenuti nella coda e di elaborarli normalmente per il recapito. Quando si tenta di elaborare la posta archiviata nella coda trattenuta o in quella dei messaggi scartati, è possibile che si ripetano gli stessi errori a seguito dei quali i messaggi erano stati inseriti in queste code e che i messaggi in questione vengano riposizionati nella stessa coda.

Sospendi/riprendi coda posta. Consente di sospendere temporaneamente l'elaborazione della coda selezionata o di riprenderla se attualmente sospesa.

Rilascia. Rilascia i messaggi della coda trattenuta. MDaemon tenterà di eseguirne la consegna ignorando eventuali errori. I messaggi non torneranno nella coda trattenuta anche se si verificano gli stessi errori che ne hanno causato originariamente l'inclusione.

Riaccoda. Questa funzione è disponibile per la coda trattenuta e svolge lo stesso ruolo descritto in precedenza per *Elabora ora*.

Abilita/disabilita coda. Consente di attivare o disattivare la coda trattenuta. In caso di disattivazione, i messaggi non verranno spostati nella coda trattenuta, a prescindere da eventuali errori.

Nella sezione *Server* è presente una voce associata a ogni server all'interno di MDaemon, che indica lo stato corrente del server, "Attivo" o "Inattivo". Sotto la voce relativa a ogni server, è presente una voce relativa al dominio (se applicabile) e la porta e l'indirizzo IP attualmente in uso per quel server o il dominio. Il menu di scelta rapida fornisce un comando che consente di attivare o disattivare ciascun server. Quando un server è inattivo, la relativa icona diventa rossa.

Monitoraggio e registrazione eventi

Il riquadro predefinito di destra dell'interfaccia principale comprende un gruppo di schede in cui vengono visualizzati lo stato e le azioni correnti dei vari server e delle varie risorse di MDaemon, costantemente aggiornate per riflettere le condizioni effettive del server. Ogni sessione attiva e ogni azione del server vengono registrate nella scheda appropriata al termine delle azioni. Se si è scelto di registrare tale attività, le

informazioni visualizzate in queste schede si riflettono nei file di registro conservati nella directory dei registri.

Nel riquadro principale della GUI di MDaemon sono incluse le schede seguenti:

Sistema. All'avvio del programma, in questa scheda viene visualizza la registrazione del processo di inizializzazione che segnala eventuali problemi relativi alla configurazione o allo stato di MDaemon. Sono inoltre mostrate altre attività, ad esempio l'avvio o l'arresto dei vari server di MDaemon.

Statistiche. In questa scheda viene visualizzato il report statistiche del server che corrisponde alle informazioni contenute nei diversi contatori relativi ai nodi principali della scheda Statistiche nel riquadro relativo alle statistiche e agli strumenti. Per modificare il tipo o la dimensione dei caratteri utilizzati per il report, modificare le seguenti impostazioni del file MDaemon.ini:

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

Ogni notte a mezzanotte, una copia del report verrà inviata via posta elettronica al Postmaster e a tutti gli indirizzi elencati nella schermata Destinatari 680 di Filtro contenuti. Si tratta dello stesso report generato con l'utilizzo del comando e-mail "Status" descritto in Comandi e-mail generali 915. Se non si desidera che il report venga inviato, disabilitare l'opzione "*Invia report statistiche al postmaster a mezzanotte*" della schermata Opzioni varie 511 di Preferenze.

Instradamento. Consente di visualizzare informazioni relative all'instradamento (To, From, Message-ID e così via) di ciascun messaggio analizzato da MDaemon.

Sicurezza. Facendo clic su questa scheda, verranno visualizzate le altre schede correlate alla sicurezza.

Filtro contenuti. In questa scheda vengono elencate le operazioni di Filtro contenuti 659. Quando un messaggio viene analizzato per la presenza di virus o risponde ai criteri di Filtro contenuti, le informazioni e le operazioni compiute in relazione al messaggio vengono registrate in questa scheda.

AntiVirus.In questa scheda vengono elencate le operazioni di AntiVirus 658. Quando un messaggio viene esaminato per rilevare l'eventuale presenza di virus, tutte le informazioni relative al messaggio e le operazioni eseguite al riguardo vengono registrate in questa scheda.

AntiSpam. Vengono visualizzate tutte le operazioni di Spam Filter 691 e le attività di prevenzione.

MDSpamD. Vengono visualizzate tutte le attività di MDaemon Spam Daemon 702.

SPF. Vengono visualizzate le attività di Sender Policy Framework 533.

DKIM. Vengono elencate tutte le attività relative a DomainKeys Identified Mail 536.

DMARC. Contiene tutte le attività DMARC 544.

VBR. In questa scheda vengono visualizzate le attività di Certificazione VBR 560.

MDPGP. In questa scheda vengono visualizzate le attività MDPGP 641.

Vaglio. In questa scheda vengono visualizzate le attività relative al tarpitting 614 e al vaglio dinamico 575.

Errori di autenticazione. Questa scheda (e il file di registro corrispondente) contengono una voce dettagliata per ogni tentativo di accesso SMTP, IMAP, e POP non riuscito. Le informazioni includono il protocollo utilizzato, l'ID sessione in modo che sia possibile cercare in altri registri, l'indirizzo IP dell'utente causa dell'errore, il valore di accesso raw che si è tentato di utilizzare (a volte si tratta di un alias) e l'account che corrisponde al tentativo di accesso (o "nessuno" se non esiste un account corrispondente). È possibile fare clic con il pulsante destro del mouse su una riga della scheda per aggiungere l'indirizzo IP causa dell'errore alle liste bloccati.

MTA-STS. visualizza tutte le attività correlate a SMTP MTA Strict Transport Security (MTA-STS).

Posta. Facendo clic su questa scheda, verranno visualizzate altre schede correlate al di sopra di essa.

SMTP (entrata). In questa scheda vengono visualizzate tutte le attività della sessione in entrata che utilizza il protocollo SMTP.

SMTP (uscita). In questa scheda vengono visualizzate tutte le attività della sessione in uscita che utilizza il protocollo SMPT.

IMAP. In questa scheda vengono registrate le sessioni di posta che utilizzano il protocollo IMAP.

POP3. In questa scheda vengono registrate le attività degli utenti che raccolgono la posta elettronica da MDaemon mediante il protocollo POP3.

MultiPOP. In questa scheda vengono visualizzate le attività di raccolta della posta MultiPOP di MDaemon.

DomainPOP. In questa scheda vengono visualizzate le attività DomainPOP di MDaemon.

LDAP. Vengono visualizzate le attività del server LDAP.

Minger. Mostra l'attività del server Minger 878.

RAW. In questa scheda vengono registrate le attività di posta RAW o generata dal sistema.

MDaemon Connector. Visualizza tutte le attività di MDaemon Connector 395.

Webmail

Webmail. Visualizza le attività correlate alla posta di MDaemon Webmail.

ActiveSync. In questa scheda viene visualizzata l'attività ActiveSync.

Code. Questa scheda consente di accedere a un altro insieme di schede sopra la scheda stessa, in cui ogni scheda corrisponde a una coda di messaggi, ad esempio locale, remota, trattenuta, quarantena, bayesiana e così via.

Plug-in. Vengono visualizzate tutte le attività correlate ai plug-in di MDaemon.

Active Directory. Vengono visualizzate tutte le attività correlate ad Active Directory.

Sessioni. Facendo clic su questa scheda, vengono visualizzate altre schede al di sopra di essa, in ciascuna delle quali viene visualizzata una voce per ogni connessione a MDaemon attiva. Che la connessione sia SMTP in ingresso o in uscita, POP in ingresso o in uscita, IMAP, Webmail o ActiveSync, in questa posizione vengono visualizzate informazioni su ciascuna sessione attiva. Facendo doppio clic su una sessione attiva, viene visualizzata la finestra Sessione 89, con la trascrizione dello stato di avanzamento della sessione SMTP.

Le informazioni visualizzate in queste schede non hanno alcun effetto sulla quantità di dati effettivamente memorizzata nei file registro. MDaemon è particolarmente flessibile per la quantità e il tipo di informazioni registrate in tali file. Per ulteriori informazioni sulle opzioni di registrazione, vedere la finestra di dialogo relativa alle opzioni di registrazione 169.

Menu di scelta rapida della finestra di monitoraggio degli eventi

Facendo clic con il pulsante destro del mouse in una qualsiasi delle schede del riquadro Monitoraggio eventi, si apre un menu di scelta rapida. Questo menu include diverse opzioni che consentono di selezionare, copiare, eliminare o salvare i contenuti di una determinata scheda. L'opzione *Stampa/Copia* del menu apre in Blocco note il testo selezionato consentendo così di stampare i dati o salvarli in un file. L'opzione *Elimina* consente di eliminare il testo selezionato. L'opzione *Ricerca* consente di aprire una finestra in cui è possibile specificare una parola o una frase da cercare nei file di registro. MDaemon eseguirà la ricerca della stringa di testo in tutti i file di registro. Successivamente, tutte le trascrizioni delle sessioni contenenti tale stringa saranno riunite in un singolo file e aperte in Blocco note per una verifica. Questa funzione si rivela utile, ad esempio, nel caso di una ricerca di una specifica intestazione Message-ID, fornendo la selezione, ricavata da tutti i file di registro, di tutte le trascrizioni delle sessioni che contengono tale Message-ID. In alcune schede sono disponibili anche opzioni per segnalare a MDaemon.com messaggi che sono stati erroneamente classificati come spam o infettati da virus oppure che avrebbero dovuto essere classificati come tali (vale a dire, falsi positivi o falsi negativi). I messaggi segnalati saranno analizzati e inviati a fornitori terzi per le necessarie azioni correttive.

Il layout dell'interfaccia grafica di MDaemon non si limita alle posizioni predefinite descritte in precedenza. Le posizioni possono essere modificate facendo clic su Finestre » Cambia riquadri nella barra dei menu.

Vista Registro misto

Nel menu Finestre della barra dei menu di MDaemon è presente l'opzione Vista Registro globale. Facendo clic su questa opzione, alla GUI verrà aggiunta una finestra in cui sono visualizzate congiuntamente le informazioni appartenenti a una o più schede del riquadro principale. Le opzioni della schermata Registro composito 171 della finestra di

dialogo Registrazione consentono di indicare le informazioni che verranno visualizzate in questa finestra.

Contatori delle prestazioni

MDaemon supporta i contatori di prestazioni di Windows, che consentono al software di monitorare lo stato di MDaemon in tempo reale. Si tratta di contatori relativi al numero di sessioni attive per i diversi protocolli, al numero di messaggi nelle code, agli stati attivo/inattivo dei server, ai tempi di attività di MDaemon e alle statistiche su sessioni e messaggi.

Per utilizzare i contatori delle prestazioni, avviare Monitor di sistema andando in Pannello di controllo | Strumenti di amministrazione | Prestazioni oppure eseguendo "perfmon". Si tratta di contatori a 32 bit, pertanto sulle macchine a 64 bit sarà necessario eseguire "mmc /32 perfmon.msc". Fare clic su Aggiungi contatori, selezionare l'oggetto delle prestazioni di MDaemon, quindi selezionare e aggiungere i contatori da visualizzare. Per visualizzare i contatori delle prestazioni da MDaemon in esecuzione su un'altra macchina, è necessario abilitare il servizio "Registro remoto" e accedere tramite i firewall.

Per ulteriori informazioni, vedere:

Finestra Sessione 89
Icona della barra delle applicazioni 87
Menu di scelta rapida 88
Registro composito 171

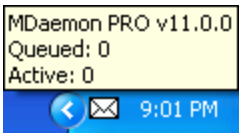
2.4 Icona della barra delle applicazioni

Quando il server MDaemon è in esecuzione, nella barra delle applicazioni è visibile un'icona. Si tratta di un'icona dinamica che, oltre a indicare se il sistema è in esecuzione, cambia colore a seconda dello stato corrente del server. Di seguito è riportato un elenco dei vari aspetti possibili dell'icona.

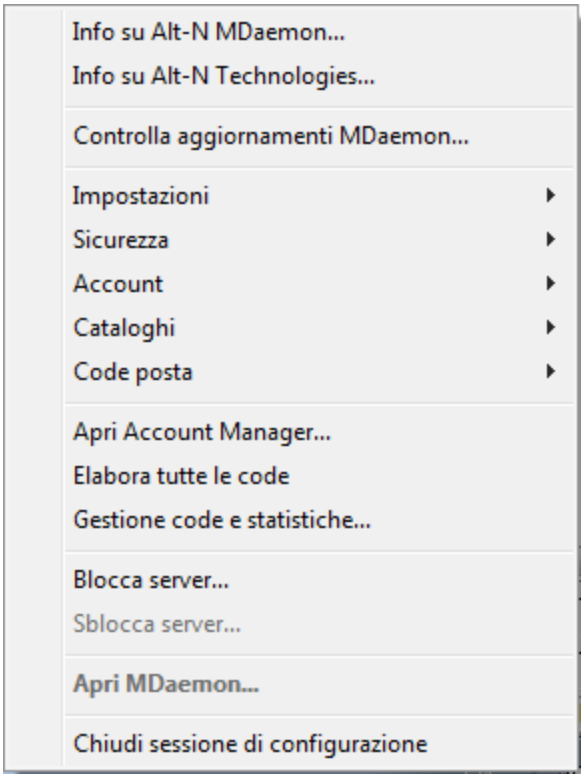
	Funzionamento regolare. Assenza di posta nelle code locali e remote.
	Funzionamento regolare. Presenza di posta nelle code locali o remote.
	Spazio su disco inferiore alla soglia (vedere Impostazioni » Preferenze » Disco 503).
	Rete inattiva, connessione non riuscita o disco pieno.

Icona lampeggiante	È disponibile una versione di MDaemon più recente.

La descrizione comandi dell'icona fornisce ulteriori informazioni sul server. Posizionare il puntatore sopra l'icona per visualizzare la descrizione comandi che consente di visualizzare il numero di messaggi attualmente in coda e il numero di sessioni attive.



Menu di scelta rapida



Per aprire il menu di scelta rapida (o menu contestuale), fare clic con il pulsante destro del mouse sull'icona MDaemon nella barra delle applicazioni. Questo menu permette di accedere rapidamente a tutti i menu e a tutte le funzionalità di MDaemon, senza dover aprire l'interfaccia utente principale.

Fare clic sulle opzioni "Info su MDaemon..." nella sezione superiore del menu di scelta rapida per visualizzare ulteriori informazioni su MDaemon o MDaemon Technologies.

Nella sezione successiva, facendo clic su "Controlla aggiornamenti MDaemon" è possibile verificare la disponibilità di versioni più recenti di MDaemon.

La terza sezione consente di accedere ai seguenti menu di MDaemon: Impostazione, Sicurezza, Account e Code. Ognuno di questi menu è identico all'omonimo menu presente nella barra dei menu dell'interfaccia principale.

Nella quarta sezione sono disponibili le opzioni che

consentono di accedere alle finestre Account Manager e Gestione code e statistiche, nonché un'opzione che permette di elaborare tutte le code di posta di MDaemon.

Nella sezione successiva sono disponibili i comandi che consentono di bloccare e sbloccare l'interfaccia di MDaemon (vedere il successivo argomento "Blocco/sblocco dell'interfaccia principale di MDaemon"), seguiti dal comando Apri MDaemon, utilizzato per aprire o ripristinare l'interfaccia di MDaemon se quest'ultima è ridotta a icona nella barra delle applicazioni.

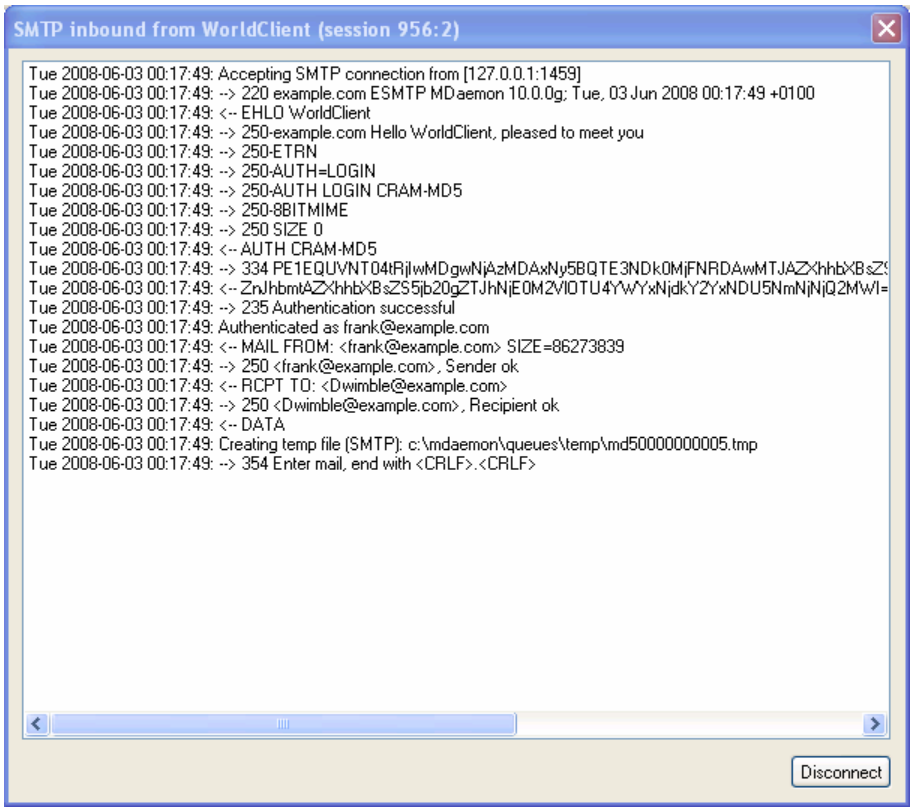
L'ultima opzione è "Chiudi sessione di configurazione" che chiude l'interfaccia di MDaemon. Chiudere la sessione di configurazione non arresta il servizio di MDaemon.

Blocco/sblocco dell'interfaccia principale di MDaemon

Per bloccare l'interfaccia utente ridurre a icona MDaemon, fare clic sulla voce di menu "Blocca server" e inserire una password nella finestra di dialogo visualizzata. Dopo aver confermato la password inserendola una seconda volta, l'interfaccia utente di MDaemon sarà bloccata. Non è possibile aprirla o visualizzarla, ma MDaemon continua a funzionare normalmente. È comunque possibile utilizzare l'opzione "Elabora tutte le code" per elaborare manualmente le code di posta. Per sbloccare MDaemon, fare doppio clic sull'icona che si trova sulla barra delle applicazioni e aprire la finestra di dialogo "Sblocca MDaemon". In alternativa, fare clic sull'icona con il pulsante destro del mouse e scegliere "Sblocca server", quindi inserire la password creata per il blocco dell'interfaccia.

2.5 Finestra Sessione

Quando si fa doppio clic su una sessione attiva di una delle schede Sessioni 75 della GUI principale, viene aperta la relativa finestra. In questa finestra viene visualizzata la trascrizione SMTP della sessione in corso. Per interrompere e disconnettere la sessione in corso, fare clic su Disconnetti nella finestra.



2.6 Flusso di lavoro SMTP di MDaemon

Quando viene stabilita una connessione SMTP, MDaemon effettua una complessa serie di passi elaborativi per determinare se accettare il messaggio e come operare in caso affermativo. Nello schema seguente viene fornita una rappresentazione grafica di questo flusso di lavoro per i messaggi SMTP in ingresso.

l'effettiva esecuzione di questi passi dipende dalla specifica configurazione in uso. Se nella configurazione una particolare funzione è disabilitata, alcuni passaggi potrebbero essere ignorati.

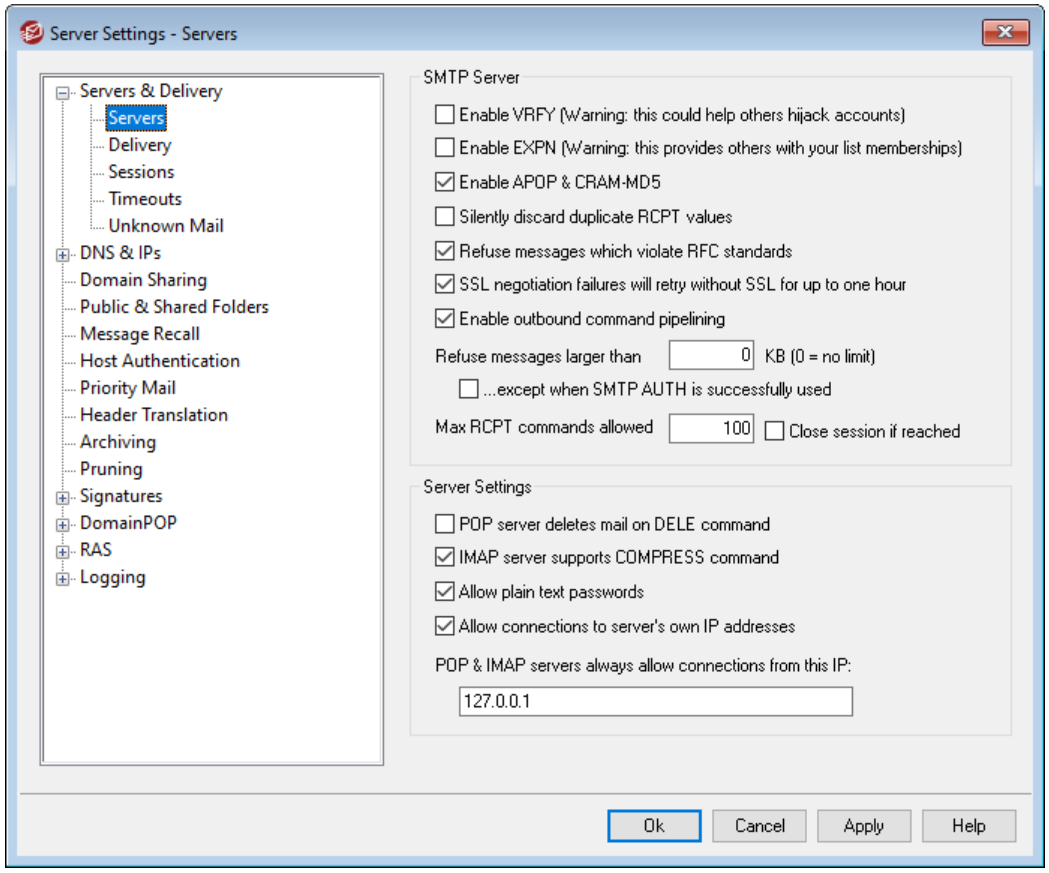
Sezione

3 Menu Impostazioni

3.1 Impostazioni server

3.1.1 Server e recapito

3.1.1.1 Server



Server SMTP

Abilita VRFY
Selezionare questa opzione per rispondere ai comandi VRFY di SMTP. Questa opzione viene utilizzata talvolta dai server che utilizzano una funzione di inoltro della chiamata o di richiamata SMTP per confermare la validità degli indirizzi e-mail del server. È disabilitata per impostazione predefinita.

Abilita EXPN
Selezionare questa casella di controllo se si desidera che MDaemon accetti i comandi EXPN.

Abilita APOP e CRAM-MD5
Per impostazione predefinita i server di MDaemon (POP, IMAP e così via) non accettano i metodi di autenticazione APOP e CRAM-MD5. Questo tipo di

autenticazione richiede la memorizzazione delle password mediante crittografia reversibile, che non è consigliata a scopo di sicurezza, per proteggere le password dalla decrittografia da parte di MDaemon, dell'amministratore o di un possibile hacker. Di conseguenza, questa opzione non è compatibile l'opzione Password 870 "*Memorizza password casella postale mediante crittografia non reversibile*" e neanche con l'autenticazione di Active Directory. Se, tuttavia, non si utilizza SSL/TLS, APOP e CRAM-MD5 possono offrire un livello di sicurezza aggiuntivo consentendo l'autenticazione degli utenti senza l'invio di password non crittografate.

Elimina valori RCPT duplicati senza avvisare
Abilitare questa opzione se si desidera che il server SMTP ignori i destinatari duplicati nella stessa sessione SMTP. MDaemon accetterà e quindi eliminerà i destinatari duplicati. L'opzione è disabilitata per impostazione predefinita.

Rifiuta messaggi che violano gli standard RFC
Questa opzione consente di respingere, durante l'elaborazione SMTP, i messaggi non conformi agli standard Internet RFC. Per superare il test di conformità, è necessario che il messaggio:

1. abbia dimensioni superiori a 32 byte (dimensione minima per includere tutte le parti necessarie);
2. disponga dell'intestazione FROM o SENDER;
3. non abbia più intestazioni FROM;
4. non abbia più intestazioni SUBJECT, anche se tale intestazione non è obbligatoria.

I messaggi che utilizzano sessioni autenticate o che provengono da domini accreditati o da indirizzi IP sono esenti da tali requisiti.

Dopo errori di negoziazione SSL continua a riprovare senza SSL per un massimo di un'ora
Questa opzione consente di riprovare temporaneamente gli IP dell'host senza SSL quando si verifica un errore SSL durante una sessione SMTP in uscita. La funzione si ripristina ogni ora.

Consenti il pipelining dei comandi in uscita
Per impostazione predefinita, MDaemon supporta l'estensione del servizio SMTP per il pipelining dei comandi. (RFC 2920), vale a dire che invierà i comandi MAIL, RCPT e DATA in batch invece che singolarmente, migliorando così le prestazioni sui collegamenti di rete a latenza elevata. Il pipelining SMTP viene sempre utilizzato per le connessioni in entrata ed è attivato per impostazione predefinita per le connessioni in uscita. Deselezionare questa casella di controllo se non si desidera utilizzare la funzionalità per le connessioni in uscita.

Rifiuta i messaggi superiori a [xx] KB (0=senza lim.)
Questo campo consente di impedire che MDaemon accetti o elabori la posta che supera una determinata dimensione. Quando si attiva questa opzione, MDaemon tenterà di utilizzare il comando ESMTP SIZE specificato in RFC-1870. Se l'agente di invio supporta questa estensione SMTP, MDaemon determinerà le dimensioni dei messaggi prima dell'effettiva consegna e rifiuterà immediatamente i messaggi non

conformi. Se il programma di invio non supporta questa estensione SMTP, MDaemon deve avviare l'accettazione dei messaggi, monitorarne regolarmente le dimensioni durante il trasferimento e rifiutarli solo al termine della transazione. Specificare "0" in questa opzione se non si desidera impostare alcun limite di dimensione. Se si desidera escludere i controlli SIZE per le sessioni autenticate, utilizzare l'opzione "*...tranne quando viene utilizzato correttamente SMTP AUTH*" riportata di seguito.

... tranne quando viene utilizzato correttamente SMTP AUTH
Questa casella consente di escludere messaggi dalla limitazione di dimensione quando la sessione SMTP è autenticata.

Max comandi RCPT consentiti
Questa opzione consente di limitare il numero di comandi RCPT che possono essere inviati per messaggio. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Chiudi la sessione se si raggiunge
Questa casella consente di chiudere la sessione appena raggiunto il numero massimo di comandi RCPT consentito.

Impostazioni server

Il server POP elimina la posta al comando DELE
Selezionare questa opzione per consentire a MDaemon di eliminare immediatamente i messaggi quando questi vengono ritirati e si riceve il comando DELE, anche se la sessione POP non viene chiusa correttamente.

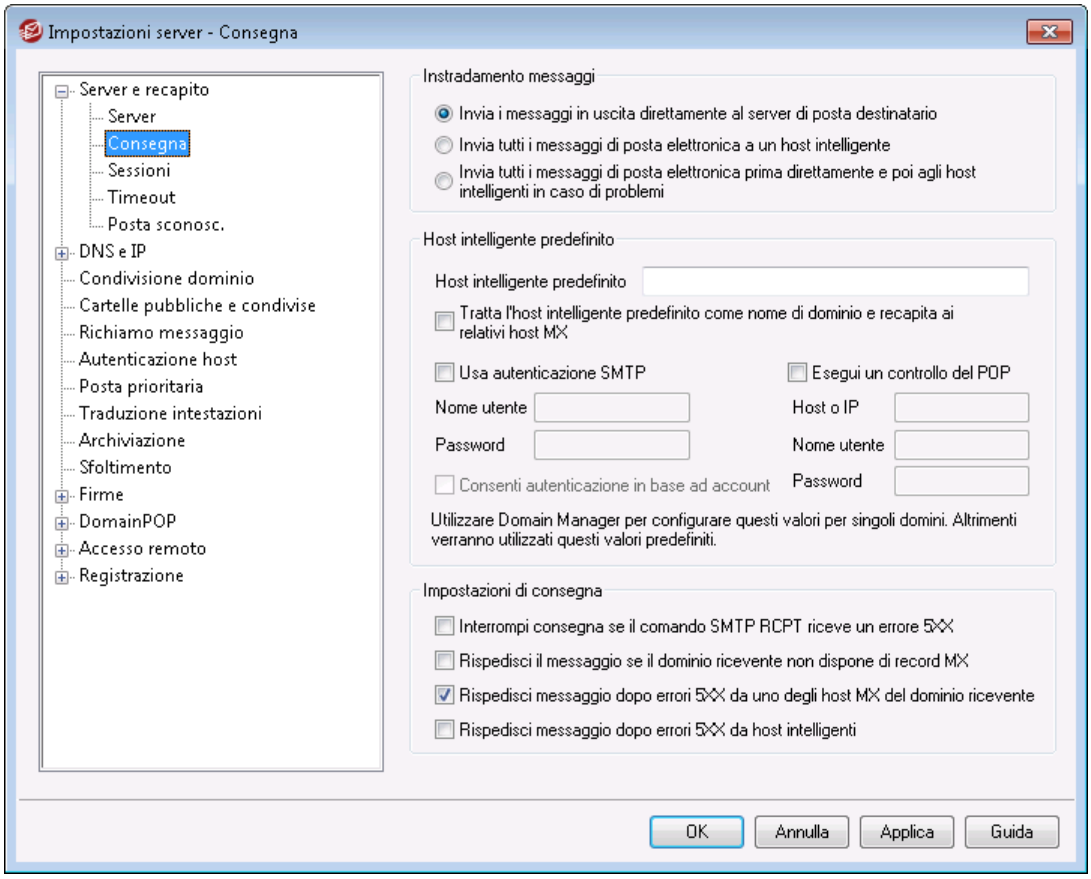
Il server IMAP supporta il comando COMPRESS
Selezionare questa casella di controllo se si desidera supportare l'estensione COMPRESS IMAP (RFC 4978), che consente di comprimere tutti i dati inviati al e dal client. COMPRESS comporta l'aumento dell'utilizzo della CPU e della memoria per la sessione IMAP.

Consenti password in chiaro
Con questa opzione si consente a MDaemon di accettare password in chiaro inviate ai server SMTP, IMAP o POP3. Se viene disabilitata, i comandi `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN` e `SMTP AUTH LOGIN` daranno come risultato un errore a meno che la connessione non utilizzi SSL.

Consenti connessioni agli indirizzi IP del server
Abilitando questa opzione, MDaemon è in grado di connettersi con sé stesso.

Server POP e IMAP consentono sempre le connessioni da questo IP
I server POP e IMAP accettano sempre le connessioni dall'indirizzo IP immesso in questo campo, indipendentemente dalle impostazioni relative a Vaglio IP e Scudo IP.

3.1.1.2 Consegna



Instradamento messaggi

Invia tutti i messaggi di posta elettronica in uscita direttamente al server di posta del destinatario
Se si seleziona questa opzione, MDaemon tenterà di inviare direttamente la posta, anziché inoltrarla a un altro host. MDaemon colloca tutti i messaggi non recapitati nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi della finestra di dialogo Code posta.

Invia tutti i messaggi e-mail in uscita a un host intelligente
Questa opzione consente di eseguire lo spool delle e-mail in uscita, indipendentemente dal dominio di destinazione, verso un host o un server per la consegna instradata. Se si seleziona questa opzione, la posta in uscita verrà inviata all'*host intelligente predefinito* specificato di seguito. Questa funzione è utile soprattutto quando il traffico è più intenso e la consegna diretta della posta può determinare un carico eccessivo per le risorse del server. Se non è possibile recapitare un messaggio al server specificato, MDaemon lo colloca nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi della finestra di dialogo Code posta.

Invia tutti i messaggi di posta elettronica prima direttamente e poi agli host intelligenti in caso di problemi
Questa opzione è una combinazione delle due opzioni di inoltro precedenti. Innanzitutto MDaemon tenterà di consegnare i messaggi di posta elettronica in uscita direttamente al server, tuttavia se la consegna non riesce li invierà all'*Host intelligente predefinito specificato di seguito*. Con posta non recapitata si indicano i messaggi indirizzati agli host che potrebbero essere stati inoltrati a un indirizzo IP non reale (ad esempio, un gateway non registrato su una rete remota) oppure i messaggi indirizzati a un host che è stato identificato correttamente ma a cui non è stato possibile collegarsi direttamente o che rifiuta la connessione diretta. Se questa opzione è selezionata, anziché restituire la posta ai rispettivi mittenti, MDaemon inoltra il messaggio a un MTA (Message Transfer Agent, Agente di trasferimento di messaggi) più potente. In alcuni casi, il sistema di posta adottato dall'ISP fa ricorso a metodi di ridistribuzione della posta non accessibili direttamente dal server locale. Se non è possibile recapitare un messaggio all'host intelligente specificato, MDaemon lo colloca nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi 888 della finestra di dialogo Code posta. Per ogni successivo tentativo di consegna, MDaemon tenterà innanzitutto di recapitare il messaggio direttamente al destinatario e, quindi, all'host intelligente specificato.

Host intelligente predefinito

Host intelligente predefinito
Inserire il nome o l'indirizzo IP dell'ISP o dell'host di posta. il valore corrisponde generalmente al server SMTP dell'ISP.

Non inserire in questa casella di testo il dominio predefinito o gli indirizzi IP di MDaemon. A questa voce deve corrispondere un ISP o un altro server di posta in grado di inoltrare la posta.

Gestire l'host intelligente predefinito come nome di dominio ed eseguire la consegna ai relativi host MX
Attivare questa opzione se si desidera che MDaemon gestisca l'*Host intelligente predefinito* come nome di dominio interrogando il relativo record DNS ed eseguendo la consegna ai relativi host MX.

Usa autenticazione SMTP

Fare clic su questa casella di controllo e inserire le credenziali di accesso riportate di seguito se l'*host intelligente predefinito* richiede autenticazione. Le credenziali verranno utilizzate per tutti i messaggi SMTP in uscita inviati all'host intelligente. Qualora si scelga di utilizzare l'opzione *Consenti autenticazione in base ad account*, MDaemon eseguirà l'autenticazione all'host per ogni messaggio utilizzando le credenziali *Accesso host intelligente* dell'account mittente, indicate nella schermata Servizi di posta 733 di Account Editor.

Nome utente
Immettere il nome utente o di login.

Password
Utilizzare questa opzione per specificare la password di accesso all'host intelligente.

Esegui prima verifica POP
Se l'host intelligente richiede una verifica POP3 prima di accettare i messaggi inviati dall'utente, selezionare questa casella di controllo e inserire le credenziali necessarie nelle caselle di testo sottostanti.

Host o IP
Immettere il nome dell'host o l'indirizzo IP a cui connettersi.

Nome utente
Indica l'ID utente o il nome dell'account POP.

Password
Indica la password dell'account POP.

Consenti autenticazione in base ad account
Selezionare questa casella di controllo se si desidera utilizzare l'autenticazione in base all'account per i messaggi SMTP in uscita inviati all'*host intelligente predefinito* specificato in precedenza. Anziché utilizzare le credenziali *Nome utente* e *Password* indicate, verranno utilizzate le credenziali *Accesso host intelligente* di ciascun account, specificate nella schermata Servizi di posta 733. Se per un dato account non sono state specificate credenziali dell'host intelligente, verranno utilizzate le suddette credenziali.

Per configurare l'*autenticazione in base ad account* in moda che venga utilizzata la *Password e-mail* di un account anziché la *Password host intelligente*, modificare la seguente chiave del file `MDaemon.ini`:

```
[AUTH]
ISPAUTHUsePasswords=Yes (il valore predefinito è No)
```

Se si abilita l'opzione `ISPAUTHUsePasswords=Yes`, con il passare del tempo tutte la password e-mail locali verranno comunicate all'host intelligente e ciò potrebbe rappresentare un rischio per la sicurezza perché queste informazioni riservate vengono comunicate a un altro server. Non è consigliabile utilizzare questa opzione a meno che l'host intelligente utilizzato non sia di assoluta fiducia e solo se questa operazione è assolutamente necessaria. Tenere presente, inoltre, che se si utilizza questa opzione e si consente agli utenti di modificare la propria *password e-mail* con Webmail o in altro modo, la modifica della *password e-mail* comporterà anche la modifica della *password dell'host intelligente*. Di conseguenza, l'autenticazione di un account potrebbe non riuscire qualora la *Password e-mail* venga cambiata localmente, ma la corrispondente *Password host intelligente* non venga modificata nell'host intelligente stesso.

Interrompi consegna se il comando SMTP RCPT riceve un errore 5XX
Se si abilita questa opzione, MDaemon interromperà i tentativi di consegna di un messaggio quando, in risposta a un comando RCPT SMTP, riceverà un errore irreversibile 5xx. L'opzione è disabilitata per impostazione predefinita.

Rispedisci messaggio se dominio ricevente non ha record MX
In genere, quando MDaemon verifica i record DNS del dominio ricevente, cerca i record MX e, in mancanza di questi, un record A. Se non ne trova alcun tipo di record, rispedisce il messaggio al mittente come non recapitato. Se si desidera che MDaemon rispedisca immediatamente il messaggio al mittente in assenza di record MX, anziché cercare anche il record A, selezionare questa opzione. L'opzione è disabilitata per impostazione predefinita.

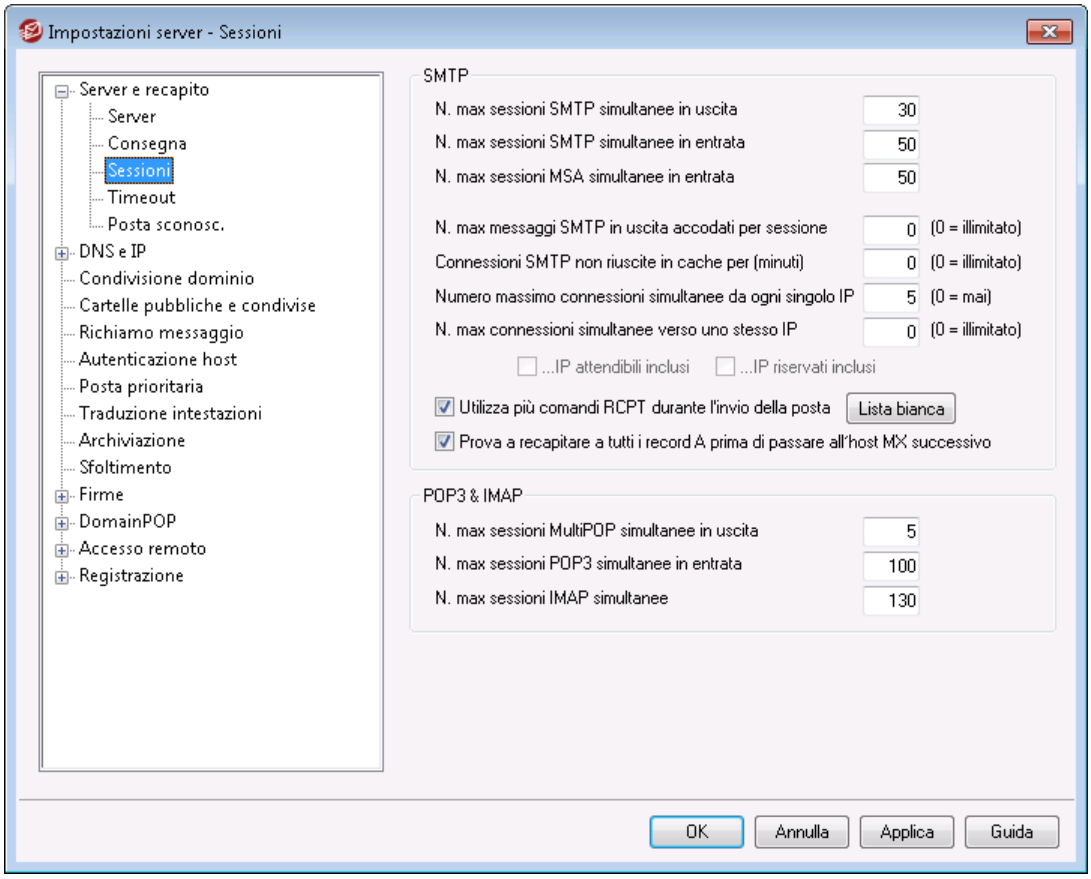
Rispedisci messaggio al primo errore 5XX da qualunque host MX del dominio ricevente
Se questa casella di controllo è abilitata, MDaemon restituisce o rispedisce il messaggio quando riceve un errore 5xx da un host MX. Di conseguenza, non tenta di consegnare il messaggio ai successivi host MX eventualmente indicati per il dominio del ricevente. Se questa opzione è disabilitata, MDaemon evita di rispedire il messaggio fino a quando almeno uno degli host MX restituisce un codice di errore 4xx. L'opzione è abilitata per impostazione predefinita.

Rispedisci messaggio dopo errori 5XX da host intelligenti
Utilizzare questa opzione per restituire o rispedire un messaggio quando riceve un errore irreversibile 5xx dagli host intelligenti in uso.

Per ulteriori informazioni, vedere:

Coda tentativi 888
Servizi di posta 733

3.1.1.3 Sessioni



SMTP

N. max sessioni SMTP simultanee in uscita
Il valore inserito in questo campo indica il numero massimo di sessioni SMTP in uscita che possono essere create al momento di inviare la posta. Ogni sessione trasmette i messaggi in uscita finché la coda non è vuota o non è stato raggiunto il valore indicato nel campo *N. max messaggi SMTP in uscita accodati per sessione*. Ad esempio, se è stato specificato il valore 5 e la coda della posta in uscita contiene 20 messaggi, al momento di inviare la posta vengono generate 5 sessioni simultanee, ciascuna delle quali trasmette consecutivamente 4 messaggi.

L'impostazione predefinita di questa opzione è 30, ma è possibile modificarlo per individuare l'impostazione più appropriata ai fini delle prestazioni in base alla larghezza di banda disponibile, evitando tuttavia di specificare un numero troppo alto che possa sovraccaricare la larghezza di banda e le risorse di Windows a scapito dell'efficienza di consegna. Tenere presente che in ciascuna sessione SMTP creata da MDaemon i messaggi vengono consegnati consecutivamente: per tale motivo, 4 sessioni che recapitano 2 messaggi ognuna offrono prestazioni migliori e più veloci di 8 sessioni che recapitano 1 messaggio ognuna. Un valido parametro di partenza potrebbe essere un valore compreso tra 5 e 10 sessioni per i modem a 56K e tra 10 e 20 per i modem a banda larga.

N. max sessioni SMTP simultanee in entrata
Questo valore controlla il numero di sessioni SMTP simultanee in entrata che il server accetta prima che ne venga segnalato il sovraccarico. Il valore predefinito è 50.

N. max sessioni MSA simultanee in entrata
Questa opzione consente di indicare il numero massimo consentito di sessioni simultanee MSA (Mail Submission Agent) in entrata.

N. max messaggi SMTP in uscita accodati per sessione
Questo parametro stabilisce un limite sul numero di singoli messaggi che verranno inviati in ciascuna sessione prima che si interrompa la consegna della posta e venga liberata la memoria. Di norma, questo valore deve essere impostato su zero, in modo che ciascuna sessione continui a consegnare i messaggi di posta fino a svuotare la coda.

Connessioni SMTP non riuscite in cache per (minuti)
Quando una connessione SMTP verso uno specifico host non riesce, MDaemon non esegue ulteriori tentativi di connessione all'host per il numero di minuti indicato nell'opzione. In tal modo è possibile evitare di tentare nuove connessioni verso un host non funzionante quando, ad esempio, sono presenti in coda numerosi messaggi indirizzati all'host e al primo tentativo di consegna si riscontra che l'host non è connesso. Il valore predefinito è di 5 minuti. Specificare "0" se non si desidera inserire nella cache gli errori SMTP.

Numero massimo connessioni simultanee da ogni singolo IP (0 = illimitate)
Indica il numero massimo di connessioni simultanee consentite da un singolo indirizzo IP prima che venga bloccato. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

N. max connessioni simultanee verso uno stesso IP (0 = illimitate)
Questa opzione consente di limitare il numero di connessioni simultanee verso uno stesso indirizzo IP durante la consegna della posta. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Questa opzione si rivela utile per impedire l'esecuzione di un numero eccessivo di connessioni simultanee verso più indirizzi IP. In fase di consegna, se per un messaggio è necessaria una connessione a un indirizzo IP che determinerebbe il superamento del limite impostato, la connessione non viene eseguita e viene utilizzato il successivo host MX o il successivo host intelligente. Se mon sono disponibili ulteriori host, il messaggio viene accodato per il successivo ciclo di consegna. Per impostazione predefinita l'opzione è disattivata, in modo da mantenere il comportamento precedente del sistema.

...IP attendibili inclusi
Per impostazione predefinita, le connessioni agli indirizzi IP attendibili sono escluse dall'opzione *Connessioni simultanee massime a qualsiasi singolo IP*. Selezionare questa casella di controllo se si desidera applicarla anche agli indirizzi IP attendibili.

...IP riservati inclusi
Per impostazione predefinita, anche le connessioni verso indirizzi IP riservati per l'uso intranet vengono escluse da questa funzionalità. Si tratta degli indirizzi IP 127.0.0.*, 192.168.*.*, 10.*.*.* e 172.16.0.0/12. Selezionare questa casella di controllo se si desidera applicarla anche agli indirizzi IP riservati.

Utilizzare più comandi RCPT per l'invio della posta
Per impostazione predefinita, per l'invio della posta MDaemon utilizza lo spooling intelligente, ovvero più comandi RCPT all'interno di una sessione. Deselezionare questa casella se si desidera utilizzare solo un comando RCPT per ciascuna sessione.

Elenco esenzioni
Questo pulsante apre l'Elenco esenzioni di Smart Spooling. Quando MDaemon invia messaggi ai domini dell'elenco, NON utilizzerà lo spooling intelligente e verrà usato solo un comando RCPT per ciascuna sessione.

Prova a recapitare a tutti i record A prima di passare all'host MX successivo
In caso di problemi o errori di recapito, per impostazione predefinita MDaemon tenterà il recapito a tutti i record A di un host MX prima di passare all'host MX successivo. Disattivare questa opzione se si desidera che MDaemon passi all'host MX successivo subito dopo aver rilevato un errore anziché tentare prima il recapito a tutti i record A.

POP3 & IMAP

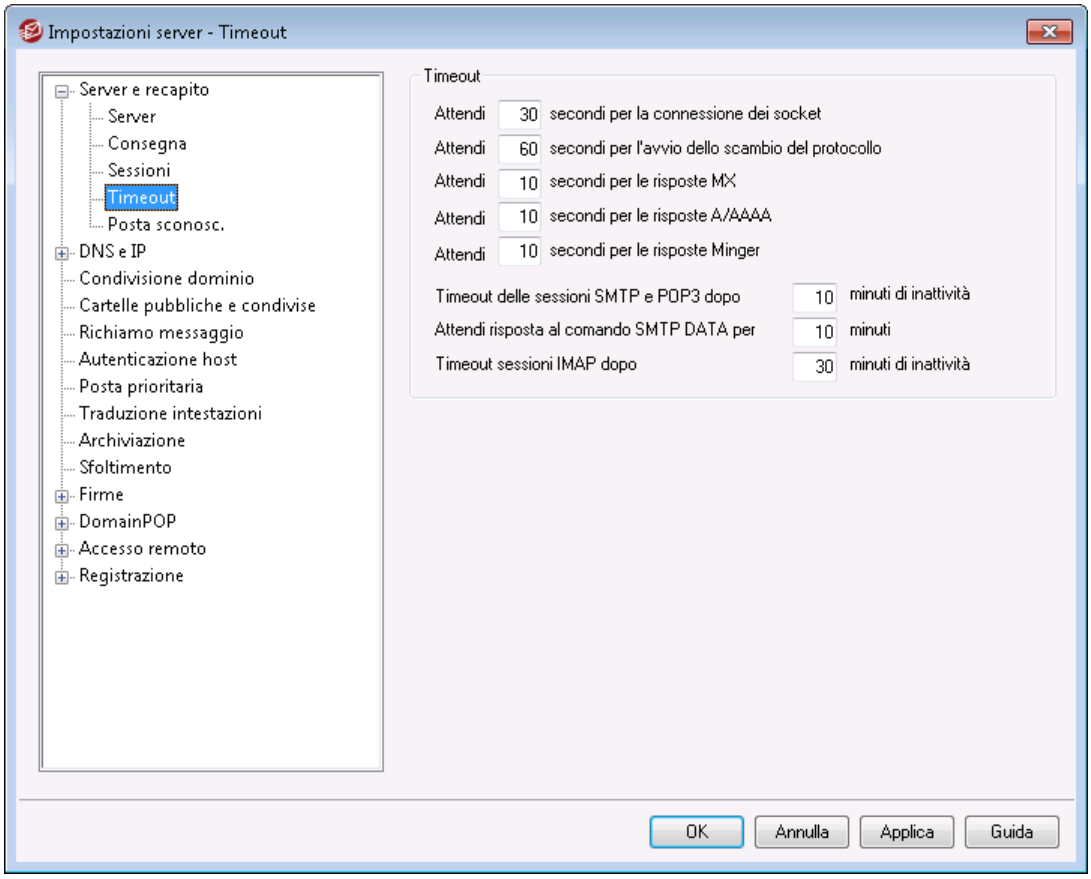
N. max sessioni MultiPOP simultanee in uscita
Si tratta del numero massimo di sessioni POP in uscita che possono essere generate al momento di raccogliere la posta MultiPOP. Ogni sessione raccoglie questo tipo di posta finché non sono stati controllati tutti i server MultiPOP e non è stata raccolta tutta la posta. Se ad esempio il valore specificato è 3 e le sessioni MultiPOP per tutti gli utenti sono 15, ciascuna sessione raccoglie la posta da 5 origini MultiPOP.

Si consiglia di eseguire più tentativi per rilevare quale numero di sessioni consenta di ottimizzare le prestazioni della larghezza di banda della rete, in modo da non specificare un numero troppo alto ed evitare di sovraccaricare la larghezza di banda o le risorse di Windows a scapito dell'efficienza di elaborazione. Tenere presente che ciascuna sessione POP generata da MDaemon procede alla raccolta della posta fino a svuotare tutte le origini. Pertanto, 4 sessioni che raccolgono la posta da 20 origini garantiscono prestazioni migliori e più veloci di 20 sessioni che raccolgono la posta da un'unica origine.

N. max sessioni POP3 simultanee in entrata
Questo valore controlla il numero massimo di sessioni POP simultanee in entrata consentite prima che il server segnali un sovraccarico.

N. max sessioni IMAP simultanee
Questo valore controlla il numero massimo di sessioni IMAP simultanee consentite prima che il server segnali un sovraccarico.

3.1.1.4 Timeout



Timeout

Attendi xx secondi per connessione socket
Una volta inoltrata una richiesta di connessione, MDaemon attende per un numero di secondi pari al valore specificato in questo campo che la connessione venga accettata dal sistema remoto. Se il sistema remoto non risponde entro questo intervallo di tempo, MDaemon invia il messaggio a un *host intelligente* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Inoltro 97 della finestra di dialogo Impostazioni server.

Attendi xx secondi per avvio scambio protocollo
Una volta stabilita la connessione a un host remoto, questo valore indica per quanti secondi MDaemon attende che l'host avvii lo scambio del protocollo SMTP o POP3. Se l'host remoto non avvia la sessione del protocollo entro questo intervallo di tempo, MDaemon invia il messaggio a un *host intelligente* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Inoltro 97 della finestra di dialogo Impostazioni server.

Attendi xx secondi per le risposte MX
Intervallo, espresso in secondi, in cui MDaemon attende la risposta relativa alla risoluzione degli host MX per i domini remoti presso i servizi DNS interrogati. Se il server DNS non risponde entro questo intervallo di tempo, MDaemon tenta di

consegnare il messaggio all'indirizzo IP specificato nel record DNS dell'host remoto. Se il tentativo non riesce, MDaemon invia il messaggio a un *host intelligente* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Inoltro 97 della finestra di dialogo Impostazioni server.

Attendi xx secondi per le risposte A/AAAA
Questo timer determina il tempo di attesa di MDaemon perché venga restituito l'indirizzo IP di un host remoto. Se il tentativo non riesce, MDaemon invia il messaggio a un *host intelligente* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Inoltro 97 della finestra di dialogo Impostazioni server.

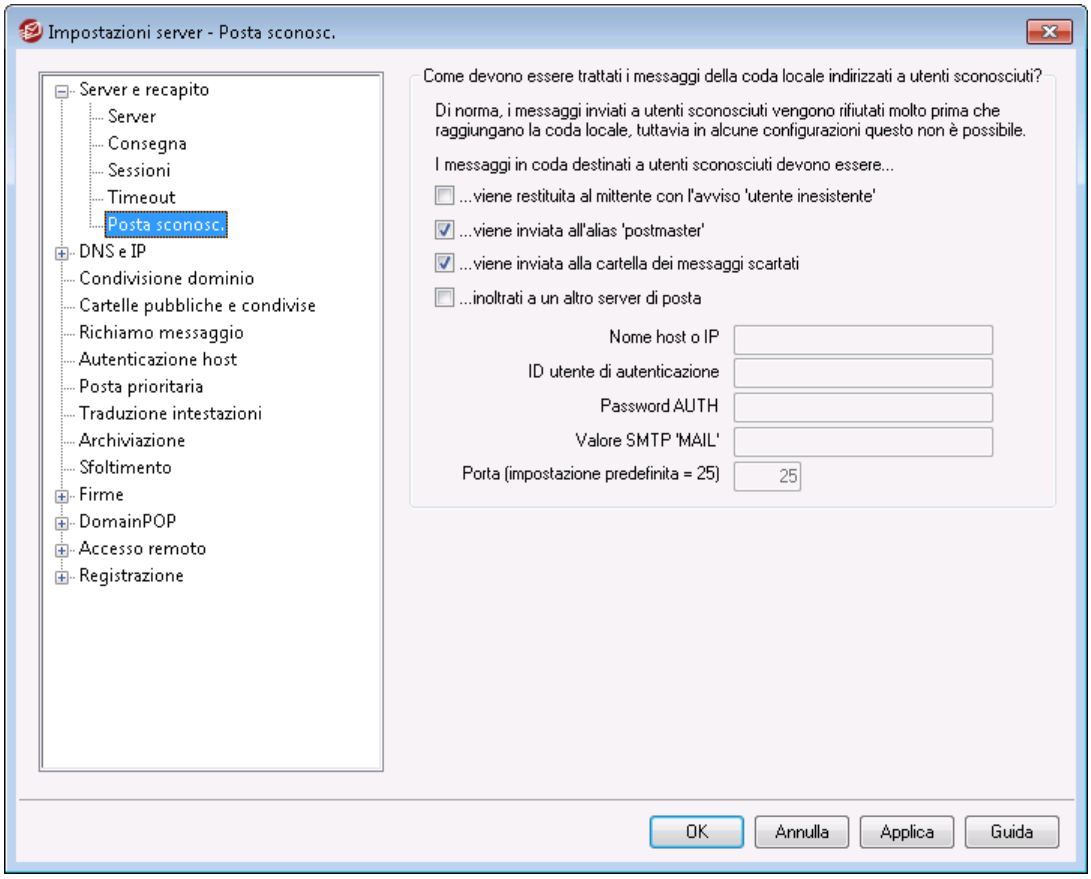
Attendi xx secondi per le risposte Minger
Questo è il numero di secondi per cui MDaemon resta in attesa di una risposta da un server Minger 878.

Timeout delle sessioni SMTP e POP3 dopo XX minuti di inattività
Se una connessione valida e operativa rimane inattiva (nessuno scambio) per questo intervallo di tempo, MDaemon chiude la transazione. MDaemon eseguirà un nuovo tentativo al successivo intervallo di elaborazione programmato.

Attendi risposta al comando SMTP DATA per XX minuti
Questa opzione gestisce il tempo per cui MDaemon resta in attesa della risposta "`250 Ok`" dopo l'invio del comando `DATA` durante l'elaborazione SMTP. Poiché alcuni server di ricezione eseguono in questa fase operazioni antispam, antivirus e altre operazioni necessarie che possono richiedere molto tempo, questa opzione può essere utilizzata per completare tali attività. Il valore predefinito è di 10 minuti.

Timeout sessioni IMAP dopo XX minuti di inattività
Trascorso questo intervallo di inattività, espresso in minuti, MDaemon chiude la sessione IMAP.

3.1.1.5 Posta sconosciuta



I messaggi in coda destinati a utenti sconosciuti devono essere...

...viene restituita al mittente con l'avviso 'utente inesistente'
Se questa opzione è abilitata, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono restituiti al mittente. Per personalizzare il contenuto del messaggio e-mail di avvertenza "Utente inesistente", è possibile creare un file di testo denominato "`NoShUser.dat`" e posizionarlo nella cartella "`MDaemon\app\`".

...inviati all'alias 'Postmaster'
Abilitando questa opzione, selezionata per impostazione predefinita, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono inoltrati all'utente definito come postmaster. Se non si desidera inviare tali messaggi all'utente Postmaster, disabilitare questa opzione.

...inviati alla cartella dei messaggi scartati
Abiltando questa casella, selezionata per impostazione predefinita, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono collocati nella coda dei messaggi scartati. Se non si desidera inviare tali messaggi alla coda dei messaggi scartati, disabilitare questa opzione.

...inoltrati a un altro server di posta
Utilizzare questa opzione per inoltrare a un altro server di posta i messaggi indirizzati a utenti locali inesistenti.

Nome host o IP
Specificare il nome host o l'indirizzo IP a cui si desidera inoltrare i messaggi.

Nelle opzioni di MDaemon in cui è consentito specificare un host a cui inoltrare, copiare o inviare posta è possibile utilizzare le convenzioni seguenti. Se l'host viene racchiuso tra parentesi quadre (ad esempio, `[esempio.com]`) MDaemon ignorerà la ricerca di record MX al momento della consegna a tale host. Ad esempio, se tale opzione contenesse "`esempio.com`", le ricerche MX verrebbero eseguite normalmente. Se, al contrario, tale opzione contenesse "`[esempio.com]`", verrebbe eseguita solo la ricerca di record A.

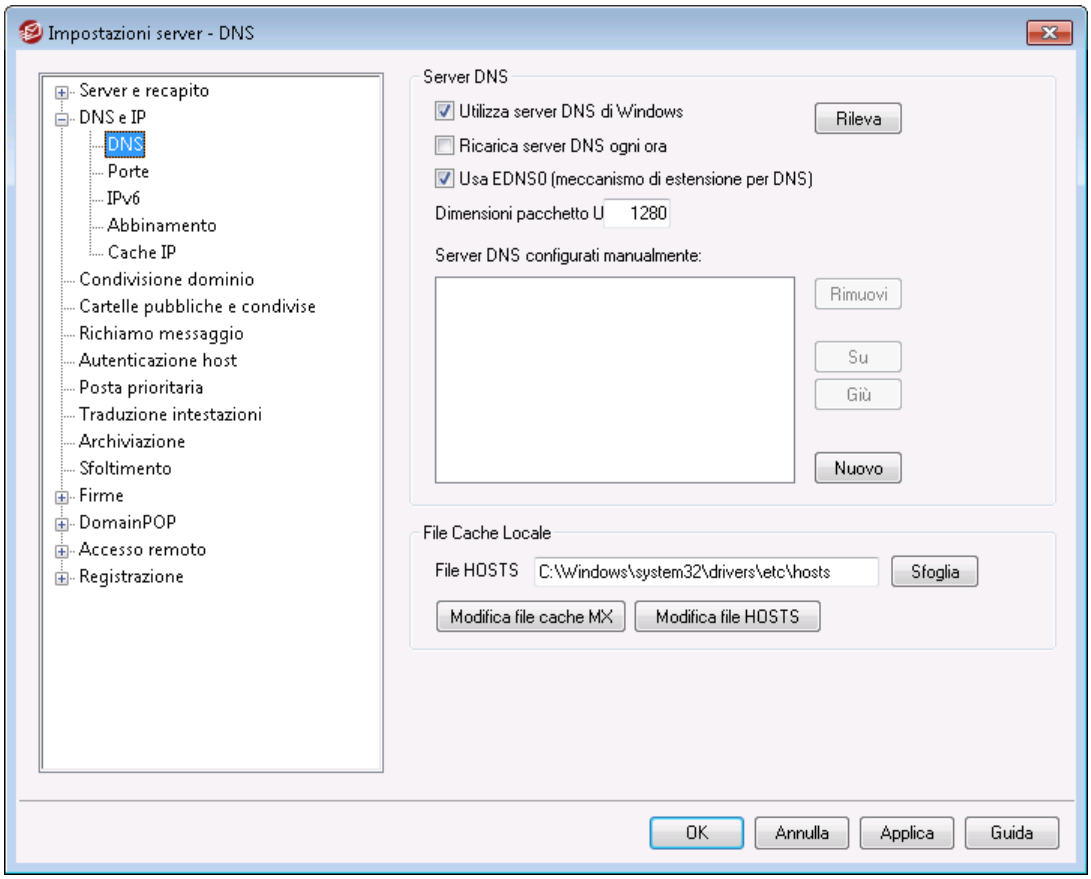
Accesso/Password AUTH
Immettere le eventuali credenziali di accesso/password necessarie per il server di posta a cui si desidera inoltrare i messaggi indirizzati a utenti inesistenti.

Valore SMTP 'MAIL'
Questo indirizzo viene utilizzato nell'istruzione SMTP "`Mail From:`" durante l'handshake della sessione con l'host di destinazione. Di norma, in questa sezione della busta SMTP viene indicato il mittente del messaggio. Per utilizzare un comando vuoto (`MAIL FROM <>`), immettere "`[trash]`" nell'opzione.

Porta (valore predefinito = 25)
Questa è la porta TCP che MDaemon utilizza per l'invio dei messaggi. Il valore predefinito è la porta 25.

3.1.2 DNS e IP

3.1.2.1 DNS



Server DNS

Utilizza server DNS Windows
Quando questa opzione è selezionata, MDaemon utilizza tutti i server DNS rilevati nella configurazione TCP/IP di Windows. MDaemon prova ciascun server DNS una volta per ogni operazione di ricerca e in sequenza, fino a utilizzare l'elenco completo di server DNS o finché non trova il primo server che funziona. Se si includono altri server DNS nell'opzione *Server DNS configurati manualmente* riportata di seguito, MDaemon proverà anche con questi server. Infine, il registro di sistema visualizza all'avvio ciascun server DNS e fornisce un'indicazione della provenienza (se configurato manualmente o estratto da Windows).

Ricaricare il server DNS ogni ora
Questa casella consente di ricaricare il server DNS ogni ora. È disabilitata per impostazione predefinita.

Usa EDNS0 (meccanismo di estensione per DNS)
Per impostazione predefinita MDaemon supporta il meccanismo di estensione per DNS (vedere RFC 2671). Deselezionare la casella di controllo se non si desidera supportarlo.

Dimensioni pacchetto UDP
Questa opzione controlla le dimensioni del pacchetto UDP. La dimensione predefinita è 1280 byte.

Server DNS configurati manualmente
MDaemon utilizzerà tutti i server DNS specificati in questa opzione durante l'esecuzione delle ricerche DNS. Inoltre, MDaemon proverà ciascun server una volta per ogni operazione di ricerca e in sequenza, fino a utilizzare l'elenco completo di server DNS o finché non trova il primo server che funziona. Se si attiva l'opzione *Utilizza server DNS Windows* sopra riportata, MDaemon interrogherà tutti i server DNS rilevati all'interno della configurazione TCP/IP di Windows. Infine, il registro di sistema visualizza all'avvio ciascun server DNS e fornisce un'indicazione della provenienza (se configurato manualmente o estratto da Windows).

File cache locale

File HOSTS
Prima di interrogare i server DNS, MDaemon tenta di risolvere un indirizzo mediante il file HOSTS di Windows. Se nel file è presente l'indirizzo IP del dominio in questione, MDaemon non ricorre all'interrogazione del server DNS.

Oltre al nome, è necessario immettere anche il percorso completo del file. MDaemon tenta di utilizzare il valore riportato di seguito come posizione predefinita del file:

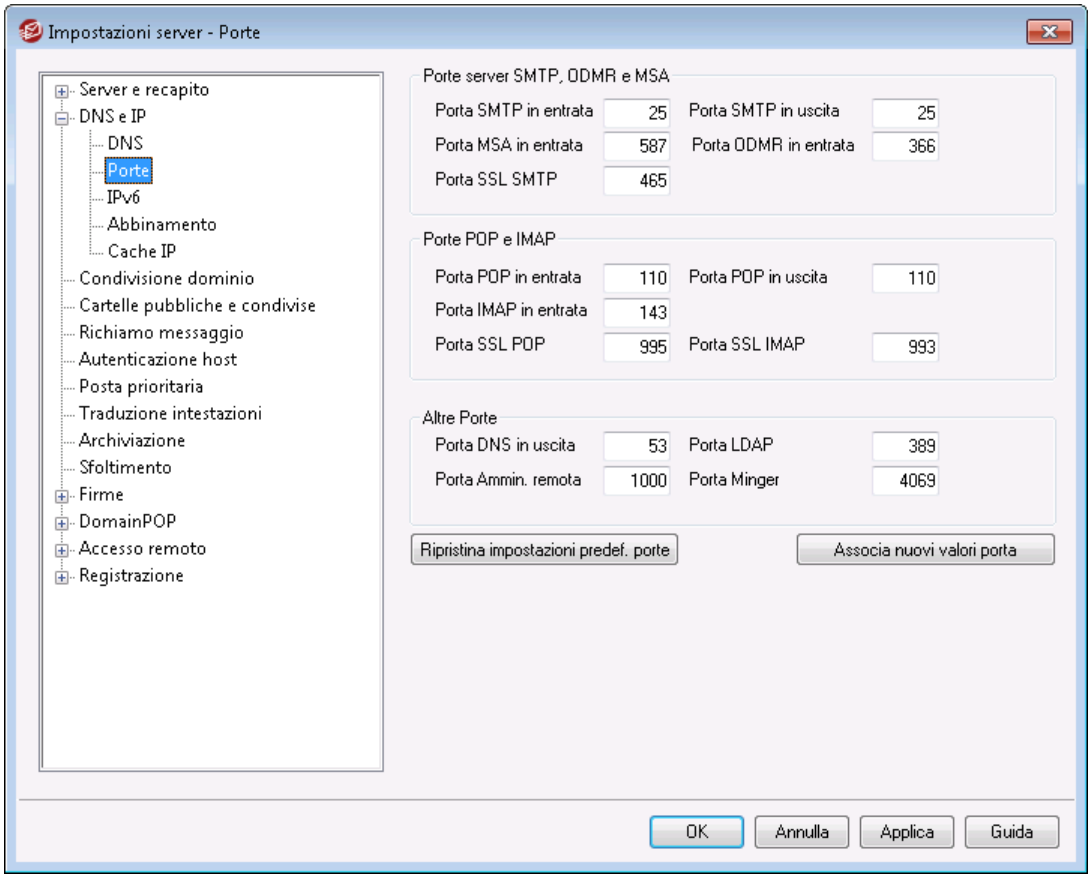
[unità]:\windows\system32\drivers\etc\hosts

Il file HOSTS è un file di Windows contenente il record A, ossia l'indirizzo IP principale relativo ai nomi di dominio. MDaemon consente anche di specificare gli indirizzi IP del record MX all'interno di un file denominato MXCACHE.DAT. Il file si trova nella cartella MDaemon\APP\ . Fare clic su **Modifica file cache MX** e leggere i commenti riportati all'inizio del file per ulteriori informazioni.

Modifica file cache MX
Fare clic su questo pulsante per visualizzare o modificare il file MXCACHE.DAT.

Modifica HOSTS
Fare clic su questo pulsante per visualizzare o modificare il file HOSTS.

3.1.2.2 Porte



Porte SMTP, ODMR e MSA

Porta SMTP in entrata
MDaemon controlla questa porta TCP per rilevare eventuali connessioni in arrivo da client SMTP. Si tratta della porta SMTP principale, che in genere viene lasciata inalterata sul valore predefinito 25.

Porta SMTP in uscita
Questa porta viene utilizzata quando la posta viene inviata ad altri server SMTP.

Porta MSA in entrata
La porta MSA (Message Submission Agent) può essere utilizzata dagli utenti in alternativa alla *Porta SMTP in entrata* specificata in precedenza. Se si utilizza questa porta alternativa l'autenticazione è obbligatoria e, di conseguenza, è necessario configurare correttamente i propri client di posta al fine di garantire l'autenticazione delle connessioni. Inoltre, poiché alcuni ISP bloccano la porta 25, gli utenti remoti hanno la possibilità di eludere tale restrizione utilizzando la porta MSA. Se non si desidera definire una porta MSA, impostare il valore su "0" per disattivarla.

Le connessioni alla porta MSA sono escluse dalle ricerche PTR e inverse, da Vaglio Host e Vaglio IP, da Scudo IP e dalla

funzione di tarpitting. Le connessioni della porta MSA utilizzano ancora la limitazione delle connessioni di attacco in base al dizionario.

Porta ODMR in entrata
MDaemon monitora questa porta per rilevare le connessioni ODMR (On-Demand Mail Relay) in entrata, ad esempio il comando `ATRN` dei gateway di dominio.

Porta SSL SMTP
Si tratta della porta dedicata per le sessioni di posta SMTP che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 585.

Porte POP e IMAP

Porta POP in entrata
MDaemon controlla questa porta per rilevare le connessioni in entrata da client POP remoti.

Porta POP in uscita
Questa porta viene utilizzata quando MDaemon recupera la posta dai server POP.

Porta IMAP in entrata
MDaemon controlla questa porta per rilevare le richieste IMAP in entrata.

Porta SSL POP
Si tratta della porta dedicata per i client di posta POP che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 585.

Porta SSL IMAP
Si tratta della porta dedicata per i client di posta IMAP che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 585.

Altre porte

Porta DNS in uscita
Specificare la porta che MDaemon deve utilizzare per l'invio e la ricezione di datagrammi da e verso il server DNS.

Porta LDAP
Questa porta viene utilizzata da MDaemon per trasmettere le informazioni relative ai database e alle rubriche destinate al server LDAP.

Vedere: Supporto delle rubriche LDAP 844

Porta Remote Admin
Indica la porta che viene assegnata a MDaemon per rilevare le connessioni Remote Administration 359.

Porta Minger
Consente di specificare la porta monitorata dal server Minger 878 per le connessioni.

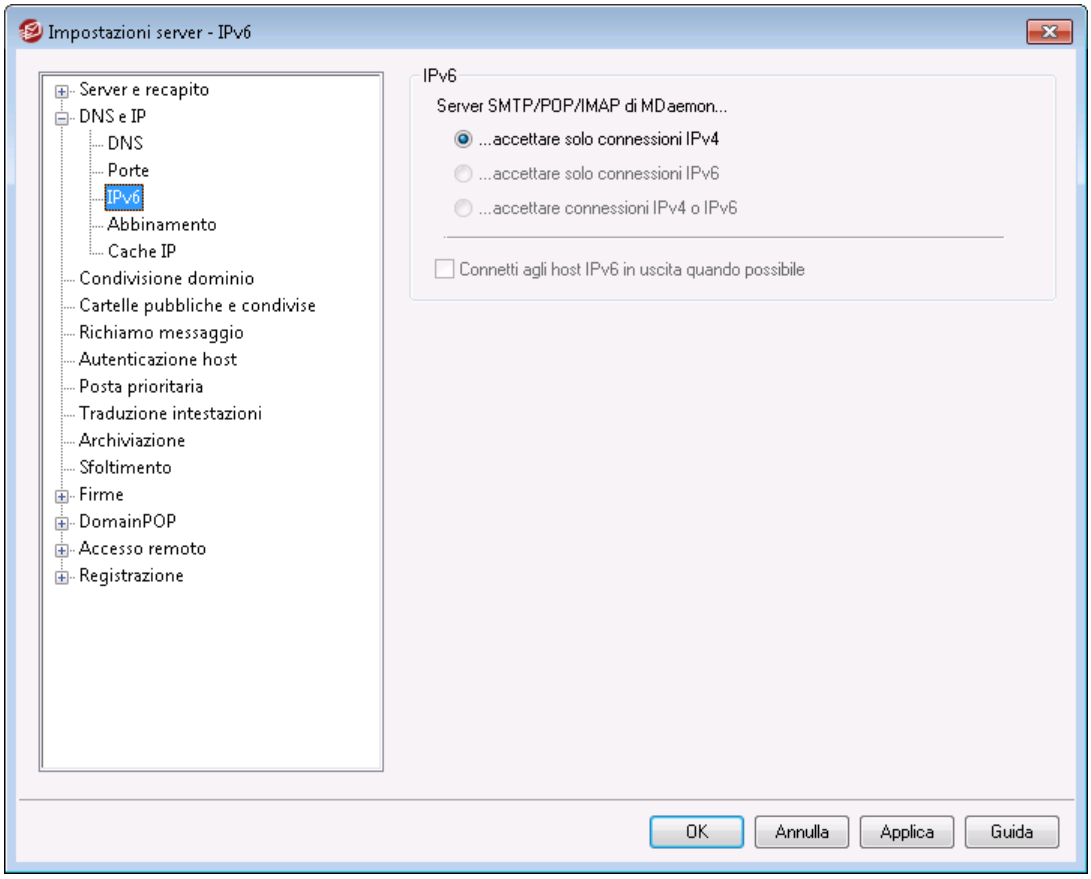
Ripristina impostazioni predefinite porte
Questo pulsante consente di ripristinare le impostazioni predefinite di tutte le porte.

Associa nuovi valori porta
Quando si modificano i valori di impostazione di una qualsiasi porta, è necessario premere questo pulsante per rendere immediatamente operative le modifiche apportate. In caso contrario, le modifiche non saranno operative se non dopo il riavvio del server.

Le impostazioni relative alle porte appena descritte rivestono un ruolo cruciale per il corretto funzionamento del server e non devono essere modificate, se non in caso di assoluta necessità. La conoscenza della configurazione delle porte usate da MDaemon è utile per collegare il server con sistemi proxy o altri software che richiedono la definizione di porte specifiche.

Ogni indirizzo IP, ossia ogni computer, dispone di diverse porte, ciascuna identificata univocamente. Se un programma tenta di accedere a una porta già utilizzata da un altro programma, un messaggio di errore informa l'utente che l'indirizzo richiesto (IP:PORTA) è già in uso.

3.1.2.3 IPv6



Per impostazione predefinita MDaemon rileva il livello di capacità IPv6 che il sistema operativo supporta e, quando possibile, opera in dual stack. In alternativa, MDaemon monitora sia IPv4 e IPv6 in modo indipendente.

IPv6

Server SMTP/POP3/IMAP di MDaemon...

...accetta solo connessioni IPv4
Scegliere questa opzione per accettare le connessioni IPv4.

...accetta solo connessioni IPv6
Scegliere questa opzione per accettare le connessioni IPv6.

...accetta connessioni IPv4 o IPv6
Scegliere questa opzione per accettare sia le connessioni IPv4 che IPv6. Questa è l'impostazione predefinita e MDaemon considera prioritarie le connessioni IPv6 rispetto a quelle IPv4, se possibile.

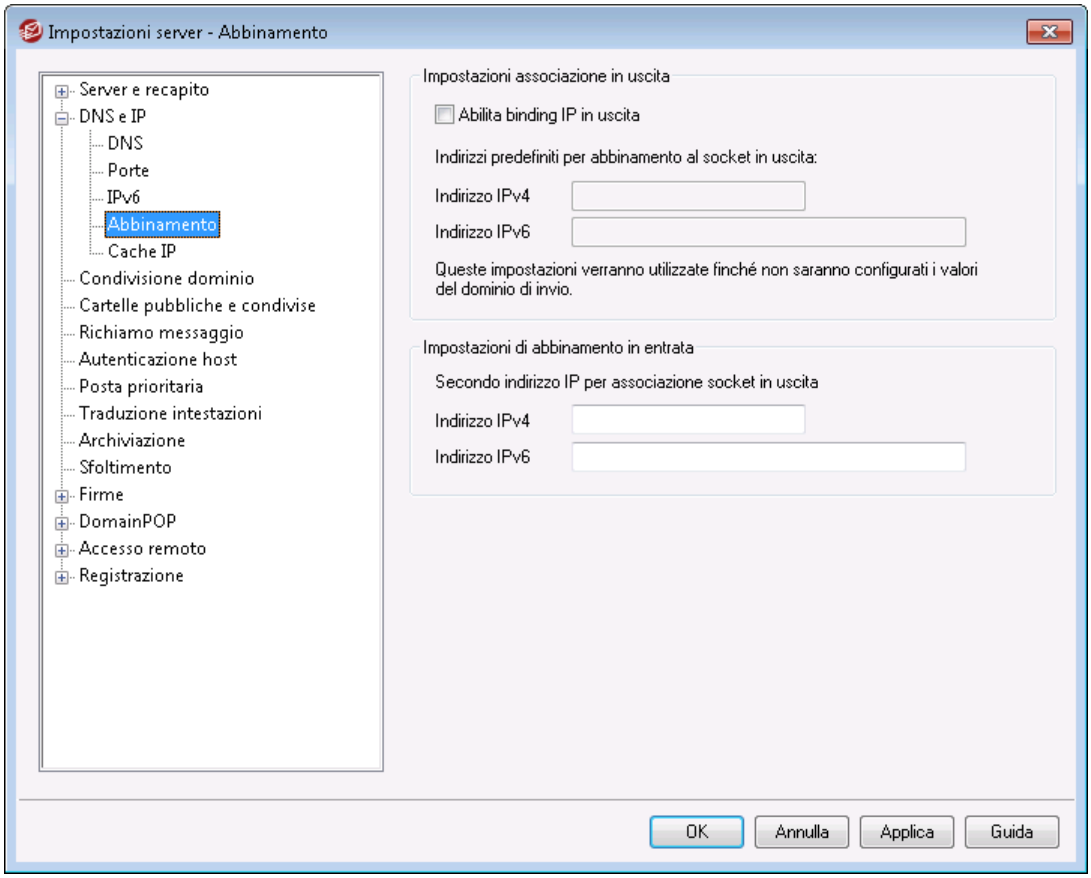
Quando possibile, connetti a host IPv6 in uscita
Attivare questa opzione se si desidera che MDaemon si connetta agli host IPv6 in uscita quando possibile.

Quando MDaemon si connette a un host IPv6 deve utilizzare un proprio indirizzo IPv6 locale. L'indirizzo IPv6 si può specificare nella schermata Domain Manager » Nome host e IP 188. Se necessario, è possibile specificare un indirizzo per l'associazione del socket in uscita nella schermata Associazione 114.

Vedere:

Associazione 114
Domain Manager » Nome host e IP 188

3.1.2.4 Associazione



Impostazioni associazione in uscita

Abilita associazione IP in uscita
Quando viene selezionata questa opzione, MDaemon associa sempre i socket in uscita. Per i domini con *Questo dominio riconosce solo le connessioni eseguite a*

questi IP 188 selezionato sulla schermata Nome host e IP 188, MDaemon utilizza l'IP configurato del dominio. In caso contrario utilizza *indirizzi predefiniti per le associazioni al socket in uscita* specificato di seguito.

Indirizzi IP predefiniti per l'associazione al socket in uscita: Indirizzi IPv4/IPv6
Si tratta degli indirizzi IP che saranno utilizzati per l'associazione del socket in uscita per i domini che non sono già associati a indirizzi IP specifici nella schermata Nome host e IP 188 di Domain Manager.

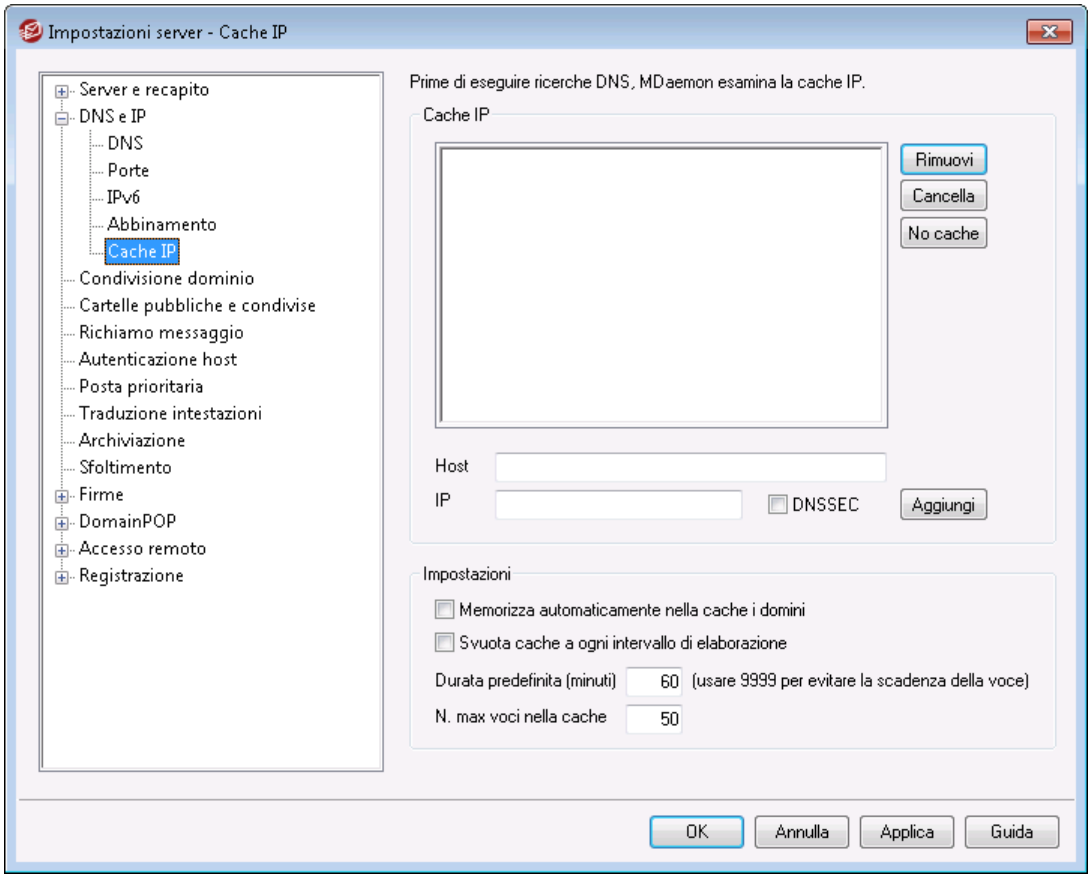
Impostazioni associazione in entrata

Secondo indirizzo IP per associazione socket in entrata: Indirizzi IPv4/IPv6
Utilizzare questa opzione se si desidera indicare un secondo set di indirizzi IP per l'associazione del socket in uscita 188.

Per ulteriori informazioni, vedere:

Domain Manager » Nome host e IP 188
IPv6 113

3.1.2.5 Cache IP



Per velocizzare la consegna dei messaggi e ridurre i tempi di elaborazione della posta, MDaemon memorizza tutti gli indirizzi IP rilevati nella cache. La cache viene controllata

ogni volta che MDaemon richiede informazioni DNS per un nome host. Se il nome host in attesa di risoluzione si trova all'interno della cache degli indirizzi IP, la ricerca DNS viene annullata, in modo da ridurre i tempi di elaborazione. Le impostazioni di questa finestra consentono di controllare i parametri operativi della cache. È inoltre possibile aggiungere e rimuovere voci manualmente, impostare se utilizzare o meno DNSSEC, impostare la dimensione massima della cache, e indicare per quanto tempo le voci devono restare nella cache. Per accedere alla cache degli indirizzi IP, selezionare "Impostazioni » Impostazioni server » Cache IP".

Cache IP

Host
Immettere l'host da aggiungere alla cache IP.

IP
Immettere l'indirizzo IP da aggiungere alla cache.

DNSSEC
Selezionare questa casella di controllo per DNSSEC.

Aggiungi
Dopo aver immesso manualmente l'host e l'indirizzo IP, fare clic su questo pulsante per aggiungerli alla cache.

Rimuovi
Se si desidera rimuovere un indirizzo dalla cache IP, selezionarlo e fare clic su questo pulsante.

Cancella
Questo pulsante consente di eliminare tutte le voci inserite nella cache IP.

No cache
Fare clic su questo pulsante per visualizzare l'elenco di nomi domini e/o indirizzi IP da non memorizzare mai nella cache.

Impostazioni

Memorizza automaticamente nella cache i domini
Questa opzione controlla il modulo interno di memorizzazione automatica nella cache di MDaemon. se si seleziona la casella di controllo, MDaemon memorizza automaticamente i domini nella cache. Per inserire manualmente le voci nella cache, deselezionare la casella.

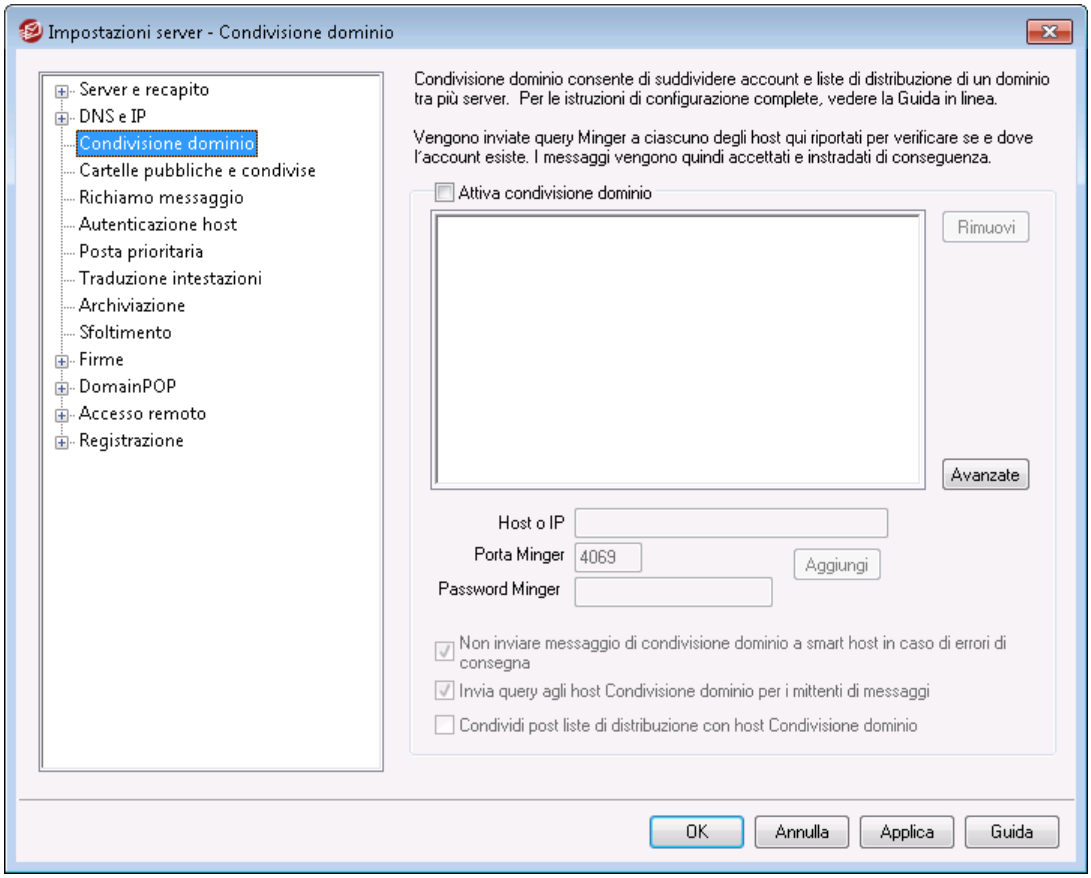
Svuota cache a ogni intervallo di elaborazione
Se questa opzione è selezionata, l'intero contenuto della cache viene cancellato all'avvio di ogni sessione di posta. In questo modo, la cache viene aggiornata a ogni intervallo di elaborazione.

Durata predefinita (minuti)
Rappresenta il valore predefinito, in minuti, per la permanenza della voce nella cache degli indirizzi IP. Una volta trascorso questo intervallo, MDaemon rimuove la voce

dalla cache. Per preservare la voce nella *cache IP* in modo permanente, immettere in questo campo il valore 9999.

N. max voci nella cache
Questo valore definisce la dimensione della cache. Una volta raggiunto il limite, se nella cache viene inserita una nuova voce, la prima (a livello cronologico) verrà rimossa.

3.1.3 Condivisione dominio



La condivisione del dominio è una funzione che consente di ripartire tra più server gli utenti di un dominio. In tal modo, i server MDaemon possono essere eseguiti in postazioni diverse, utilizzando tutti gli stessi nomi di dominio, ma con account utente diversi. Parte degli account utente del dominio si trova in un server, mentre un'altra in uno o più altri server. La finestra di dialogo Condivisione dominio consente di specificare la posizione di ciascuno degli altri server. Quando arriva un messaggio per un utente locale privo di casella postale locale, Condivisione dominio esegue una query negli altri server mediante Minger per stabilire se l'utente dispone di un account in uno di essi. Se l'indirizzo si dimostra valido, MDaemon accetta il messaggio e lo instrada al server nel quale si trova l'account.

Se, ad esempio, si sceglie di utilizzare Condivisione dominio per uffici distribuiti in varie città è possibile offrire a ogni dipendente un indirizzo e-mail che termina con "@esempio.com". Il server MDaemon di ciascun ufficio ospiterà solo una parte dei messaggi di e-mail di esempio.com, relativa agli account dei dipendenti locali che lavorano in quell'ufficio. Per ogni ufficio, quindi, viene configurato Condivisione dominio in modo che ogni messaggio venga instradato all'ufficio appropriato.

Poiché Condivisione dominio verifica gli indirizzi utilizzando il server Minger 878, per il funzionamento della query è necessario aver abilitato e configurato correttamente Minger in ciascun server. Se, tuttavia, si verifica un errore durante la query Minger, ad esempio nel caso uno dei server sia temporaneamente non disponibile, MDaemon risponde con il codice di errore temporaneo "451", in modo che il server mittente possa tentare di recapitare nuovamente il messaggio in seguito. Quando un indirizzo è stato verificato, inoltre, viene memorizzato nella cache per cinque giorni in modo che MDaemon possa accettare subito i messaggi successivi per quell'indirizzo e instradarli all'host appropriato.

Per evitare, infine, i potenziali problemi che potrebbero verificarsi qualora si crei lo stesso account in più server, prima della creazione di un nuovo account viene eseguita una query in tutti i server di Condivisione dominio.

È disponibile l'opzione "*L'esecuzione di ricerche in Minger attiva anche l'esecuzione di ricerche di Condivisione dominio*" nella schermata Impostazioni 274 di Gateway Editor. Questa opzione consente di far sì che MDaemon esegua una query anche negli host di Condivisione dominio ogniqualvolta un gateway utilizzi la verifica Minger 264.

Abilita Condivisione dominio
Per attivare Condivisione dominio, selezionare questa casella di controllo. Dopo aver abilitato Condivisione dominio e aver aggiunto all'elenco tutti gli host o gli indirizzi IP di Condivisione dominio, assicurarsi che anche Minger 878 sia stato abilitato e configurato in modo da poter rispondere alle query degli host che tentano di verificare gli indirizzi locali.

Rimuovi
Per eliminare una delle voci di Condivisione dominio, selezionarla nell'elenco e fare clic su questo pulsante.

Avanzate
Questo pulsante consente di aprire un file nel quale è possibile configurare i nomi dei domini ai quali è consentito utilizzare la Condivisione dominio. Se il file è vuoto (condizione predefinita), tutti domini possono utilizzare la Condivisione dominio. Per ulteriori informazioni, consultare le istruzioni nella parte superiore del file.

Host o IP
In questa casella è possibile inserire l'host o l'indirizzo IP che condivide uno o più domini. Se per l'invio di messaggi SMTP all'host si desidera utilizzare una porta specifica che non sia quella predefinita, è possibile aggiungere il carattere due punti

e il numero di una porta, ad esempio `posta.esempio.com:2525`. Questa porta differisce dalla porta Minger.

Porta Minger
Porta utilizzata da Minger per le query all'host. La porta predefinita è 4069.

Password Minger (facoltativa)
È possibile inserire la password Minger eventualmente necessaria per l'host aggiunto. L'impostazione di Minger per la richiesta di una password è facoltativa, ma consigliata.

Aggiungi
Dopo aver inserito l'host o l'indirizzo IP, la porta e la password, fare clic su questo pulsante per aggiungere all'elenco la nuova voce di Condivisione dominio.

Non inviare la posta di Condivisione dominio all'host intelligente in caso di errori di recapito
Quando questa opzione è abilitata, se MDaemon rileva un errore durante il tentativo di consegnare un messaggio di posta elettronica di condivisione dominio (ad esempio quando l'host di condivisione dominio è offline), il messaggio resterà in coda 888 anziché essere inviato all'host intelligente 97. L'invio di questi messaggi di posta elettronica all'host intelligente spesso può causare un loop di posta. L'opzione è abilitata per impostazione predefinita.

Invia query agli host di Condivisione dominio per i mittenti dei messaggi
Per impostazione predefinita MDaemon accetterà posta da account esistenti su altri server di Condivisione dominio. Se si preferisce non eseguire ricerche di condivisione dominio sul mittente di posta SMTP MAIL, disattivare questa opzione.

Condividi post liste di distribuzione con host Condivisione dominio
Attivare questa opzione se si desidera condividere le liste di distribuzione con gli host di Condivisione dominio. Quando arriva un messaggio per una lista di distribuzione viene creata una copia per ciascun host di Condivisione dominio che conserva anche una versione di tale lista (viene fatta una query per controllare). Quando questi host ricevono le loro copie, recapiteranno il messaggio a tutti i membri della lista che servono. In questo modo le liste di distribuzione possono essere suddivise su più server senza alcuna perdita di funzionalità. Perché questo funzioni, ogni host di Condivisione dominio deve includere gli indirizzi IP degli altri host nella configurazione degli IP attendibili 527. In caso contrario i messaggi della lista possono essere rifiutati con un errori di tipo "Il mittente non è membro della lista".

Vedere:

Minger 878
Gestione domini 185

3.1.4 Cartelle pubbliche e condivise

MDaemon supporta la condivisione delle cartelle IMAP sia pubbliche sia a livello di utente. Cartelle pubbliche (gestite da Gestione cartelle pubbliche 317) sono cartelle supplementari che non appartengono ad alcun account in particolare ma possono essere rese disponibili per più utenti IMAP. Le cartelle utente sono cartelle IMAP che appartengono a singoli account di MDaemon. A ciascuna cartella condivisa, pubblica o a livello di utente, deve essere associato un elenco di utenti di MDaemon e solo i membri di tale lista possono accedere a essa mediante MDaemon Webmail o un client e-mail IMAP.

Quando gli utenti IMAP accedono all'elenco delle cartelle personali, visualizzano anche le cartelle pubbliche condivise e le cartelle utente condivise a cui possono accedere. In questo modo, è possibile che alcune cartelle di posta vengano condivise da più utenti e che vengano anche richieste le credenziali di connessione di ogni singolo utente. Inoltre, avere accesso a una cartella non significa necessariamente godere di un accesso completo di lettura/scrittura o amministrativo. I diritti di accesso specifici possono essere accordati ai singoli utenti, con possibilità di impostare per ciascuno di essi un livello di accesso diverso. Ad esempio, è possibile autorizzare solo alcuni utenti a eliminare i messaggi.

Dopo avere creato una cartella pubblica o utente, è possibile utilizzare la funzione Filtro contenuti per impostare i criteri secondo cui determinati messaggi vengono spostati in essa. Ad esempio, una regola utile potrebbe essere quella di spostare nella cartella pubblica `Assistenza` i messaggi contenenti `assistenza@esempio.com` nell'intestazione `TO:`. Le Azioni di filtro contenuti 661 "`Sposta il messaggio nella cartella pubblica`" e "`Copia il messaggio nella cartella`" lo consentono. Per le cartelle utente condivise, è possibile utilizzare i filtri IMAP personali 751 per instradare a esse messaggi specifici. Oltre a utilizzare Filtro contenuti e i filtri IMAP, è possibile associare un account specifico a una cartella condivisa in modo che i messaggi destinati a tale "indirizzo di invio" vengano instradati automaticamente alla cartella condivisa. Tuttavia, solo gli utenti a cui sia stata accordata l'autorizzazione a inviare nella cartella sono in grado di effettuare invii a tale indirizzo.

Per maggiore comodità, anche l'editor della lista di distribuzione contiene una schermata Cartelle pubbliche 306 che consente di associare una cartella pubblica a una lista specifica. Se questa funzione è abilitata, una copia di ciascun messaggio della lista viene collocata nella cartella pubblica specifica. Tutte le cartelle pubbliche vengono memorizzate nella directory `\Public Folders\` all'interno della gerarchia delle directory di MDaemon.

Cartelle documenti Webmail

I temi Webmail supportano la condivisione dei documenti mediante l'uso di cartelle documenti. Le cartelle documenti supportano in modo completo Access Control List (ACL) 319 come le altre cartelle condivise, che è possibile utilizzare per impostare le autorizzazioni e la condivisione delle regole. Il sistema consente inoltre di condividere tutti i tipi di file. I file possono essere caricati dagli utenti Webmail nelle cartelle documenti utilizzando gli strumenti integrati. Quando si utilizza il tema LookOut, i browser che supportano l'API di trascinamento HTML5, ad esempio Chrome e Firefox, consentono di caricare i file anche trascinandoli dal desktop alla finestra del browser. I nomi dei file si possono cercare e modificare, mentre i file possono essere allegati ai nuovi messaggi che si compongono.

Per abilitare/disabilitare le cartelle documenti, e altre cartelle condivise, a livello di singolo dominio e a livello di singolo utente è sufficiente modificare rispettivamente i file `\WorldClient\Domains.ini` e `\Users\..\WC\user.ini`. È possibile configurare sia impostazioni predefinite che impostazioni personalizzate. Le impostazioni personalizzate ignorano le impostazioni predefinite. Ad esempio,

```
[Predefinito:UtenteImpostazionipredefinite]
NomeCartelladocumenti=Documenti
AbilitaDocumenti=Sì

[esempio.com:UtenteImpostazionipredefinite]
NomeCartelladocumenti=Documenti di esempio
AbilitaDocumenti=Sì

[superControllodominio.gov:UtenteImpostazionipredefinite]
AbilitaDocumenti=No
AbilitaCalendario=No
AbilitaNote=No
AbilitaAttività=No
```

Impostazione della dimensione massima per i file

È possibile limitare le dimensioni dei singoli file che possono essere caricati nelle cartelle documenti aggiungendo questa chiave al file `domains.ini`: `MaxAttachmentSize=<valore in KB>` Il valore predefinito è `0`, che indica che non esiste alcun limite.

Blocco o autorizzazione di tipi di file

Per impedire il caricamento di determinati tipi di file nella cartella documenti, aggiungere la chiave `BlockFileTypes=` al file `domains.ini`, elencando i tipi di file che si desidera bloccare separati da uno spazio o una virgola, ad esempio "`BlockFileTypes=exe dll js`".

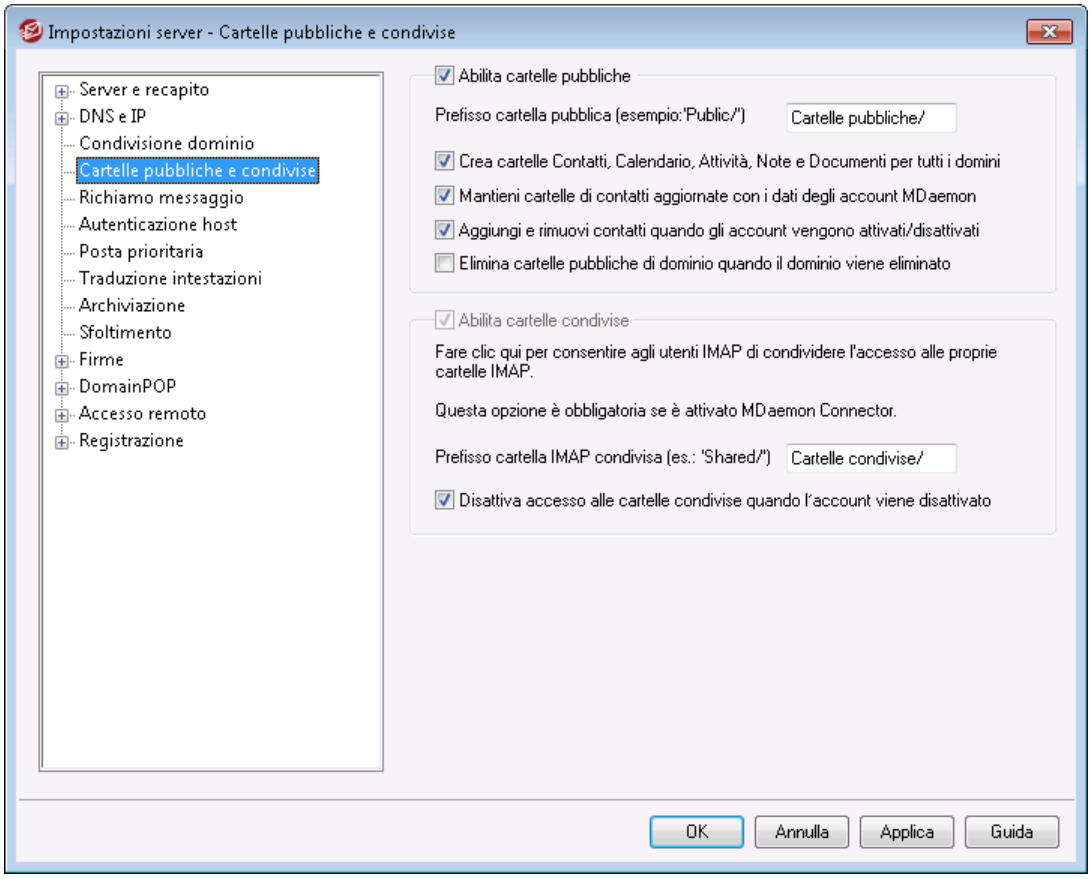
Per consentire il caricamento solo di determinati tipi di file nella cartella documenti, aggiungere la chiave `AllowFileTypes=` al file `domains.ini`, elencando i tipi di file per i quali si desidera consentire il caricamento separati da uno spazio o una virgola, ad esempio "`AllowFileTypes=jpg png doc docx xls xlsx`".

Quando vengono utilizzate entrambe le chiavi, in caso di confitto, viene data priorità ai file bloccati; se in entrambi gli elenchi è presente un'estensione, quest'ultima verrà bloccata. Se viene utilizzata una chiave senza un valore (senza un elenco di estensioni), tale chiave non verrà utilizzata. Le estensioni dei file possono includere il carattere "." (ad esempio .exe .dll), ma questo carattere non è obbligatorio.

Per ulteriori informazioni, vedere:

Cartelle pubbliche e condivise 122
Gestione cartelle pubbliche 317
Elenco controllo accessi 319
Account Editor » Cartelle condivise 757
Lista distribuzione » Cartelle pubbliche 306

3.1.4.1 Cartelle pubbliche e condivise



Per aprire la schermata Cartelle pubbliche e condivise, fare clic su "Impostazioni » Impostazioni Server » Cartelle pubbliche e condivise".

Abilita cartelle pubbliche

Fare clic su questa casella di controllo per consentire agli utenti di accedere alle cartelle pubbliche. Gli utenti autorizzati ad accedere a tali cartelle e il livello di accesso accordato vengono specificati sotto ogni cartella in Gestione cartelle pubbliche 317. Deselezionare questa casella di controllo se si desidera nascondere le cartelle pubbliche a tutti gli utenti.

Stringa prefisso cartella pubblica IMAP (es: 'Public/')
Le cartelle pubbliche sono precedute da una sequenza composta da un massimo di 20 caratteri, ad esempio "#" o "Cartelle pubbliche/". In questo modo, gli utenti possono distinguere facilmente le cartelle pubbliche da quelle private del client e-mail. Utilizzare questa casella di testo per specificare la serie di caratteri da usare per contrassegnare le cartelle pubbliche.

Crea cartelle Contatti, Calendario, Attività, Diario e note per tutti i domini
Fare clic su questa casella di controllo se si desidera garantire che le cartelle esistano per tutti i domini. Le cartelle vengono create ogni qualvolta si aggiunge a MDaemon un Dominio 185.

Mantieni cartelle di contatti aggiornate con i dati degli account MDaemon
Se questa opzione è selezionata, MDaemon manterrà le cartelle dei contatti sincronizzate con l'elenco degli account.

Aggiungi e rimuovi contatti quando gli account vengono attivati/disattivati
Per impostazione predefinita, quando si disattiva un account, l'account verrà rimosso dalla cartella pubblica dei contatti del dominio. Quindi, se si riattiva l'account, questo verrà aggiunto nuovamente ai contatti. Questa opzione è attivata per impostazione predefinita per evitare che gli account disattivati siano visualizzati nel sistema di completamento automatico di Webmail.

Elimina cartelle pubbliche di dominio quando il dominio viene eliminato
Fare clic su questa casella di controllo se si desidera eliminare le cartelle pubbliche del dominio quando il dominio viene eliminato.

Abilita cartelle condivise

Fare clic su questa casella di controllo per consentire agli utenti IMAP di condividere l'accesso alle proprie cartelle IMAP. Gli utenti autorizzati ad accedervi e il livello di accesso accordato vengono specificati in base a ogni cartella nella schermata Cartelle condivise 757 di Account Editor, disponibile in Account » Account Manager » [Account utente] » Cartelle condivise. Deselezionare questa casella di controllo se si desidera impedire agli utenti la condivisione dell'accesso alle proprie cartelle e la visualizzazione della schermata Cartelle condivise in Account Editor.

Quando si utilizza MDaemon Connector 395, questa opzione non sarà disponibile. Non è possibile disattivarla poiché, per il corretto funzionamento di MDaemon Connector, è necessaria la condivisione delle cartelle utente.

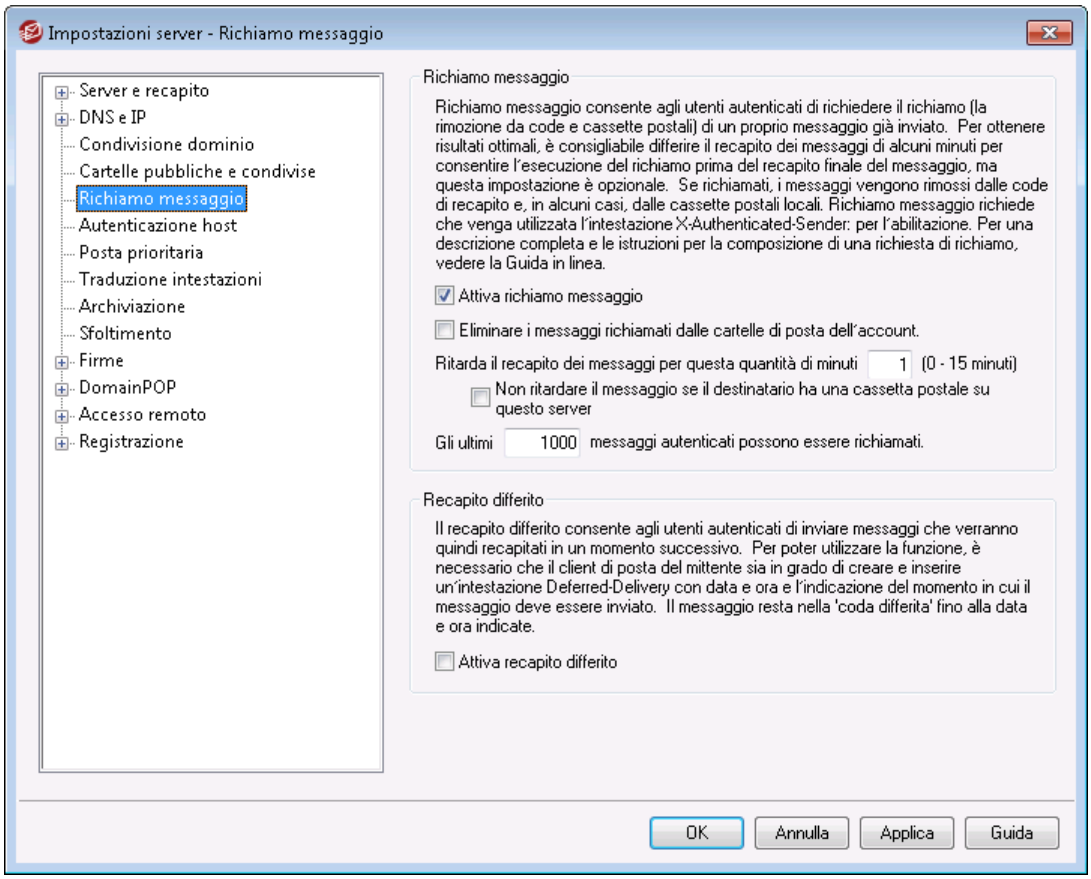
Stringa prefisso cartella IMAP condivisa (es: 'Shared/')
Le cartelle pubbliche sono precedute da una sequenza composta da un massimo di 20 caratteri, ad esempio "Cartelle pubbliche/". In questo modo, gli utenti possono distinguere facilmente le cartelle condivise da quelle private del client e-mail. Utilizzare questa casella di testo per specificare la serie di caratteri da usare per contrassegnare le cartelle utente condivise.

Disattiva accesso alle cartelle condivise quando l'account viene disattivato
Per impostazione predefinita i server IMAP, WebMail e ActiveSync di MDaemon non forniscono l'accesso alle cartelle condivise degli account disattivati. Deselezionare questa casella di controllo se si desidera consentire l'accesso alle cartelle condivise dell'account anche quando un account è disattivato.

Vedere:

Panoramica sulle cartelle pubbliche 120
Gestione cartelle pubbliche 317
Elenco controllo accessi 319
Account Editor » Cartelle condivise 757
Lista distribuzione » Cartelle pubbliche 306

3.1.5 Richiamo messaggio



Sistema di richiamo dei messaggi

MDaemon offre un sistema di richiamo dei messaggi che è possibile utilizzare per ritardare i messaggi in arrivo inviati da utenti locali autenticati per un periodo che va da 0 a 15 minuti, per offrire agli utenti un breve periodo di tempo durante il quale possono tentare di interrompere il recapito di un messaggio. Durante tale periodo i messaggi vengono inseriti in una coda Differiti dedicata invece di passare direttamente alla coda della posta In ingresso. I messaggi nella coda Differiti hanno la data per la quale sono impostati per lasciare la coda codificata nel nome file. MDaemon controlla la coda una volta al minuto e quando è il momento che il messaggio lasci la coda, questo viene spostato nella coda In ingresso ed è soggetto alle normali operazioni di elaborazione e

recapito dei messaggi. L'attività viene registrata nella scheda Instradamento e nel file di registro.

È possibile impostare il tempo di ritardo su "0" se si desidera, ma questo aumenta la possibilità che un messaggio che l'utente desidera richiamare possa essere già stato recapitato. Pertanto si consiglia un ritardo di almeno 1 o 2 minuti per dare agli utenti il tempo necessario per decidere di richiamare un messaggio, inviare la richiesta di richiamo e lasciare abbastanza tempo a MDaemon per elaborare la richiesta. Tuttavia, poiché MDaemon è in grado di rimuovere i messaggi richiamati dalla coda remota, nella quale può già essere stato applicato un ritardo, alcuni amministratori potrebbero considerare questo ritardo di recapito non necessario.

Richiamo di un messaggio

È possibile richiamare un messaggio in diversi modi.

1. In MDaemon Webmail, fare clic sul pulsante Richiama visualizzato quando si visualizzano i messaggi inviati di recente nella cartella Posta inviata. Se si fa clic sul pulsante prima che scada il limite di tempo impostato per il richiamo, Webmail invierà un messaggio RECALL a MDaemon.
2. Inviare un messaggio all'account di sistema mdaemon@example.com, con la parola word "RECALL" (senza le virgolette) come oggetto del messaggio. In questo modo è possibile richiamare l'ultimo messaggio inviato. Ma verrà richiamato solo l'ultimo messaggio inviato.
3. Nella cartella Posta inviata, individuare il messaggio che si desidera richiamare, selezionare l'opzione "Inoltra come allegato" e inviare il messaggio all'account di sistema mdaemon@example.com utilizzando "RECALL" come oggetto del messaggio.
4. Visualizzare le intestazioni di un messaggio, copiare l'intestazione "Message-ID: <message-ID value>" e creare un nuovo messaggio con "RECALL Message-ID: <message-ID value>" nell'oggetto (senza le virgolette).

Indipendentemente dal metodo scelto per il richiamo, MDaemon invia un messaggio di e-mail all'utente con indicazioni sulla riuscita o meno del richiamo. Quando un messaggio viene richiamato correttamente, MDaemon elimina il messaggio dalla coda, come se non fosse mai stato inviato. Inoltre, se è attivata l'opzione *Eliminare i messaggi richiamati dalle cartelle di posta dell'account*, MDaemon tenterà anche di eliminare il messaggio richiamato dalle cartelle di posta locali dell'utente nelle quali potrebbe essere già stato recapitato. I messaggi inviati a più destinatari saranno tutti richiamati mediante una singola richiesta. Infine, il sistema di Richiamo messaggi non funziona senza l'intestazione `X-Authenticated-Sender` per garantire la sicurezza e per impedire agli utenti di richiamare messaggi generati da altri. Pertanto, l'opzione per disabilitare l'intestazione 506 sarà ignorata se è attivato il richiamo dei messaggi.

Richiamo messaggio

Attiva richiamo messaggio
Selezionare questa casella di controllo per attivare il sistema di richiamo dei messaggi. L'opzione è disabilitata per impostazione predefinita.

Eliminare i messaggi richiamati dalle cartelle di posta dell'account
Selezionare questa casella di controllo se si desidera eliminare i messaggi richiamati anche dalle cartelle di posta degli account MDaemon locali qualora siano già stati recapitati prima di essere richiamati. Questo può far sì che i messaggi spariscano dai client di posta e dai telefoni degli utenti. L'opzione è disabilitata per impostazione predefinita.

Ritarda il recapito dei messaggi per questa quantità di minuti XX (0-15 minuti)
Il numero di minuti per cui MDaemon tratterrà i messaggi in arrivo inviati da utenti locali autenticati. Se viene ricevuto un messaggio RECALL durante il periodo di ritardo, MDaemon eliminerà il messaggio cui viene fatto riferimento prima che venga effettuato qualsiasi tentativo. L'opzione si può impostare su un valore compreso tra 0 e 15 minuti. 1 minuto è l'impostazione predefinita.

Non ritardare il messaggio se il destinatario ha una casella postale su questo server
Selezionare questa casella di controllo se non si desidera ritardare i messaggi quando la casella postale del destinatario si trova sullo stesso server MDaemon di quella del mittente. Nota: quando si utilizza l'opzione "*Eliminare i messaggi richiamati dalle cartelle di posta dell'account*" riportata sopra, è possibile richiamare dalla casella postale di un utente anche i messaggi già recapitati.

Gli ultimi [xx] messaggi autenticati possono essere richiamati
MDaemon ricorda gli ID e le posizioni dei messaggi di un numero specificato di e-mail più recenti inviate da utenti autenticati. I tentativi di richiamo non riusciranno se il messaggio da richiamare non è compreso in questo gruppo di messaggi. Pertanto quando si usa l'opzione *Eliminare i messaggi richiamati dalle cartelle di posta dell'account* riportata sopra, questo consente di richiamare i messaggi dalle caselle di posta degli utenti, anche quando sono già stati recapitati. Per impostazione predefinita, questa opzione è configurata su 1000 messaggi.

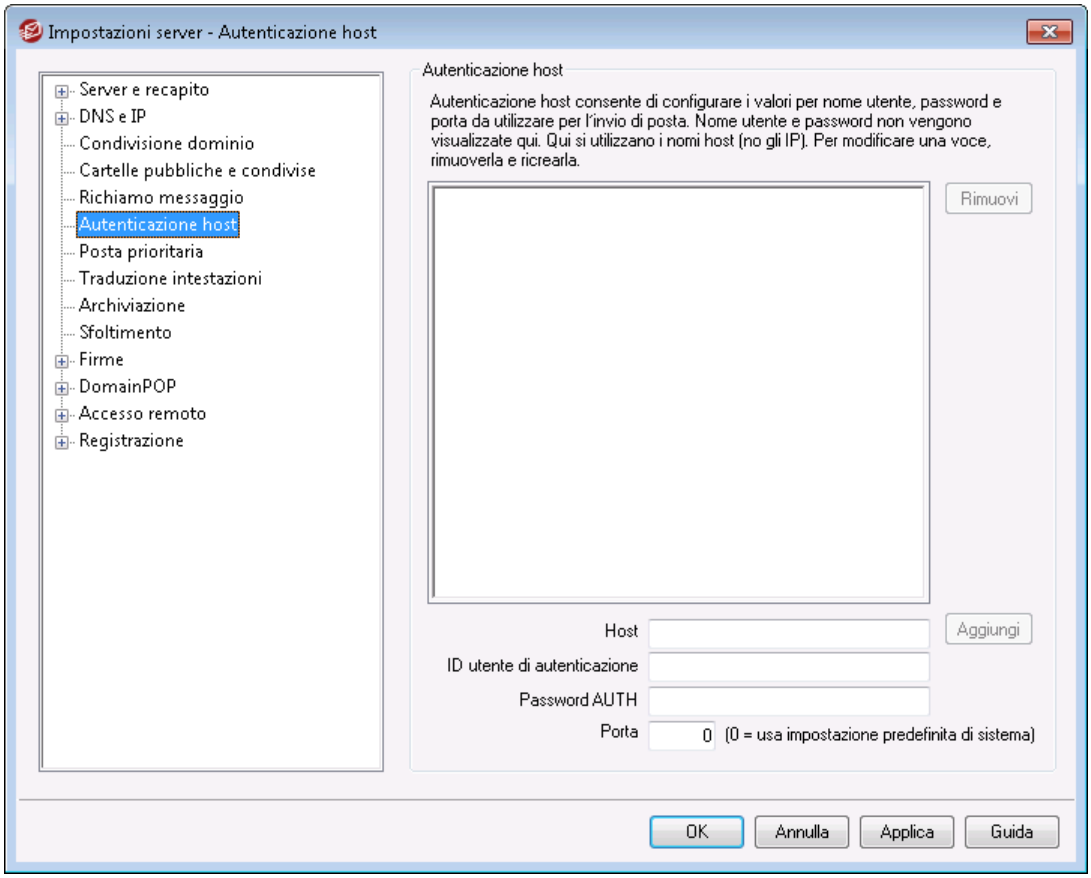
Recapito differito

L'opzione Recapito differito consente ai client autenticati di inviare messaggi che saranno consegnati in una data e ora pianificati. Webmail include questa opzione, consentendo agli utenti di fare clic su "Invia più tardi" e di specificare la data e l'ora di invio del messaggio. Il messaggio include l'intestazione `Deferred-Delivery` contenente la data e l'ora in cui tentare il recapito del messaggio. Se l'opzione Richiamo messaggio è attivata e si riceve la richiesta di richiamo di un messaggio pianificato per recapito differito, MDaemon tenterà di rimuovere il messaggio richiamato.

Attiva recapito differito
Attivare questa opzione se si desidera consentire ai client autenticati di utilizzare l'intestazione `Deferred-Delivery` per pianificare messaggi per recapito differito. Quando è selezionata questa opzione, per gli utenti di Webmail sarà disponibile l'opzione **Invia in seguito** nei temi WorldClient e Lookout. L'opzione è disabilitata per impostazione predefinita.

Sostituisci "Date:" con l'ora corrente al rilascio del messaggio
Attivare questa opzione se si desidera sostituire l'intestazione "Date:" con la data e l'ora correnti al momento del rilascio del messaggio dalla Coda differita. È disabilitata per impostazione predefinita.

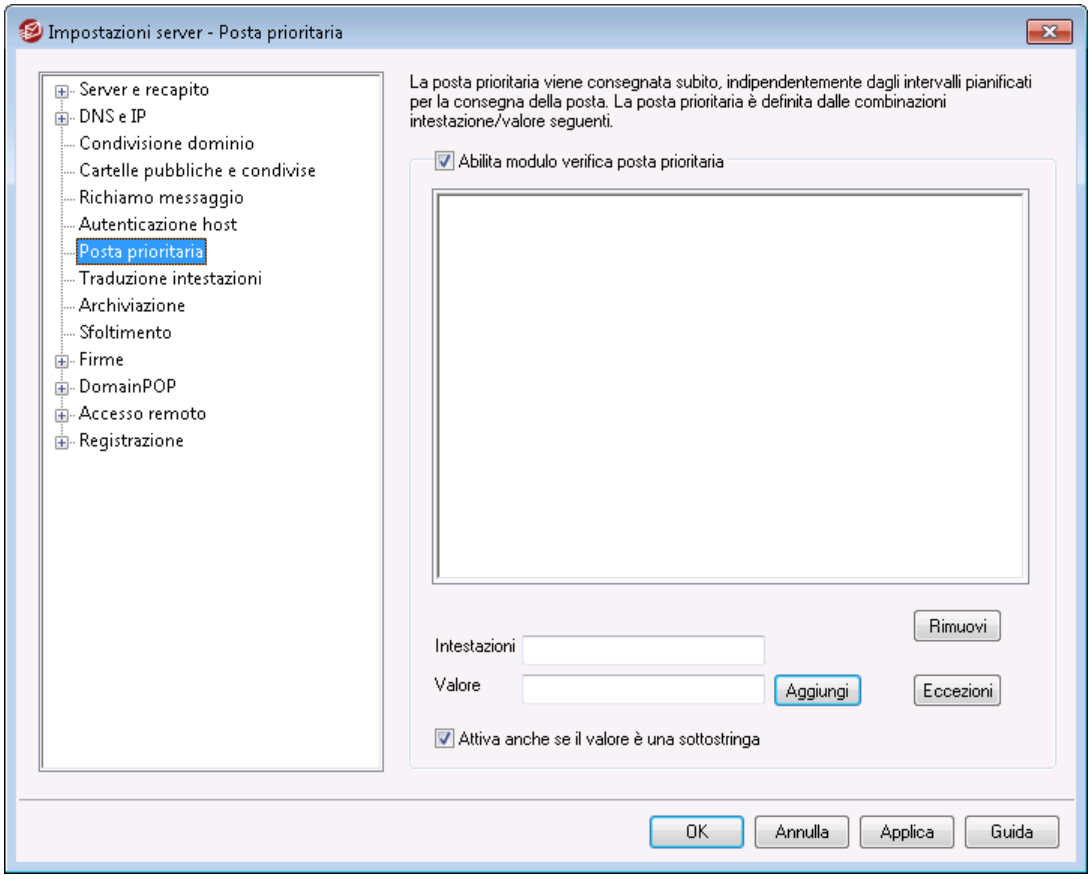
3.1.6 Autenticazione host



Autenticazione host

Utilizzare questa schermata per configurare i valori per nome utente, password e porta per qualsiasi host. Quando MDaemon invia posta SMTP all'host verranno utilizzate le credenziali associate specificate in questa posizione. Si noti che queste credenziali sono un'alternativa e sono utilizzate solo quando altre credenziali più specifiche dell'attività non sono disponibili. Ad esempio, se si configurano impostazioni di accesso e password per le opzioni di inoltro di Account Editor o le opzioni di rimozione dalla coda di Gateway Manager o una delle molte altre impostazioni specifiche delle attività, verranno utilizzate le relative credenziali, andando a sovrascrivere quanto configurato in questa posizione. Questa funzione è utilizzabile solo con i nomi degli host e non con gli indirizzi IP.

3.1.7 Posta prioritaria



Per accedere alla schermata Posta prioritaria, selezionare "Impostazioni » Impostazioni Server » Posta prioritaria". Questa schermata consente di definire le caratteristiche della posta prioritaria nel sistema. La posta prioritaria viene immediatamente consegnata da MDaemon, indipendentemente dagli intervalli pianificati per l'elaborazione della posta. All'arrivo di un nuovo messaggio, MDaemon lo analizza per confrontarne le intestazioni con le varie combinazioni intestazione/valore specificate in questa finestra di dialogo. Se riscontra una corrispondenza, MDaemon considera il messaggio come missiva di elevata priorità e tenta di consegnarlo immediatamente.

Posta prioritaria

Abilita modulo verifica posta prioritaria
Selezionare questa casella di controllo per abilitare la funzione Posta prioritaria. MDaemon verificherà lo stato di priorità dei messaggi in entrata.

Intestazione
Immettere in questo campo l'intestazione del messaggio. Non includere il carattere finale di due punti (:).

Valore
Immettere in questo campo il valore da ricercare nell'intestazione specificata che, se presente, attribuisce al messaggio una priorità elevata.

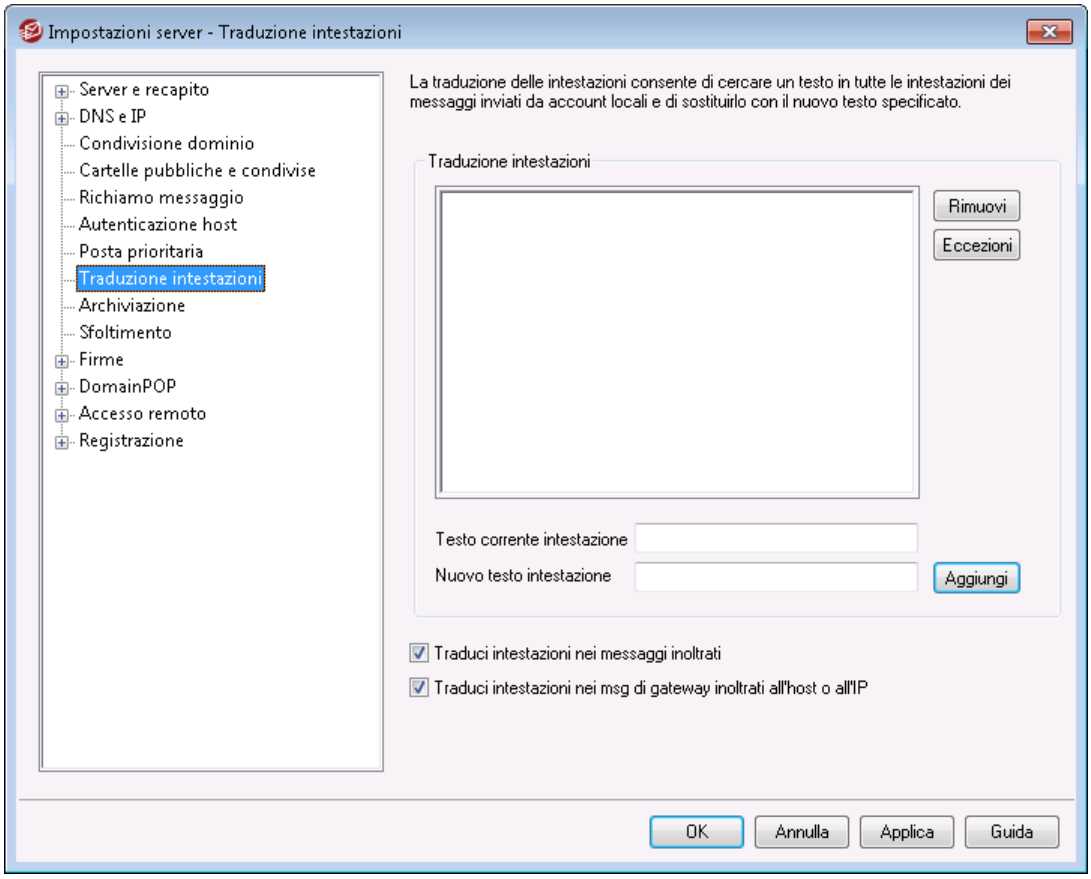
Attiva anche se il valore è una sottostringa
Quando si immette una nuova impostazione relativa al livello di priorità della posta, è possibile selezionare questa funzione per verificare anche una porzione (o sottostringa) del valore di un'intestazione. Ad esempio, si supponga di avere creato un'impostazione di posta prioritaria in cui l'intestazione "`To`" è associata al valore "`Boss`". Tutta la posta contenente "`Boss@qualunquedominio`" nell'intestazione verrà considerata posta prioritaria. Se questa funzione non è abilitata, il valore dell'intestazione deve corrispondere esattamente al valore specificato nel campo: la corrispondenza di una porzione non è sufficiente.

Aggiungi
Una volta immesse le informazioni intestazione/valore nelle caselle di testo specificate e indicato se tali informazioni devono essere valide anche per le sottostringhe, fare clic su *Aggiungi* per creare la nuova voce di posta prioritaria.

Rimuovi
Fare clic su questo pulsante per rimuovere una voce selezionata dalla finestra *Intestazione/valore per posta prioritaria*.

Eccezioni
Questo pulsante consente di definire combinazioni intestazione/valore in base alle quali un messaggio verrà considerato come un'eccezione alle impostazioni di posta prioritaria. La funzione può quindi essere adattata alle più svariate situazioni.

3.1.8 Traduzione intestazioni



La funzione Traduzione intestazione consente di modificare qualsiasi porzione del testo dell'intestazione di un messaggio in uscita dal dominio verso un host remoto. È sufficiente specificare il testo da ricercare e il valore corrispondente con cui sostituirlo. MDaemon ricerca il testo in tutte le intestazioni dei messaggi e ne sostituisce ogni occorrenza con il valore specificato. È inoltre possibile specificare le intestazioni che **non** devono essere modificate (ad esempio, "Subject:" o "Received:"). A tale scopo, fare clic sul pulsante *Eccezioni* della finestra di dialogo.

Questa funzione è necessaria per alcune configurazioni di MDaemon in cui il nome dominio locale è fittizio o diverso da quello che deve figurare nella posta in uscita. In tali situazioni, la funzione Traduzione intestazione può essere efficacemente utilizzata per modificare ogni occorrenza di "`@dominiolocale`" in "`@dominioremoto`".

Traduzione intestazioni

In questo elenco sono contenute le porzioni di testo da ricercare nelle intestazioni dei messaggi in uscita, nonché il testo che sostituirà la porzione eventualmente rilevata.

Rimuovi
Selezionare una voce nell'elenco Traduzione intestazioni, quindi fare clic su questo pulsante per rimuoverla.

Eccezioni
Fare clic su questo pulsante per aprire la finestra di dialogo Eccezioni alla traduzione intestazioni 131 e specificare le intestazioni da escludere dal processo di traduzione.

Testo corrente intestazione
Immettere il testo da sostituire nelle intestazioni dei messaggi in uscita.

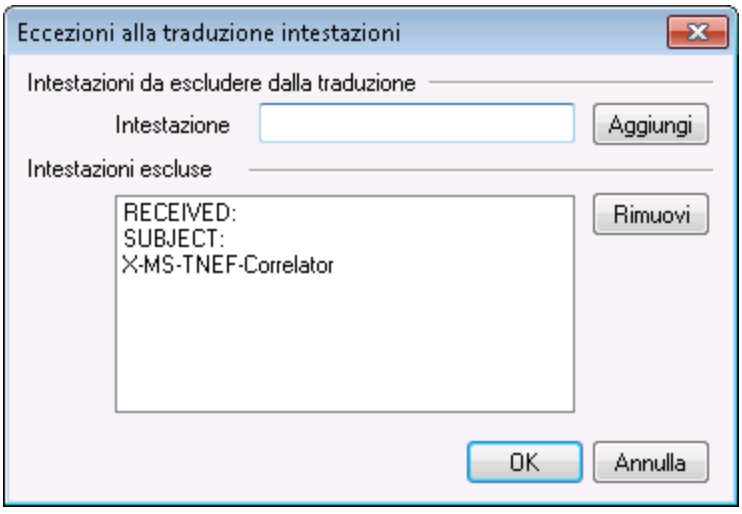
Nuovo testo intestazione
Questo testo sostituisce quello specificato nel campo *Testo corrente intestazione*.

Aggiungi
Fare clic su questo pulsante per aggiungere i nuovi parametri all'elenco *Traduzione intestazioni*.

Traduci intestazioni nei messaggi inoltrati
Selezionare questa casella di controllo per eseguire le traduzioni delle intestazioni anche per i messaggi automaticamente inoltrati da un dominio locale a un dominio esterno.

Traduci intestazioni nei msg di gateway inoltrati all'host o all'IP
Selezionare questa casella di controllo se si desidera che le intestazioni vengano convertite nei messaggi inoltrati sul gateway di dominio. Per ulteriori informazioni, vedere la schermata Inoltro 268 di Gateway Editor.

3.1.8.1 Eccezioni alla traduzione intestazioni



Intestazioni da escludere dalla traduzione

Intestazione
Immettere l'intestazione da escludere dal processo di traduzione delle intestazioni 130.

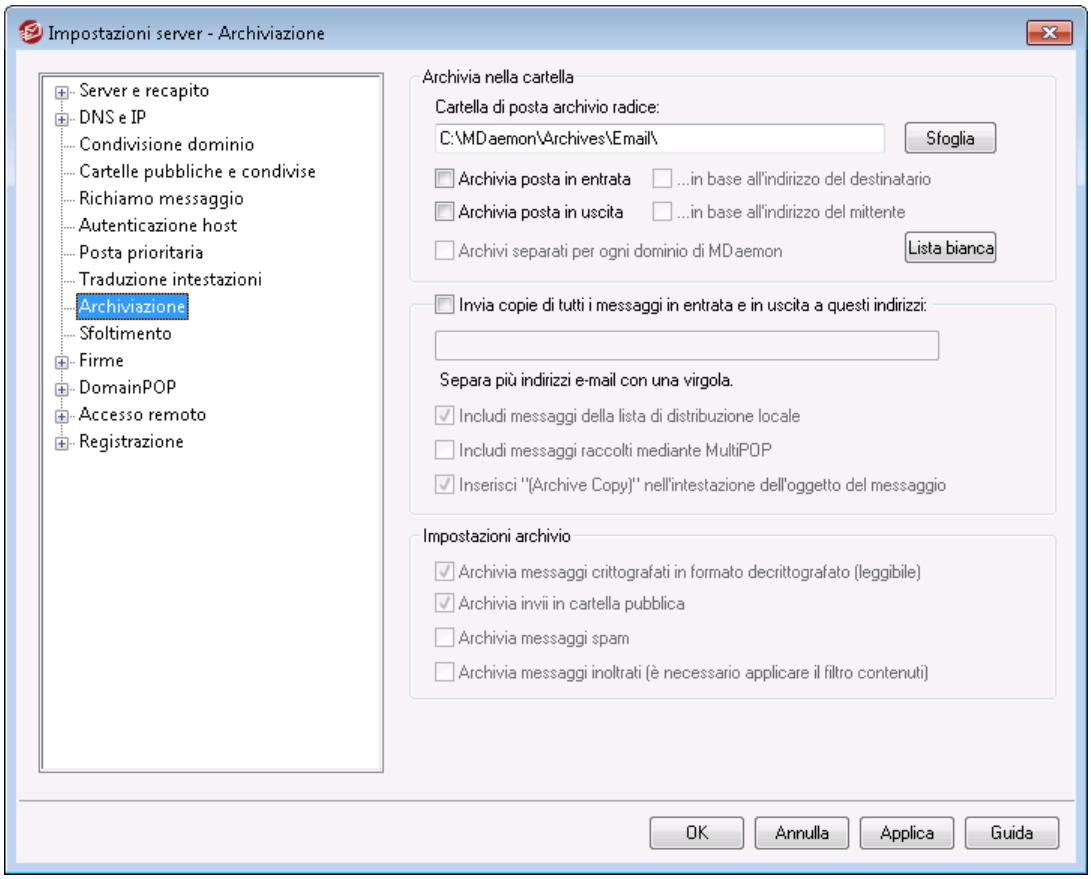
Aggiungi
Fare clic su questo pulsante per aggiungere una nuova intestazione all'elenco.

Intestazioni escluse

Le intestazioni indicate verranno escluse dalla ricerca e dalla sostituzione del testo.

Rimuovi
Selezionare un'intestazione nell'elenco, quindi fare clic su questo pulsante per rimuoverla.

3.1.9 Archiviazione



Utilizzare questa funzione per archiviare i messaggi in entrata e in uscita in una cartella. La posizione predefinita della cartella è `C:\MDaemon\Archives\Email\`, ma è possibile impostarla in una qualsiasi cartella a scelta. È possibile scegliere di archiviare i messaggi in ingresso indirizzati agli utenti locali, i messaggi in uscita dagli utenti locali o entrambi i tipi di messaggi. Il traffico delle liste di distribuzione, i messaggi in corso di trasmissione, i messaggi a livello di sistema e le risposte automatiche non sono mai archiviati. Non vengono archiviati nemmeno i messaggi spam o quelli contenenti virus.

I messaggi in entrata e in uscita verranno memorizzati nelle sottocartelle `\In\` e `\Out\`, rispettivamente. Possono inoltre essere suddivisi utilizzando le opzioni riportate di seguito relative all'*...archivio in base all'indirizzo del destinatario* e all'*...archivio in base all'indirizzo del mittente* . È anche possibile gestire gli indirizzi separati per ciascun dominio utilizzando l'opzione *Archivi separati per ogni dominio di MDaemon*.

I messaggi archiviati sono salvati nello stato finale in cui vengono visualizzati nella cartella della posta dell'utente locale oppure nello stato "pronti per la consegna" se si tratta di messaggi in uscita. Ciò indica che, ad esempio, se sono presenti modifiche del Filtro contenuti apportate a un messaggio, quali un'aggiunta di intestazione, il messaggio archiviato conterrà tale modifica.

Per sfogliare la cartella archivio utilizzare uno degli account di posta (o crearne uno nuovo) e indirizzare la Cartella della posta 732 nella stessa cartella utilizzata per l'archivio. Se più persone necessitano dell'accesso all'archivio, accedere all'account dell'archivio e condividere 757 le cartelle desiderate utilizzando l'Elenco controllo accessi 319.

Esiste una coda di sistema nascosta in: "`\MDaemon\Queues\ToArchive\`". Questa coda viene controllata a intervalli regolari in relazione ai messaggi inseriti (manualmente, da un plugin o in altro modo). Quando un messaggio viene trovato in questa coda, viene immediatamente archiviato ed eliminato. I messaggi non idonei all'archiviazione vengono semplicemente eliminati. La schermata o il registro Instradamento mostreranno i dettagli ogni volta che un messaggio viene archiviato correttamente.

Archivia in cartella

Specificare qui la cartella della posta in archivio. L'impostazione predefinita è `C:\MDaemon\Archives\Email\`, ma è possibile impostarla in una qualsiasi cartella a scelta.

Archivia posta in entrata
Selezionare questa casella di controllo per salvare una copia di tutti i messaggi diretti a un utente locale. I messaggi delle liste di distribuzione e quelli contenenti virus non vengono archiviati.

...in base all'indirizzo del destinatario
Selezionare questa opzione per organizzare l'archivio della posta in entrata in base all'indirizzo e-mail del destinatario.

Archivia posta in uscita
Selezionare questa casella di controllo per salvare una copia di tutti i messaggi provenienti da un utente locale. I messaggi delle liste di distribuzione e quelli contenenti virus non vengono archiviati.

...in base all'indirizzo del mittente
Selezionare questa opzione per organizzare l'archivio della posta in uscita in base all'indirizzo e-mail del mittente.

Archivi separati per ogni dominio di MDaemon
Selezionare questa casella di controllo per disporre di un archivio separato per ogni dominio.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'Elenco esenzioni archiviazione. Qui è possibile elencare gli indirizzi "a" e "da" che si desidera escludere dall'archiviazione.

Invia copie di tutti i messaggi in entrata e in uscita a questi indirizzi

Inserire gli indirizzi ai quali inviare i messaggi da archiviare separandoli con una virgola. È possibile specificare indirizzi locali e remoti, nonché alias.

Includi messaggi della lista di distribuzione locale
Quando questa opzione è attivata, verranno inviate agli indirizzi anche copie dei messaggi della lista di distribuzione locale.

Includi messaggi raccolti mediante MultiPOP
Attivare questa opzione se si desidera inviare i messaggi raccolti mediante la funzione MultiPOP 754 di MDaemon.

Inserisci "(Archive Copy)" nell'intestazione dell'oggetto del messaggio
Quando questa opzione è attivata, viene inserito "(Copia di archiviazione)" nell'intestazione `Oggetto:` dei messaggi inviati.

Impostazioni archivio

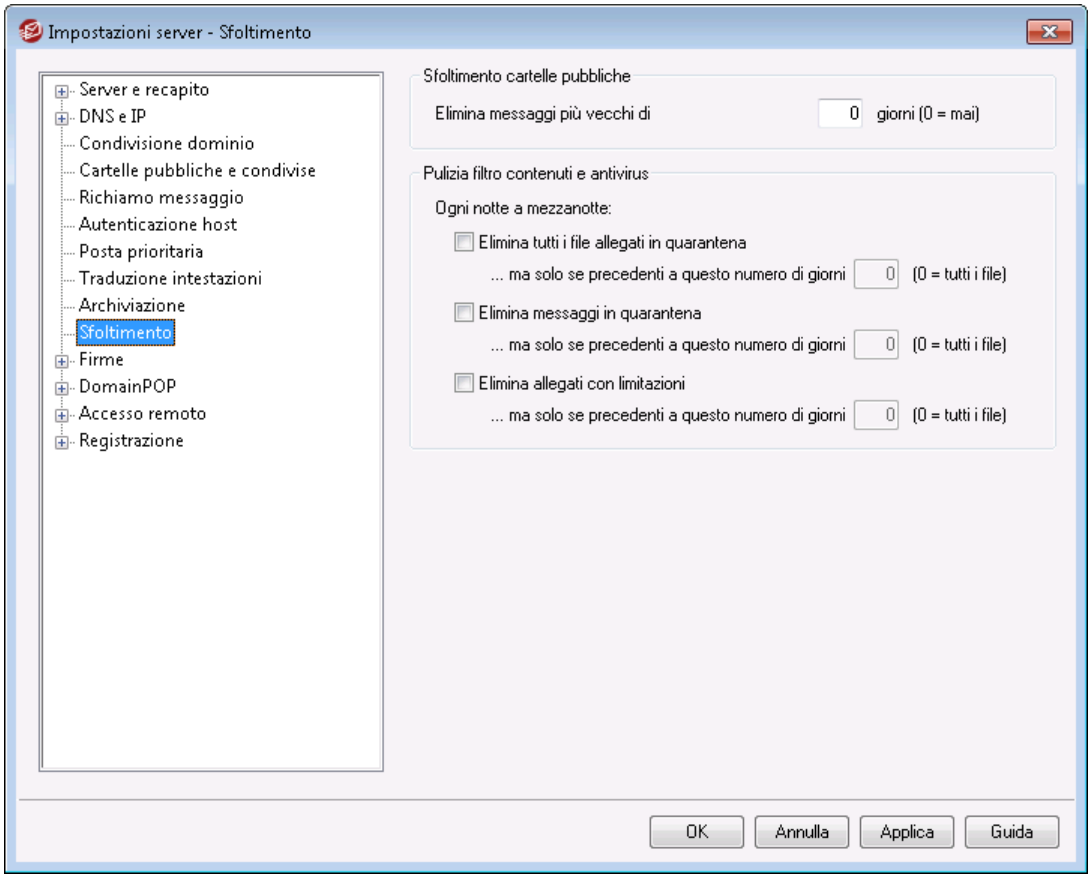
Archivia messaggi crittografati in formato decrittografato (leggibile)
Per impostazione predefinita nell'archivio vengono memorizzate copie non crittografate dei messaggi crittografati. Se tuttavia un messaggio non può essere decrittografato, verrà invece memorizzato il formato crittografato. Disattivare questa opzione se si preferisce memorizzare versioni crittografate anche quando è possibile la decrittografia.

Archivia invii in cartella pubblica
Per impostazione predefinita, i messaggi inviati agli indirizzi di invio delle cartelle pubbliche vengono archiviati. Disattivare questa opzione se non si desidera archiviare questi messaggi.

Archivia messaggi spam
Attivare questa opzione se si desidera che gli archivi e le copie dei messaggi inviati includano i messaggi contrassegnati come spam.

Archivia messaggi inoltrati (è necessario applicare il filtro contenuti)
Attivare questa opzione se si desidera che gli archivi e le copie dei messaggi inviati includano i messaggi inoltrati, che per impostazione predefinita, non vengono archiviati.

3.1.10 Sfoltimento



Sfoltimento cartelle pubbliche

Elimina i messaggi più vecchi di XX giorni (0 = mai)
Specificare il numero di giorni in questo campo se si desidera che i vecchi messaggi vengano eliminati da Cartelle pubbliche 120.

Pulizia filtro contenuti e antivirus

Elimina file in quarantena
Selezionare questa opzione se si desidera che ogni notte vengano eliminati gli allegati in quarantena.

... ma solo se precedenti a questo numero di giorni [xx] (0 = tutti i file)
Per impostazione predefinita saranno eliminati tutti i file in quarantena. Specificare un numero di giorni in quest'opzione se si desidera solo eliminare i file precedenti a quel numero di giorni.

Elimina messaggi in quarantena
Selezionare questa opzione se si desidera che ogni notte vengano eliminati i messaggi in quarantena.

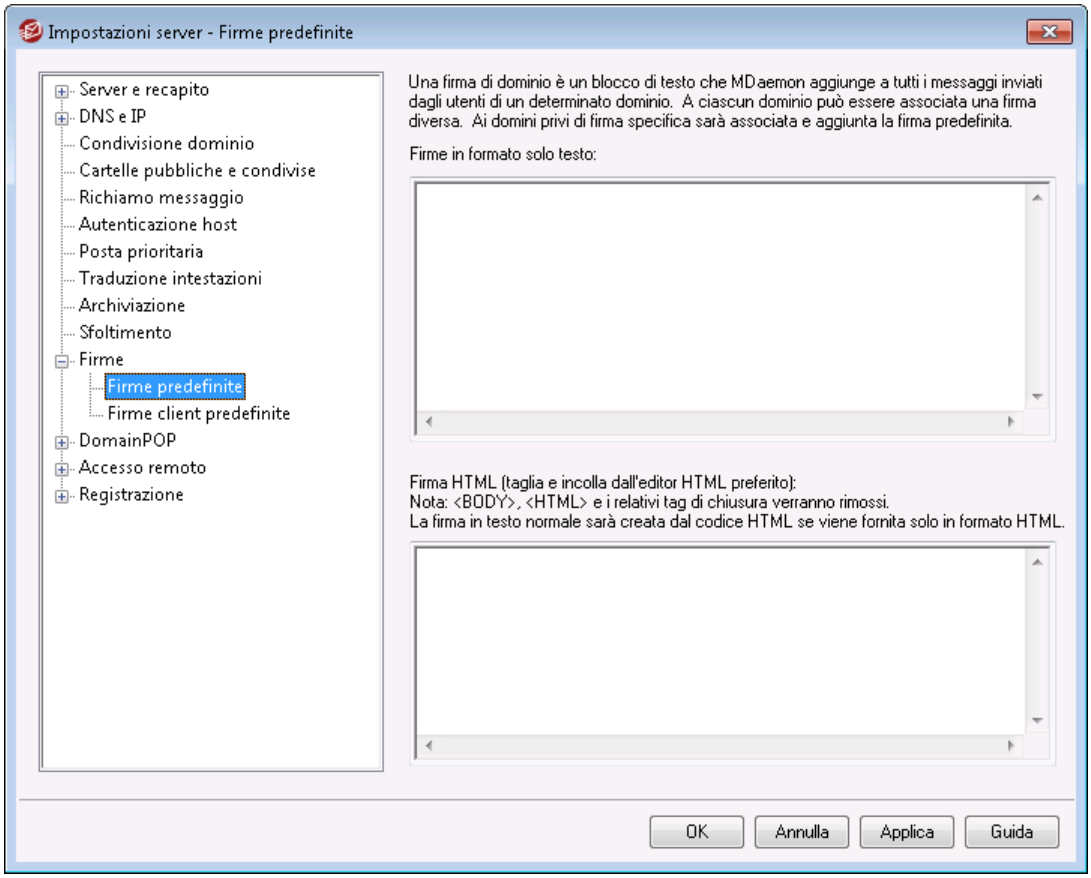
... ma solo se precedenti a questo numero di giorni [xx] (0 = tutti i file)
Per impostazione predefinita saranno eliminati tutti i messaggi in quarantena. Specificare un numero di giorni in quest'opzione se si desidera solo eliminare i messaggi precedenti a quel numero di giorni.

Elimina allegati con limitazioni
Selezionare questa opzione se si desidera che ogni notte vengano eliminati gli allegati con restrizioni.

... ma solo se precedenti a questo numero di giorni [xx] (0 = tutti i file)
Per impostazione predefinita saranno eliminati tutti gli allegati con restrizioni. Specificare un numero di giorni in quest'opzione se si desidera solo eliminare gli allegati con restrizioni precedenti a quel numero di giorni.

3.1.11 Firme

3.1.11.1 Firme predefinite



Utilizzare questa schermata per aggiungere una firma a tutti i messaggi inviati dagli utenti MDaemon. Utilizzare la schermata Firme 206 in Gestione domini se si desidera utilizzare firme diverse per utenti di domini specifici; qualora sia disponibile una firma specifica del dominio, verrà utilizzata al posto di quella predefinita. Le firme vengono aggiunte in fondo ai messaggi, ad eccezione dei messaggi delle liste di distribuzione che utilizzano il piè di pagina 304; in tal caso, il piè di pagina viene aggiunto al di sotto della

firma. Per aggiungere singole firme per ogni account è inoltre possibile utilizzare la funzione Firma[769] di Account Editor. Le firme dell'account vengono aggiunte prima di quelle del dominio o predefinite.

Firme in formato solo testo

Quest'area è destinata all'inserimento di una firma in formato solo testo. Per indicare una firma html corrispondente da utilizzare nella parte testo html dei messaggi multipart, utilizzare l'area *Firma HTML*. Se una firma è inclusa in entrambe le posizioni, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non viene specificata alcuna firma html, in entrambe le parti viene utilizzata la firma in formato solo testo.

Firma HTML (copiare e incollare la firma dall'editor HTML desiderato)

Quest'area è destinata all'inserimento di una firma html da utilizzare nella parte testo/html dei messaggi multipart. Se viene inclusa una firma qui e nel campo *Firme in formato solo testo* riportato sopra, MDaemon utilizzerà quella appropriata per ciascuna parte del messaggio multipart. Se non è specificata una firma in formato solo testo, verrà utilizzato il formato HTML per crearne una.

Per creare la firma html, digitare il codice HTML manualmente o tagliarlo e incollarlo direttamente dall'editor HTML desiderato. Per includere le immagini in linea nella firma HTML, è possibile utilizzare la macro `$ATTACH_INLINE:path_to_image_file$`.

Ad esempio,

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

È inoltre possibile utilizzare diversi metodi per inserire immagini in linea nelle firme dall'interfaccia Web di MDaemon Remote Administration[359]:

- Nella schermata Firme predefinite in Remote Administration, fare clic sul pulsante della barra degli strumenti "Immagine" nell'editor HTML e selezionare la scheda di caricamento.
- Nella schermata Firme predefinite in Remote Administration, fare clic sul pulsante della barra degli strumenti "Aggiungi immagine" nell'editor HTML.
- Trascinare un'immagine nella Schermata Firme predefinite dell'editor HTML con Chrome, FireFox, Safari o MSIE 10+
- Copiare e incollare un'immagine dagli Appunti nella schermata Firme predefinite dell'editor HTML con Chrome, FireFox, MSIE 11+

I tag <body></body> e <html></html> non sono consentiti nelle firme e saranno rimossi se trovati.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. `Ad esempio, $CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e `$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**

ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**
Numeri di telefono e fax	
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**

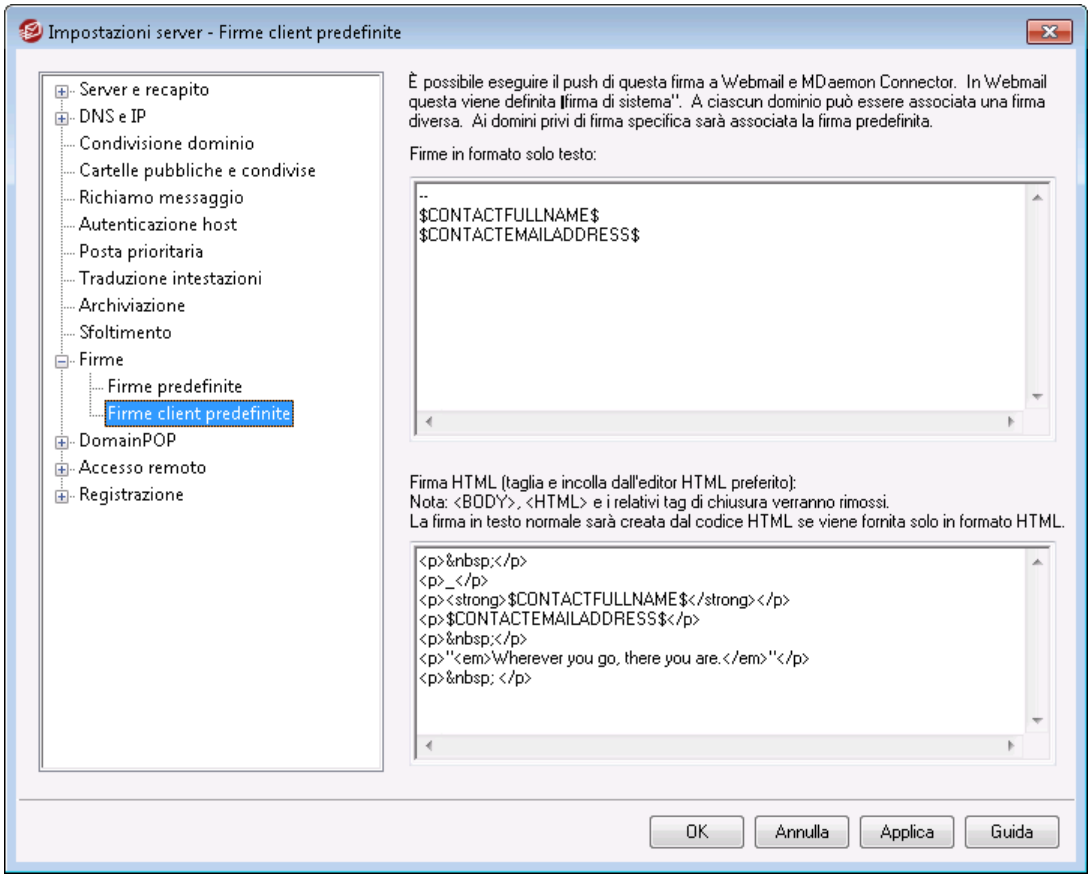
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**
Mansione lavorativa	**$CONTACTBUSINESSTITLE$**
Ufficio	**$CONTACTBUSINESSOFFICE$**
Reparto dell'azienda	**$CONTACTBUSINESSDEPARTMENT$**
Responsabile dell'azienda	**$CONTACTBUSINESSMANAGER$**
Assistente in azienda	**$CONTACTBUSINESSASSISTANT$**
Telefono assistente in azienda	**$CONTACTBUSINESSASSISTANTPHONE$**
Telefono principale dell'azienda	**$CONTACTBUSINESSMAINPHONE$**
Telefono al lavoro	**$CONTACTBUSINESSPHONE$**
Telefono al lavoro 2	**$CONTACTBUSINESSPHONE2$**
Telefono IP al lavoro	**$CONTACTBUSINESSIPPHONE$**
Fax di lavoro	**$CONTACTBUSINESSFAX$**
Cercapersone in azienda	**$CONTACTBUSINESSPAGER$**
Radiotelefono in azienda	**$CONTACTBUSINESSRADIO$**
Indirizzo di lavoro	**$CONTACTBUSINESSADDRESS$**
Città di lavoro	**$CONTACTBUSINESSCITY$**
Provincia di lavoro	**$CONTACTBUSINESSSTATE$**
CAP di lavoro	**$CONTACTBUSINESSZIPCODE$**
Paese di lavoro	**$CONTACTBUSINESSCOUNTRY$**
Indirizzo Web aziendale	**$CONTACTBUSINESSWEBADDRESS$**
Altro	
Coniuge	**$CONTACTSPOUSE$**

Figli	**$CONTACTCHILDREN$**
Categorie	**$CONTACTCATEGORIES$**
Commento	**$CONTACTCOMMENT$**

Vedere:

Gestione domini » Firme 206
Account Editor » Firma 769

3.1.11.2 Firme client predefinite



Utilizzare questa schermata per creare una firma client predefinita di cui è possibile eseguire il push in MDaemon Webmail 354 e in MDaemon Connector 413, per l'uso da parte degli utenti quando creano messaggi e-mail. È possibile utilizzare le macro 142 riportate di seguito per personalizzare la firma, in modo che sia unica per ciascun utente, includendo elementi come nome utente, indirizzo e-mail, numero di telefono e campi simili. Utilizzare la schermata Firme client 211 in Domain Manager se si desidera utilizzare una firma diversa per gli utenti di domini specifici. Quando esiste una firma specifica del dominio, verrà utilizzata al posto della firma client predefinita. Utilizzare l'opzione *Esegui push firma client* 354 se si desidera eseguire il push della firma client in Webmail e l'opzione *Estendi firma del client a Outlook* 413 se si desidera eseguire il push in MDaemon Connector. Nelle opzioni di composizione di Webmail, la firma client di cui si è

eseguito il push è denominata "Sistema". Per MDaemon Connector è possibile assegnare un nome alla firma che sarà visualizzata in Outlook.

Firme in formato solo testo

Quest'area è destinata all'inserimento di una firma in formato solo testo. Per indicare una firma html corrispondente da utilizzare nella parte testo/html dei messaggi multipart, utilizzare l'area *Firma HTML*. Se una firma è inclusa in entrambe le posizioni, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non viene specificata alcuna firma html, in entrambe le parti viene utilizzata la firma in formato solo testo.

Firma HTML (copiare e incollare la firma dall'editor HTML desiderato)

Quest'area è destinata all'inserimento di una firma html da utilizzare nella parte testo/html dei messaggi multipart. Se una firma è inclusa qui e nell'area *Firme in formato solo testo*, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non è specificata una firma in formato solo testo, verrà utilizzato il formato HTML per crearne una.

Per creare la firma html, digitare il codice HTML manualmente o tagliarlo e incollarlo direttamente dall'editor HTML desiderato. Per includere le immagini in linea nella firma HTML, è possibile utilizzare la macro `$ATTACH_INLINE:path_to_image_file$`.

Ad esempio,

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

È inoltre possibile utilizzare diversi metodi per inserire immagini in linea nelle firme dall'interfaccia Web di MDaemon Remote Administration 359:

- Nella schermata Firme client predefinite in Remote Administration, fare clic sul pulsante "Immagine" della barra degli strumenti nell'editor HTML e selezionare la scheda di caricamento.
- Nella schermata Firme client predefinite in Remote Administration, fare clic sul pulsante "Aggiungi immagine" della barra degli strumenti nell'editor HTML.
- Trascinare un'immagine nella schermata Firme client predefinite dell'editor HTML con Chrome, FireFox, Safari o MSIE 10+
- Copiare e incollare un'immagine dagli Appunti nella schermata Firme client predefinite dell'editor HTML con Chrome, FireFox, MSIE 11+

I tag <body></body> e <html></html> non sono consentiti nelle firme e saranno rimossi se trovati.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. `Ad esempio, $CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e `$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**

ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**
Numeri di telefono e fax	
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**

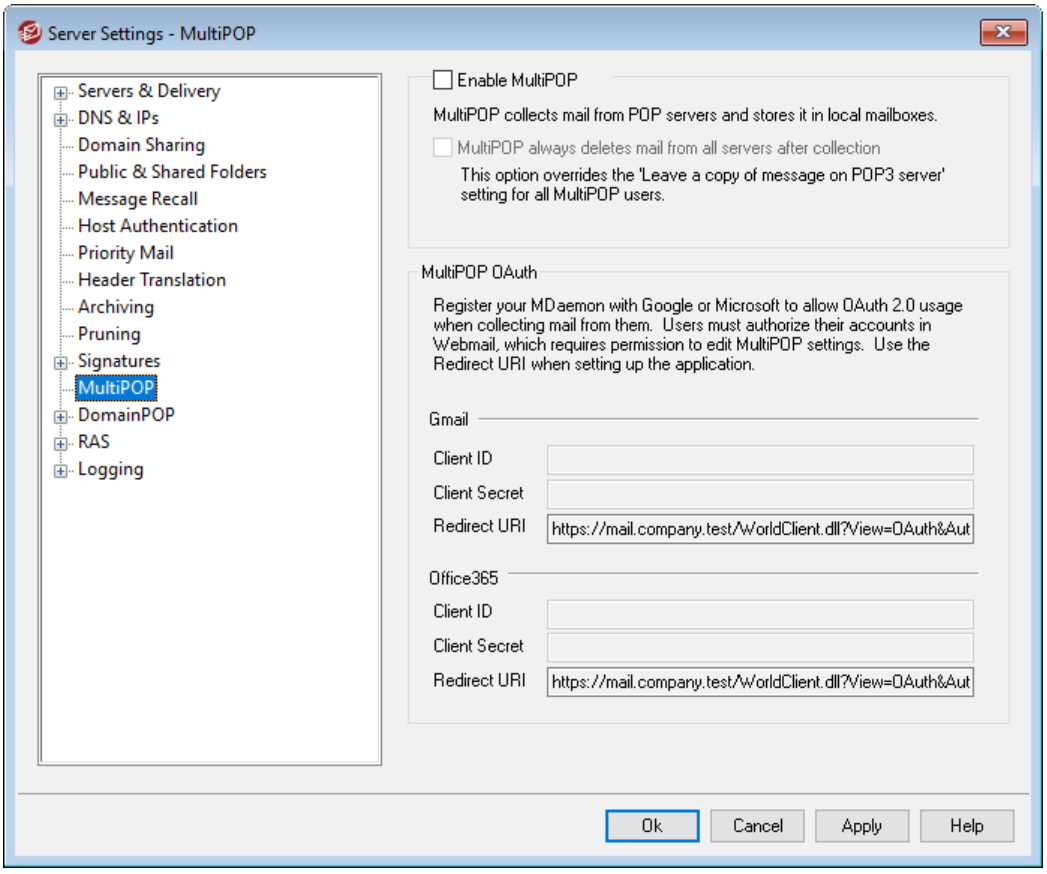
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**
Mansione lavorativa	**$CONTACTBUSINESSTITLE$**
Ufficio	**$CONTACTBUSINESSOFFICE$**
Reparto dell'azienda	**$CONTACTBUSINESSDEPARTMENT$**
Responsabile dell'azienda	**$CONTACTBUSINESSMANAGER$**
Assistente in azienda	**$CONTACTBUSINESSASSISTANT$**
Telefono assistente in azienda	**$CONTACTBUSINESSASSISTANTPHONE$**
Telefono principale dell'azienda	**$CONTACTBUSINESSMAINPHONE$**
Telefono al lavoro	**$CONTACTBUSINESSPHONE$**
Telefono al lavoro 2	**$CONTACTBUSINESSPHONE2$**
Telefono IP al lavoro	**$CONTACTBUSINESSIPPHONE$**
Fax di lavoro	**$CONTACTBUSINESSFAX$**
Cercapersone in azienda	**$CONTACTBUSINESSPAGER$**
Radiotelefono in azienda	**$CONTACTBUSINESSRADIO$**
Indirizzo di lavoro	**$CONTACTBUSINESSADDRESS$**
Città di lavoro	**$CONTACTBUSINESSCITY$**
Provincia di lavoro	**$CONTACTBUSINESSSTATE$**
CAP di lavoro	**$CONTACTBUSINESSZIPCODE$**
Paese di lavoro	**$CONTACTBUSINESSCOUNTRY$**
Indirizzo Web aziendale	**$CONTACTBUSINESSWEBADDRESS$**
Altro	
Coniuge	**$CONTACTSPOUSE$**

Figli	**$CONTACTCHILDREN$**
Categorie	**$CONTACTCATEGORIES$**
Commento	**$CONTACTCOMMENT$**

Vedere:

Firme predefinite 136
Domain Manager » Firme 206
Domain Manager » Firme client 211
Account Editor » Firma 769
Impostazioni di Webmail 354
Impostazioni client MC » Firma 413

3.1.12 MultiPOP



Abilita MultiPOP

Selezionare questa casella per abilitare il server MultiPOP. MultiPOP raccoglie la posta dai server POP per conto degli utenti e la archivia nelle rispettive cassette postali locali. La funzione MultiPOP consente di creare un numero illimitato di combinazioni host/utente/password POP3 per la raccolta di messaggi di posta provenienti da più

origini. Si tratta di uno strumento utile per gli utenti che dispongono di account di posta su più server ma preferiscono raccogliere tutta la posta in un'unica postazione. Prima di essere collocata nella casella postale dell'utente, la posta MultiPOP raccolta viene inserita nella coda di posta per l'elaborazione, analogamente a tutti i messaggi per cui sono stati applicati la risposta automatica e i filtri di contenuto. Le opzioni di pianificazione della funzione MultiPOP sono disponibili in: Impostazioni » Pianificazione eventi » Pianificazione della posta » Raccolta MultiPOP 391.

MultiPOP elimina sempre la posta da tutti i server dopo la raccolta
Selezionare questa casella di controllo per eseguire l'override dell'opzione *Lascia una copia del messaggio sul server POP* presente nella schermata MultiPOP 754 di Account Editor. Una volta raccolti, i messaggi verranno eliminati da ciascun server MultiPOP.

MultiPOP OAuth

OAuth 2.0 è un moderno metodo di autenticazione che Gmail e Microsoft (Office) 365 richiedono (o richiederanno presto) dopo la disabilitazione del supporto dell'autenticazione tradizionale/di base. Affinché la funzione MultiPOP di MDaemon utilizzi OAuth 2.0 per raccogliere la posta da Gmail o Office 365 per conto degli utenti, è necessario registrare il server MDaemon con Google o Microsoft, rispettivamente, creando un'app OAuth 2.0 con la Google API Console o con Azure Active Directory di Microsoft. Questa procedura è simile a quella richiesta per l'utilizzo dell'integrazione con Dropbox 345 di MDaemon per gli utenti Webmail.

Per configurare MultiPOP per la raccolta della posta da Gmail o Microsoft (Office) 365 per gli utenti:

1. Selezionare l'opzione **Abilita MultiPOP** sopra descritta.
2. Seguire le istruzioni riportate di seguito per la **Creazione e collegamento dell'app MultiPOP OAuth** 148 per Gmail o Office 365.
3. Nella pagina MultiPOP di Account Editor 754 selezionare **Abilita MultiPOP** per tutti gli utenti che si desidera autorizzare all'utilizzo di MultiPOP per il recupero dei messaggi e-mail da Gmail o Office 365.
4. Aggiungere l'account Gmail (`pop.gmail.com:995`) o Office 365 (`outlook.office365.com:995`) per ciascuno degli utenti, quindi selezionare l'opzione **Utilizza OAuth**. Facoltativamente, si può chiedere agli utenti di eseguire questa operazione da soli in Webmail 325. **Nota:** per gli account Gmail, tutti gli account Gmail devono essere aggiunti agli utenti di test nell'app OAuth di Gmail (vedere la nota **Stato della pubblicazione** nelle istruzioni *Creazione e collegamento dell'app MultiPOP OAuth* 148 riportate di seguito).
5. Nella pagina Servizi Web di Account Editor 735 attivare l'opzione "**...modificare le opzioni MultiPOP**" per ciascuno di questi utenti.
6. Ogni utente deve accedere a Webmail, passare alla propria pagina **Cassette postali** in Opzioni, aggiungere il proprio account Gmail o Office 365 (se non già aggiunti), quindi fare clic su **Autorizza** per accedere all'account Gmail o Office 365 e procedere con i passaggi per autorizzare MDaemon a raccogliere la posta da tale posizione.

Gmail/Office 365

ID client
È l'ID client univoco assegnato all'app MultiPOP OAuth 2.0 quando questa viene creata nella Google API Console o nel portale Microsoft Azure Active Directory. Dopo aver creato l'app, copiare il relativo ID client e incollarlo qui.

Segreto client
È il segreto client univoco assegnato all'app MultiPOP OAuth 2.0 quando questa viene creata nella Google API Console o nel portale Microsoft Azure Active Directory.Dopo aver creato l'app, copiare il relativo Segreto client e incollarlo qui. **Note:** quando si crea il segreto client per un'applicazione Azure, è necessario copiarlo durante la creazione dell'app, perché in seguito non sarà più visibile. Se non viene copiato in quel momento, sarà necessario eliminare il segreto e crearne uno nuovo.

URI di reindirizzamento
Quando si crea la propria app OAuth 2.0 per Gmail o Office 365, è necessario specificare un URI di reindirizzamento. L'URI di reindirizzamento visualizzato nella schermata MultiPOP è un esempio costruito a partire dal nome dell'host SMTP del dominio predefinito 185 *** 188, che dovrebbe funzionare per gli utenti di quel dominio che accedono a Webmail. È necessario aggiungere altri URI di reindirizzamento all'app per qualsiasi altro dominio MDaemon che gli utenti utilizzano per accedere a Webmail. Ad esempio, "https://mail.esempio.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" funziona per tutti gli utenti che utilizzano mail.esempio.com per accedere a Webmail. Vedere: **Creazione e collegamento dell'app MultiPOP OAuth** di seguito per ulteriori informazioni.

Esempio di URI di reindirizzamento:

```
https://mail.esempio.com/WorldClient.dll?
   View=OAuth&AuthRequest=Gmail

https://mail.example.com/WorldClient.dll?
   View=OAuth&AuthRequest=Office365
```

Creazione e collegamento dell'app MultiPOP OAuth

Istruzioni dettagliate per la creazione dell'app MultiPOP OAuth 2.0.

Per Google Gmail

Attenersi alla procedura riportata di seguito per creare un'app Google che consenta l'autenticazione MultiPOP mediante Oauth 2.0 per la raccolta della posta da Gmail per gli utenti.

1. Con il browser in uso passare alla console API Google.
2. Dall'interno dell'elenco dei progetti, fare clic su **NUOVO PROGETTO** oppure, dalla pagina di gestione delle risorse, fare clic su **(+) CREA PROGETTO**.
3. Digitare un **nome del progetto,** quindi fare clic su **Modifica** per modificare l'ID del progetto oppure lasciarlo impostato sul valore predefinito. **Nota:** l'ID del progetto non può essere modificato dopo la creazione.

4. Nel riquadro a sinistra, passare ad **API e servizi | schermata del consenso OAuth**.
5. Selezionare **Esterno** e fare clic su **Crea**.
6. Immettere il **nome dell'app** (ad esempio MultiPOP OAuth 2.0 per Gmail), un **indirizzo email per l'assistenza** che gli utenti possono contattare, quindi un **indirizzo e-mail dello sviluppatore** che Google può contattare per richiedere modifiche al progetto. Questo è tutto ciò che viene richiesto in questa pagina per la configurazione ma, a seconda dell'organizzazione o dei requisiti di verifica, è possibile inserire anche il logo dell'azienda e i collegamenti ai termini e condizioni del servizio 372 e all'informativa sulla privacy. I campi dei **domini autorizzati** saranno popolati automaticamente quando si aggiungono gli *URI di reindirizzamento* nella fase successiva riportata di seguito. **Nota:** Queste informazioni vengono utilizzate per la schermata di consenso che verrà visualizzata dagli utenti per autorizzare MultiPOP a raccogliere la posta da Gmail.
7. Fare clic su **Salva e continua**.
8. Fare clic su **AGGIUNGI O RIMUOVI AMBITI**, quindi in "Aggiungi ambiti manualmente" immettere **https://mail.google.com/**. Fare clic su**AGGIUNGI A TABELLA**, quindi fare clic su **Aggiorna**.
9. Fare clic su **Salva e continua**.
10. In Utenti di prova, fare clic su **AGGIUNGI UTENTI**, immettere ciascun account Gmail da cui si intende raccogliere la posta e fare clic su **AGGIUNGI** (vedere la nota di seguito relativa allo stato di pubblicazione 149 dell'app).
11. Fare clic su **Salva e continua**.
12. In Riepilogo, fare clic su **TORNA ALLA DASHBOARD** in fondo alla pagina.
13. Fare clic su **Credenziali** nel riquadro a sinistra, scegliere **(+) Crea credenziali**, quindi selezionare **ID client OAuth**.
14. Nella casella di riepilogo a discesa "Tipo applicazione" selezionare **Applicazione Web** e in "URI di reindirizzamento autorizzati" selezionare **+ AGGIUNGI URI**. Immettere gli URI di reindirizzamento. L'URI di reindirizzamento visualizzato nella schermata MultiPOP è un esempio costruito a partire dal nome dell'host SMTP del dominio predefinito 185 *** 188, che dovrebbe funzionare per gli utenti di quel dominio che accedono a Webmail. È necessario aggiungere altri URI di reindirizzamento all'app per qualsiasi altro dominio MDaemon che gli utenti utilizzano per accedere a Webmail. Ad esempio, "https://mail.esempio.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" funziona per tutti gli utenti che utilizzano mail.esempio.com per accedere a Webmail.
15. Fare clic su **CREA**.
16. Copiare i valori di **ID client** e **Segreto client** nelle caselle ID client Gmail e Segreto client nella pagina MultiPOP.

Stato di pubblicazione - Queste istruzioni riguardano la creazione di un'app Google con lo Stato di pubblicazione impostato su "**Prova**". A tale scopo è necessaria l'aggiunta di ogni specifico account Google che utilizzerà l'app per raccogliere la posta da Gmail ed è previsto un limite di 100 utenti. Inoltre, in Webmail, quando agli utenti viene chiesto di autorizzare MDaemon a raccogliere la posta da Gmail, viene visualizzato un messaggio di avviso "per confermare che l'utente dispone dell'accesso in prova al progetto, ma deve considerare i rischi associati alla concessione a un'applicazione non verificata dell'autorizzazione all'accesso ai propri dati". Inoltre, l'autorizzazione scade dopo sette giorni, quindi ogni utente dovrà riautorizzare la raccolta da Gmail ogni settimana.

Per eliminare questi requisiti e limitazioni, è necessario modificare lo stato in "**In produzione**", operazione che potrebbe richiedere o meno il passaggio attraverso un processo di verifica. Per ulteriori informazioni sulla verifica delle app e sullo stato di pubblicazione, consultare i seguenti articoli di Google: Impostazione della schermata di consenso OAuth e FAQ sulla verifica dell'API OAuth.

Per Microsoft (Office) 365

Attenersi alla procedura riportata di seguito per creare un'app Microsoft Azure che consenta l'autenticazione MultiPOP mediante Oauth 2.0 per la raccolta delle e-mail Office 365 per gli utenti.

1. Passare alla pagina Microsoft Azure Active Directory sul portale Azure Portal e fare clic su **Registrazioni app** nel riquadro a sinistra (è necessario registrarsi per un account Azure gratuito o a pagamento, se non se ne possiede già uno).
2. Fare clic su **+ Nuova registrazione**.
3. Inserite il nome dell'applicazione nel campo **Nome** (ad esempio "Mailbox OAuth per Office 365").
4. In "Tipi di account supportati" selezionare **Account in qualsiasi directory organizzativa (qualsiasi directory Azure AD - Multitenant)**.
5. Per "URI di reindirizzamento" selezionare **Web** quindi immettere l'**URI di reindirizzamento** di Office 365. L'URI di reindirizzamento visualizzato nella schermata MultiPOP è un esempio costruito a partire dal nome dell'host SMTP del dominio predefinito 185 *** 188, che dovrebbe funzionare per gli utenti di quel dominio che accedono a Webmail. È necessario aggiungere altri URI di reindirizzamento all'app per qualsiasi altro dominio MDaemon che gli utenti utilizzano per accedere a Webmail. Ad esempio, "https://mail.esempio.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" funziona per tutti gli utenti che utilizzano mail.esempio.com per accedere a Webmail.
6. Fare clic su **Registra**.
7. Prendere nota dell'**ID applicazione (client)** (accanto c'è un pulsante per copiare negli Appunti). Sarà possibile trovare questo ID in un secondo momento facendo clic su **Panoramica** nel riquadro a sinistra.

8. Se è necessario aggiungere altri URI di reindirizzamento, fare clic sul pulsante **URI di reindirizzamento: 1 collegamento Web** sulla destra. Fare clic su **Aggiungi URI** e immettere l'URI, ripetendo se necessario, quindi fare clic su **Salva**.
9. Fare clic su **Autorizzazioni API** nel riquadro a sinistra.
10. Fare clic su **+ Aggiungi un'autorizzazione**.
11. Fare clic su **Microsoft Graph**.
12. Fare clic su **Autorizzazioni delegate**.
13. Scorrere verso il basso fino a **POP** e selezionare **POP.AccessAsUser.All**, quindi sotto **Utente** selezionare **User.Read** (User.Read è già selezionato per impostazione predefinita).
14. Fare clic su **Aggiungi autorizzazioni**.
15. Nel riquadro a sinistra fare clic su **Certificati e segreti**.
16. Fare clic su **+ Nuovo segreto client**.
17. Immettere una descrizione (ad esempio, "Segreto del client per l'applicazione MultiPOP OAuth di Office 365").
18. Selezionare dopo quanto tempo il segreto client deve scadere.
19. Fare clic su **Aggiungi**.
20. Prendere nota del segreto del client generato nel campo **Valore** (accanto c'è un pulsante per copiare negli Appunti). **NOTA:** il segreto client non sarà più visualizzabile in questa pagina. Sarà disponibile un'icona **Elimina** accanto alla voce, che consente di eliminarlo e creare un nuovo segreto client, se necessario.
21. Immettere i valori di ID applicazione (client) e segreto client nei campi **ID client** e **Segreto client** nella sezione Office 365 della pagina MultiPOP di MDaemon, sotto Impostazioni server.

Vedere:

Account Editor | MultiPOP 754
Pianificazione della posta | Raccolta MultiPOP 391

3.1.13 DomainPOP

Per configurare MDaemon in modo che scarichi la posta da una casella postale POP remota e la ridistribuisca agli utenti, è necessario utilizzare Raccolta posta DomainPOP, disponibile in "Impostazioni » Impostazioni server » DomainPOP". Questa funzione utilizza il protocollo POP3 per scaricare la posta presente nella casella POP dell'ISP associata all'ID utente specificato. Una volta raccolti, i messaggi vengono analizzati in base ai parametri impostati in questa finestra, quindi collocati nelle caselle postali degli utenti oppure nella coda postale remota per essere consegnati da MDaemon, come se i messaggi fossero stati recapitati al server mediante le transazioni SMTP convenzionali.

È importante tenere presente che i messaggi memorizzati nelle caselle postali POP e ritirati mediante il protocollo POP3 vengono privati di importanti informazioni di instradamento (la cosiddetta "busta" del messaggio) che di solito accompagnano i messaggi consegnati mediante il protocollo SMTP, che offre funzioni più potenti rispetto a POP. Senza tali informazioni, MDaemon deve "leggere" il messaggio ed esaminarne l'intestazione per tentare di identificare il destinatario originale. Tale procedura non è affidabile al 100%. In genere, le informazioni riportate nelle intestazioni dei messaggi non sono sufficienti per identificare il destinatario. Nonostante la mancanza di informazioni essenziali, ovvero il destinatario, costituisca un fattore sorprendente, è opportuno considerare che il protocollo inizialmente utilizzato per la consegna del messaggio non è il protocollo POP. Con il protocollo SMTP, il contenuto del messaggio risulta irrilevante, poiché è il protocollo stesso che indica al server il destinatario del messaggio durante la transazione postale.

Affinché il ritiro e la consegna POP dei messaggi di posta siano affidabili e coerenti, MDaemon utilizza una serie di potenti opzioni di elaborazione delle intestazioni. Dopo avere scaricato un messaggio da un'origine POP remota, MDaemon ne analizza tutte le intestazioni pertinenti e genera un insieme di potenziali destinatari. Ogni indirizzo e-mail rilevato nelle intestazioni esaminate viene incluso in questo elenco.

Al termine del processo l'elenco dei destinatari viene suddiviso in due gruppi, uno locale e uno remoto. Prima di questa suddivisione, inoltre, tutti gli indirizzi analizzati e inseriti nell'elenco dei potenziali destinatari vengono elaborati mediante la funzione di conversione degli alias[847]. Ogni membro del gruppo locale, composto dagli indirizzi il cui dominio corrisponde a uno dei domini locali di MDaemon, riceve una copia del messaggio. L'elaborazione degli indirizzi del gruppo locale viene gestita in base alle impostazioni di questa finestra di dialogo. Le opzioni consentono di ignorare semplicemente questi indirizzi, di inoltrare un elenco riepilogativo al postmaster oppure di accettarli. In quest'ultimo caso, MDaemon consegna di fatto una copia del messaggio al destinatario remoto. In rari casi, viene garantita la consegna dei messaggi ai destinatari remoti.

È necessario adottare alcune precauzioni per evitare la duplicazione dei messaggi o un ciclo infinito di consegne. La perdita della busta SMTP, ad esempio, causa un problema nella posta delle liste di distribuzione. Di norma, nel corpo dei messaggi distribuiti da una lista di distribuzione non è presente alcun riferimento all'indirizzo dei destinatari. Il modulo della lista inserisce semplicemente il nome della lista di distribuzione nel campo `TO:`. Ne risulta che, se il campo `TO:` contiene il nome della lista di distribuzione, è possibile che MDaemon scarichi il messaggio, ne analizzi il campo `TO:` (che restituisce il nome della lista di distribuzione) e rispedisca il messaggio alla medesima lista. MDaemon quindi consegnerebbe un'altra copia dello stesso messaggio alla casella postale POP da cui aveva scaricato il messaggio originale, ripetendo lo stesso ciclo all'infinito. Per risolvere problemi di questo tipo, gli amministratori di posta devono essere in grado di utilizzare gli strumenti e le impostazioni di MDaemon per l'eliminazione della posta della lista di distribuzione o per la generazione di alias, così da garantire che i messaggi vengano consegnati ai destinatari locali corretti. Per consegnare correttamente i messaggi, è anche possibile utilizzare le regole di Filtro contenuti o quelle di instradamento.

Questo tipo di raccolta della posta può anche causare una duplicazione indesiderata dei messaggi. È infatti probabile che si generino dei duplicati superflui della posta ritirata mediante DomainPOP e consegnata alla casella postale POP dell'ISP mediante SMTP. Si supponga ad esempio che un messaggio venga inviato a un utente di un dominio di MDaemon e una copia a conoscenza venga inviata a un altro utente dello stesso

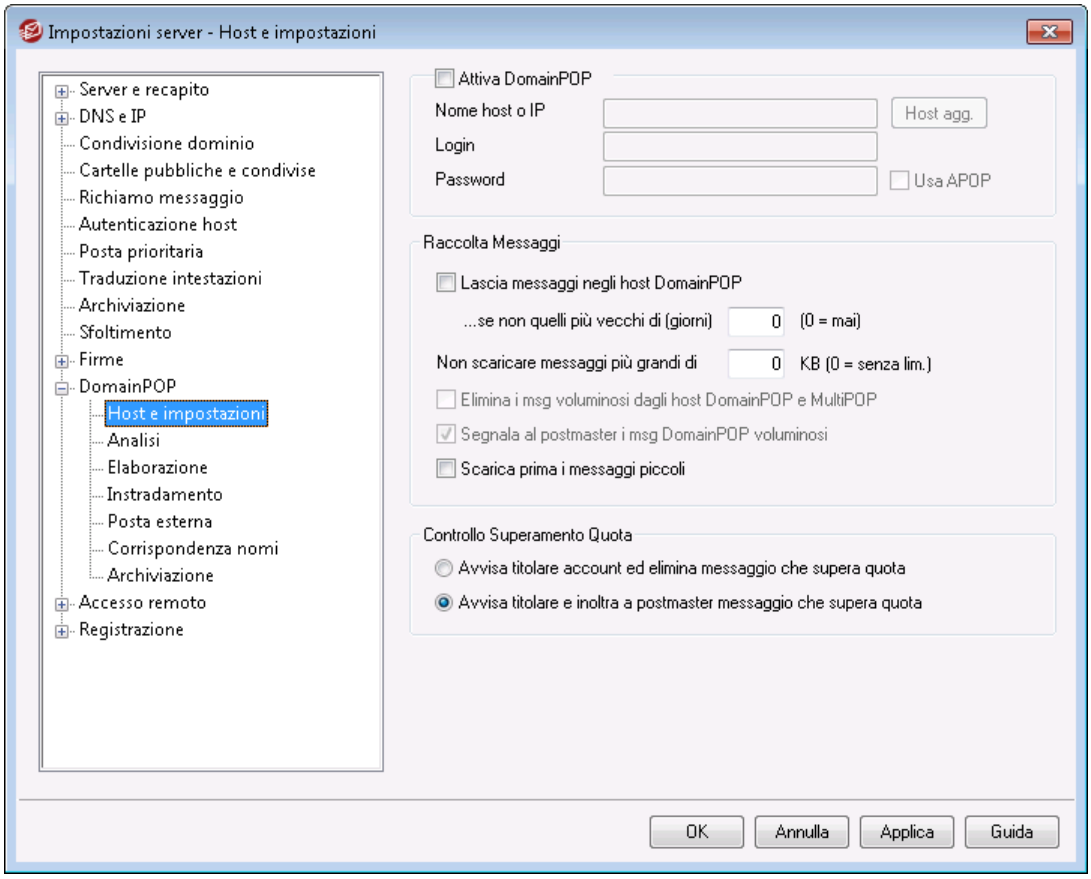
dominio. In questa situazione, SMTP consegna **due** copie dello stesso messaggio alla casella dell'ISP, una per ogni destinatario. Ciascuno dei due messaggi contiene i riferimenti a **entrambi** i destinatari: uno nel campo `TO:` e l'altro nel campo `CC:`. MDaemon raccoglierà entrambi questi messaggi identici e analizzerà gli indirizzi riportati in ognuno. In questo modo, ciascuno dei due destinatari riceverà un messaggio duplicato superfluo. Per prevenire questo tipo di duplicazione, in MDaemon è disponibile un comando che consente di specificare un'intestazione che verrà esaminata per la presenza di eventuali duplicazioni. Il campo `Message-ID` è ottimale a questi fini. Nell'esempio precedente i due messaggi sono identici e nel campo `Message-ID` presentano pertanto lo stesso valore. Questo valore può essere utilizzato da MDaemon per individuare e rimuovere il secondo messaggio durante la fase di scaricamento, prima di effettuare l'analisi delle informazioni relative all'indirizzo.

Per evitare che i messaggi vengano duplicati e le consegne ripetute all'infinito, è anche possibile monitorare il numero di passaggi (in inglese "hop", salti) effettuati dal messaggio nel sistema di trasporto. A ogni elaborazione, il server di posta SMTP inserisce nel messaggio un'intestazione "Received" per contrassegnarlo come ricevuto. MDaemon conta tutte le intestazioni di questo tipo alla prima elaborazione del messaggio. Se il numero totale di server di posta supera un valore specificato, è probabile che il messaggio sia stato coinvolto in un ciclo di consegne ripetute e che debba essere ritirato dal flusso della posta e collocato nella directory dei messaggi scartati. Questo valore può essere configurato nella Coda tentativi 888.

Vedere:

Filtri dei contenuti 658
Liste di distribuzione 275

3.1.13.1 Host e impostazioni



Proprietà host DomainPOP

Abilita il modulo di raccolta posta DomainPOP
Se questa casella è selezionata, MDaemon utilizza le impostazioni fornite in questa finestra per raccogliere la posta da un host di posta DomainPOP per poi ridistribuirla a livello locale.

Nome host o IP
Immettere in questo campo il nome dominio o l'indirizzo IP dell'host DomainPOP.

Host agg.
Fare clic su questo pulsante per aprire il file `DpopXtra.dat` nel quale è possibile indicare gli host aggiuntivi utilizzati per la raccolta della posta DomainPOP. Per ulteriori informazioni, vedere il contenuto del file stesso.

Login
Immettere in questo campo l'ID utente dell'account POP utilizzato da DomainPOP.

Password
Immettere in questo campo la password dell'account POP o APOP.

Usa APOP
Selezionare questa casella per utilizzare il comando APOP e l'autenticazione CRAM-MD5 durante il ritiro della posta. Questo comando consente di autenticarsi senza inviare password in testo non crittografato.

Raccolta messaggi

Lascia messaggi negli host DomainPOP
Se questa casella è selezionata, MDaemon scaricherà ma non rimuoverà i messaggi dall'host di posta DomainPOP.

...se non quelli più vecchi di (giorni) (0=mai)
Specificare il numero di giorni per cui si desidera conservare i messaggi nell'host DomainPOP prima di eliminarli. Inserire "0" se non si desidera eliminare alcun messaggio.

Alcuni ISP pongono un limite sulla quantità di messaggi che possono essere contenuti nella casella postale.

Non scaricare messaggi più grandi di [XX] KB (0 = senza lim.)
I messaggi di dimensioni uguali o superiori al valore specificato in questo campo non vengono scaricati dall'host di posta DomainPOP. Se si specifica il valore "0", i messaggi vengono scaricati a prescindere dalla dimensione.

Elimina i msg voluminosi dagli host DomainPOP e MultiPOP
Selezionare questa opzione per eliminare i messaggi che superano la dimensione massima indicata in precedenza. I messaggi vengono semplicemente rimossi dagli host di posta DomainPOP e MultiPOP senza essere scaricati.

Segnala al postmaster i msg DomainPOP voluminosi
Selezionare questa opzione per inviare un avviso al postmaster e segnalare la presenza di un messaggio di grandi dimensioni nella casella postale DomainPOP.

Scarica prima i messaggi piccoli
Selezionare questa casella di controllo per scaricare i messaggi in base alla dimensione, a partire dai più piccoli.

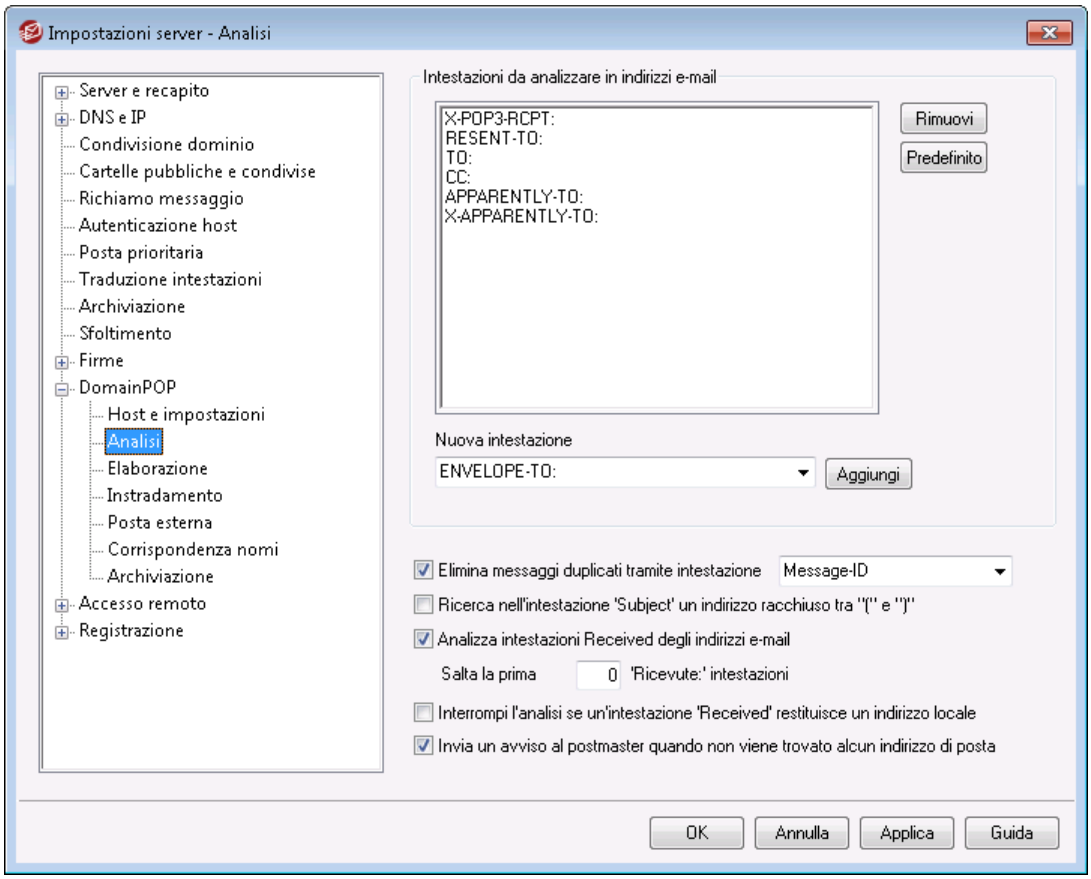
Questa opzione consente di velocizzare il ritiro dei messaggi di dimensione ridotta, ma non di aumentare i tempi di ordinamento ed elaborazione interni.

Controllo superamento quota

Avvisa titolare account ed elimina messaggio che supera quota
Se questa opzione è selezionata e viene raccolto un messaggio per un account il cui valore di quota (specificato nella schermata Quote 746 di Account Editor) è stato superato, MDaemon elimina il messaggio e segnala all'utente che l'account ha superato la quota consentita.

Avvisa titolare e inoltra a postmaster messaggio che supera quota
Se questa opzione è selezionata e viene raccolto un messaggio per un account il cui valore di quota è stato superato, MDaemon inoltra il messaggio al postmaster e segnala all'utente che l'account ha superato la quota consentita.

3.1.13.2 Analisi



Intestazioni da analizzare in indirizzi e-mail

In quest'area viene fornito l'elenco delle intestazioni analizzate da MDaemon per l'estrazione degli indirizzi. Gli indirizzi vengono cercati in tutte le intestazioni presenti nell'elenco.

Rimuovi
Questo pulsante consente di rimuovere le voci selezionate dall'elenco delle intestazioni.

Predefinito
Questo pulsante consente di cancellare il contenuto corrente dell'elenco delle intestazioni e inserire l'elenco predefinito delle intestazioni di MDaemon. Di solito, le intestazioni predefinite sono sufficienti per estrarre tutti gli indirizzi dal messaggio.

Nuova intestazione
Consente di immettere l'intestazione da aggiungere all'elenco.

Aggiungi
Dopo aver specificato un'intestazione nell'opzione *Nuova intestazione*, per aggiungerla all'elenco fare clic su questo pulsante.

Rileva messaggi duplicati utilizzando questa intestazione
Se questa opzione è abilitata, MDaemon memorizza il valore dell'intestazione specificata e non elabora gli altri messaggi con valore identico raccolti durante stesso ciclo di elaborazione. `Message-ID` è l'intestazione predefinita utilizzata per questa opzione.

Ricerca nell'intestazione 'Subject' un indirizzo racchiuso tra "(" e ")"
Se questa opzione è abilitata e MDaemon trova un indirizzo racchiuso tra parentesi "( )" nell'intestazione "Subject:" di un messaggio, tale indirizzo viene aggiunto all'elenco dei destinatari del messaggio insieme agli altri indirizzi analizzati.

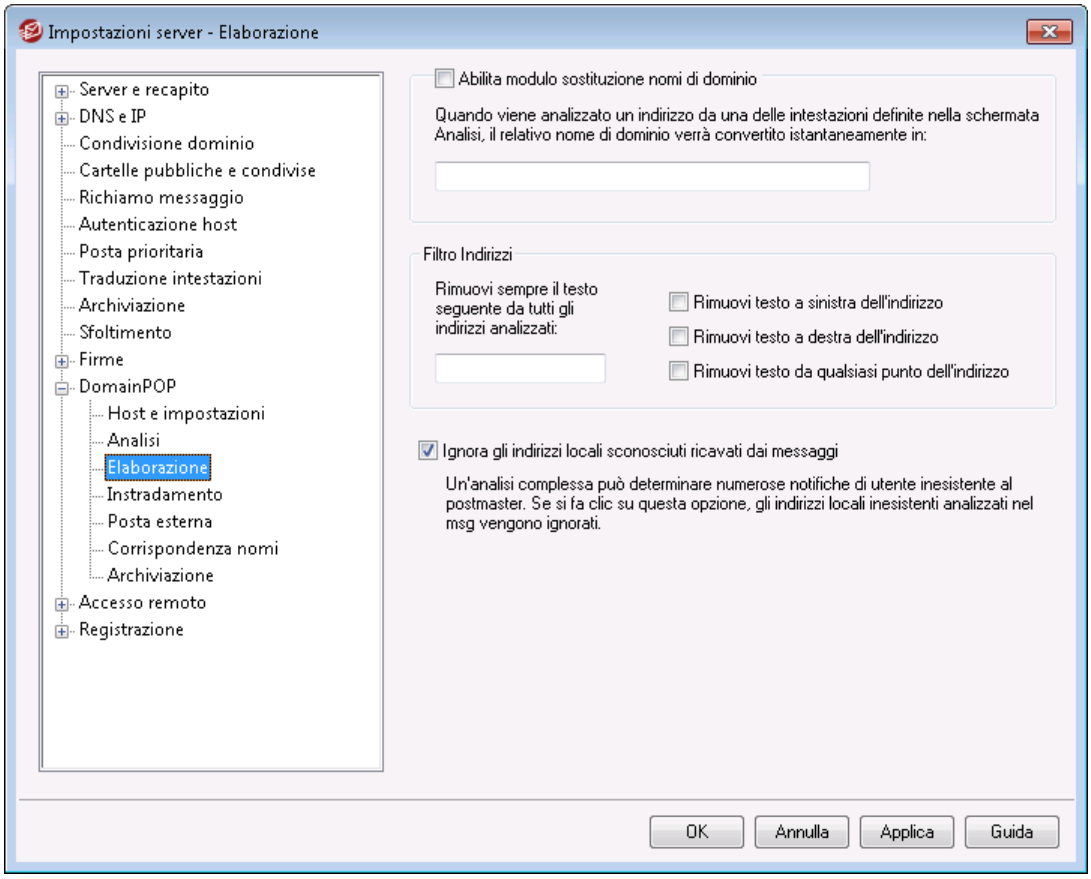
Analizza intestazioni Received degli indirizzi e-mail
È possibile memorizzare le informazioni relative al destinatario, normalmente presenti solo nelle intestazioni "Received" della busta del messaggio. In questo modo, l'analisi del messaggio rileva l'indirizzo effettivo del destinatario semplicemente esaminando in seguito le intestazioni Received. Selezionare questa casella di controllo per analizzare tutte le intestazioni "Received" trovate nel messaggio al fine di individuare gli indirizzi validi.

Ignora le prime xx intestazioni "Received"
In alcune configurazioni del server, è possibile voler analizzare le intestazioni Received, ma ignorare alcune delle prime. Questa impostazione consente di inserire il numero di intestazioni "Received" che verranno ignorate da MD prima di iniziare l'analisi.

Interrompi analisi se un'intestazione "Received" restituisce un indirizzo locale
Se questa opzione è selezionata e l'analisi sintattica di un'intestazione "Received" rileva un indirizzo locale valido, MDaemon interromperà il processo di analisi e non cercherà altri potenziali indirizzi di consegna.

Invia un avviso al postmaster quando non viene trovato alcun indirizzo di posta
Per impostazione predefinita MDaemon invia una e-mail di avviso al postmaster quando non viene trovato un indirizzo dal processo di analisi. Deselezionare la casella di controllo se non si desidera inviare l'avviso.

3.1.13.3 Elaborazione



Sostituzione dei nomi di dominio

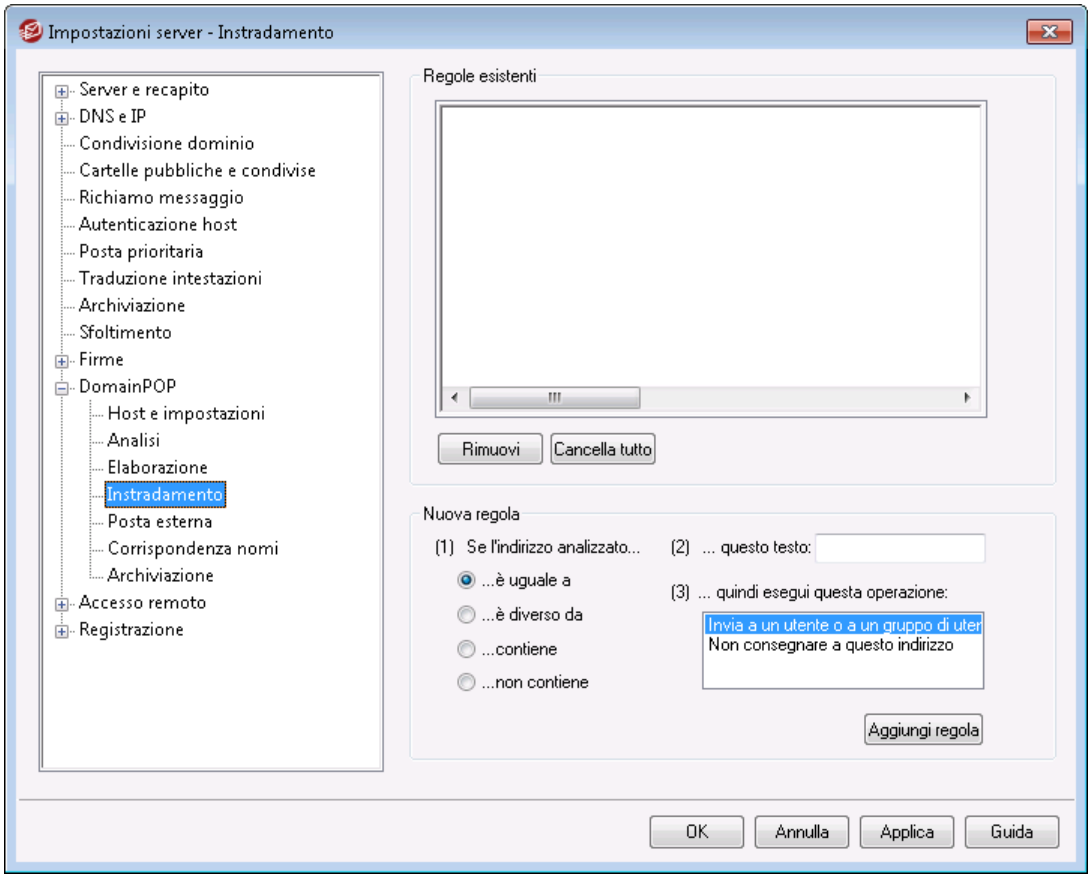
Abilita modulo sostituzione nomi di dominio
Questa opzione consente di ridurre il numero di alias richiesti dal sito. Quando un messaggio viene scaricato, i nomi di dominio di tutti gli indirizzi analizzati per quel messaggio vengono convertiti nel nome di dominio specificato in questa sede.

Filtro indirizzi

Rimuovi sempre il testo seguente da tutti gli indirizzi analizzati
Alcuni host contrassegnano ogni messaggio con una riga che indica il destinatario del messaggio e aggiungono alcune informazioni sull'instradamento a destra o a sinistra dell'indirizzo. Questo contrassegno costituirebbe lo strumento ideale per analizzare la sintassi dell'indirizzo del destinatario se le informazioni aggiuntive sull'instradamento non rendessero indispensabile un notevole numero di alias per gli account. Per ovviare a questo inconveniente, è possibile specificare semplicemente il valore del testo aggiuntivo nella casella di testo di questa funzione, in modo che MDaemon rimuova ogni occorrenza del testo dagli indirizzi analizzati.

Ignora gli indirizzi locali sconosciuti ricavati dai messaggi
Come indicato in precedenza, la funzione di sostituzione dei nomi di dominio modifica il nome dominio in tutti gli indirizzi e-mail analizzati nel messaggio, sostituendolo con quello specificato in questa finestra. Di conseguenza, è possibile che ad alcuni indirizzi non corrisponda alcun account presso il server. Poiché il nome di dominio è valido, ma la casella postale no, MDaemon considera tali indirizzi come appartenenti a utenti locali sconosciuti. In questi casi, viene generato normalmente il messaggio "Utente inesistente". Abilitare questa casella se si desidera impedire che il modulo di sostituzione dei nomi di dominio generi questi messaggi.

3.1.13.4 Instradamento



Regole esistenti

In questo elenco vengono visualizzate le regole create in precedenza che verranno applicate ai messaggi.

Rimuovi
Per eliminare una regola, selezionarla nell'elenco e fare clic su questo pulsante.

Cancella tutto
Questo pulsante consente di rimuovere tutte le regole esistenti.

Nuova regola

(1) Se l'indirizzo analizzato...

è uguale a, è diverso da, contiene, non contiene
Questi pulsanti di opzione indicano il tipo di confronto che verrà effettuato tra l'indirizzo e la regola di instradamento. MDaemon cerca in ogni indirizzo la stringa specificata nel campo "*il testo*" e procede in base all'impostazione di questo comando. In altri termini, si comporta in modo diverso a seconda che il testo completo dell'indirizzo corrisponda esattamente, non corrisponda esattamente, includa o non includa il testo specificato.

(2) ...il testo:
Immettere il testo da ricercare durante la scansione degli indirizzi.

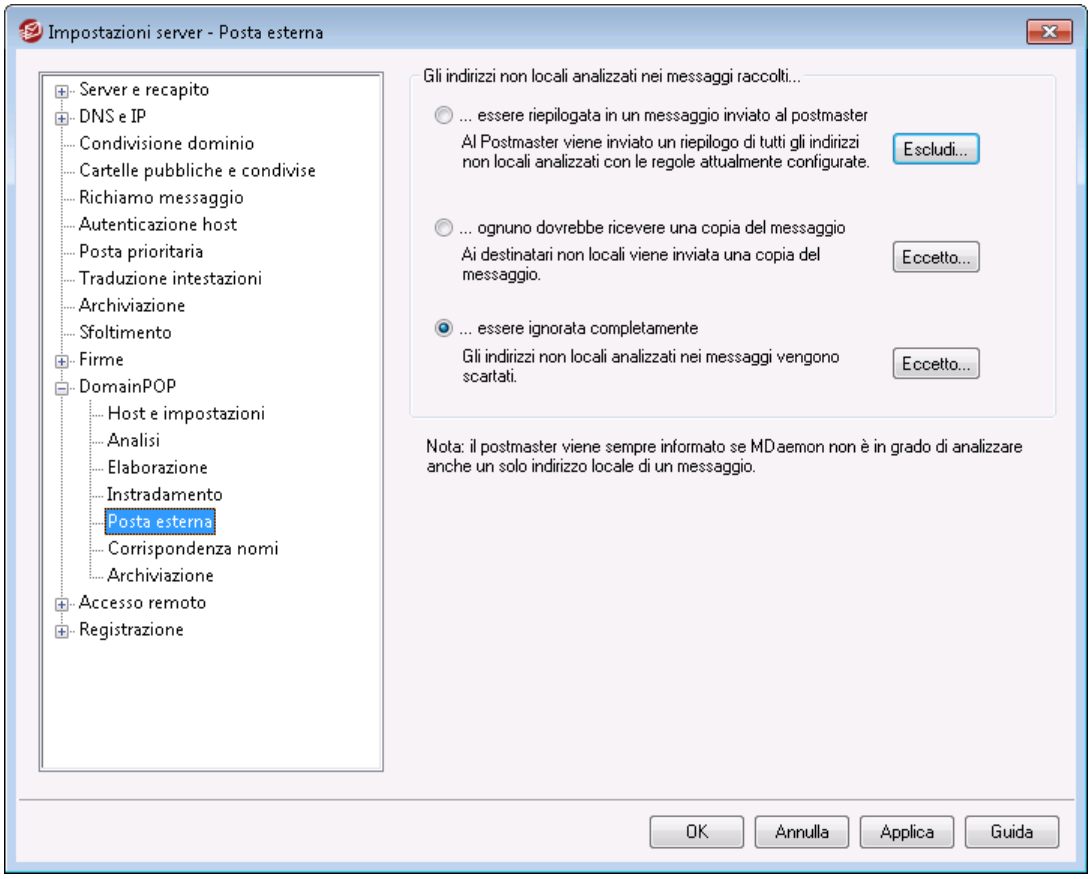
(3) ...procedi come segue:
In questa casella vengono elencate le azioni che è possibile eseguire quando l'esito della regola è positivo. È possibile scegliere una delle azioni seguenti:

Non consegnare a questo indirizzo - Questa azione impedisce la consegna del messaggio all'indirizzo specificato.

Invia a un utente o a un gruppo di utenti - Questa azione apre una finestra di dialogo che consente di creare l'elenco degli indirizzi e-mail a cui deve essere inviata una copia del messaggio in corso di elaborazione.

Aggiungi regola
Dopo aver impostato i parametri della nuova regola, fare clic su *Aggiungi regola* per aggiungere la regola all'elenco.

3.1.13.5 Posta esterna



Gli indirizzi non locali analizzati nei messaggi raccolti...

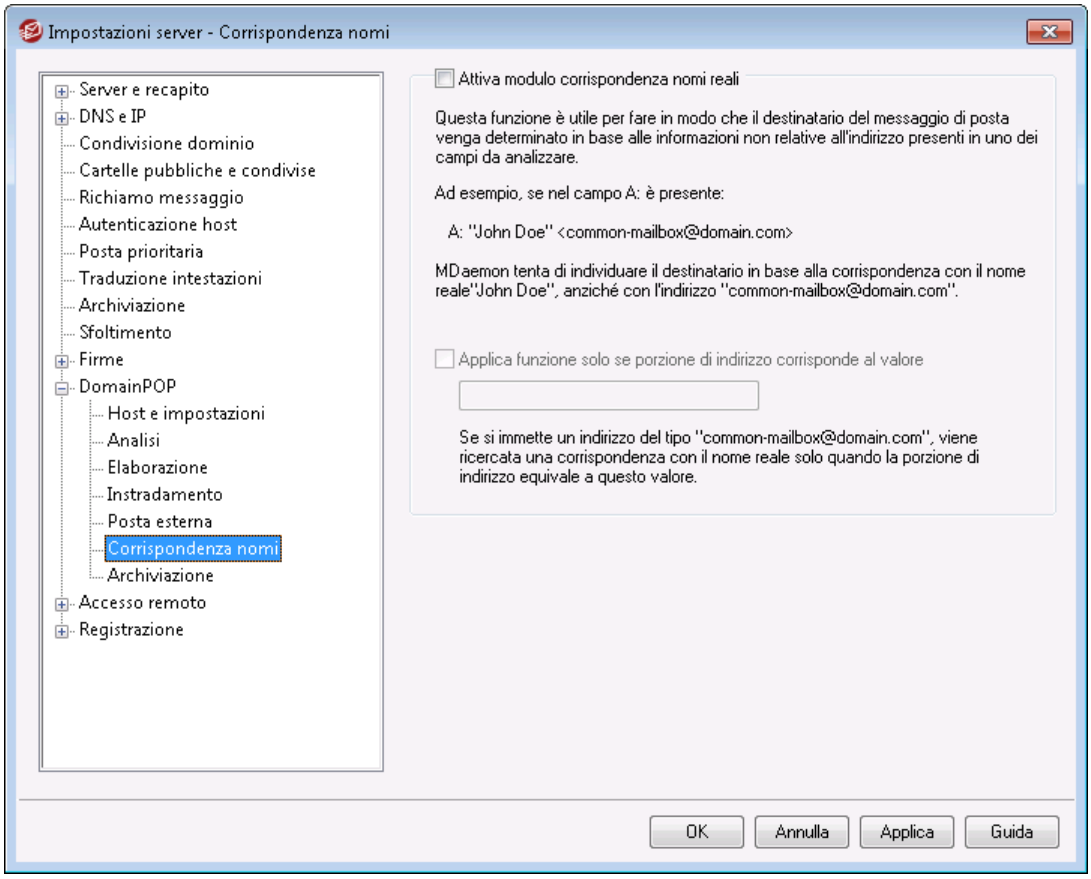
... vengono inclusi in un messaggio inviato al postmaster
Se questa opzione è selezionata, MDaemon invierà al postmaster una singola copia del messaggio insieme a un riepilogo degli indirizzi non locali estratti dall'analisi sintattica mediante la serie corrente di intestazioni e regole.

...ricevono una copia del messaggio
Se questa opzione è selezionata, MDaemon consegna una copia del messaggio ai destinatari non locali eventualmente rilevati nelle intestazioni analizzate.

...vengono ignorati
Se questa opzione è selezionata, MDaemon rimuove dall'elenco dei destinatari tutti gli indirizzi non locali, come se non avesse mai analizzato la sintassi degli indirizzi remoti relativi ai messaggi originali scaricati.

I pulsanti *Escludi...* ed *Eccetto...* consentono di definire gli indirizzi che rappresentano eccezioni ai fini dell'opzione selezionata.

3.1.13.6 Corrispondenza nomi



La funzione Corrispondenza nomi può essere utilizzata solo insieme al modulo Raccolta posta DomainPOP. Per utilizzare questa funzione, abilitare DomainPOP. Per accedere a DomainPOP, selezionare "Impostazioni » Impostazioni Server » DomainPOP".

Corrispondenza nomi reali

Attiva modulo corrispondenza nomi reali
Questa funzione consente a MDaemon di individuare il destinatario di un messaggio DomainPOP in base a una porzione di testo inclusa nell'indirizzo anziché all'indirizzo e-mail vero e proprio. In genere, si tratta del nome reale del destinatario.

Si supponga, ad esempio, che un messaggio abbia l'intestazione TO seguente:

```
TO: "Michele Masone" <utente01@esempio.com>
```

oppure

```
TO: Michele Masone <utente01@esempio.com>
```

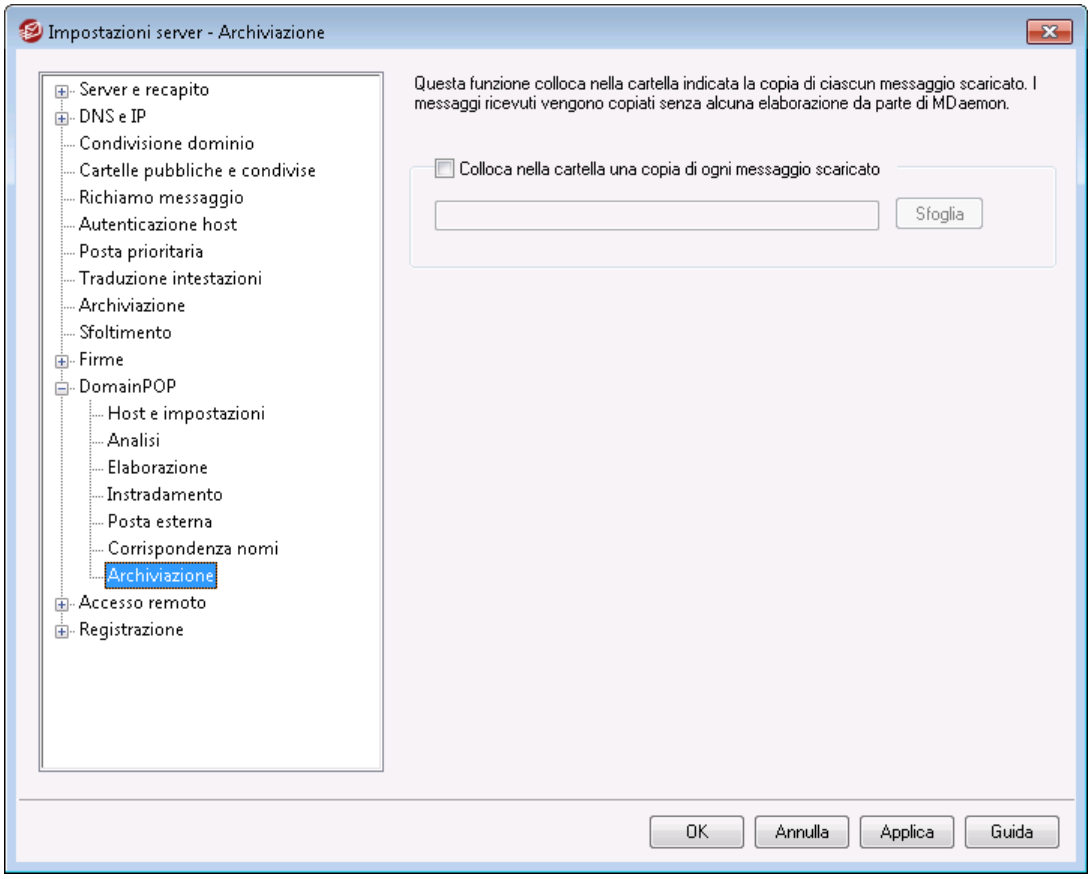
La funzione Corrispondenza nomi ignora la parte "utente01@esempio.com" dell'indirizzo, estrae il nome "Michele Masone" e verifica se tale nome corrisponde a un utente di MDaemon. In caso di corrispondenza con il campo del nome reale di un account, per la consegna verrà utilizzato l'indirizzo di posta elettronica locale di tale account. In caso contrario, MDaemon consegnerà il messaggio all'indirizzo di posta elettronica determinabile dai dati (in questo caso particolare, utente01@esempio.com).

La parte relativa al nome reale non può includere i caratteri virgola, punto e virgola o due punti.

Applica funzione solo se porzione di indirizzo corrisponde al valore
Questa opzione consente di specificare un indirizzo e-mail che deve essere presente nei dati estratti per avviare il processo di corrispondenza del nome reale. Rappresenta un criterio per determinare quando la funzione Corrispondenza nomi verrà utilizzata. Ad esempio, se l'indirizzo specificato è "utente01@esempio.com", la funzione Corrispondenza nomi potrà essere utilizzata solo per gli indirizzi corrispondenti a tale valore.

Se si immette in questa opzione il valore "utente01@esempio.com", "**`TO: 'Michele Masone' <utente01@esempio.com>`**" sarà un candidato valido per la corrispondenza dei nomi, diversamente da "**`TO: 'Michele Masone' <utente02@esempio.com>`**.

3.1.13.7 Archiviazione

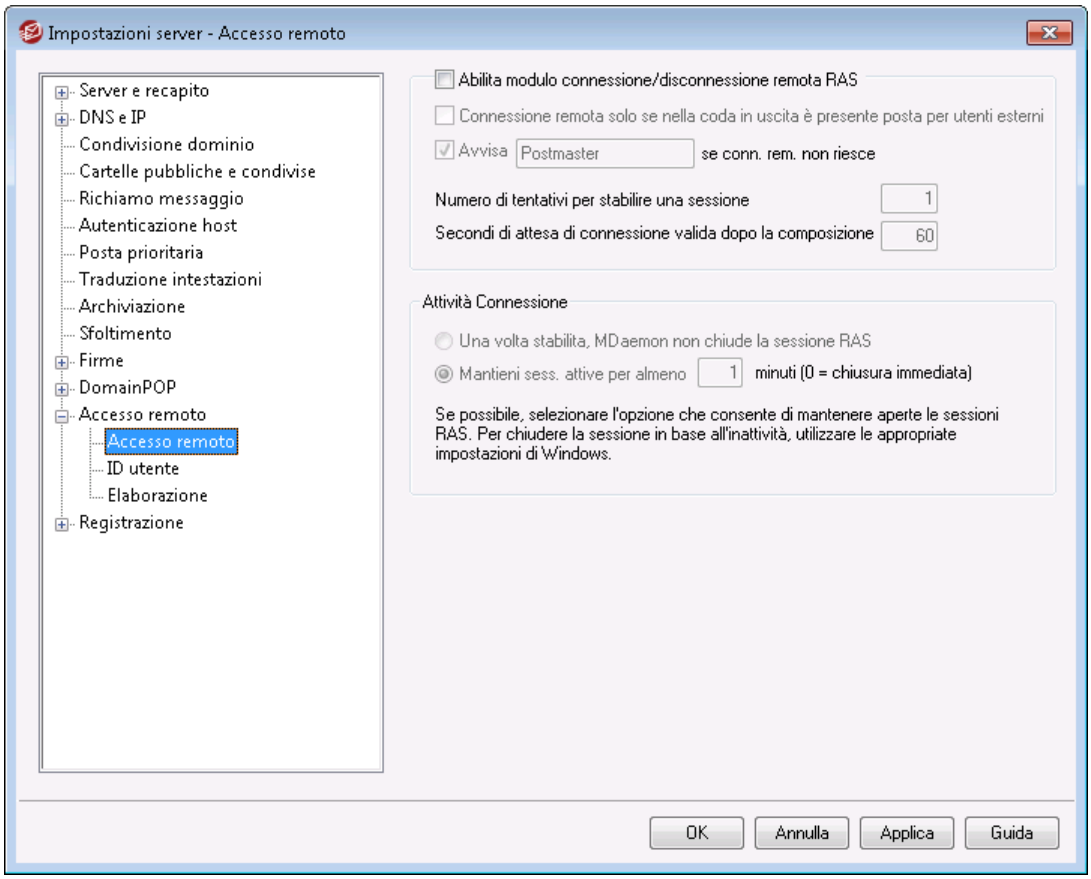


Archiviazione

Colloca nella cartella una copia di ogni messaggio scaricato
La selezione di questa opzione impedisce che un'analisi sintattica non prevista o eventuali errori nello scaricamento di notevoli quantitativi di posta causino una perdita di messaggi. Selezionare la casella di controllo se si desidera salvare nella cartella specificata una copia di ciascun messaggio scaricato. Tali copie vengono collocate nella cartella senza alcuna elaborazione da parte di MDaemon.

3.1.14 RAS

3.1.14.1 Accesso remoto



Fare clic su "Impostazioni » Impostazioni Server » RAS" per configurare le impostazioni di connessione remota. Questa finestra è disponibile solo se nel sistema è installato il Servizio di Accesso Remoto (RAS, Remote Access Service), che viene utilizzato da MDaemon per collegarsi all'ISP immediatamente prima di un evento di elaborazione della posta remota.

Abilita modulo connessione/disconnessione remota RAS
Se questa opzione è selezionata, MDaemon usa le impostazioni specificate per connettersi a un host remoto prima dell'invio e/o della ricezione della posta remota.

Connessione remota solo se nella coda in uscita è presente posta per utenti esterni
Se questa opzione è selezionata, MDaemon non si connette all'ISP, a meno che nella coda remota non sia presente posta remota in attesa. Nonostante sia vantaggiosa in talune circostanze, tenere presente che se MDaemon non attiva una connessione remota non verrà eseguita neanche la **raccolta** della posta, se non mediante la LAN locale.

Avvisa [indirizzo] se connessione remota non riesce
Se questa casella è selezionata, MDaemon invia un messaggio all'indirizzo specificato per segnalare che la connessione non è riuscita a causa di un errore.

Numero di tentativi per stabilire una sessione
Questo valore indica quante volte MDaemon ha tentato di connettersi all'host remoto prima di abbandonare l'operazione.

Secondi di attesa di connessione valida dopo la composizione
Questo valore indica il tempo trascorso da MDaemon in attesa della risposta e del completamento della connessione RAS da parte del computer remoto.

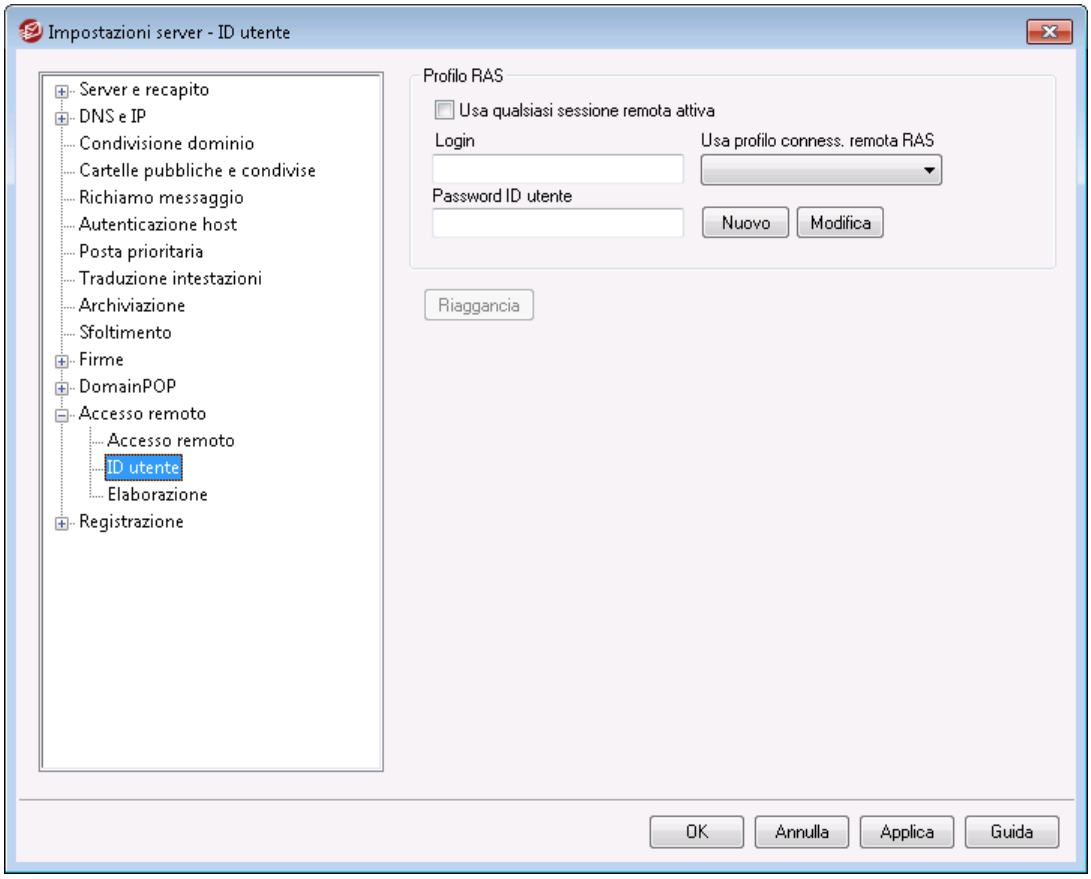
Attività connessione

Una volta stabilita, MDaemon non chiude la sessione RAS
Per impostazione predefinita, MDaemon chiude la connessione subito dopo la conclusione di tutte le transazioni postali, quando la sessione non è più utilizzata. Se questa opzione è selezionata, la connessione rimane aperta anche dopo il completamento di tutte le transazioni.

MDaemon non chiude mai una connessione creata da un altro server.

Mantieni sessioni attive per almeno xx minuti
Quando questa opzione è selezionata, una sessione RAS creata da MDaemon rimane aperta per almeno il numero di minuti specificato oppure fino alla conclusione di tutte le transazioni postali, a seconda della situazione.

3.1.14.2 Connessione



Profilo RAS

Usa qualsiasi sessione remota attiva
Selezionare questa casella di controllo se si desidera che MDaemon utilizzi altri profili di connessione quando ne rileva uno attivo. Al momento di effettuare la connessione, MDaemon verifica se esiste una connessione attiva prima di stabilirne una.

Login
Il valore specificato in questo campo viene passato all'host remoto durante il processo di autenticazione.

Password ID utente
Il valore specificato in questo campo rappresenta la password trasmessa all'host remoto durante il processo di autenticazione.

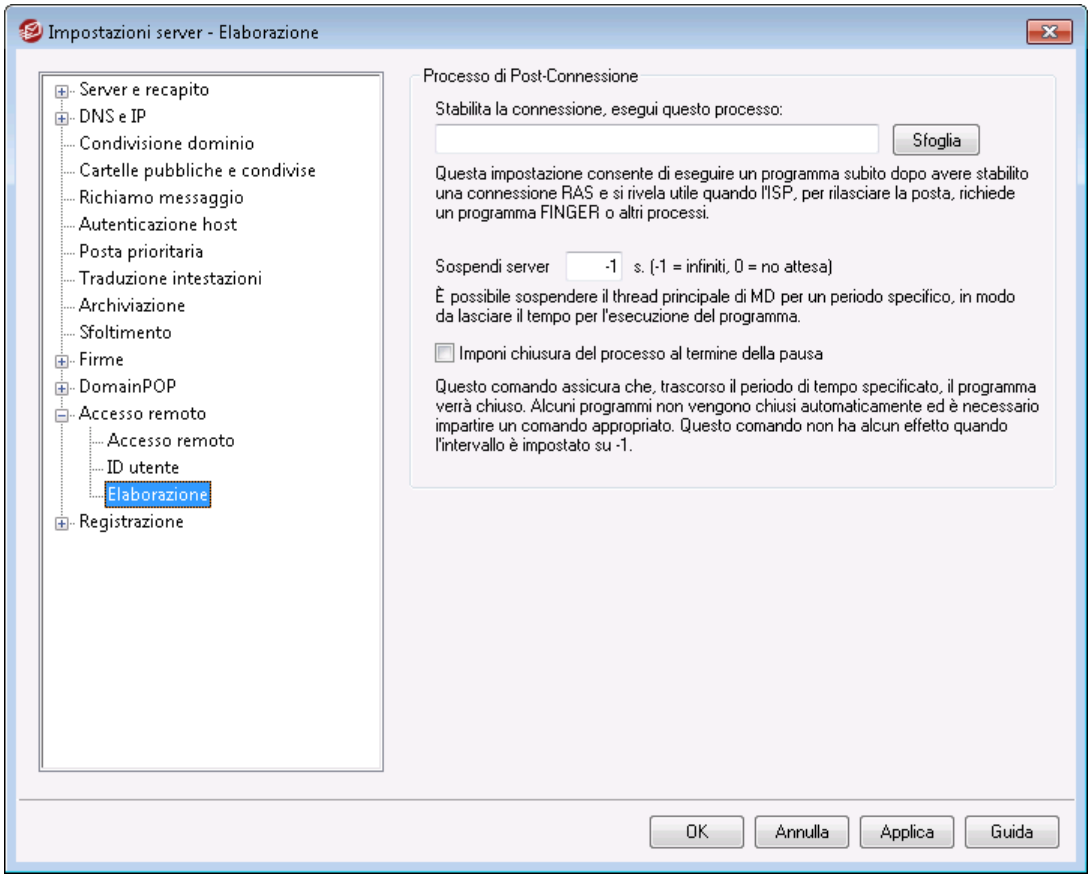
Usa profilo connessione remota RAS
In questo elenco a discesa è possibile di selezionare un profilo di sessione definito precedentemente con le opzioni di Accesso remoto di Windows.

Nuovo
Fare clic su questo pulsante per creare un nuovo profilo di accesso remoto o RAS.

Modifica
Fare clic su questo pulsante per modificare il profilo di accesso remoto o RAS correntemente selezionato.

Riaggancia
Se si fa clic su questo pulsante, la connessione all'ISP verrà chiusa. L'opzione è attiva solo se la sessione RAS è stata avviata da MDaemon.

3.1.14.3 Elaborazione



Processo di post-connessione

Stabilita la connessione, esegui questo processo
Se in questo campo viene specificato un programma, MDaemon genera un thread ed esegue il processo. Questa funzione è particolarmente utile quando si utilizza `Finger` o un altro programma per sbloccare la casella postale dell'ISP.

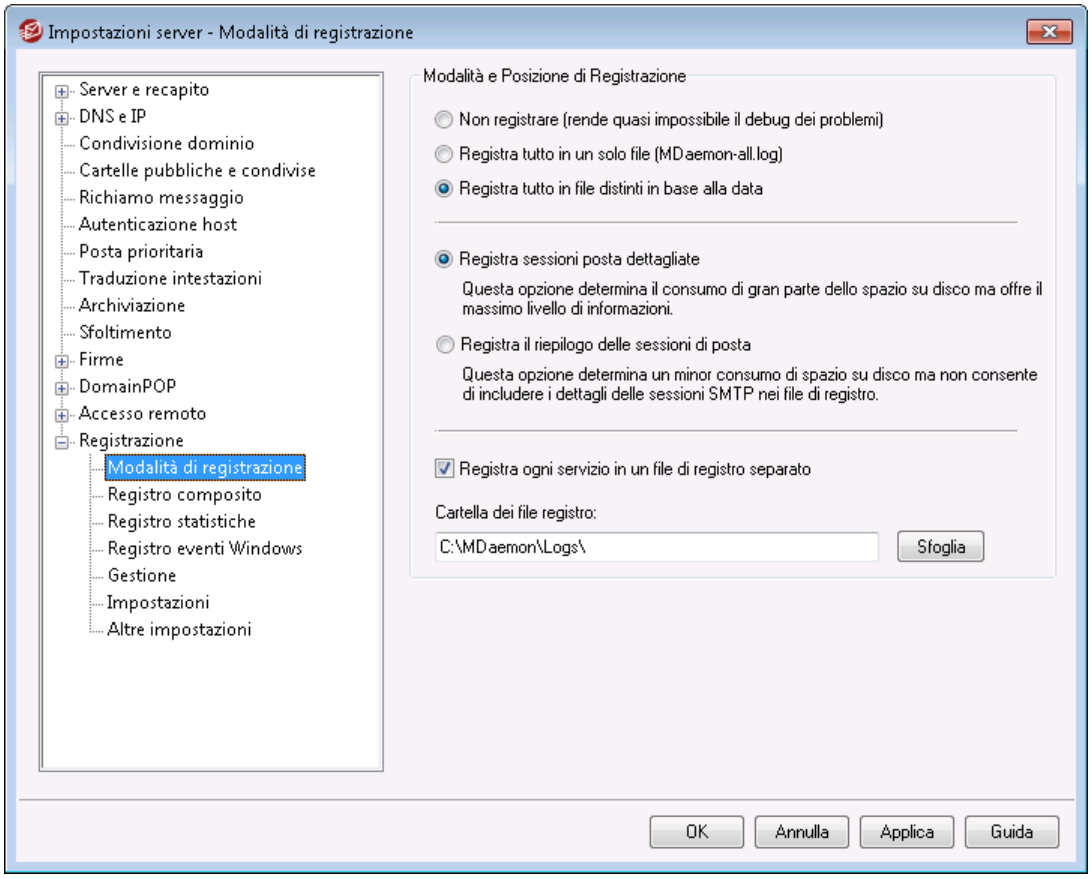
Sospendi server xx s. (-1 = infinito, 0 = no attesa)
Se in *Stabilita la connessione, esegui questo processo* è specificata una voce valida, il server sospende le attività per il numero di minuti indicato in questo campo e

attende il risultato del processo in esecuzione. Se si immette il valore "-1", il server continuerà ad attendere il risultato del processo.

Imponi chiusura del processo al termine della pausa
In alcuni casi, è possibile che il programma da eseguire non si chiuda automaticamente al completamento: la chiusura di alcuni programmi richiede l'intervento dell'utente. Questa condizione non è accettabile se il software deve essere poter essere eseguito senza la costante supervisione dell'utente. È possibile risolvere il problema selezionando questa opzione per terminare il thread del processo una volta trascorsi i secondi indicati nel campo *Server in pausa per XX secondi*. Si noti che la funzione non è attiva se il server è configurato per attendere all'infinito il risultato del processo.

3.1.15 Registrazione

3.1.15.1 Modalità di registrazione



Per configurare le impostazioni di registrazione, fare clic su "Impostazioni » Impostazioni server » Registrazione". La registrazione si rivela utile per la diagnosi dei problemi e il monitoraggio delle operazioni del server durante le attività eseguite senza la supervisione di un utente.

Nella finestra di dialogo Preferenze sono presenti numerosi comandi che consentono di gestire i dati di registro da visualizzare nella finestra Monitoraggio eventi dell'interfaccia principale di MDaemon. Per ulteriori informazioni, vedere Preferenze » IU 497.

Modalità e posizione di registrazione

Non registrare
Scegliendo questa opzione non verrà attivata alcuna registrazione. Verranno ancora creati i file di registro, ma in essi non verrà scritto alcun dato.

Non è consigliabile utilizzare questa opzione. Senza i registri può risultare estremamente difficile, se non impossibile, eseguire un'analisi o il debug di qualunque eventuale problema legato alla posta.

Registra tutto in un solo file (MDaemon-all.log)
Scegliere questa opzione se si desidera registrate tutte le attività in un unico file denominato `MDaemon-all.log`.

Registra tutto in file distinti in base alla data
Se questa opzione è selezionata, MDaemon genera un registro separato per ogni giorno. Il nome di ogni file corrisponde alla data di creazione.

Registra sessioni posta dettagliate
Selezionare questa opzione per copiare nel file registro una trascrizione completa di ogni transazione di posta.

Registra il riepilogo delle sessioni di posta
Selezionare questa opzione per copiare nel file registro un riepilogo di ogni transazione di posta.

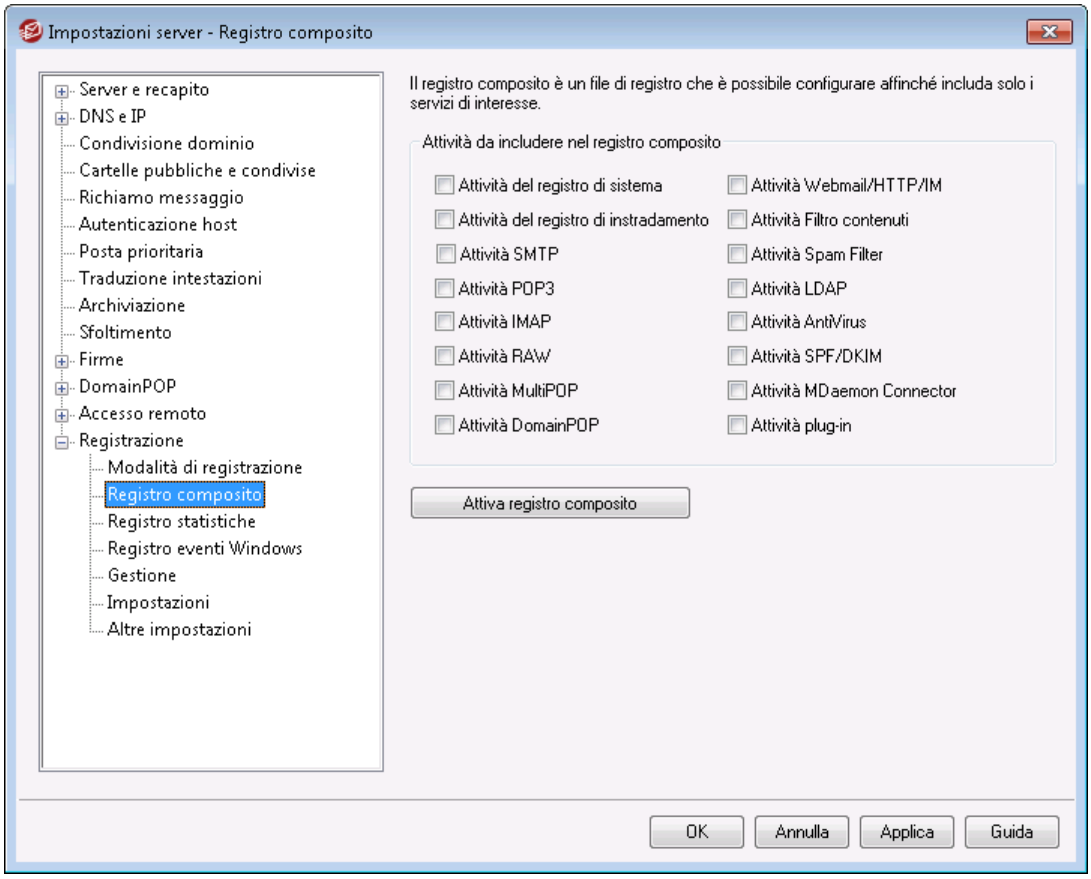
Registra ogni servizio in un file di registro separato
Selezionare questa casella di controllo se si desidera che MDaemon gestisca registri separati per servizio anziché in un unico file. Se si specifica questo comando, ad esempio, MDaemon registrerà l'attività SMTP nel file `MDaemon-SMTP.log` e l'attività IMAP nel file `MDaemon-IMAP.log`. È necessario selezionare questa opzione quando si esegue una sessione di configurazione o un'istanza Servizi terminal di MDaemon, in modo che le informazioni registrate vengano visualizzate nelle schede dell'interfaccia.

Cartella dei file registro:
Utilizzare questa opzione per specificare il percorso della cartella dei file registro.

File BadAddress.txt

Oltre ai file di registro, MDaemon mantiene il file `BadAddress.txt` nella cartella dei registri. Quando il recapito a un indirizzo ha come risultato un errore 5xx, l'indirizzo verrà aggiunto al file. Questo può essere d'aiuto, ad esempio, per identificare gli indirizzi non validi nella lista di distribuzione più rapidamente rispetto a cercare nei registri SMTP in uscita. Il file viene rimosso automaticamente ogni notte a mezzanotte per impedire che le dimensioni aumentino troppo.

3.1.15.2 Registro composito



Registro composito

Attività da includere nel registro composito

L'opzione Vista registro composito è disponibile nel menu Finestre della barra dei menu di MDaemon. Se si fa clic su questa opzione, nella visualizzazione principale di MDaemon verrà aggiunta una finestra in cui sono riportate informazioni appartenenti a una o più schede di Monitoraggio eventi. Utilizzare i comandi di questa sezione per specificare le schede di cui visualizzare le informazioni nella finestra di visualizzazione del registro composito. È possibile combinare le informazioni provenienti dalle schede seguenti:

Sistema - Attività di sistema, quali l'inizializzazione dei servizi e l'abilitazione/disabilitazione dei vari server di MDaemon.

Instradamento - Informazioni relative all'instradamento (To, From, Message-ID e così via) di ciascun messaggio analizzato da MDaemon.

SMTP - Attività di invio/ricezione delle sessioni che utilizzano il protocollo SMTP.

POP3 - Attività degli utenti che raccolgono la posta elettronica da MDaemon mediante il protocollo POP3.

IMAP - Sessioni di posta in cui è utilizzato il protocollo IMAP.

RAW - Attività di posta RAW o generata dal sistema.

MultiPOP - Attività di raccolta della posta MultiPOP di MDaemon.

DomainPOP - Attività DomainPOP di MDaemon.

Webmail/HTTP/IM - Attività di Webmail e attività relativa ai messaggi istantanei.

Filtro contenuti - Operazioni di Filtro contenuti.

Spam Filter - Attività di Spam Filter.

LDAP - Vengono visualizzate le attività del server LDAP.

AntiVirus - Operazioni antivirus.

SPF/DKIM - Attività SPF (Sender Policy Framework) e DKIM.

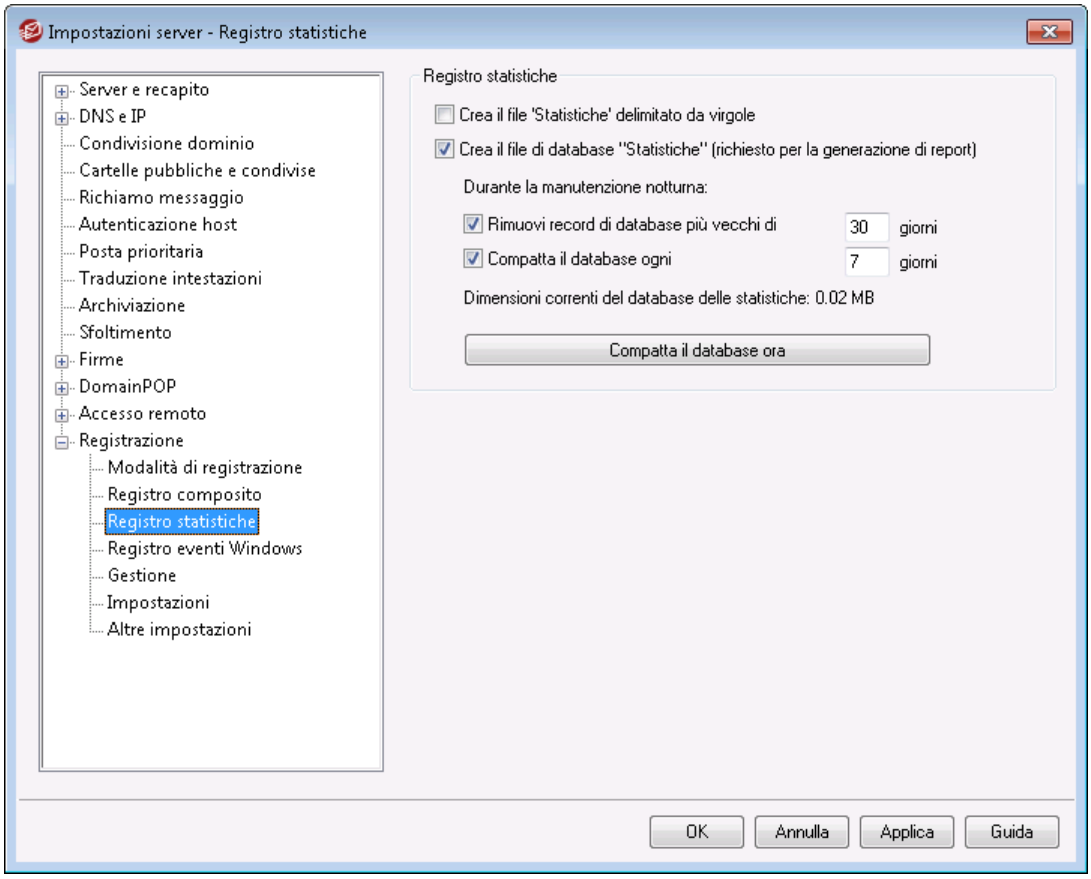
MDaemon Connector - Attività di MDaemon Connector.

Attività plug-in - Attività dei plug-in di MDaemon.

Attiva registro composito

Fare clic su questo pulsante per avviare la finestra del registro composito nella finestra principale di MDaemon. La finestra può essere attivata anche dal menu Finestre della barra dei menu di MDaemon.

3.1.15.3 Log statistiche



Log statistiche

Crea file di log "Statistiche" delimitato da virgole
Utilizzare questa opzione per gestire un file delle statistiche delimitato da virgole, che contenga i dati relativi al numero dei messaggi in entrata e in uscita, le statistiche dello spam, statistiche dell'antivirus e simili. L'opzione è disabilitata per impostazione predefinita.

Crea file di database "Statistiche" (richiesto per i rapporti)
Selezionare questa casella per registrare le informazioni statistiche relative all'attività di MDaemon in un file di database SQLite. Il database contiene informazioni sull'utilizzo della larghezza di banda da parte di MDaemon, il numero di messaggi in entrata e in uscita, le statistiche sullo spam e simili. Per impostazione predefinita, questo database è memorizzato nella cartella "`MDaemon\StatsDB`" e vengono conservati 30 giorni di dati, ma è possibile definire il periodo di conservazione dei dati per aumentare o ridurre i 30 giorni predefiniti. I dati che eccedono i limiti definiti vengono rimossi durante il processo di manutenzione notturno. È inoltre possibile specificare con quale frequenza MDaemon deve compattare il database per risparmiare spazio.

La pagina dei rapporti nell'interfaccia Web di Remote Administration di MDaemon utilizza questo database per generare una varietà di report messi a disposizione degli

amministratori globali. Per ogni report, i dati possono essere generati per intervalli di date diversi predefiniti o l'amministratore può specificare un intervallo di date personalizzato. È possibile scegliere uno dei report seguenti:

- Reporting avanzato sulla larghezza di banda
- Confronto tra messaggi in entrata e in uscita
- Confronto tra messaggi buoni e messaggi indesiderati (percentuale di posta elettronica indesiderata o virus)
- Messaggi in entrata elaborati
- Destinatari principali per numero di messaggi
- Destinatari principali per dimensioni dei messaggi
- Messaggi in uscita elaborati
- Fonti principali di spam (domini)
- Principali destinatari dei messaggi di spam
- Virus bloccati per tempo
- Virus bloccati per nome

Durante la manutenzione notturna:
Le opzioni riportate di seguito consentono di controllare le attività relative al database che MDaemon deve eseguire durante la manutenzione notturna.

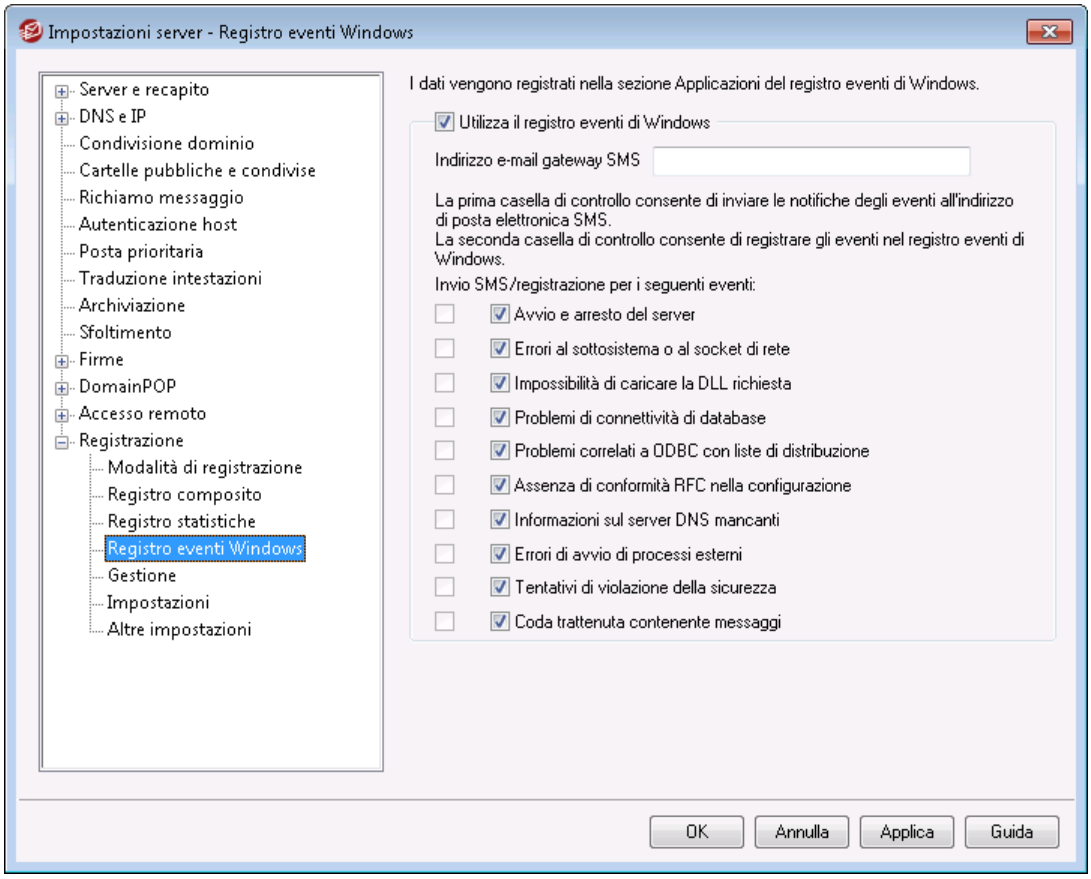
Rimuovere i record del database più vecchi di
Utilizzare questa opzione per specificare il numero di giorni di record di database delle statistiche che si desidera conservare. L'impostazione predefinita è abilitata e impostata su 30 giorni.

Comprimi database ogni
Utilizzare questa opzione per compattare periodicamente il database e risparmiare spazio. Per impostazione predefinita, l'opzione è attivata e impostata per la compattazione del database ogni 7 giorni.

Dimensioni correnti del database delle statistiche:
Le dimensioni effettive del database delle statistiche sono riportate qui.

Comprimi database ora
Fare clic su questo pulsante per avviare immediatamente la compattazione del database.

3.1.15.4 Registro eventi Windows



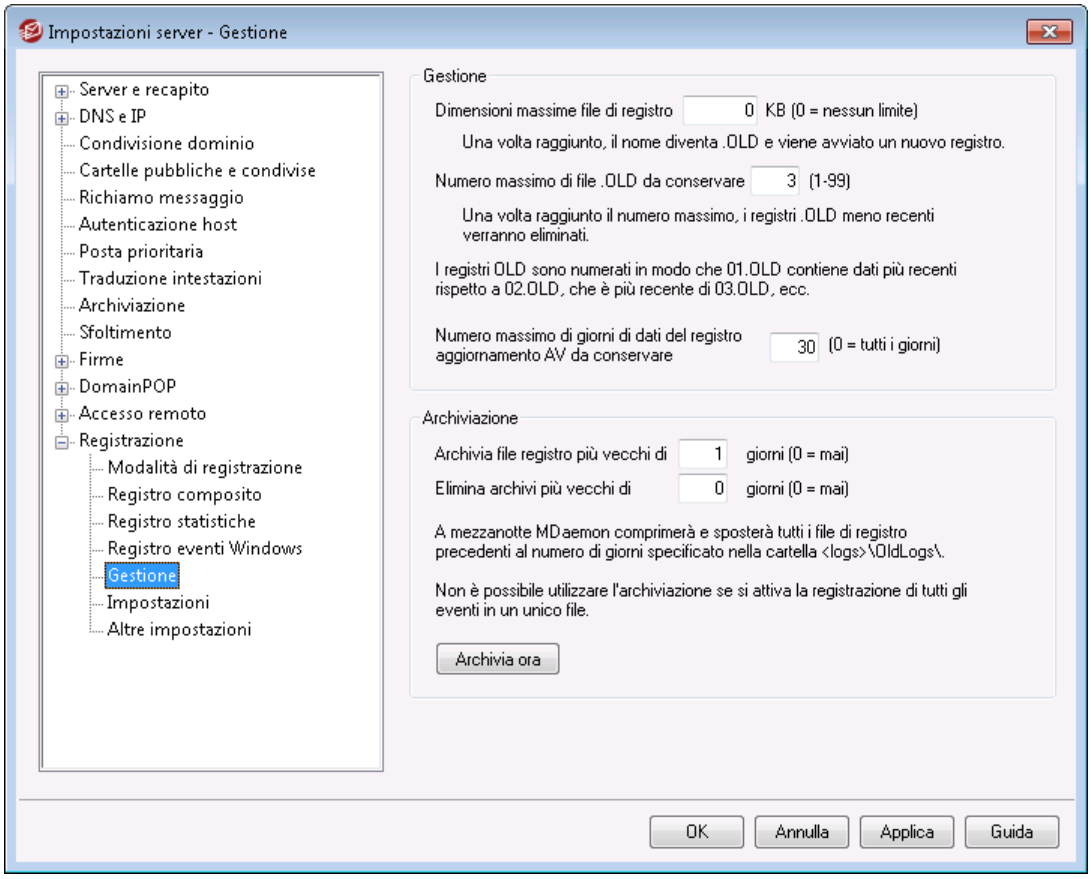
Utilizza il registro eventi di Windows
Fare clic su questa casella di controllo se si desidera registrare errori di sistema critici, avvisi e altri eventi nella sezione Applicazioni del registro eventi di Windows.

Indirizzo e-mail gateway SMS
Utilizzare questa opzione se si desidera inviare i dati dell'evento per qualsiasi evento indicato sotto a un dispositivo in un messaggio di testo SMS. A tal fine, specificare l'indirizzo e-mail del gateway da e-mail a SMS (messaggi di testo) del proprio provider di telefonia, ad esempio quello di Verizon, che è `NumeroTelefono@vtext.com` (ad es. `8175551212@vtext.com`). Utilizzare quindi le caselle di controllo nella colonna SMS per specificare gli eventi che si desidera inviare al dispositivo.

Invio SMS | Registrazione per i seguenti eventi:
Utilizzare le opzioni SMS per indicare gli eventi che si desidera inviare a un dispositivo mediante messaggio di testo. Utilizzare l'opzione di registrazione per indicare gli eventi che si desidera registrare nella sezione Applicazione del registro eventi Windows. Per inviare i messaggi SMS è necessario specificare l'indirizzo e-mail del gateway da e-mail a SMS del proprio provider di telefonia nell'opzione indicata sopra. Inoltre, qualsiasi evento che generi un messaggio di notifica al gateway SMS causerà l'elaborazione della coda remota; le notifiche verranno considerate e trattate come messaggi e-mail "urgenti".

L'opzione SMS per gli eventi di *Avvio e arresto del server* invieranno solo un messaggio da e-mail a SMS per gli eventi di avvio, non per quelli di arresto.

3.1.15.5 Gestione



Gestione

Dimensione max file registro [xx] KB
Indica la dimensione massima in kilobyte consentita per i file registro. Una volta raggiunta tale dimensione, il file di registro viene copiato in "`LOGFILENAME.01.OLD`" e viene creato un nuovo file di registro. Se il file `LOGFILENAME.01.OLD` esiste già, il file preesistente sarà eliminato o rinominato "`LOGFILENAME.02.OLD`," a seconda del valore impostato nell'opzione "*Numero massimo di file .OLD da conservare*" sotto. Specificare "0" in questa opzione se non si desidera limitare le dimensioni del file. Per impostazione predefinita, questa opzione è impostata su "0".

Numero massimo di file .OLD da conservare (1-99)
Quando si utilizza l'opzione indicata sopra per limitare le dimensioni del file di registro, questa opzione regola il numero di iterazioni di un determinato file `.OLD` saranno

mantenute prima dell'eliminazione del meno recente. Questi file di backup vengono rinominati "LOGFILENAME.01.OLD," "LOGFILENAME.02.OLD" e così via, con il file più recente sempre elencato per primo. Ad esempio, SMTP(out).log.01.old contiene dati più recenti di SMTP(out).log.02.old, e così via. Quando viene raggiunto il numero massimo, viene eliminato il file meno recente quando viene creato un nuovo file.

Numero massimo di giorni di dati del registro aggiornamento AV (0=nessun limite)
Questa opzione regola il numero massimo di giorni per cui il registro di aggiornamento dell'antivirus (vale a dire avupdate.log) conserverà i dati. Ogni notte a mezzanotte e anche a ogni avvio di dopo l'aggiornamento, i dati meno recenti saranno eliminati dal file. Specificare "0" in questa opzione se non si desidera impostare un limite di tempo. Per impostazione predefinita vengono conservati gli ultimi 30 giorni di dati.

Il registro di aggiornamento AV viene conservato per impostazione predefinita e le relative dimensioni sono limitate a 5120 KB. Se si desidera cambiare il limite di dimensioni o disabilitare il registro di aggiornamento AV, le relative opzioni sono disponibili nella finestra di dialogo Configurazione aggiornamento AV 690, raggiungibile in: **Sicurezza » AntiVirus » Aggiornamento AV » Configurazione aggiornamento » Varie**.

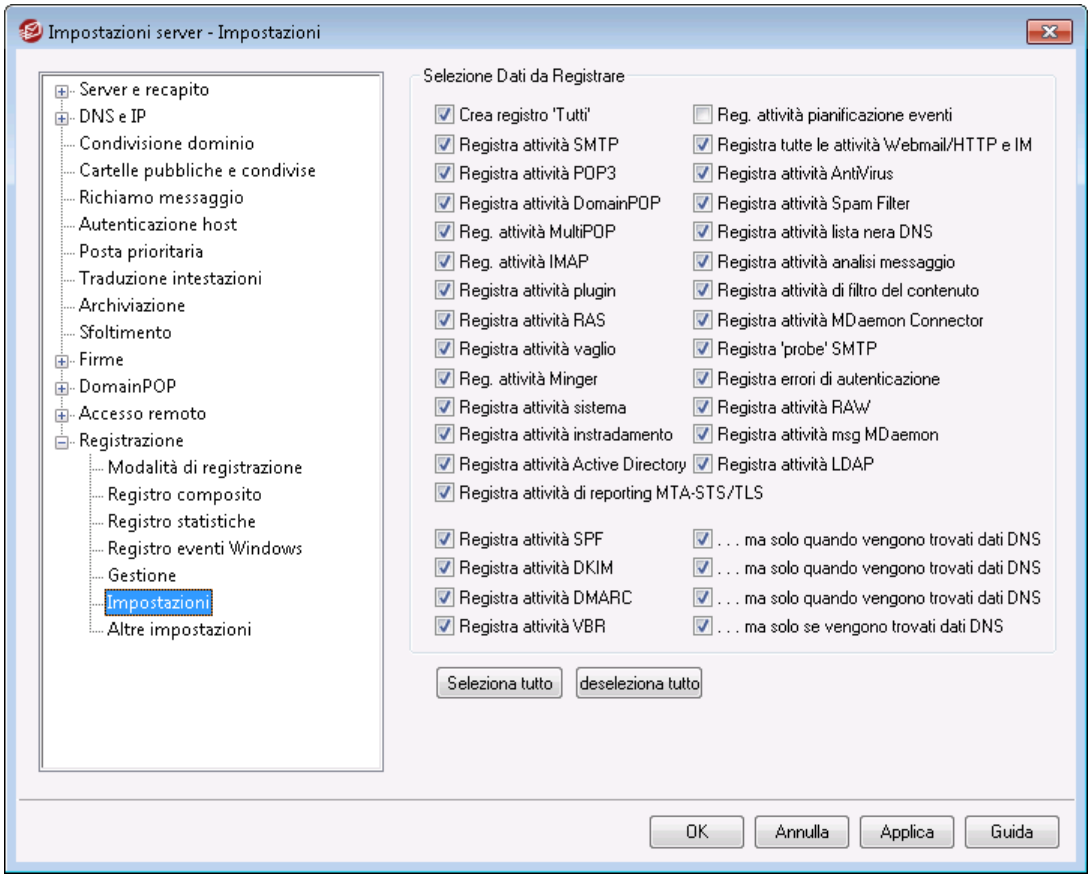
Archiviazione

Archivia file registro precedenti a [XX] giorni (0=mai)
Specificare questa opzione per archiviare i file registro che esistono da più giorni di quelli indicati. Ogni giorno, a mezzanotte, MDaemon comprimerà mediante ZIP i file con estensione .log e .old esistenti e li sposterà nella sottocartella \Logs\OldLogs\, eliminando i file originali. Da questo processo vengono esclusi i file in uso. Inoltre, se nella schermata "*Registra tutto in un solo file (MDaemon-all.log)*" nella schermata Modalità registrazione 169.

Elimina gli archivi più vecchi di XX giorni (0 = mai)
Utilizzare questa opzione per eliminare automaticamente i file registro archiviati che esistono da più giorni di quelli specificati. Utilizzare "0" in questa opzione se non si desidera eliminare automaticamente gli archivi. Gli archivi vengono eliminati durante le operazioni di pulizia a mezzanotte di ogni giorno.

Archivia ora
Se si fa clic su questo pulsante, i file registro precedenti verranno archiviati immediatamente anziché a mezzanotte.

3.1.15.6 Impostazioni



Seleziona dati da registrare

Crea registro 'All'
Selezionare questa opzione per generare il file "`*-all.log`" contenente l'insieme di tutte le attività registrate.

Registra attività SMTP
Selezionare questa opzione per registrare tutte le attività SMTP di invio/ricezione di MDaemon.

Registra attività POP3
Selezionare questa casella di controllo per registrare tutte le attività di posta POP, ossia le sessioni di raccolta della posta POP di tutti gli utenti.

Registra attività DomainPOP
Selezionare questa casella di controllo per registrare tutte le attività di posta DomainPOP.

Registra attività MultiPOP
Selezionare questa casella di controllo per registrare tutte le attività di posta MultiPOP degli utenti.

Registra attività IMAP
Attivando questa opzione tutte le sessioni IMAP degli utenti saranno incluse nei file di registro di MDaemon.

Registra attività plugin
Questa opzione consente di registrare tutte le attività correlati ai plugin.

Registra attività RAS
Selezionare questa opzione per copiare nel file registro le attività di connessione/disconnessione RAS. Tali informazioni sono utili per la diagnosi dei problemi di connessione remota.

Registra attività di screening
Fare clic su questa casella di controllo per includere le attività di screening di MDaemon nel file di registro di MDaemon.

Registra attività Minger
Selezionare questa casella di controllo per registrare tutte le attività del server Minger.

Registra attività sistema
Questa opzione consente di registrare tutte le attività di sistema.

Registra attività instradamento
Questa opzione consente di registrare tutte le attività di analisi delle code in ingresso, locali e remote.

Registra attività Active Directory
Questa opzione consente di registrare le attività di Active Directory correlate a MDaemon.

Registra attività di reporting MTA-STS/TLS
Registra tutte le attività correlate a SMTP MTA Strict Transport Security (MTA-STS).

Reg. attività pianificazione eventi
Attivare questa casella di controllo se si desidera registrare tutte le attività dell'Utilità di pianificazione degli eventi 388.

Registra tutte le attività Webmail/HTTP/IM
Selezionare questa opzione per registrare tutte le attività Webmail e HTTP, nonché le attività di MDaemon Instant Messenger. Se questa opzione è disattivata, i registri di Webmail e HTTP vengono creati, ma includono solo la data e l'ora di avvio e di arresto di Webmail. Le altre attività Webmail, HTTP o IM non vengono registrate.

Registra attività AntiVirus
Questa opzione consente di registrare tutte le attività dell'AntiVirus.

Registra attività Spam Filter
Selezionare questa opzione per registrare le attività Spam Filter

Registra attività lista bloccati DNS
Questa opzione configura MDaemon in modo che registri l'attività della lista bloccati DNS. L'utilizzo di questa opzione consente di disporre di un facile riferimento ai siti registrati come bloccati.

Registra attività analisi messaggio
Per determinare i destinatari dei messaggi, MDaemon svolge regolarmente un'intensa attività di analisi sintattica dei messaggi. Selezionare questa casella di controllo per includere tali informazioni nel file registro.

Registra attività filtro contenuti
Selezionare questa casella per includere nel file di registro le attività della funzione Filtro contenuti.

Registra attività MDaemon Connector
Tramite questa opzione è possibile scegliere di registrare le attività MDaemon Connector.

Registra "probe" SMTP
Scegliere questa opzione per registrare le sessioni SMTP quando non vengono trasferiti dati di messaggio dal server di invio, ossia nel caso in cui il server di invio non utilizza il comando DATA.

Registra errori di autenticazione
Utilizzare questa opzione per registrare gli errori di autenticazione.

Registra attività RAW
Registra le attività dei messaggi RAW di MDaemon.

Registra attività msg MDaemon
Registra le attività dei messaggi.

Registra attività LDAP
Registra tutte le attività LDAP.

Registra attività SPF
Selezionare questa casella di controllo per registrare le attività di ricerca SPF.

> **...ma solo se vengono trovati dati DNS**
> Specificare questa opzione se si registrano le attività SPF ma si desidera, durante la ricerca DSN, tenere traccia solo delle ricerche SPF con esito positivo anziché registrare ogni singola operazione.

Registra attività DKIM
Selezionare questa opzione se si desidera registrare le attività DomainKeys Identified Mail (DKIM).

...ma solo se vengono trovati dati DNS
Specificare questa opzione se si registrano le attività DKIM ma si desidera tenere traccia solo delle istanze contenenti dati DNS anziché registrare ogni singola operazione.

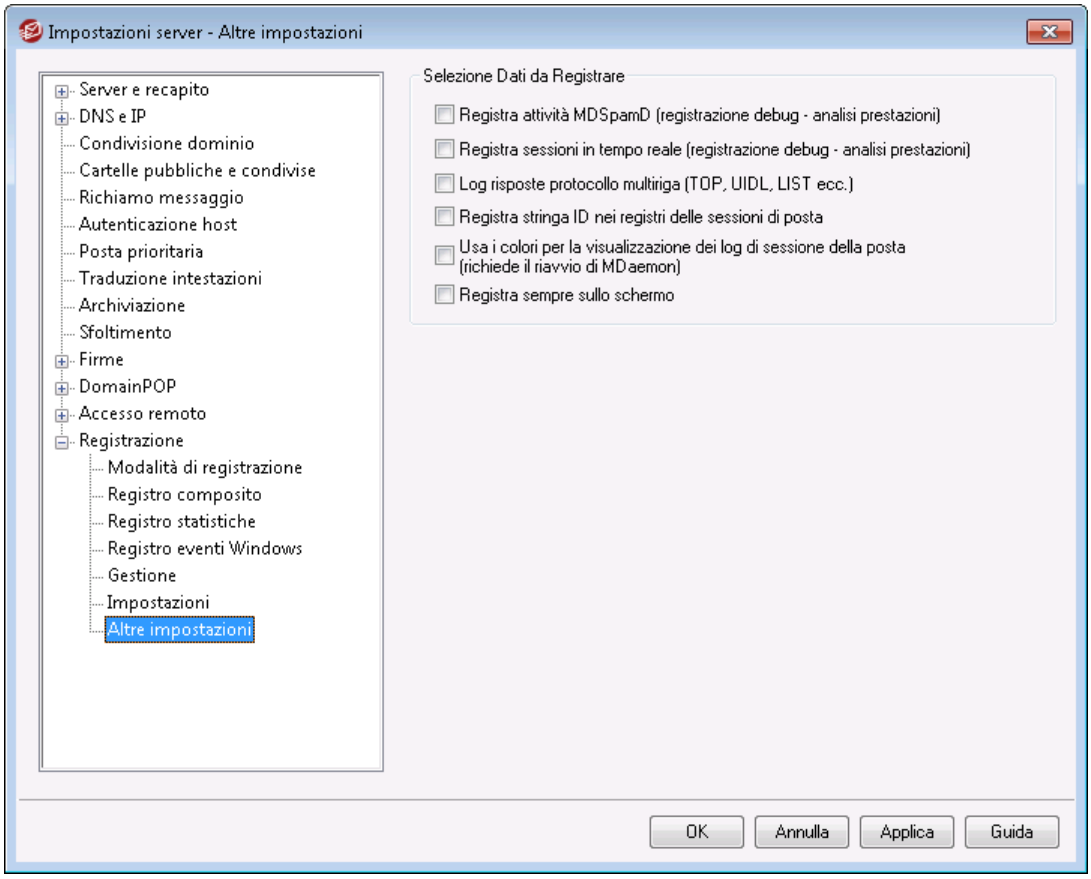
Registra attività DMARC
Selezionare questa casella di controllo per registrare le attività DMARC.

...ma solo se vengono trovati dati DNS
Specificare questa opzione se si registrano le attività DMARC ma si desidera tenere traccia solo delle istanze contenenti dati DNS anziché registrare ogni singola operazione.

Registra attività VBR
Selezionare questa casella di controllo per registrare tutte le attività di certificazione dei messaggi 560.

...ma solo quando vengono trovati dati DNS
Se si registra l'attività di certificazione dei messaggi, questa opzione consente di eseguire la registrazione solo dei dati di certificazione individuati durante le ricerche DNS.

3.1.15.7 Altre impostazioni



Seleziona dati da registrare

Registra tutte le attività MDSpamD locali (registrazione debug - esaurimento prestazioni)
Selezionare questa opzione per registrare tutte le attività locali di MDSpamD. Vedere l'avviso riportato di seguito.

Registra sessioni in tempo reale (registrazione debug - esaurimento prestazioni)
Per ottimizzare le risorse, le informazioni sulla sessione vengono di solito registrate al termine della sessione. Selezionare questa opzione per registrare le attività in tempo reale.

Se si utilizzano una o entrambe le opzioni di registrazione precedenti, è possibile che le prestazioni del sistema di posta risultino ridotte, in base al computer in uso e al livello di attività. In genere, è opportuno utilizzare queste opzioni solo a scopo di debug.

Registra le risposte di protocolli multiriga (ad esempio UIDL e LIST)
Le risposte alle richieste di protocollo possono occupare più righe. Selezionare questa casella di controllo per registrare anche le righe aggiuntive.

Se si seleziona questa opzione, è possibile che la quantità di informazioni registrate aumenti eccessivamente. Poiché il numero di righe in una risposta non può essere determinato in anticipo e poiché alcune risposte possono "riempire" il file di registro con informazioni potenzialmente non necessarie (POP TOP, ad esempio, elenca il contenuto effettivo del messaggio), non si consiglia di usare questa funzione se le dimensioni del file di registro o la lunghezza dei dati costituiscono un fattore rilevante.

Registra stringa ID nei registri delle sessioni di posta
Selezionare questa casella di controllo per includere stringhe di identificazione `[%d:%d]` nelle registrazioni delle sessioni di posta.

Usa i colori per la visualizzazione dei registri delle sessioni di posta (richiede il riavvio di MDaemon)
Selezionare questa opzione se si desidera applicare colori al testo visualizzato nelle diverse schede Monitoraggio e registrazione eventi[75] nell'interfaccia utente di MDaemon. Questa opzione è disattivata per impostazione predefinita e l'attivazione/disattivazione richiede un riavvio di MDaemon prima che la modifica diventi effettiva. Vedere: "Registri di sessioni contraddistinti da colori" per ulteriori informazioni.

Registra sempre su schermo
Selezionare questa opzione se si desidera che i dati registrati vengano copiati nell'interfaccia utente di MDaemon anche quando è ridotta a icona o è in esecuzione nella barra delle applicazioni.

Se la casella di controllo è deselezionata, i dati di registrazione non vengono copiati nella finestra Monitoraggio eventi quando MDaemon è in esecuzione nella barra delle applicazioni. Di conseguenza, l'attività più recente non sarà riportata in nessuna delle schede del riquadro Monitoraggio eventi quando si apre MDaemon per la prima volta, ma verranno visualizzate le informazioni registrate a partire da quel punto.

Registri di sessioni contraddistinti da colori

Nell'interfaccia utente di Mdaemon[75], le schede dell'interfaccia utente in cui vengono visualizzate le attività relative a instradamento, posta in ingresso SMTP, posta in uscita SMTP, IMAP, POP, MultiPOP e DomainPOP ora possono essere contraddistinte da colori che consentono di separare visivamente gli eventi durante una sessione. Questa funzione è disattivata per impostazione predefinita, ma è attivabile tramite l'opzione "*Usa i colori per la visualizzazione dei registri delle sessioni di posta*" disponibile in: Registrazione » Altre impostazioni[182] e Preferenze » Interfaccia utente[497]. È possibile modificare i colori predefiniti del testo modificando la sezione `[Colori]` del file `LogColors.dat`. Per un elenco dei colori predefiniti, consultare il grafico.

Se si desidera utilizzare i colori ma non si desidera applicare colori a uno o più degli elementi in elenco, impostare il valore di tali elementi su zero (ad esempio `SpamFilter=0`). In questo modo gli elementi prescelti utilizzeranno il colore

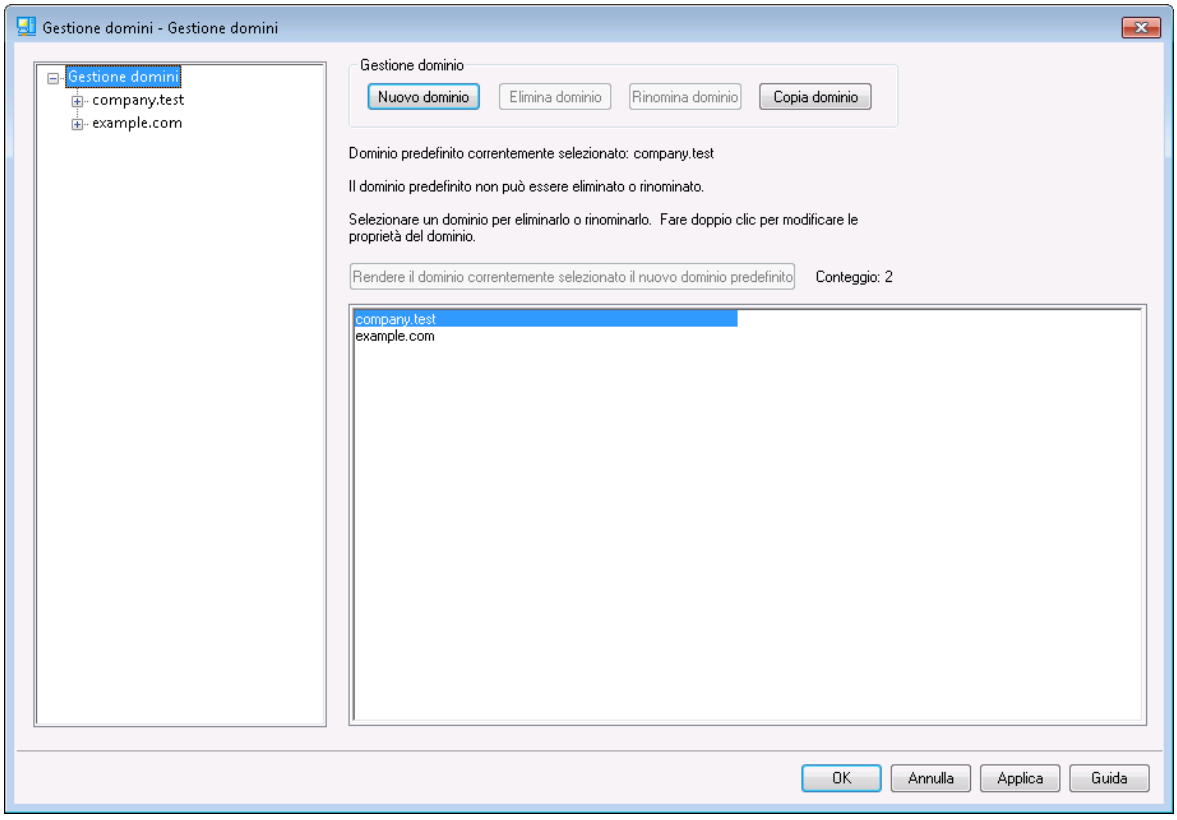
`Predefinito`. Per `Background` e `SelectedBackground` l'impostazione del valore su zero non funziona. Se si desidera modificare uno di questi elementi, è necessario fornire un nuovo valore di colore. I valori dei colori vengono specificati nel seguente formato esadecimale: "`0xbbggrr`", dove "bb" indica l'intensità relativa per il colore blu, "gg" per il verde e "rr" per il rosso. Ad esempio, "`Error=0x0000ff`" imposta il testo dell'errore su rosso. **Nota:** si tratta di un ordine di colori opposto rispetto a quello tradizionale, che solitamente è "`rrggbb`". Se i colori vengono modificati è necessario riavviare MDaemon o creare un file denominato `COLORS.SEM` e collocarlo nella cartella `\APP\` di MDaemon.

Colori di registro predefiniti

Background=0x000000	Colore di sfondo; Nero
SelectedBackground=0xff0000	Colore di sfondo selezionato; Blu
Default=0xffffff	Colore testo predefinito; Bianco
Processing=0x00ffff	Attività di elaborazione e analisi interna; il valore predefinito è Giallo
DataIn=0x008040	Dati in arrivo da un altro server; il valore predefinito è Verde scuro
DataOut=0x00ff00	Dati in uscita inviati a un altro server; il valore predefinito è Verde brillante
Error=0x0000ff	Messaggi di errore; il valore predefinito è Rosso
TCPIP=0xff8000	Attività relative a TCP/UDP/DNS/PTR; il valore predefinito è Azzurro
SpamFilter=0x0080ff	Filtro spam; il valore predefinito è Arancione
AntiVirus=0xdda0dd	Elaborazione di AntiVirus; il valore predefinito è Prugna
DKIM=0xff00ff	Attività relative a DKIM; il valore predefinito è Fucsia
VBR=0x40c0ff	Attività relative a VBR (Vouch-by-Reference); il valore predefinito è Arancione chiaro
SPF=0x808080	Attività relativa a SPF (Sender Policy Framework); il valore predefinito è Grigio
Plugins=0x0080c0	Qualsiasi messaggio inviato da un plug-in; il valore predefinito è Marrone
Localq=0x00ffff	Instradamento alla coda locale; il valore predefinito è Giallo
Spam=0x0080ff	Instradamento di messaggi spam; il valore predefinito è Arancione

Restricted=0x40c0ff	Instradamento di messaggi con restrizioni; il valore predefinito è Arancione chiaro
BlackList=0x808080	Instradamento dei messaggi in lista bloccati; il colore predefinito è il grigio
Gateway=0x00ff00	Instradamento di messaggi al gateway; il valore predefinito è Verde chiaro
Inboundq=0xff8000	Instradamento di messaggi in entrata; il valore predefinito è Azzurro
PublicFolder=0xdda0dd	Instradamento di messaggi di cartelle pubbliche; il valore predefinito è Prugna

3.2 Gestione domini



MDaemon offre il supporto completo per più domini, gestiti mediante Domain Manager. In Domain Manager è infatti possibile gestire nomi di dominio, indirizzi IP, impostazioni di eliminazione di account e messaggi, impostazioni di Webmail e altre opzioni specifiche dei domini.

MDaemon supporta indirizzi IP sia singoli che multipli. Questi indirizzi possono essere univoci per singoli domini o condivisi. Alcune funzioni essenziali, inoltre, quali Account,

Liste di distribuzione e Impostazioni sicurezza, vengono utilizzate a livello di singolo dominio. Quando, ad esempio, si crea un account, occorre specificare il dominio di appartenenza del nuovo account, analogamente alle liste di distribuzione. Di conseguenza alcune funzioni, ad esempio Vaglio IP 571 e Scudo IP 528 sono legate al singolo dominio.

Altre funzioni invece, ad esempio Corrispondenza nomi 162 di DomainPOP 151, sono legate esclusivamente al dominio predefinito. Tale dominio viene anche visualizzato per impostazione predefinita in diverse opzioni, ad esempio quando si creano nuovi account o liste di distribuzione. Inoltre, per supportare la gestione dei messaggi di sistema di MDaemon, esistonoAlias 847 predefiniti che puntano a numerosi nomi di caselle postali riservate al nome di dominio predefinito di MDaemon, anziché agli altri domini:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

Infine, per il supporto di domini multipli, per impostazione predefinita, MDaemon richiede ai propri utenti di utilizzare l'indirizzo di posta elettronica completo, ad esempio "`utente01@esempio.com`", come valore dell'ID utente anziché solo la parte dell'indirizzo relativa alla casella postale, ad esempio "`utente01`"). Tuttavia, alcuni client di posta di versioni precedenti non supportano l'uso del simbolo "@" nel campo riservato all'ID utente. Di conseguenza, per gestire tali client, è possibile specificare un carattere alternativo nella schermata Sistema 501 > Preferenze. Questo valore può contenere fino a 10 caratteri, il che consente di immettere una stringa di caratteri che funga da delimitatore invece di un singolo carattere come "$". Ad esempio, l'utilizzo di "**`.at.`**" consente di creare l'ID utente "`utente02.at.esempio.com`". È possibile inoltre disabilitare il requisito indirizzo di posta completo, consentendo in tal modo l'uso esclusivo della parte dell'indirizzo relativa alla casella postale come valore dell'ID utente. Tale procedura, tuttavia, non è consigliata e potrebbe determinare problemi nel caso in cui si disponga di più di un dominio.

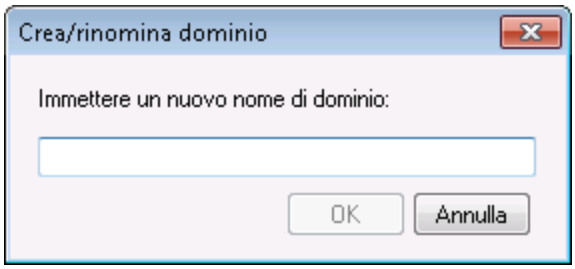
Elenco domini

Nella sezione sul lato sinistro di questa finestra di dialogo è possibile visualizzare l'elenco dei domini, con i collegamenti a ciascuna schermata utilizzati per configurare le diverse impostazioni specifiche del dominio. Il Dominio predefinito rappresenta il primo dell'elenco seguito da tutti gli altri domini visualizzati in ordine alfabetico. L'elenco sulla destra viene utilizzato per eliminare e rinominare i domini e per specificare il dominio predefinito. È possibile fare doppio clic su un dominio dell'elenco per cambiare il dominio e configurarne le impostazioni.

Gestione dominio

Nuovo dominio

Per creare un nuovo dominio: selezionare *Nuovo dominio*, digitare il nome del nuovo dominio nella finestra di dialogo Crea/aggiorna dominio, quindi fare clic su *OK*.



Normalmente, il valore inserito in questo campo corrisponde al nome del dominio Internet registrato che un server DNS trasforma nell'indirizzo IP del sistema locale su cui è in esecuzione il server oppure in un alias qualificato di quel nome. In alternativa, è possibile utilizzare come nome del dominio in uso un nome a uso interno o un nome di dominio privato e non altrimenti valido, ad esempio "`company.mail`". Affinché la posta possa essere distribuita correttamente in questo tipo di configurazione del server, può essere necessario utilizzare la funzione Traduzione intestazione 130 e/o Sostituzione nomi di dominio 158.

Elimina dominio
Per eliminare un dominio: selezionare il dominio dall'elenco sottostante, fare clic su *Elimina dominio*, quindi confermare la decisione di eliminare il dominio facendo clic su *Sì*.

> Non è possibile eliminare o rinominare il dominio predefinito. Per eliminarlo o rinominarlo, è necessario specificare prima un dominio diverso come dominio predefinito.

Rinomina dominio
Per rinominare un dominio: selezionare un dominio dall'elenco sottostante, fare clic su *Rinomina dominio*, digitare il nuovo nome del dominio nella finestra di dialogo Crea/aggiorna dominio, quindi fare clic su *OK*.

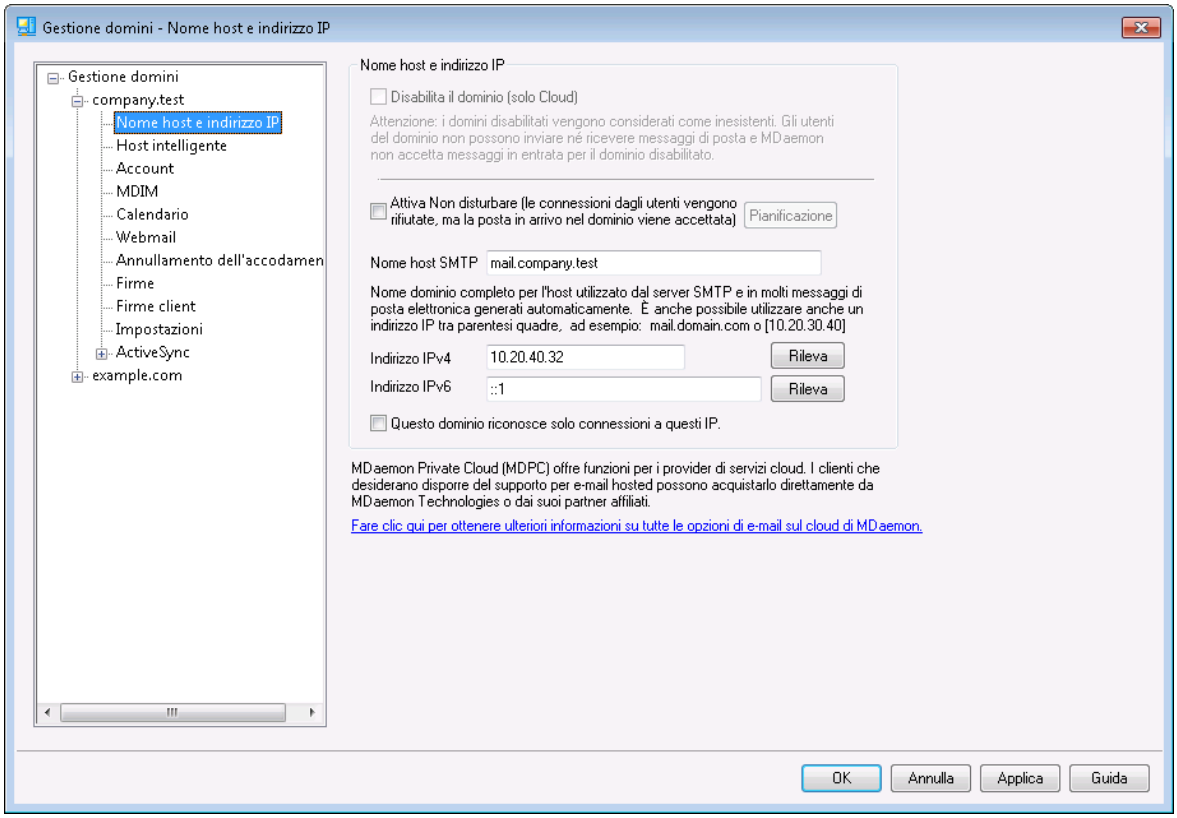
Copia dominio
Per creare un nuovo dominio con impostazioni che corrispondono a un altro dominio, selezionare un dominio dall'elenco, fare clic su questo pulsante e specificare un nome per il nuovo dominio. Accounts, elenchi ed elementi simili non verranno copiati nel nuovo dominio.

Rendere il dominio correntemente selezionato il nuovo dominio predefinito
Se si desidera cambiare il dominio predefinito di MDaemon, selezionare il dominio desiderato dall'elenco sotto e fare clic su questo pulsante.

Vedere:

Preferenze » Sistema 501

3.2.1 Nome host e indirizzo IP



Nome e IP host

Disattiva dominio (solo cloud)
Selezionare questa casella di controllo per disabilitare il dominio. I domini disabilitati sono trattati da MDaemon come se non esistessero. Gli utenti del dominio non saranno in grado di inviare o ricevere messaggi di e-mail e MDaemon non accetterà posta in arrivo per il dominio. L'opzione è disponibile solo in MDaemon Private Cloud.

Attiva Non disturbare
Utilizzare questa opzione per attivare la modalità Non disturbare per un dominio. Quando attiva, il dominio rifiuterà tutte le connessioni da parte di tutti gli utenti per tutti i servizi ma continuerà ad accettare messaggi dall'esterno.

Pianificazione
Fare clic su questo pulsante per pianificare l'avvio e l'arresto della modalità "Non disturbare". Se ad esempio si configura dal 1 maggio 2020 al 30 giugno 2020 dalle 17:00 alle 7:00, dal Lunedì al Venerdì, significa che nessun servizio di posta sarà disponibile per gli utenti di quel dominio nei giorni specificati, a partire dalle 17:00 e i servizi riprenderanno alle 7:01 purché la data rientri tra il 1 maggio e il 30 giugno 2020. La cancellazione della data di inizio pianificata disattiverà la pianificazione, con l'effetto di **impostare l'opzione "Non disturbare" per il dominio per sempre**.

Nome host SMTP
Questo valore rappresenta il nome di dominio completo (FQDN, Fully Qualified Domain Name) utilizzato nell'istruzione `SMTP HELO/EHLO` al momento di inviare la posta relativa al dominio. Nel caso di connessioni in entrata, se viene utilizzata l'opzione *Il dominio riconosce solo le connessioni effettuate all'indirizzo IP dell'host*, il dominio è associato al proprio indirizzo IP e, per le connessioni effettuate al dominio, viene utilizzato il valore FQDN appropriato. Per garantire il funzionamento, tale opzione non è indispensabile, ma se sono disponibili due o più domini che utilizzano lo stesso indirizzo IP in uscita, il valore FQDN utilizzato sarà quello associato al primo dominio in ordine alfabetico.

Nella maggior parte dei casi, il valore FQDN corrisponde al *Nome dominio* o a un suo sottodominio, ad esempio, "`posta.esempio.com`", ma è possibile utilizzare anche la sintassi letterale IP, ad esempio "`[192.0.2.0]`". Se non si specifica il valore FQDN, MDaemon utilizza il valore FQDN del dominio predefinito.

Indirizzi IPv4/IPv6
Immettere gli indirizzi IPv4 e IPv6 da associare a questo dominio. Se un indirizzo IP risulta mancante, MDaemon tenterà automaticamente di rilevare un indirizo adatto per essere utilizzato.

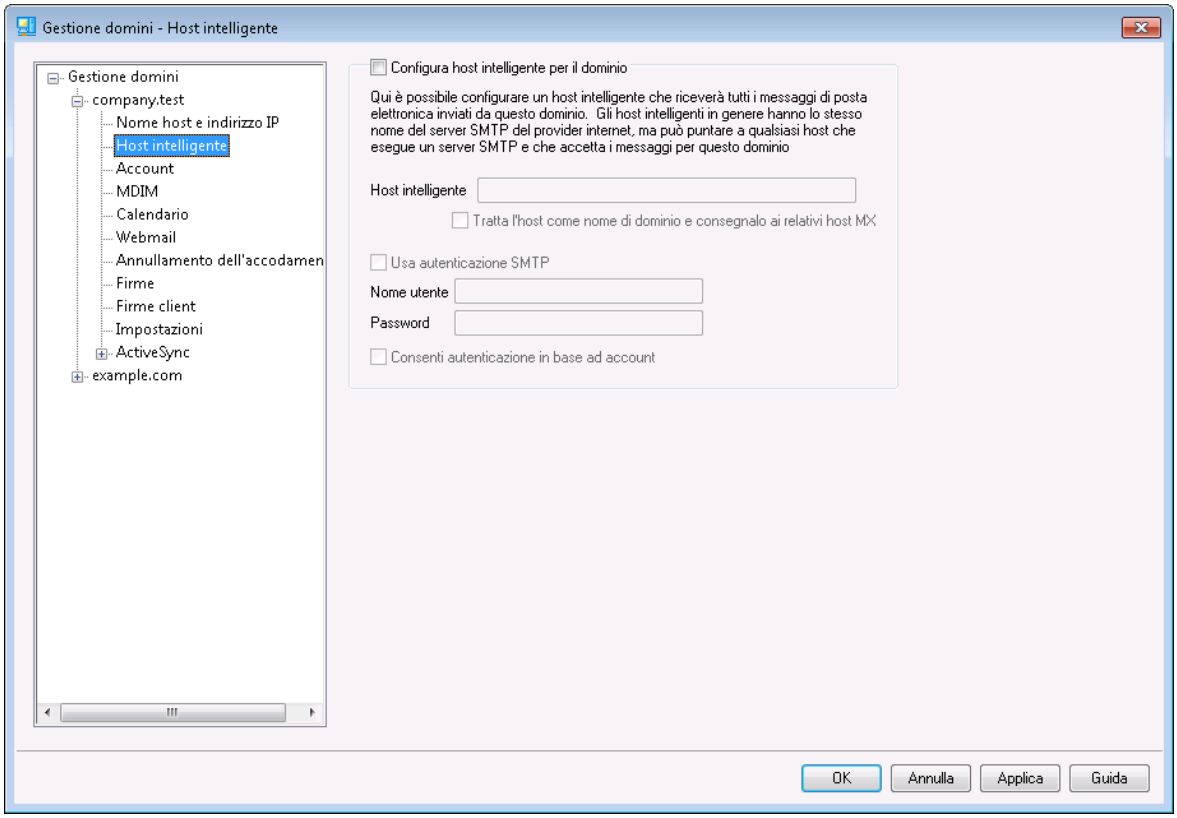
Rileva
Utilizzare questi pulsanti per rilevare gli indirizzi IPv4 e IPv6 IP che è possibile utilizzare nelle opzioni relative agli indirizzi IP corrispondenti. È possibile scegliere uno degli indirizzi IP riportati nell'elenco.

Questo dominio riconosce solo le connessioni eseguite a questi indirizzi IP
Selezionare questa casella di controllo se si desidera limitare le connessioni in ingresso al dominio agli indirizzi IP specificati sopra. Per impostazione predefinita, questa funzione è valida solo per le connessioni in entrata. L'associazione del socket in uscita è regolata da un'opzione in "Impostazioni server » Associazione 114".

Vedere:

Gestione domini 185
Preferenze » Sistema 501
Associazione 114
IPv6 113

3.2.2 Host intelligente



Configura host intelligente per il dominio

Per instradare la posta in uscita di questo dominio attraverso un host intelligente specifico invece di utilizzare le opzioni di Inoltro 97 predefinite di MDaemon, selezionare questa casella e specificare l'host intelligente. Tutta la posta in uscita del dominio sarà instradata verso l'host.

Host intelligente
Inserire il nome o l'indirizzo IP dell'ISP o dell'host di posta. Il valore corrisponde generalmente al server SMTP dell'ISP.

Non inserire in questa casella di testo il dominio predefinito o gli indirizzi IP di MDaemon. A questa voce deve corrispondere un ISP o un altro server di posta in grado di inoltrare la posta.

Considera host come nome dominio e consegna ai relativi host MX
Selezionare questa casella se si desidera considerare l'host come nome di dominio anziché come un server specifico. In questo modo MDaemon recupererà gli host MX associati al dominio ed eseguirà la connessione agli stessi.

Usa autenticazione SMTP
Fare clic su questa casella di controllo e inserire le credenziali di accesso riportate di seguito se l'*host intelligente* richiede autenticazione. Le credenziali verranno

utilizzate per tutti i messaggi SMTP in uscita inviati all'host intelligente. Se si sceglie di utilizzare l'opzione *Consenti autenticazione in base ad account*, MDaemon eseguirà l'autenticazione all'host per ogni messaggio utilizzando le credenziali *Accesso host intelligente* dell'account mittente, indicate nella schermata Servizi di posta 733 di Account Editor.

Nome utente
Immettere il nome utente o di login.

Password
Utilizzare questa opzione per specificare la password di accesso all'host intelligente.

Consenti autenticazione in base ad account
Selezionare questa casella di controllo se si desidera utilizzare l'autenticazione in base all'account per i messaggi SMTP in uscita inviati all'*host intelligente* specificato in precedenza. Anziché utilizzare le credenziali *Nome utente* e *Password* indicate, verranno utilizzate le credenziali *Accesso host intelligente* di ciascun account, specificate nella schermata Servizi di posta 733. Se per un dato account non sono state specificate credenziali dell'host intelligente, verranno utilizzate le suddette credenziali.

Per configurare l'*autenticazione in base ad account* in modo che venga utilizzata la *Password e-mail* di un account anziché la *Password host intelligente*, modificare la seguente chiave del file `MDaemon.ini`:

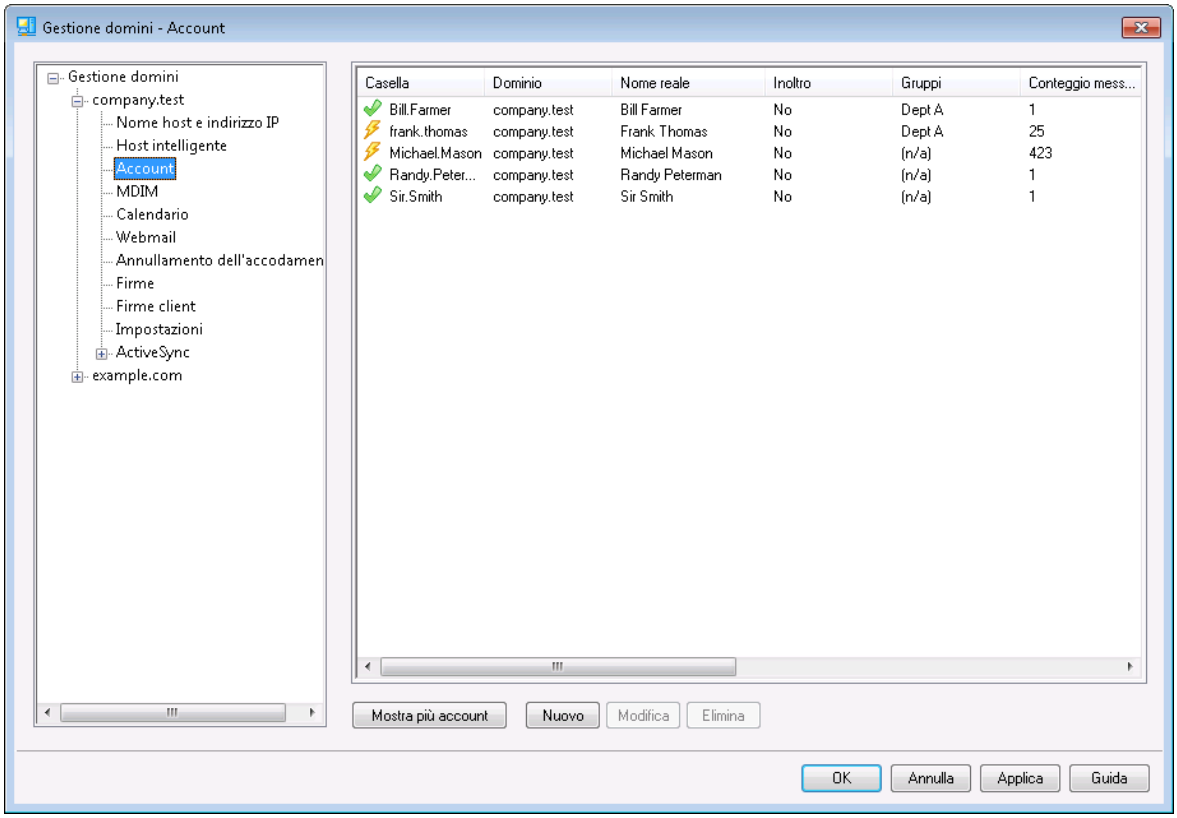
```
[AUTH]
ISPAUTHUsePasswords=Yes (il valore predefinito è No)
```

Se si abilita l'opzione `ISPAUTHUsePasswords=Yes`, con il passare del tempo tutte la password e-mail locali verranno comunicate all'host intelligente e ciò potrebbe rappresentare un rischio per la sicurezza perché queste informazioni riservate vengono comunicate a un altro server. Non è consigliabile utilizzare questa opzione a meno che l'host intelligente utilizzato non sia di assoluta fiducia e solo se questa operazione è assolutamente necessaria. Inoltre, si noti che se si utilizza questa opzione e si concede agli utenti l'autorizzazione per modificare la *password e-mail* via Webmail o in altro modo, la modifica della *password e-mail* comporterà anche la modifica della *password dell'host intelligente*. Di conseguenza, l'autenticazione di un account potrebbe non riuscire qualora la *Password e-mail* venga cambiata localmente, ma la corrispondente *Password host intelligente* non venga modificata nell'host intelligente stesso.

Vedere:

Gestione domini 185
Impostazioni server » Consegna 97
Account Editor » Servizi di posta 733

3.2.3 Account



Nella pagina degli account viene visualizzato l'elenco di tutti gli account MDaemon del dominio. Per ogni voce dell'elenco esistono delle icone relative allo stato dell'account (vedere di seguito), la casella postale, il "nome reale" del titolare dell'account, eventuali gruppi di appartenenza dell'account, il numero di messaggi e la quantità di spazio su disco utilizzato (in MB). L'elenco può essere organizzato in ordine ascendente o discendente in base a qualsiasi colonna. Fare clic su un'intestazione di colonna per applicare all'elenco l'ordine ascendente in base a tale colonna. Fare di nuovo clic sulla colonna per applicare l'ordine discendente.

Icone di stato dell'account

L'account è un amministratore globale o di dominio.


Account con accesso completo. Sono abilitati sia gli accessi POP che IMAP.


Account con accesso limitato. POP, IMAP o entrambi sono disattivati.


L'account è bloccato. MDaemon accetta la posta per l'account, ma l'utente non può inviare o controllare la posta.


Account disabilitato. È disabilitato qualsiasi accesso all'account.

Nuovo
Per creare un nuovo account, fare clic su questo pulsante e aprire Account Editor 729 .

Modifica
Selezionare un account nell'elenco, quindi fare clic su questo pulsante per aprirlo in Account Editor 729. È inoltre possibile fare doppio clic sull'account per aprirlo.

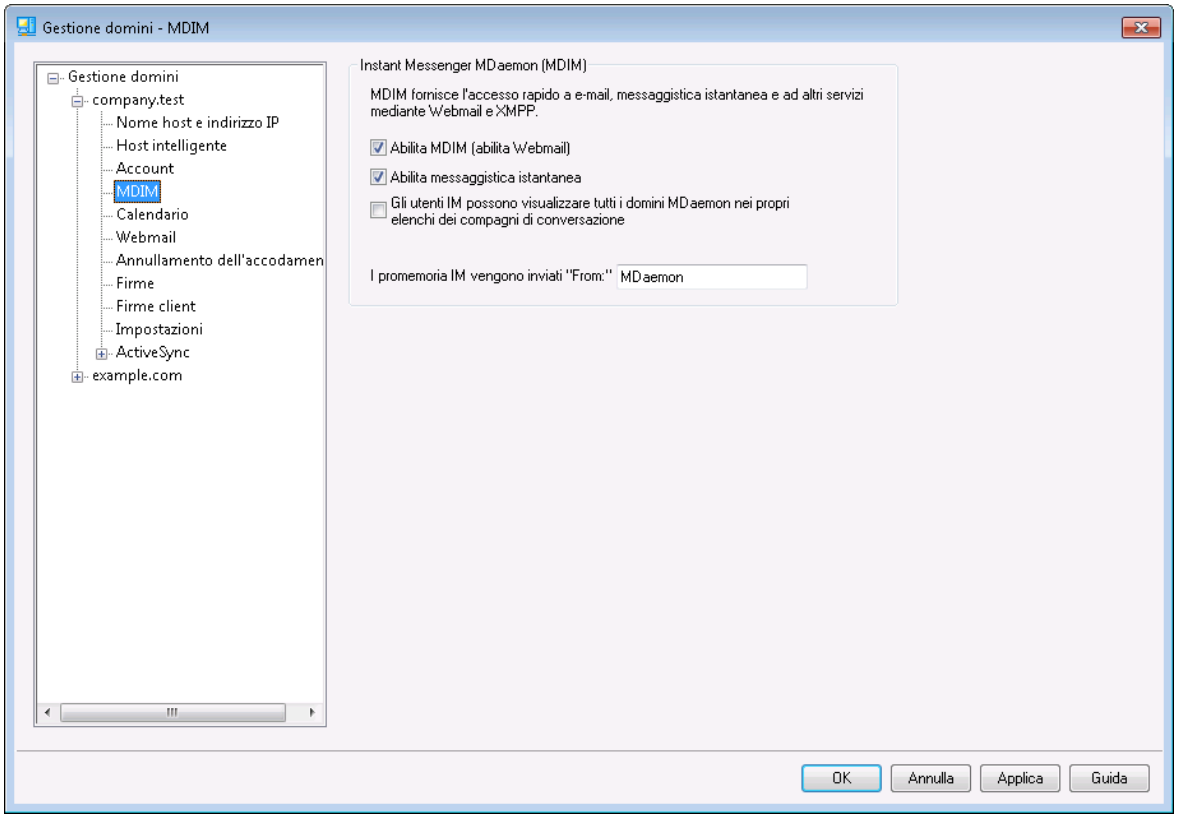
Elimina
Per eliminare un account, selezionarlo e fare clic su questo pulsante. Verrà chiesto di confermare l'operazione.

Mostra più account
L'elenco visualizza solo 500 account alla volta. Se nel dominio selezionato esistono più di 500 account, fare clic su questo pulsante per visualizzare i successivi 500.

Per ulteriori informazioni, vedere:

Account Manager 726
Account Editor 729
Modello Nuovi account 807

3.2.4 MDIM



Questa schermata controlla diversi aspetti di MDaemon Instant Messenger (MDIM) 326 per il dominio. Le impostazioni iniziali della schermata sono determinate dalle impostazioni predefinite di MDaemon Instant Messenger 340 della finestra di dialogo Web e Servizi IM. È possibile abilitare o disabilitare i servizi MDIM per account o gruppi specifici tramite le schermate Servizi Web 735 e Proprietà gruppo 798.

MDaemon Instant Messenger (MDIM)

Abilita MDIM (abilita Webmail)
Attivare questa opzione se si desidera rendere disponibile MDaemon Instant Messenger per il download da Webmail per impostazione predefinita per gli utenti del dominio. L'utilità può essere scaricata dalla pagina *Opzioni » MDaemon Instant Messenger*. Il file di installazione scaricato viene personalizzato automaticamente in base all'account di ciascun utente, così da facilitare l'installazione e la configurazione. Questa opzione rende possibile per MDIM l'uso delle funzionalità delle cartelle My Mail, consentendo all'utente di controllare la presenza di nuovi messaggi e aprire Webmail direttamente dal menu di scelta rapida di MDIM. MDIM è attivato per impostazione predefinita.

Abilita messaggistica istantanea
Per impostazione predefinita, gli account possono utilizzare MDIM e i client XMPP 381 di terze parti per scambiare messaggi istantanei con altri membri del dominio. Deselezionare questa casella di controllo se non si desidera consentire agli utenti di questo domino di utilizzare la messaggistica istantanea.

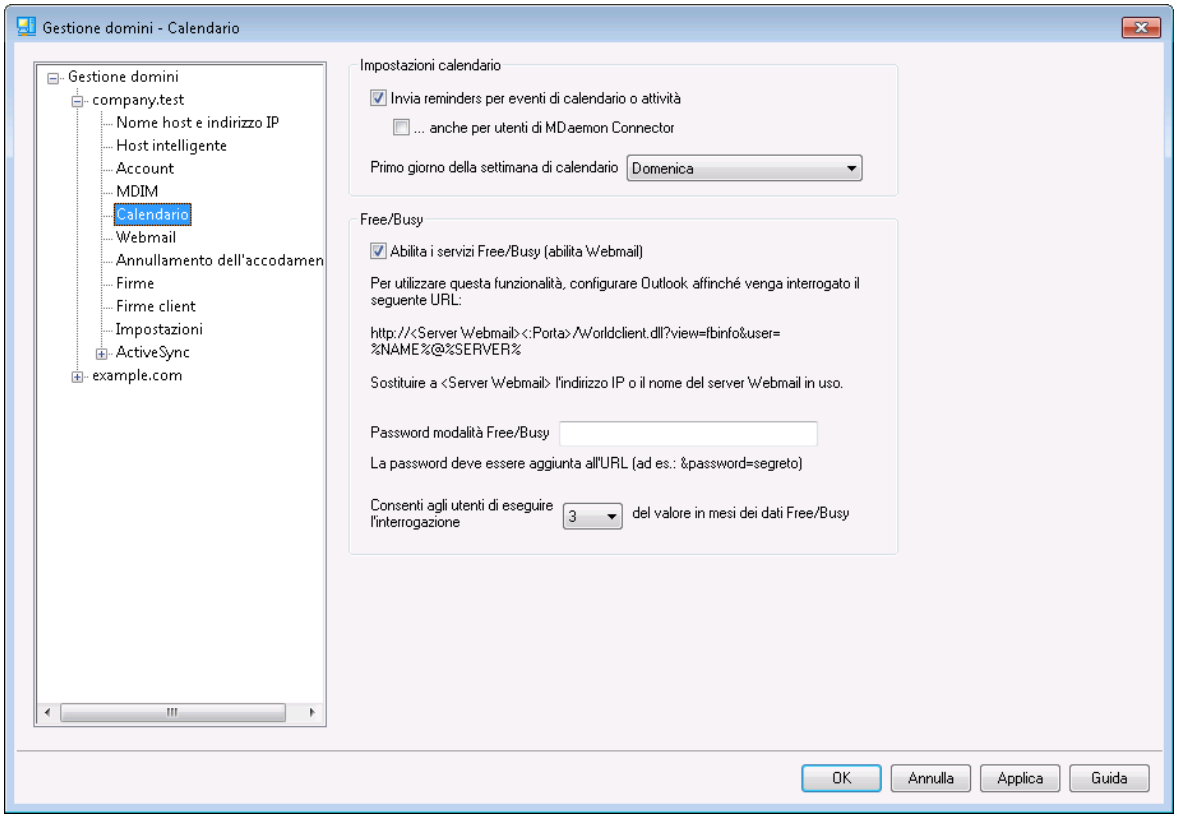
Gli utenti IM vedono tutti i domini MDaemon nei propri elenchi amici
Fare clic su questa opzione se si desidera che gli utenti del dominio siano in grado per impostazione predefinita di aggiungere contatti agli elenchi amici da tutti i domini MDaemon. Quando questa opzione è disattivata, i contatti devono essere nello stesso dominio. Se ad esempio MDaemon effettua l'hosting di esempio.com e esempio.org, attivando questa opzione per esempio.com, agli utenti di tale dominio viene consentito di aggiungere i contatti di messaggistica istantanea da entrambi i domini. Quando si disattiva l'opzione gli utenti di esempio.com possono aggiungere solo altri utenti di esempio.com. L'opzione è disabilitata per impostazione predefinita.

Promemoria IM inviati con 'From:' [*testo*]
Quando sul calendario di un utente di Webmail è pianificato un appuntamento, l'evento può essere impostato per inviare un promemoria all'utente a un'ora specifica. Se per il dominio dell'utente il sistema IM è attivo, il promemoria verrà inviato in un messaggio istantaneo all'utente. Utilizzare questa casella di testo per specificare il nome che si desidera compaia nel campo "Da:".

Vedere:

Gestione domini 185
Webmail » MDIM 340
Account Editor » Servizi Web 735
Proprietà gruppo 798

3.2.5 Calendario



In questa pagina è possibile controllare le funzioni di calendario di MDaemon per il dominio. Le impostazioni iniziali della schermata sono determinate dalla schermata Calendario[342] della finestra di dialogo Web e Servizi IM.

Calendar Settings (Impostazioni calendario)

Invia promemoria per eventi di calendario o attività
Selezionare questa casella di controllo per consentire l'invio agli utenti del calendario e dei promemoria delle attività di Webmail tramite posta elettronica e MDaemon Instant Messenger.

...anche a utenti MDaemon Connector
Se l'opzione "*Invia promemoria per eventi di calendario o attività*" è attivata, selezionare questa opzione se si desidera attivare i promemoria anche per gli utenti MDaemon Connector[395].

Primo giorno della settimana
Scegliere un giorno dall'elenco a discesa. La selezione verrà visualizzata nei calendari come primo giorno della settimana.

Free/Busy

MDaemon include un server Free/Busy che consente a un pianificatore di riunioni di visualizzare la disponibilità dei potenziali partecipanti. Per accedere a questa

funzione, fare clic su Pianificazione in Webmail quando si crea un nuovo appuntamento. Viene aperta la finestra Pianificazione che contiene l'elenco dei partecipanti e una griglia calendario con codifica cromatica che presenta una riga per ciascuno dei partecipanti. La riga di ciascun partecipante è contraddistinta da un colore specifico a indicare gli orari in cui questi sarà disponibile per una riunione. Ai colori corrispondono le modalità Occupato, Incerto, Fuori sede e Nessuna informazione. Con il pulsante Passa al successivo è inoltre possibile interrogare il server a proposito della successiva fascia oraria in cui tutti i partecipanti potrebbero essere disponibili. Al termine della creazione dell'appuntamento, verrà inviato un invito a tutti i partecipanti che potranno quindi accettarlo o declinarlo.

Il server Free/Busy di Webmail è inoltre compatibile con Microsoft Outlook. Per utilizzarlo, configurare Outlook affinché venga interrogato il seguente URL per cercare dati relativi alla disponibilità. Ad esempio, in Outlook 2002 le opzioni Free/Busy si trovano in "Strumenti » Opzioni » Opzioni calendario... » Opzioni disponibilità..."

URL del server Free/Busy per Outlook:

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Sostituire "<Webmail>" con l'indirizzo IP o il nome dominio del server Webmail e "<:Port>" con il relativo numero di porta se non si utilizza la porta Web predefinita. Ad esempio:

```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Per ulteriori informazioni sull'utilizzo delle funzioni di Free/Busy di Webmail per la pianificazione degli appuntamenti, vedere la Guida in linea di Webmail.

Abilita i servizi Free/Busy (Webmail abilitato)
Fare clic su questa opzione se si desidera consentire l'accesso alle funzioni del server Free/Busy agli utenti.

Password modalità Free/Busy
Per richiedere una password agli utenti che tentano di accedere alle funzioni del server Free/Busy tramite Outlook, inserire la password in questo campo. È necessario aggiungere la password all'URL (nel formato: "&password=FBServerPass") quando vengono configurate le impostazioni di disponibilità in Outlook. Ad esempio:

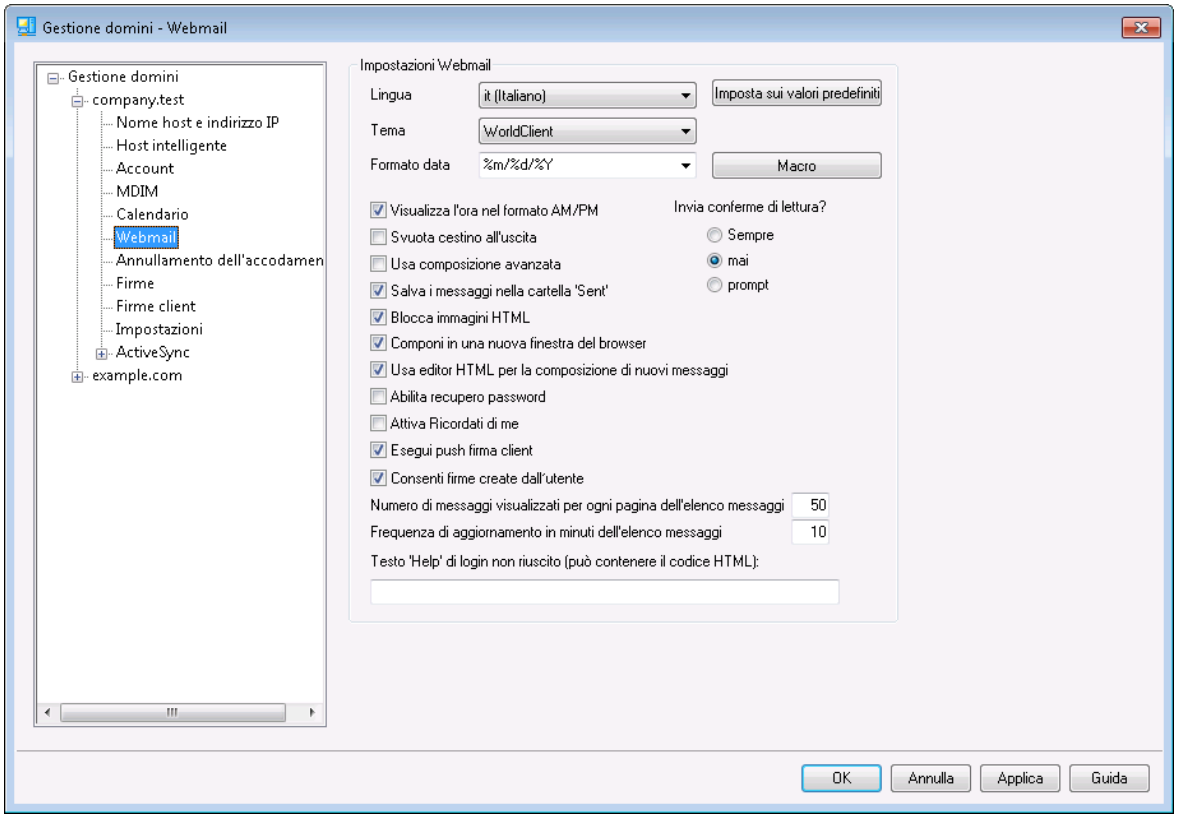
```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

Consenti agli utenti di eseguire l'interrogazione del valore in mesi dei dati Free/Busy
Utilizzare questa opzione per specificare l'intervallo dei dati relativi alla disponibilità che è possibile interrogare, espresso in numero di mesi.

Vedere:

Webmail » Calendario 342

3.2.6 Webmail



Questa schermata contiene varie opzioni a livello client di Webmail per il dominio. Quando un utente accede a Webmail, queste funzioni regolano il modo in cui Webmail inizialmente funziona per quell'utente. Molte di queste impostazioni sono personalizzabili dall'utente tramite le pagine Opzioni di Webmail. Le impostazioni predefinite di questa schermata sono determinate dalla schermata Webmail » Impostazioni 354 della finestra di dialogo Web e Servizi IM.

Impostazioni di Webmail

Imposta sui valori predefiniti
Questo pulsante consente di ripristinare le impostazioni predefinite di Webmail 354 per un dominio.

Lingua
Utilizzare questa casella di riepilogo a discesa per scegliere la lingua predefinita con cui l'interfaccia di Webmail viene visualizzata agli utenti durante la prima registrazione al dominio selezionato. Gli utenti possono modificare le impostazioni personali della lingua mediante la pagina di accesso a Webmail e mediante un'opzione di Opzioni » Personalizza in Webmail.

Tema
Questa casella di riepilogo a discesa consente di indicare il tema predefinito di Webmail da utilizzare per il primo accesso degli utenti al dominio selezionato. È

possibile personalizzare l'impostazione del tema mediante Opzioni » Personalizza in Webmail.

Formato data
Utilizzare questa casella di testo per specificare la formattazione delle date per il dominio selezionato. Fare clic sul pulsante *Macro* per visualizzare un elenco di codici macro utilizzabili in questa casella di testo. Sono disponibili le seguenti macro:

%A — Nome completo del giorno

%B — Nome completo del mese

%d — Giorno del mese (visualizzato nel formato "01-31")

%m — Mese (visualizzato nel formato "01-12")

%y — Anno nel formato a 2 cifre

%Y — Anno nel formato a 4 cifre

Ad esempio, la data "`%d/%m/%Y`" può essere in Webmail nel modo seguente "`25/12/2011`".

Macro
Fare clic su questo pulsante per visualizzare un elenco di codici macro utilizzabili in *Formato data*.

Invia conferme di lettura
Questa opzione determina la risposta di Webmail ai messaggi in arrivo che contengono una richiesta di conferma di lettura.

sempre
Se si seleziona questa opzione, MDaemon invia una notifica di avvenuta lettura al mittente. All'utente di Webmail che ha ricevuto il messaggio non viene segnalato che è stata richiesta o soddisfatta una conferma di lettura.

mai
Questa opzione indica a Webmail di ignorare le richiesta di conferma di lettura.

prompt
Con questa opzione, agli utenti di Webmail viene richiesto se inviare una conferma di lettura ogni volta che viene aperto un messaggio che lo richiede.

Visualizza l'ora nel formato AM/PM
Selezionare questa opzione se si desidera che in Webmail l'ora del dominio selezionato venga visualizzata nel formato orario basato su 12 ore (AM/PM). Deselezionare questa casella di controllo per utilizzare il formato basato su 24 ore. I singoli utenti possono modificare questa impostazione mediante l'opzione "*Visualizza gli orari in formato AM/PM*" situata nella pagina Opzioni » Calendario in Webmail.

Svuota cestino all'uscita
Se si seleziona questa opzione, il cestino dell'utente verrà svuotato all'uscita da Webmail. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Personalizza in Webmail.

Usa composizione avanzata
Selezionare questa casella se si desidera che, per impostazione predefinita, gli utenti del dominio visualizzino la schermata Composizione avanzata di Webmail, anziché la normale schermata Componi. I singoli utenti possono modificare questa impostazione in Opzioni » Componi in Webmail.

Salva i messaggi nella cartella "Posta inviata"
Selezionare questa opzione se si desidera che una copia di ogni messaggio inviato venga salvata nella cartella *Posta inviata*. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi in Webmail.

Blocca immagini HTML
Questa casella di controllo consente di impedire la visualizzazione automatica di immagini remote durante la visualizzazione di messaggi di posta elettronica HTML con Webmail. Per visualizzare le immagini, è necessario selezionare la barra visualizzata al di sopra del messaggio nella finestra del browser. Si tratta di una funzione anti spam, perché molti messaggi spam contengono immagini con particolari URL che identificano l'indirizzo di posta elettronica dell'utente che ha visualizzato le immagini, confermando così al mittente che si tratta di un indirizzo valido e operativo. L'opzione è abilitata per impostazione predefinita.

Componi in una nuova finestra del browser
Selezionare questa casella se si desidera che per la composizione dei messaggi venga aperta una nuova finestra del browser. In caso contrario, si passerà dalla finestra principale alla schermata di composizione. Deselezionare la casella se non si desidera che venga aperta una finestra separata. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi in Webmail.

Usa editor HTML per la composizione di nuovi messaggi
Abilitare questa casella se si desidera che, per impostazione predefinita, gli utenti del dominio possano visualizzare l'editor di composizione HTML di Webmail. Gli utenti possono modificare questa impostazione in Opzioni » Componi in **Webmail**.

Abilita recupero password
Se questa opzione è abilitata, gli utenti del dominio che dispongono dell'autorizzazione di modifica della password 735 potranno inserire un indirizzo e-mail alternativo in Webmail, al quale verrà inviato un collegamento per resettare la password nel caso la dimentichino. Per impostare questa funzionalità, gli utenti devono immettere sia l'indirizzo di posta elettronica per il recupero della password che la propria password corrente in Webmail, nella pagina Opzioni » Sicurezza. Dopo aver configurato questa impostazione, quando un utente tenta di accedere a Webmail con una password non corretta, viene visualizzato il collegamento "password dimenticata?". Il collegamento porta alla pagina in cui viene richiesto di confermare l'indirizzo di posta elettronica per il recupero della password. Se immette l'indirizzo di posta elettronica corretto, l'utente riceverà un messaggio e-mail con un

collegamento alla pagina per la modifica della password. Questa funzione è disabilitata per impostazione predefinita.

È possibile abilitare o disabilitare l'opzione per ogni singolo utente, aggiungendo il seguente codice al file `user.ini` dell'utente di Webmail (ad esempio `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (oppure "=No" per disabilitare l'opzione
per l'utente)
```

Consenti l'autenticazione a due fattori Ricordati di me (valido anche per Remote Admin)
Quando si utilizza l'autenticazione a due fattori (2FA) per accedere a Webmail o Remote Admin, nella pagina di autenticazione 2FA è di norma disponibile l'opzione Ricordati di me, che impedisce al server di richiedere nuovamente la 2FA per tale utente per un determinato numero di giorni (vedere l'opzione "*Consenti memorizzazione autenticazione*" di seguito). Deselezionare questa casella di controllo se non si desidera visualizzare l'opzione Ricordati di me della 2FA, in modo che tutti gli utenti con 2FA attivato debbano immettere un codice 2FA a ogni accesso. **Nota:** l'opzione è disponibile solo nell'interfaccia Web di MDaemon Remote Administration (MDRA) 359.

Attiva Ricordati di me
Selezionare questa casella se si desidera che nella pagina di accesso di MDaemon Webmail sia presente una casella di controllo *Ricordati di me* quando gli utenti del dominio si connettono attraverso la porta https 336. Se gli utenti selezionano questa casella all'accesso, le rispettive credenziali saranno ricordate per il dispositivo utilizzato. Quindi ogni volta che useranno quel dispositivo per connettersi a Webmail in futuro accederanno automaticamente fino a quando non eseguiranno la disconnessione manuale dall'account o il token di Ricordami scadrà.

Per impostazione predefinita, le credenziali dell'utente restano memorizzate per un massimo di 30 giorni prima che l'utente sia obbligato a eseguire di nuovo l'accesso. Se si desidera spostare la data di scadenza, è possibile modificare il valore dei token *Scadenza Ricordati di me dopo questo numero di giorni* nell'interfaccia Web MDaemon Remote Administration (MDRA) 359. È anche possibile cambiarla modificando la chiave `RememberUserExpiration=30` nel file `Domains.ini` che si trova nella cartella `\MDaemon\WorldClient\`. Il valore della scadenza può essere impostato su massimo 365 giorni. **Nota:** L'autenticazione a due fattori 735 (2FA) ha una propria chiave per la scadenza di Ricordati di me (`TwoFactorAuthRememberUserExpiration=30`), che si trova nella sezione `[Default:Settings]` del file `Domains.ini` nella cartella `\MDaemon\WorldClient\`. Pertanto l'autenticazione 2FA sarà nuovamente richiesta all'accesso quando il token di Ricordati di me di 2FA scadrà, anche se il normale token è ancora valido.

L'opzione*Ricordati di me* è disabilitata per impostazione predefinita e si applica solo a questo dominio. L'opzione globale si trova nella schermata Impostazioni 354 di Webmail.

Dato che l'opzione *Ricordati di me* consente agli utenti di avere un accesso permanente su più dispositivi, agli utenti

> deve essere ricordato che l'uso di Ricordati di me su reti pubbliche può essere pericoloso. Inoltre, se si sospetta una violazione della sicurezza per un account, in MDRA è disponibile un pulsante *Ripristina Ricordati di me* che è possibile utilizzare per reimpostare i token Ricordati di me per tutti gli utenti. Questo richiederà a tutti gli utenti di eseguire di nuovo l'accesso con le proprie credenziali.

Esegui push firma client
Selezionare questa casella di controllo per eseguire il push delle firme del client 211 agli utenti Webmail del dominio. In Webmail questa selezione provocherà la creazione di una firma denominata "Sistema" nelle opzioni per la firma in: **Opzioni » Componi**. Gli utenti potranno quindi scegliere di inserire automaticamente questa firma nella vista della composizione durante la redazione di un nuovo messaggio. Se questa opzione è attivata ma non è stata creata una firma client nella schermata Firme client di Domain Manager, verrà invece utilizzata l'opzione Firme client predefinite 141. Se non è disponibile nemmeno una firma client predefinita, in Webmail non sarà disponibile l'opzione di firma di Sistema.

Consenti firme create dall'utente
Selezionare questa casella di controllo per consentire agli utenti del dominio di creare le proprie firme personalizzate in Webmail. Gli utenti potranno quindi scegliere quale firma inserire automaticamente nella vista della composizione durante la redazione dei messaggi. Quando non si consente la creazione delle firme create dall'utente, ma si attiva l'opzione *Esegui push firma client* indicata sopra, è possibile inserire automaticamente solo la firma client 141 (vale a dire, la firma "Sistema" di Webmail). In Webmail le opzioni per la firma sono disponibili in: **Opzioni » Componi**.

Numero di messaggi visualizzati per ogni pagina dell'elenco messaggi
Indica il numero di messaggi che vengono visualizzati su ciascuna pagina dell'elenco dei messaggi per ogni cartella di posta. Se in una cartella è contenuto un numero di messaggi superiore a quello specificato in questo campo, sopra e sotto l'elenco verranno visualizzati dei comandi che consentono di passare alle altre pagine. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza in Webmail.

Frequenza di aggiornamento in minuti dell'elenco messaggi
Indica per quanti minuti Webmail attende prima di aggiornare automaticamente l'elenco dei messaggi. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza in Webmail.

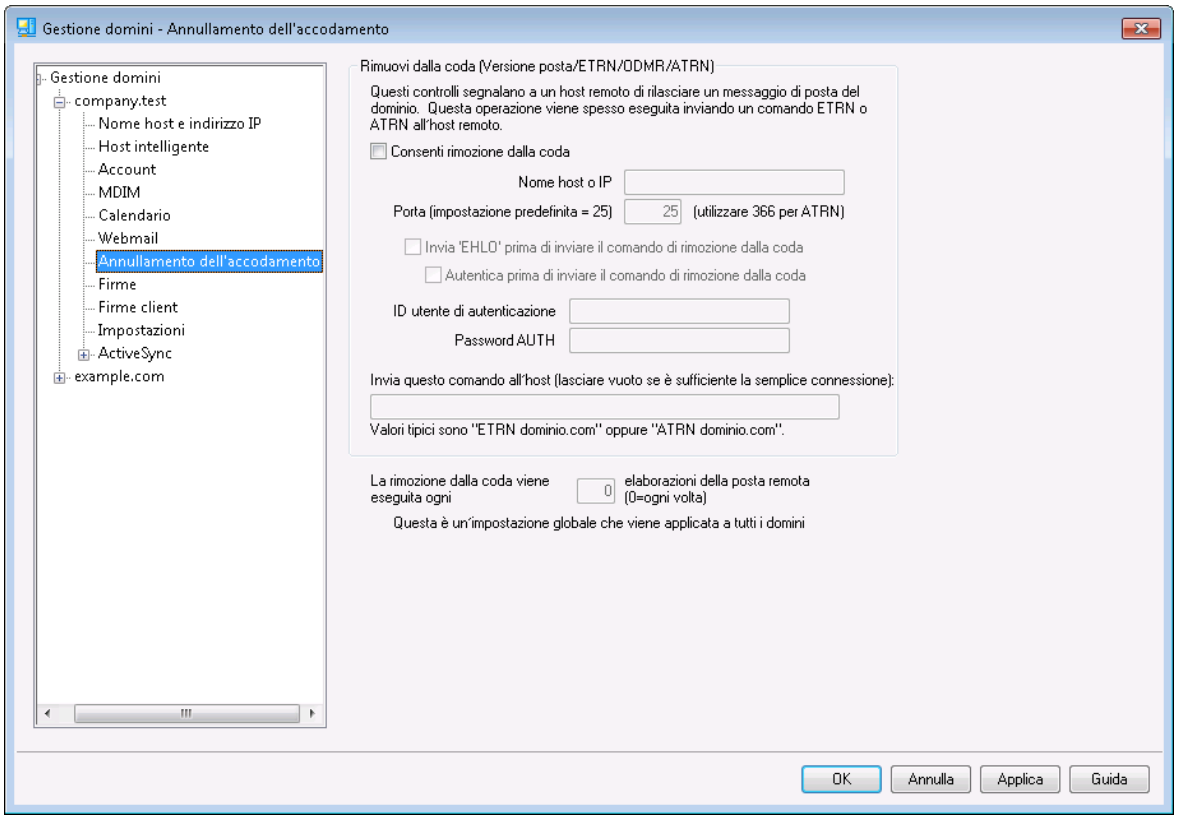
Testo 'Guida' errore di accesso (può contenere codice HTML)
Questa opzione consente di specificare una frase testuale, in testo semplice o HTML, da visualizzare nella schermata di registrazione di Webmail quando si verifica un problema di accesso. Il testo viene visualizzato al di sotto del seguente testo predefinito: "*Accesso errato, riprovare. Se è necessaria assistenza, contattare l'amministratore della posta elettronica*". Il testo può essere utilizzato per dirigere gli utenti a una data pagina o per ottenere informazioni relative all'accesso a Webmail.

Perché questa funzionalità possa essere utilizzata correttamente con più domini, è richiesta la configurazione di un nome host SMTP[188] valido per ciascun dominio. In caso contrario sarà utilizzato il testo del dominio predefinito[185]. Quindi, se ad esempio si dispone di molti domini ma si indirizzano tutti gli utenti Webmail a un singolo nome host per l'accesso, il *testo corretto, specifico del dominio, visualizzato in caso di errore di accesso* potrebbe non essere visualizzato.

Vedere:

Webmail » Impostazioni[354]

3.2.7 Annullamento dell'accodamento



Rimuovi dalla coda (Versione posta/ETRN/ODMR/ATRN)

Consenti rimozione dalla coda
Durante l'elaborazione della posta remota, MDaemon è in grado di connettersi a qualsiasi server o porta e inviare una stringa. Questa funzionalità si rivela particolarmente quando è necessario segnalare a un server remoto il rilascio della posta mediante una determinata stringa, ad esempio, `ATRN`, `ETRN` o `QSND`. Questa

funzione è efficace anche qualora l'ISP o l'host remoto richiedano una breve sessione FINGER o TELNET per verificare lo stato online del server in uso.

Nome host o IP
È l'host a cui è necessario inviare il segnale di rilascio della posta.

Porta
Specificare la porta da utilizzare per la connessione. Il valore predefinito 25 (porta SMTP) è adatto al metodo di segnalazione ETRN o QSND. La porta 366 viene di norma usata per la trasmissione di segnali ATRN, mentre la porta 79 per i segnali FINGER.

Invia "EHLO" prima della stringa di testo
Se questa casella di controllo è selezionata, per richiedere il rilascio della posta è necessario connettersi a un server SMTP. Questa opzione fa in modo che, avviata una sessione SMTP con l'host specificato, la trasmissione della stringa di sblocco avvenga dopo l'invio dell'istruzione SMTP "EHLO".

Autenticazione prima di invio stringa di testo (richiesto per ATRN)
Come misura di sicurezza, per rilasciare i messaggi in attesa alcuni host o server richiedono l'autenticazione dei client mediante ESMTP AUTH. Se questo è il caso dell'host di posta, selezionare la casella di controllo e immettere le credenziali di autenticazione necessarie.

L'autenticazione viene richiesta quando si utilizza il comando ATRN per annullare l'accodamento della posta.

Accesso AUTH
Inserire il parametro ID utente AUTH richiesto dall'host.

Password AUTH
Inserire la password AUTH.

Invia questo comando all'host (lasciare vuoto se è sufficiente la semplice connessione)
In questo campo è possibile specificare la stringa di testo che deve essere trasmessa per il rilascio della posta. Ad esempio, il metodo ETRN richiede l'inserimento del testo "ETRN" seguito dal nome del dominio del sito in coda; altri metodi, invece, richiedono l'invio di stringhe diverse. Per ulteriori informazioni sulle stringhe da inviare per sbloccare la coda di posta, consultare l'ISP. Quando si utilizza un metodo di annullamento dell'accodamento basato su un host di posta, è consigliabile utilizzare il metodo ODMR (On-Demand Mail Relay)  , se possibile. Per il metodo ODMR, utilizzare in questo campo il comando ATRN.

La rimozione dalla coda viene eseguita ogni [xx] volte di elaborazione della posta remota (0 = ogni volta)
Per impostazione predefinita, il segnale di annullamento dell'accodamento viene trasmesso a ogni elaborazione della posta remota. Il valore immesso in questo campo consente di regolare la frequenza di invio del segnale, che avverrà per un numero di

volte pari al valore impostato. Ad esempio, se il valore è "3", il segnale viene trasmesso ogni tre elaborazioni della posta remota.

Questa è un'impostazione globale che viene applicata a tutti i domini.

ODMR (On-Demand Mail Relay)

Se è necessario utilizzare un metodo di accodamento o annullamento dell'accodamento per l'hosting e il rilascio della posta, è consigliabile utilizzare il metodo ODMR (On-Domain Mail Relay), se possibile. Il metodo ODMR risulta superiore a ETRN e ad altri sistemi perché richiede un processo di autenticazione prima che venga eseguito il rilascio della posta. Inoltre, utilizza un comando ESMTP chiamato `ATRN`, in base al quale non è necessario che il client possegga un indirizzo IP statico, in quanto inverte il flusso di dati tra il client e il server e rilascia i messaggi senza dover effettuare una nuova connessione (a differenza di ETRN).

Dal lato client, MDaemon offre un supporto completo per ODMR mediante il comando `ATRN` e i comandi di autenticazione presenti nella scheda Rilascio posta 203. Per quanto riguarda il lato server, il supporto consiste in funzioni di gateway di dominio presenti nella schermata Annullamento dell'accodamento 269 di Gateway Editor.

Poiché alcuni server di posta non supportano ancora il metodo ODMR, è necessario verificarne la disponibilità presso il proprio provider prima di utilizzarlo.

Per ulteriori informazioni, vedere:

Rilascio posta 203
Gateway Editor » Annullamento dell'accodamento 269

3.2.7.1 ODMR (On-Demand Mail Relay)

Se è necessario utilizzare un metodo di accodamento o annullamento dell'accodamento per l'hosting e il rilascio della posta, è consigliabile utilizzare il metodo ODMR (On-Domain Mail Relay), se possibile. Il metodo ODMR risulta superiore a ETRN e ad altri sistemi perché richiede un processo di autenticazione prima che venga eseguito il rilascio della posta. Inoltre, utilizza un comando ESMTP chiamato `ATRN`, in base al quale non è necessario che il client possegga un indirizzo IP statico, in quanto inverte il flusso di dati tra il client e il server e rilascia i messaggi senza dover effettuare una nuova connessione (a differenza di ETRN).

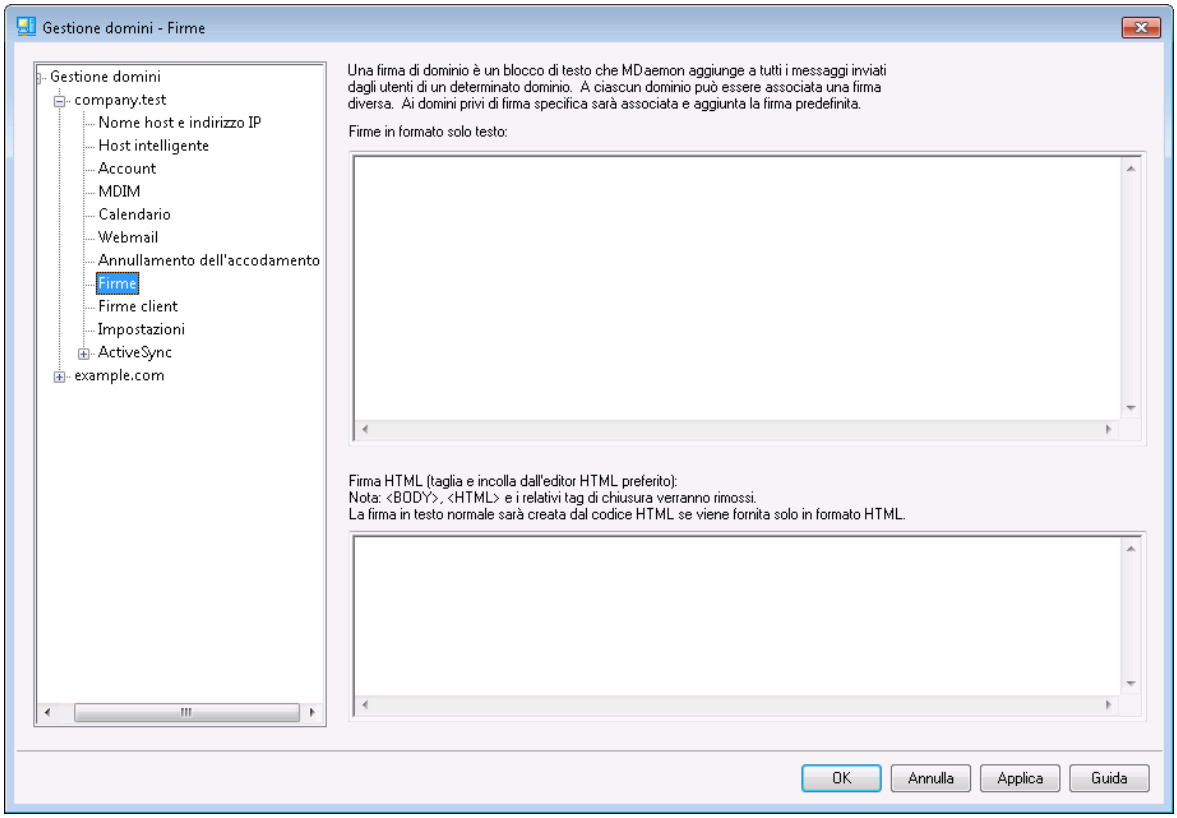
Dal lato client, MDaemon offre un supporto completo per ODMR mediante il comando `ATRN` e i comandi di autenticazione presenti nella scheda Rilascio posta 203. Per quanto riguarda il lato server, il supporto consiste in funzioni di gateway di dominio presenti nella schermata Annullamento dell'accodamento 269 di Gateway Editor.

Poiché alcuni server di posta non supportano ancora il metodo ODMR, è necessario verificarne la disponibilità presso il proprio provider prima di utilizzarlo.

Per ulteriori informazioni, vedere:

Rilascio posta 203
Gateway Editor » Annullamento dell'accodamento 269

3.2.8 Firme



Utilizzare questa schermata per aggiungere una firma a tutti i messaggi inviati dagli utenti di questo dominio. Se qui non è specificata alcuna firma, verrà aggiunta la Firma predefinita 136. Le firme vengono aggiunte in fondo ai messaggi, ad eccezione dei messaggi delle liste di distribuzione che utilizzano il piè di pagina 304; in tal caso, il piè di pagina viene aggiunto sotto la firma. Per aggiungere singole firme per ogni account è inoltre possibile utilizzare la funzione Firma 769 di Account Editor. Le firme dell'account vengono aggiunte prima di quelle del dominio o predefinite.

Firme in formato solo testo

Quest'area è destinata all'inserimento di una firma in formato solo testo. Per indicare una firma html corrispondente da utilizzare nella parte testo html dei messaggi multipart, utilizzare l'area *Firma HTML*. Se una firma è inclusa in entrambe le posizioni, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non

viene specificata alcuna firma html, in entrambe le parti viene utilizzata la firma in formato solo testo.

Firma HTML (copiare e incollare la firma dall'editor HTML desiderato)

Quest'area è destinata all'inserimento di una firma html da utilizzare nella parte testo/html dei messaggi multipart. Se una firma è inclusa qui e nell'area *Firme in formato solo testo*, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non è specificata una firma in formato solo testo, verrà utilizzato il formato HTML per crearne una.

Per creare la firma html, digitare il codice HTML manualmente o tagliarlo e incollarlo direttamente dall'editor HTML desiderato. Per includere le immagini in linea nella firma HTML, è possibile utilizzare la macro `$ATTACH_INLINE:path_to_image_file$`.

Ad esempio,

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

È inoltre possibile utilizzare diversi metodi per inserire immagini in linea nelle firme dall'interfaccia Web di MDaemon Remote Administration 359:

- Nella schermata Firme in Remote Administration, fare clic sul pulsante "Immagine" della barra degli strumenti nell'editor HTML e selezionare la scheda di caricamento.
- Nella schermata Firme in Remote Administration, fare clic sul pulsante "Aggiungi immagine" della barra degli strumenti nell'editor HTML.
- Trascinare un'immagine nella schermata Firme dell'editor HTML con Chrome, FireFox, Safari o MSIE 10+
- Copiare e incollare un'immagine dagli Appunti nella schermata Firme dell'editor HTML con Chrome, FireFox, MSIE 11+

I tag <body></body> e <html></html> non sono consentiti nelle firme e saranno rimossi se trovati.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. Ad esempio, `$CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono

riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e `$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**
ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**

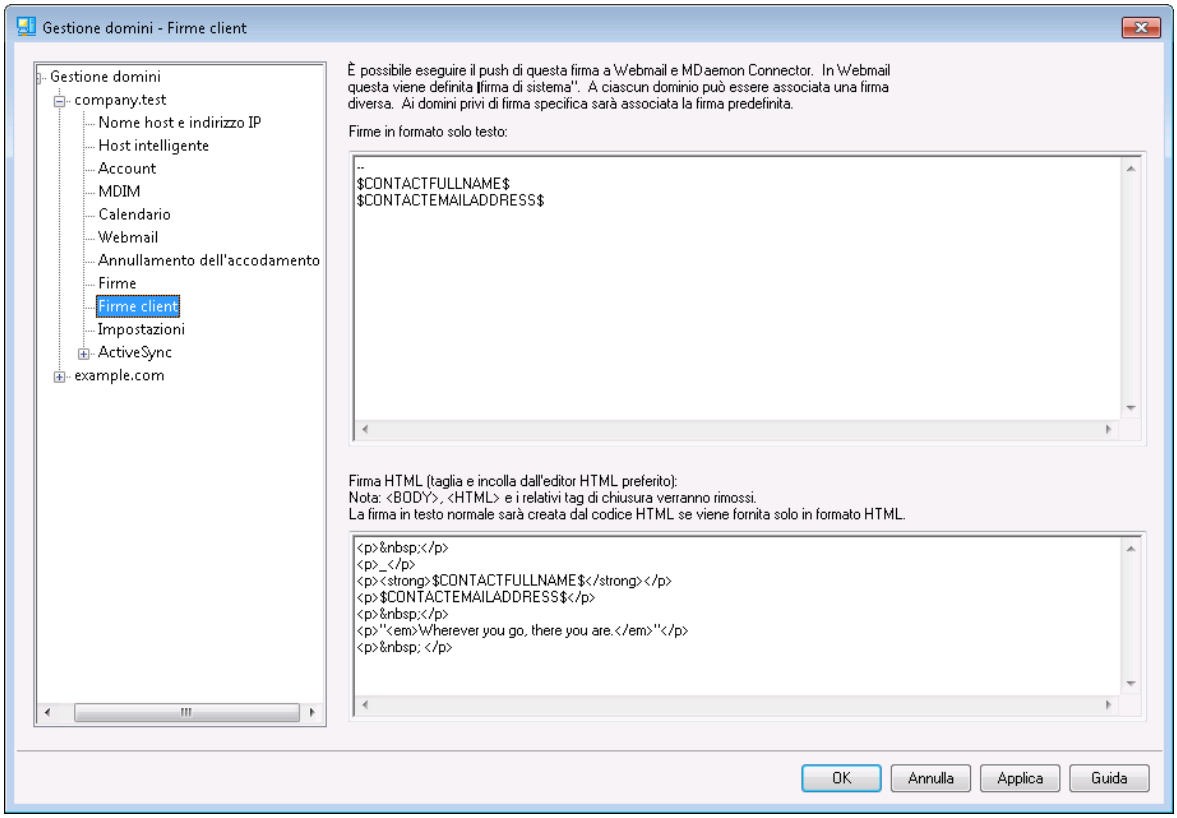
Numeri di telefono e fax	
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**

Mansione lavorativa	$CONTACTBUSINESSTITLE$
Ufficio	$CONTACTBUSINESSOFFICE$
Reparto dell'azienda	$CONTACTBUSINESSDEPARTMENT$
Responsabile dell'azienda	$CONTACTBUSINESSMANAGER$
Assistente in azienda	$CONTACTBUSINESSASSISTANT$
Telefono assistente in azienda	$CONTACTBUSINESSASSISTANTPHONE$
Telefono principale dell'azienda	$CONTACTBUSINESSMAINPHONE$
Telefono al lavoro	$CONTACTBUSINESSPHONE$
Telefono al lavoro 2	$CONTACTBUSINESSPHONE2$
Telefono IP al lavoro	$CONTACTBUSINESSIPPHONE$
Fax di lavoro	$CONTACTBUSINESSFAX$
Cercapersone in azienda	$CONTACTBUSINESSPAGER$
Radiotelefono in azienda	$CONTACTBUSINESSRADIO$
Indirizzo di lavoro	$CONTACTBUSINESSADDRESS$
Città di lavoro	$CONTACTBUSINESSCITY$
Provincia di lavoro	$CONTACTBUSINESSSTATE$
CAP di lavoro	$CONTACTBUSINESSZIPCODE$
Paese di lavoro	$CONTACTBUSINESSCOUNTRY$
Indirizzo Web aziendale	$CONTACTBUSINESSWEBADDRESS$
Altro	
Coniuge	$CONTACTSPOUSE$
Figli	$CONTACTCHILDREN$
Categorie	$CONTACTCATEGORIES$
Commento	$CONTACTCOMMENT$

Vedere:

Firme predefinite 136
Account Editor » Firma 769

3.2.9 Firme client



Utilizzare questa schermata per creare una firma client di cui è possibile eseguire il push in MDaemon Webmail 198 e MDaemon Connector 413, per l'uso da parte degli utenti quando creano messaggi e-mail. È possibile utilizzare le macro 212 riportate di seguito per personalizzare la firma, in modo che sia unica per ciascun utente, includendo elementi come nome utente, indirizzo e-mail, numero di telefono e campi simili. Utilizzare la schermata Firme client predefinite 141 se si desidera creare una firma diversa che sarà utilizzata quando non è stata creata una firma client specifica del dominio. Quando esiste una firma specifica del dominio, verrà utilizzata al posto della firma client predefinita. Utilizzare l'opzione *Esegui push firma client* 198 se si desidera eseguire il push della firma client in Webmail e l'opzione *Estendi firma del client a Outlook* 413 se si desidera eseguire il push in MDaemon Connector. Nelle opzioni di composizione di Webmail, la firma client di cui si è eseguito il push è denominata "Sistema". Per MDaemon Connector è possibile assegnare un nome alla firma che sarà visualizzata in Outlook.

Firme in formato solo testo

Quest'area è destinata all'inserimento di una firma in formato solo testo. Per indicare una firma html corrispondente da utilizzare nella parte testo/html dei messaggi multipart, utilizzare l'area *Firma HTML*. Se una firma è inclusa in entrambe le posizioni, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non viene specificata alcuna firma html, in entrambe le parti viene utilizzata la firma in formato solo testo.

Firma HTML (copiare e incollare la firma dall'editor HTML desiderato)

Quest'area è destinata all'inserimento di una firma html da utilizzare nella parte testo/html dei messaggi multipart. Se una firma è inclusa qui e nell'area *Firme in formato solo testo*, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non è specificata una firma in formato solo testo, verrà utilizzato il formato HTML per crearne una.

Per creare la firma html, digitare il codice HTML manualmente o tagliarlo e incollarlo direttamente dall'editor HTML desiderato. Per includere le immagini in linea nella firma HTML, è possibile utilizzare la macro `$ATTACH_INLINE:path_to_image_file$`.

Ad esempio,

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

È inoltre possibile utilizzare diversi metodi per inserire immagini in linea nelle firme dall'interfaccia Web di MDaemon Remote Administration 359:

- Nella schermata Firme client in Remote Administration, fare clic sul pulsante "Immagine" della barra degli strumenti nell'editor HTML e selezionare la scheda di caricamento.
- Nella schermata Firme client in Remote Administration, fare clic sul pulsante "Aggiungi immagine" della barra degli strumenti nell'editor HTML.
- Trascinare un'immagine nella schermata Firme client dell'editor HTML con Chrome, FireFox, Safari o MSIE 10+
- Copiare e incollare un'immagine dagli Appunti nella schermata Firme client dell'editor HTML con Chrome, FireFox, MSIE 11+

I tag <body></body> e <html></html> non sono consentiti nelle firme e saranno rimossi se trovati.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. Ad esempio, `$CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e

`$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**
ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**
Numeri di telefono e fax	
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**

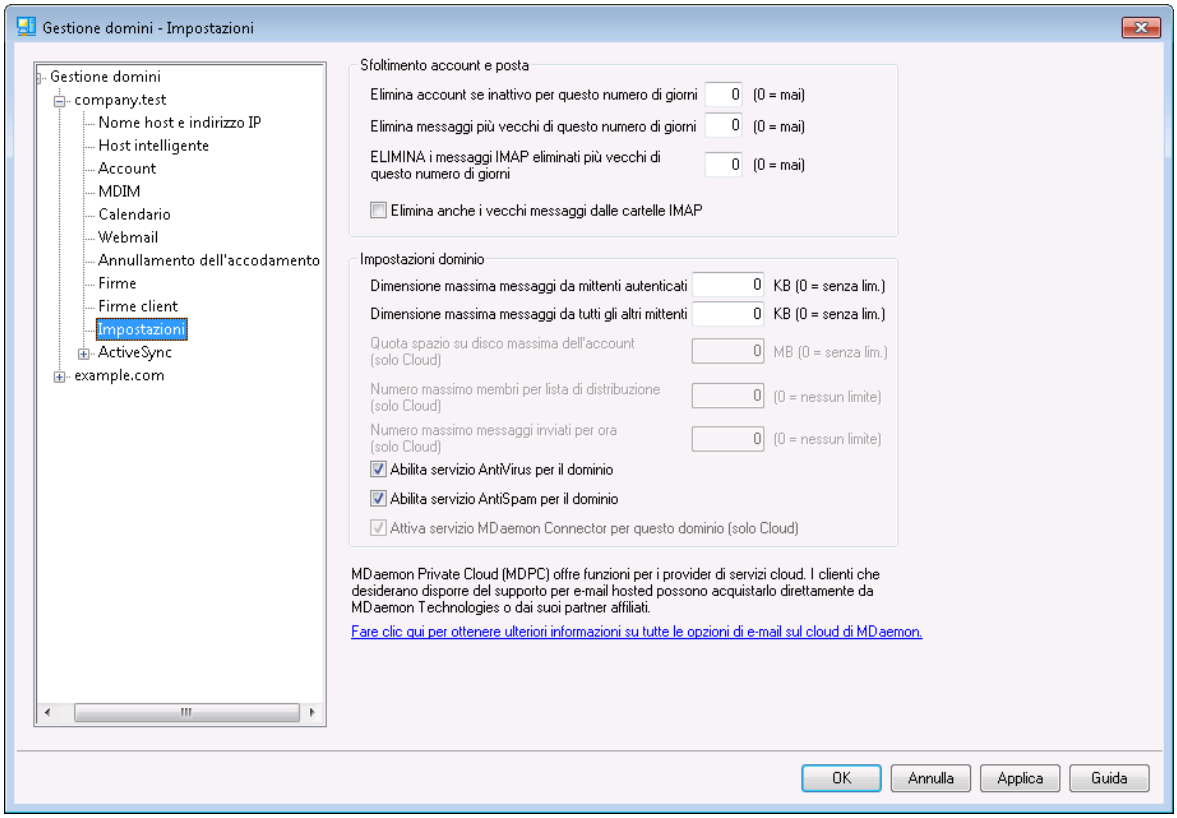
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**
Mansione lavorativa	**$CONTACTBUSINESSTITLE$**
Ufficio	**$CONTACTBUSINESSOFFICE$**
Reparto dell'azienda	**$CONTACTBUSINESSDEPARTMENT$**

Responsabile dell'azienda	$CONTACTBUSINESSMANAGER$
Assistente in azienda	$CONTACTBUSINESSASSISTANT$
Telefono assistente in azienda	$CONTACTBUSINESSASSISTANTPHONE$
Telefono principale dell'azienda	$CONTACTBUSINESSMAINPHONE$
Telefono al lavoro	$CONTACTBUSINESSPHONE$
Telefono al lavoro 2	$CONTACTBUSINESSPHONE2$
Telefono IP al lavoro	$CONTACTBUSINESSIPPHONE$
Fax di lavoro	$CONTACTBUSINESSFAX$
Cercapersone in azienda	$CONTACTBUSINESSPAGER$
Radiotelefono in azienda	$CONTACTBUSINESSRADIO$
Indirizzo di lavoro	$CONTACTBUSINESSADDRESS$
Città di lavoro	$CONTACTBUSINESSCITY$
Provincia di lavoro	$CONTACTBUSINESSSTATE$
CAP di lavoro	$CONTACTBUSINESSZIPCODE$
Paese di lavoro	$CONTACTBUSINESSCOUNTRY$
Indirizzo Web aziendale	$CONTACTBUSINESSWEBADDRESS$
Altro	
Coniuge	$CONTACTSPOUSE$
Figli	$CONTACTCHILDREN$
Categorie	$CONTACTCATEGORIES$
Commento	$CONTACTCOMMENT$

Vedere:

Firme client predefinite 141
Firme predefinite 136
Domain Manager » Firme 206
Account Editor » Firma 769
Domain Manager » Impostazioni Webmail 198
Impostazioni client MC » Firma 413

3.2.10 Impostazioni



Sfoltimento account e posta

Queste opzioni vengono utilizzate per specificare se e quando MDaemon deve eliminare gli account inattivi o i vecchi messaggi. Ogni giorno a mezzanotte MDaemon elimina tutti i messaggi e gli account che hanno superato i limiti di tempo impostati. Esistono opzioni simili nella schermata Quote 746 di Account Editor utilizzabili per modificare queste impostazioni predefinite per singoli account.

Per ulteriori informazioni e per le opzioni della riga di comando, vedere `AccountPrune.txt` nella cartella "...`MDaemon\App\`".

Elimina account se inattivo per il seguente numero di giorni (0 = mai)
Consente di specificare per quanti giorni un account del dominio può rimanere inattivo prima di essere eliminato. Specificando il valore "0", gli account non vengono mai eliminati per inattività.

Elimina messaggi più vecchi del seguente numero di giorni (0 = mai)
Il valore di questo comando indica per quanti giorni un messaggio può rimanere nella casella postale di un utente prima di essere eliminato automaticamente. Il valore "0" indica che, anche se di vecchia data, i messaggi non vengono mai eliminati. **Nota:** L'impostazione di questa opzione non si applica ai messaggi contenuti nelle cartelle

IMAP a meno che non si abiliti anche l'opzione "*Elimina anche i vecchi messaggi dalle cartelle IMAP*" di seguito.

Elimina messaggi IMAP cestinati più vecchi del seguente numero di giorni (0 = mai)
Utilizzare questo comando per specificare per quanti giorni i messaggi IMAP contrassegnati per l'eliminazione devono rimanere nelle cartelle. I messaggi contrassegnati per l'eliminazione che esistono da più di XX giorni vengono eliminati dalle rispettive caselle postali. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Elimina anche i vecchi messaggi dalle cartelle IMAP
Selezionare questa casella di controllo se si desidera applicare l'opzione "*Elimina i messaggi più vecchi del seguente numero di giorni*" anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i normali messaggi contenuti nelle cartelle IMAP non vengono eliminati in base al periodo di permanenza nelle cartelle in questione.

Impostazioni dominio

Dimensione massima messaggi da mittenti autenticati [xx] KB (0=nessun limite)
Questa opzione consente di impostare un limite alle dimensioni dei messaggi che un utente autenticato può inviare al dominio. Il valore è espresso in Kilobyte e impostato su "0" in modo predefinito, a significare che non viene applicato alcun limite. Per impostare un limite alla dimensione dei messaggi per i mittenti non autenticati, utilizzare l'opzione "*...da tutti gli altri mittenti*" riportata di seguito.

Dimensione massima messaggi da tutti gli altri mittenti [xx] KB (0=nessun limite)
Questa opzione consente di impostare un limite alle dimensioni dei messaggi che un utente non autenticato può inviare al dominio. Il valore è espresso in Kilobyte e impostato su "0" in modo predefinito, a significare che non viene applicato alcun limite. Per impostare un limite alla dimensione dei messaggi per i mittenti autenticati, utilizzare l'opzione "...da mittenti autenticati" riportata sopra.

Quota spazio su disco massima dell'account [xx] MB (0=nessun limite) (solo Cloud)
Utilizzare questa opzione per impostare un limite sulla quantità di spazio su disco utilizzabile dal dominio. L'opzione è disponibile solo in MDaemon Private Cloud.

Numero massimo membri per lista di distribuzione [xx] (0=nessun limite) (solo Cloud)
Questa opzione consente di impostare il numero massimo di membri consentito per ciascuna lista di distribuzione del dominio. Esiste un'opzione globale corrispondente nella schermata Impostazioni 278 di Mailing List Manager. L'opzione è disponibile solo in MDaemon Private Cloud.

Numero massimo messaggi inviati per ora [xx] (0=nessun limite) (solo Cloud)
Questa opzione consente di impostare un limite al numero massimo dii messaggi che il dominio può inviare ogni ora. Una volta raggiunto tale limite, gli altri messaggi restano in coda fino all'azzeramento del conteggio. Il conteggio dei messaggi viene reimpostato ogni ora e al riavvio del server. L'opzione è disponibile solo in MDaemon Private Cloud.

Abilita servizio AntiVirus per il dominio
Fare clic su questa casella di controllo se si desidera che le impostazioni AntiVirus 658 vengano applicate a questo dominio.

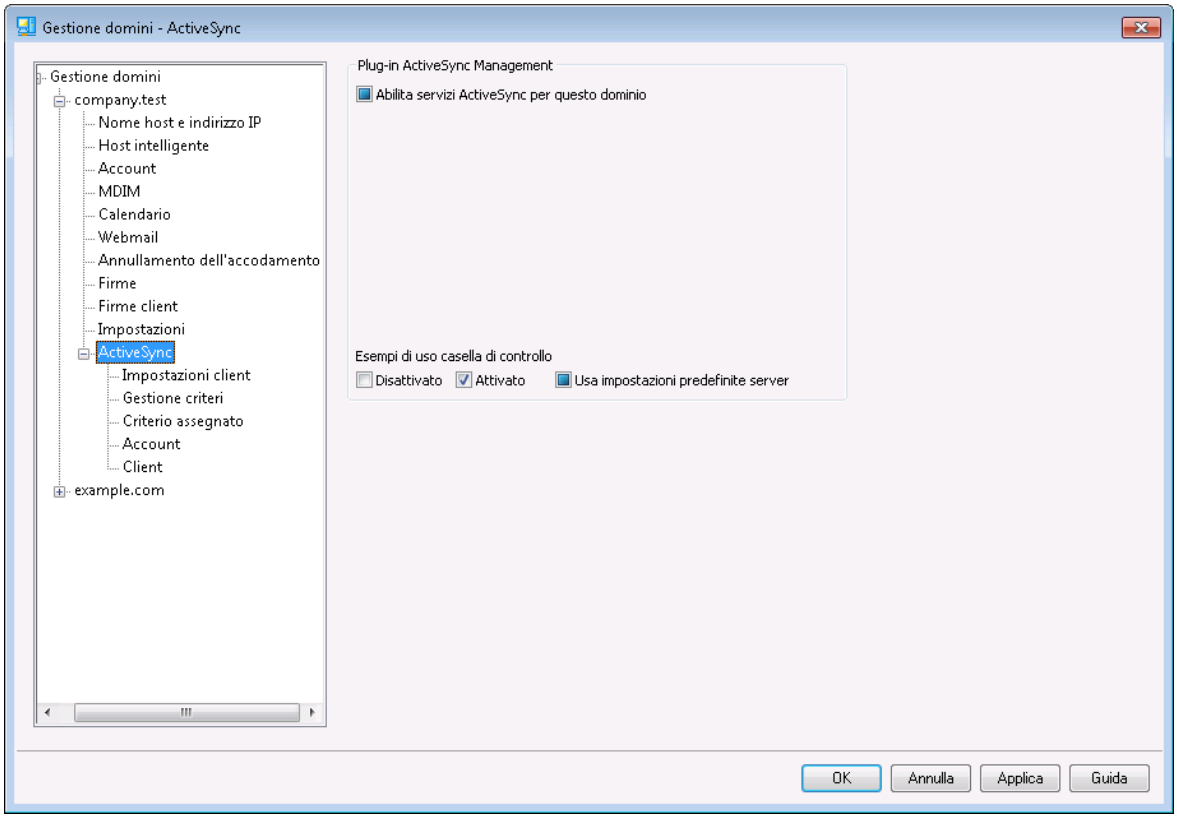
Abilita servizio AntiSpam per il dominio
Attivare questa casella di controllo per applicare le impostazioni Spam Filter correnti anche a questo dominio.

Attiva servizio MDaemon Connector per questo dominio (solo Cloud)
Selezionare questa casella se si desidera attivare il servizio MDaemon Connector 395 per il dominio.

Vedere:

Account Editor » Quote 746

3.2.11 ActiveSync



Utilizzare questa sezione di Domain Manager per l'amministrazione delle impostazioni di ActiveSync 425 del dominio. È possibile gestire le impostazioni e le impostazioni predefinite di ActiveSync per tutti i domini dalla schermata Domini 444 della gestione di ActiveSync.

Plug-in di gestione di ActiveSync per MDaemon

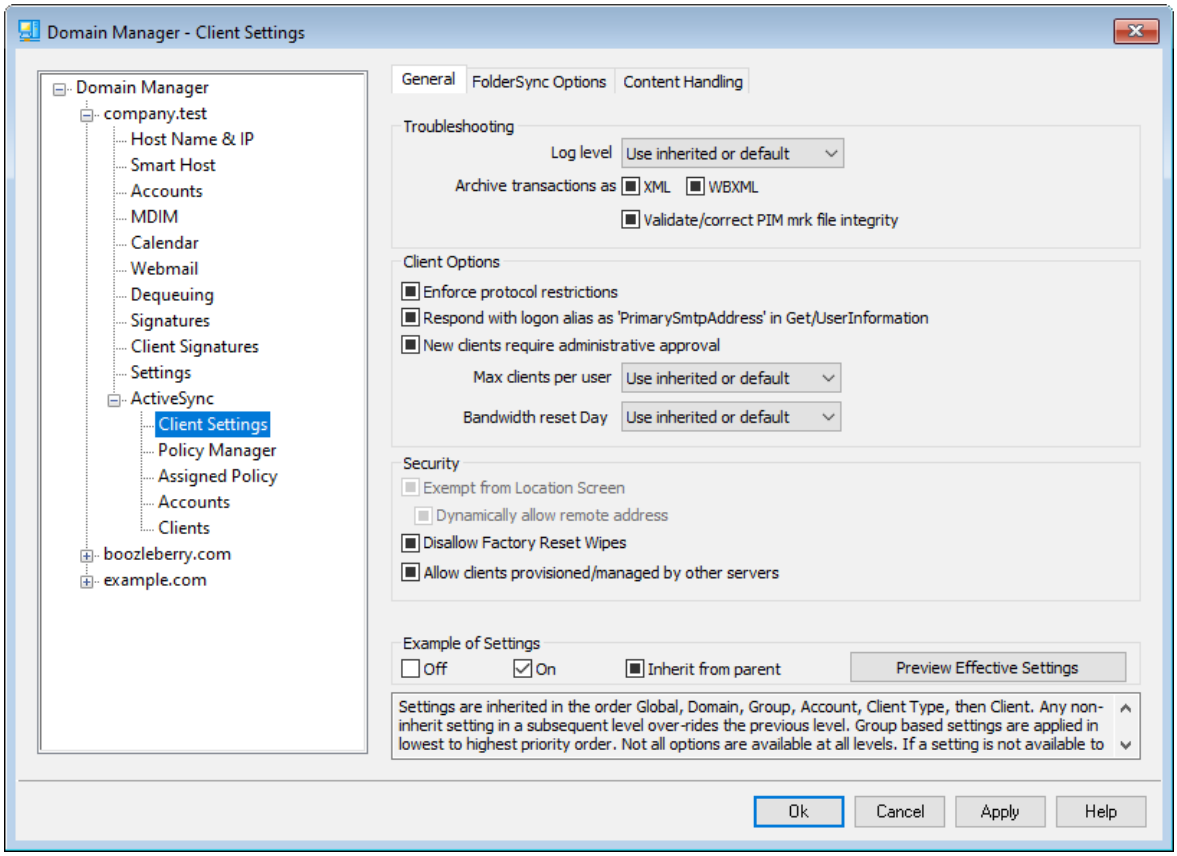
Abilita servizio ActiveSync per il dominio
Questa opzione controlla se gli utenti del dominio saranno in grado o meno di utilizzare un client ActiveSync per accedere alle e-mail e ai dati PIM per impostazione predefinita. Per impostazione predefinita lo stato di questa impostazione viene ereditato dallo stato predefinito di ActiveSync 444, ma è possibile ignorare tale impostazione se si desidera, attivando o disattivando la casella di controllo. Questa impostazione può essere ignorata anche per gli account 461 o client 470 che non si desidera utilizzino l'impostazione del dominio. **NOTA:** se si disattiva ActiveSync per questo dominio, viene visualizzata una finestra di conferma con cui si chiede all'utente di confermare la revoca dell'accesso ad ActiveSync per tutti gli utenti del dominio specificato. Scegliere **No** se si desidera che gli utenti del dominio specificato possano continuare a utilizzare ActiveSync. Se si sceglie **Sì**, ActiveSync verrà disabilitato per tutti gli utenti del dominio specificato.

Questa impostazione controlla se agli account del dominio sarà consentito o meno utilizzare ActiveSync per impostazione predefinita, quando il servizio ActiveSync è in funzione. L'opzione globale **Attiva protocollo ActiveSync** 425 deve essere abilitata per consentire l'accesso ad ActiveSync ai domini o account autorizzati.

Per ulteriori informazioni, vedere:

ActiveSync » Domini 444
ActiveSync » Account 461
ActiveSync » Client 470

3.2.11.1 Impostazioni client



Questa schermata consente di gestire le impostazioni predefinite per gli account e i client associati al dominio.

Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Impostazioni client globali 430. Allo stesso modo, gli account 192 di questo dominio erediteranno le impostazioni da questa schermata, poiché questa è la loro schermata principale. Le modifiche apportate alle opzioni in questa schermata verranno riportate anche nelle altre schermate degli account. Oltre a quello, i singoli client 246 avranno anche schermate di impostazioni che ereditano la relativa configurazione dalle impostazioni a livello di account. Questa configurazione rende possibile all'utente apportare modifiche a tutti i client e gli account del dominio semplicemente inserendo le modifiche in quest'unica schermata, consentendo inoltre all'utente di sovrascrivere tali impostazioni per qualsiasi account o client quando necessario.

Generale

Risoluzione dei problemi

Livello di registrazione

ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di

dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a

cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un

aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

Anteprima impostazioni applicate

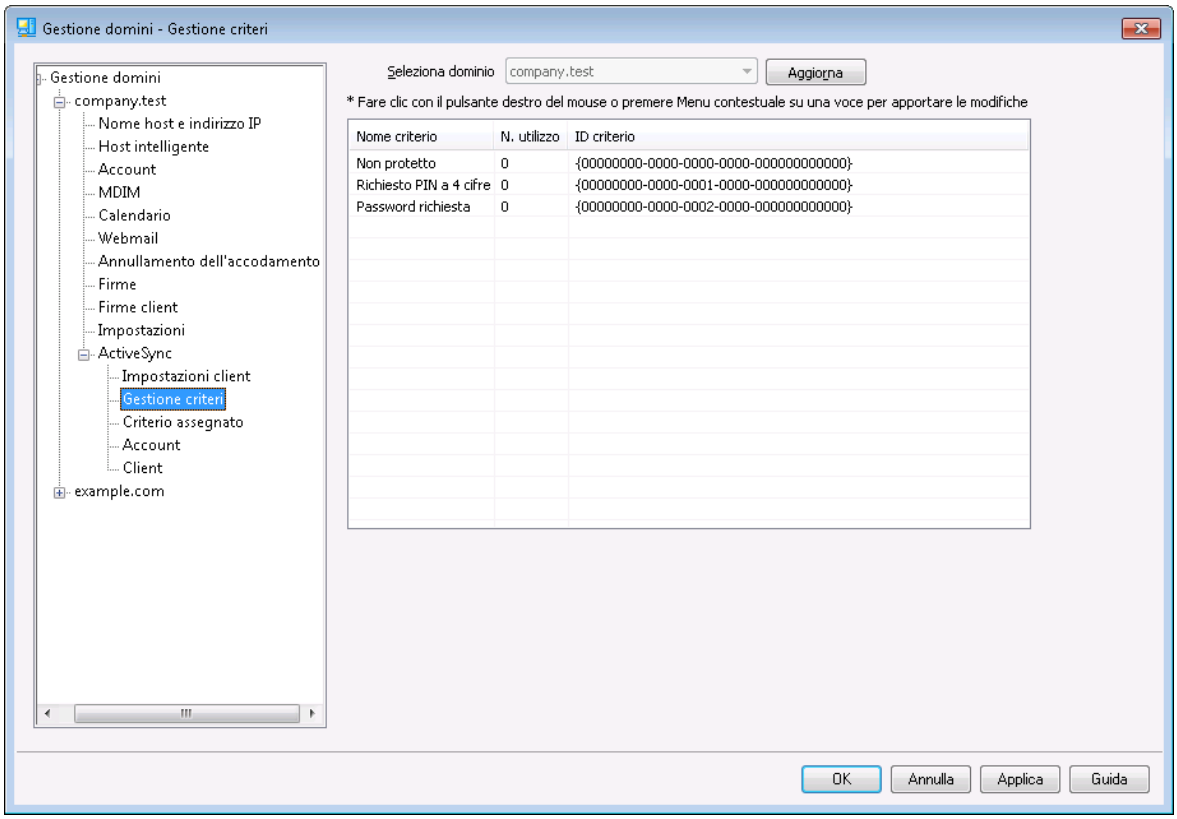
Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali

impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

ActiveSync » Impostazioni client 430
ActiveSync » Account 461
ActiveSync » Client 470

3.2.11.2 Policy Manager



Utilizzare questa schermata per gestire i criteri ActiveSync che è possibile assegnare ai dispositivi degli utenti per regolare diverse opzioni. Sono disponibili criteri predefiniti ed è possibile creare, modificare ed eliminare criteri personalizzati. È possibile assegnare criteri predefiniti e criteri che sostituiscono criteri esistenti al dominio e a ciascun account 461 e client 470 nelle rispettive schermate Criterio assegnato.

Non tutti i dispositivi ActiveSync riconoscono o applicano i criteri in modo coerente. Alcuni potrebbero ignorare del tutto i criteri o alcuni elementi dei criteri, mentre altri potrebbero richiedere un riavvio del dispositivo per rendere effettive le modifiche. Inoltre, quando si tenta di assegnare un nuovo criterio a un dispositivo, il criterio viene applicato solo alla successiva connessione del dispositivo al server ActiveSync;

non è possibile inviare i criteri ai dispositivi fino a quando questi ultimi non eseguono la connessione.

Criteri ActiveSync

Fare clic con il pulsante destro del mouse sull'elenco per aprire un menu di scelta rapida con le seguenti opzioni:

Crea criterio
Fare clic su questa opzione per aprire l'editor dei criteri di ActiveSync, che consente di creare e modificare i criteri.

Elimina
Per eliminare un criterio, selezionare un criterio personalizzato dall'elenco, quindi fare clic su **Elimina**. Fare clic su **Sì** per confermare l'azione. Non è possibile eliminare i criteri predefiniti.

Modifica criterio
Per modificare un criterio, fare clic con il pulsante destro su un criterio personalizzato dell'elenco e scegliere **Modifica criterio**. Una volta apportate le modifiche desiderate nell'editor dei criteri, fare clic su**OK**. Non è possibile modificare i criteri predefiniti.

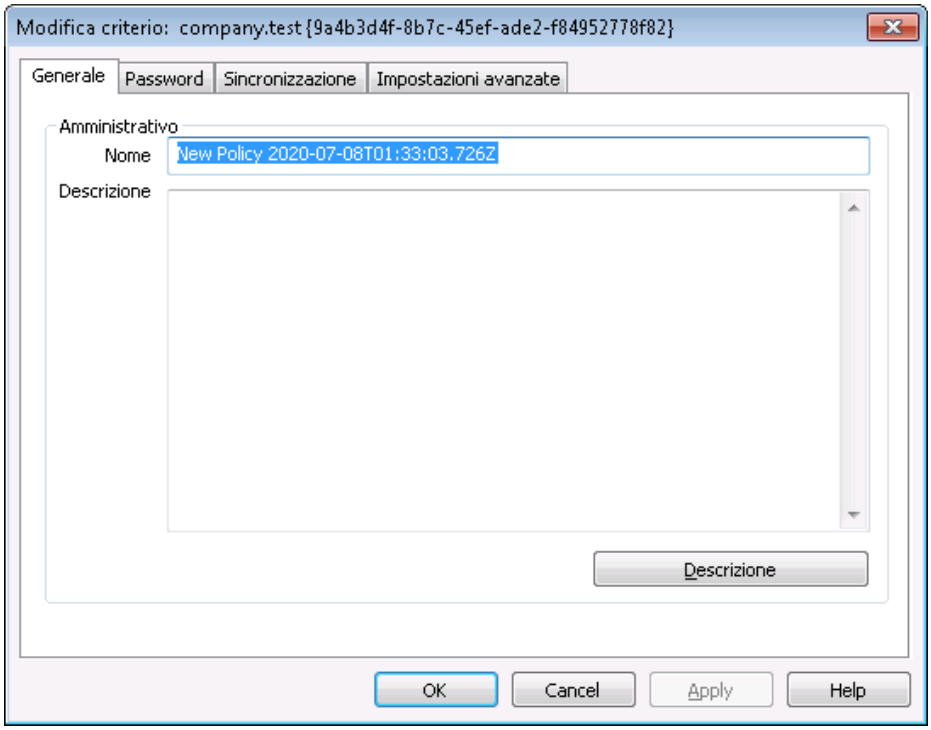
Visualizza utilizzo criterio
Fare clic con il pulsante destro su un criterio, quindi scegliere questa opzione per visualizzare un elenco di tutti i domini, gli account e i client configurati per l'utilizzo di questo criterio.

Editor criteri ActiveSync

Editor criteri ActiveSync contiene quattro schede: Generale, Password, Sincronizzazione e Impostazioni avanzate. La scheda Impostazioni avanzate resta nascosta fino a che non si attiva *Consenti modifica impostazioni avanzate criteri*425, disponibile nella schermata Sistema ActiveSync.

Generale

Utilizzare questa schermata per specificare un nome e una descrizione per il criterio. È possibile anche visualizzare l'anteprima del documento XML del criterio.



Amministrativo

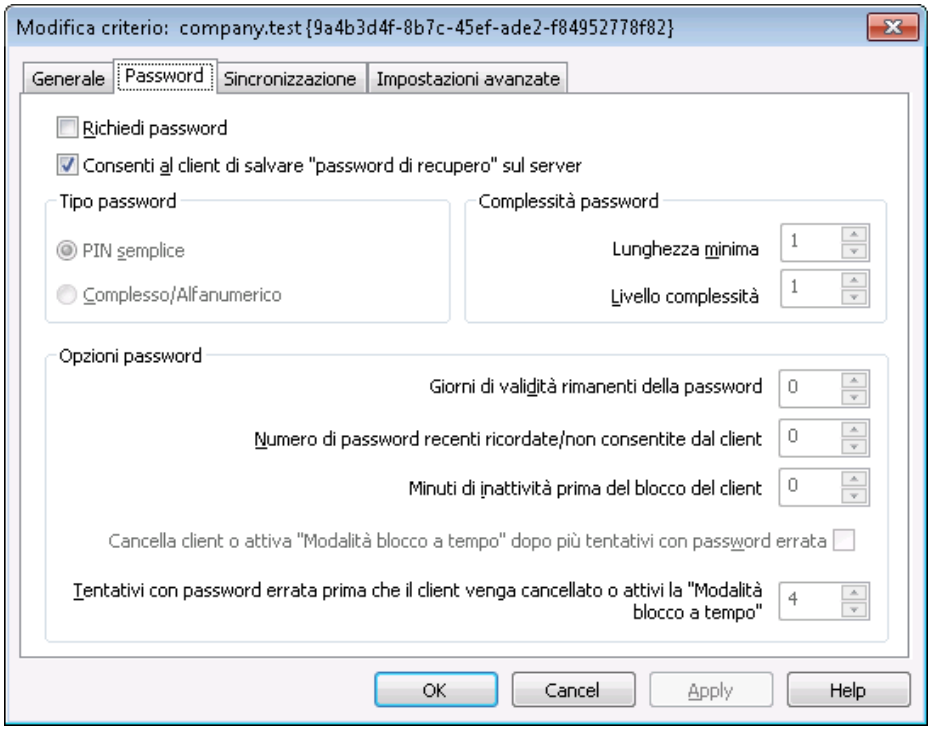
Nome
Consente di specificare il nome del criterio personalizzato.

Descrizione
Quest'area consente di descrivere il criterio personalizzato. La descrizione viene visualizzata nella finestra di dialogo Applica criterio quando si seleziona un criterio da applicare a un dominio, account o client.

Anteprima documento criterio
Fare clic su questo pulsante per visualizzare l'anteprima del documento XML per questo criterio.

Password

Opzioni e requisiti della password per il criterio si possono specificare in questa scheda.



Richiedi password
Selezionare questa casella per richiedere una password per il dispositivo. Questa opzione è disabilitata per impostazione predefinita.

Consenti al dispositivo di salvare "password di recupero" sul server
Attivare questa opzione per consentire ai client di utilizzare l'opzione di recupero della password di ActiveSync, che permette a un dispositivo di salvare una password di recupero temporanea sul server per sbloccare il dispositivo in caso di password dimenticata. L'amministratore può trovare la password di recupero nei Dettagli 470 del client. La maggior parte dei dispositivi non supporta questa funzionalità.

Tipo password

PIN semplice
Il modo in cui viene implementata questa opzione dipende in larga parte dal dispositivo, ma se si seleziona *PIN semplice* come tipo di password, in genere significa che non vengono imposte limitazioni o requisiti di complessità particolari per la password del dispositivo, a parte l'opzione *Lunghezza minima password* riportata di seguito. In questo modo si consentono password semplici come: "111", "aaa", "1234", "ABCD" e simili.

Complessa/Alfanumerica
Utilizzare questa opzione del criterio per richiedere password del dispositivo più complesse e sicure rispetto all'opzione *PIN semplice*. Utilizzare l'opzione *Livello*

complessità riportata di seguito per definire esattamente il livello di complessità della password. Questa è l'opzione predefinita quando il criterio richiede una password.

Sicurezza password

Lunghezza minima
Utilizzare questa opzione per impostare il numero minimo di caratteri, compreso tra 1 e 16, che la password del dispositivo deve contenere. Per impostazione predefinita, questa opzione è impostata su "1".

Livello complessità
Utilizzare questa opzione per impostare il requisito del livello di complessità per la password del dispositivo di tipo *Complessa/Alfanumerica*. Il livello equivale al numero dei diversi tipi di caratteri che la password deve contenere: lettere maiuscole, lettere minuscole, numeri e caratteri non alfanumerici (come punteggiatura o caratteri speciali). È possibile richiedere da 1 a 4 tipi di caratteri. Se, ad esempio, si imposta questa opzione su "2", allora la password deve contenere almeno due dei quattro tipi di carattere: maiuscole e numeri, maiuscole e minuscole, numeri e simboli e così via. Per impostazione predefinita, questa opzione è impostata su "1".

Opzioni password

Giorni fino alla scadenza della password (0 = mai)
Indica il numero di giorni che devono trascorrere prima che diventi obbligatorio modificare la password del dispositivo. Questa opzione è disabilitata per impostazione predefinita (impostata su "0").

Numero di password recenti ricordate/non consentite dal dispositivo (0 = nessuno)
Utilizzare questa opzione se si desidera impedire al dispositivo di riutilizzare un numero specificato di password precedenti. Se, ad esempio, questa opzione è impostata su "2" e si modifica la password del dispositivo, non sarà possibile reimpostare una delle ultime due password utilizzate. L'opzione è disabilitata per impostazione predefinita (impostata su "0").

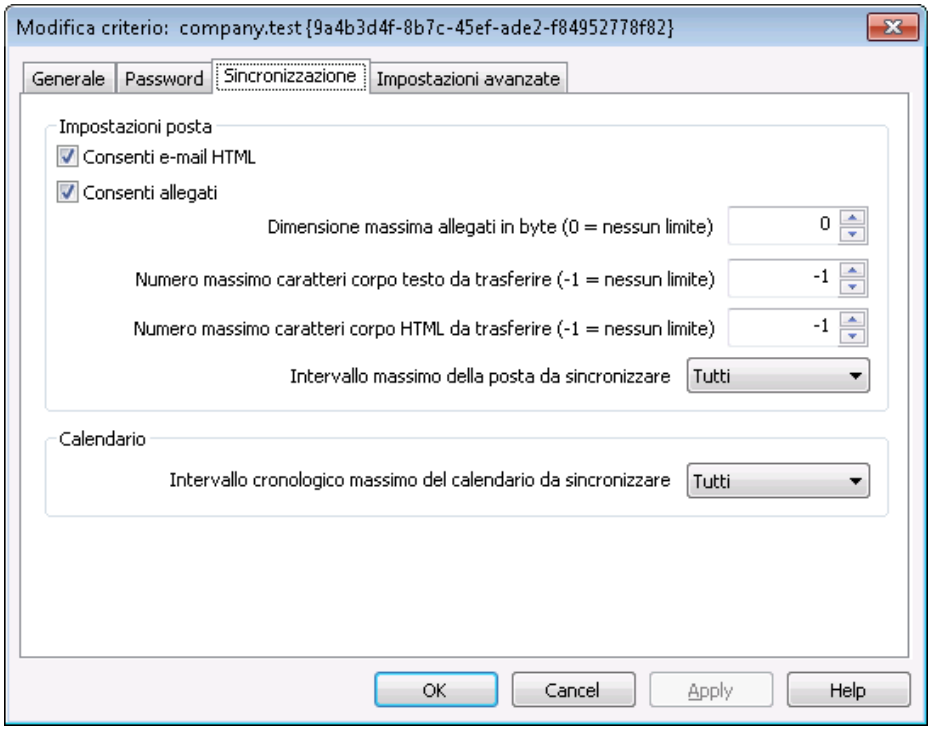
Minuti di inattività prima del blocco del dispositivo (0 = mai)
Indica il numero di minuti in cui un dispositivo può essere utilizzato senza alcun input dell'utente prima che si blocchi automaticamente. Questa opzione è disabilitata per impostazione predefinita (impostata su "0").

Pulisci dispositivo o attiva "Modalità blocco a tempo" dopo più tentativi con password errata
Quando si attiva questa opzione e un utente immette una password errata nel dispositivo per il numero di tentativi specificato, il dispositivo si blocca automaticamente per un determinato periodo di tempo oppure esegue la cancellazione di tutti i dati, a seconda del dispositivo. L'opzione è disabilitata per impostazione predefinita.

Tentativi con password errata prima che il dispositivo cancelli i dati o attivi la "Modalità blocco a tempo"
Quando si attiva l'opzione di *cancellazione dei dati* sopra specificata e un utente immette una password errata per il numero di tentativi indicato, il dispositivo cancella i dati o si attiva la "Modalità blocco a tempo", a seconda del dispositivo.

Sincronizzazione

In questa schermata sono disponibili le impostazioni per i messaggi e-mail in HTML, gli allegati, la limitazione del numero di caratteri da trasferire e il numero massimo di messaggi e il periodo di calendario da sincronizzare.



Impostazioni e-mail

Consenti e-mail in HTML
Per impostazione predefinita è possibile sincronizzare i messaggi e-mail in HTML con i client ActiveSync. Deselezionare questa casella di controllo per inviare solo messaggi in testo normale.

Consenti allegati
Consente il download dei file allegati sul dispositivo. L'opzione è abilitata per impostazione predefinita.

Dimensioni massime allegati in byte (0 = nessun limite)
Rappresenta la dimensione massima dell'allegato che può essere scaricato automaticamente sul dispositivo. L'impostazione predefinita non prevede alcun limite di dimensione ("0").

Numero massimo di caratteri di testo da trasferire (-1 = nessun limite)
Questo è il numero massimo di caratteri del corpo dei messaggi e-mail in testo normale che verranno inviati al client. Se il corpo del messaggio contiene più caratteri di quelli consentiti, il corpo del messaggio viene troncato al limite specificato. L'impostazione predefinita non prevede alcun limite (opzione impostata su "-1"). Se si imposta l'opzione su "0", viene inviata solo l'intestazione del messaggio.

Numero massimo di caratteri HTML da trasferire (-1 = nessun limite)
Questo è il numero massimo di caratteri del corpo dei messaggi e-mail in HTML che verranno inviati al client. Se il corpo del messaggio contiene più caratteri di quelli consentiti, il corpo del messaggio viene troncato al limite specificato. L'impostazione predefinita non prevede alcun limite (opzione impostata su "-1"). Se si imposta l'opzione su "0", viene inviata solo l'intestazione del messaggio.

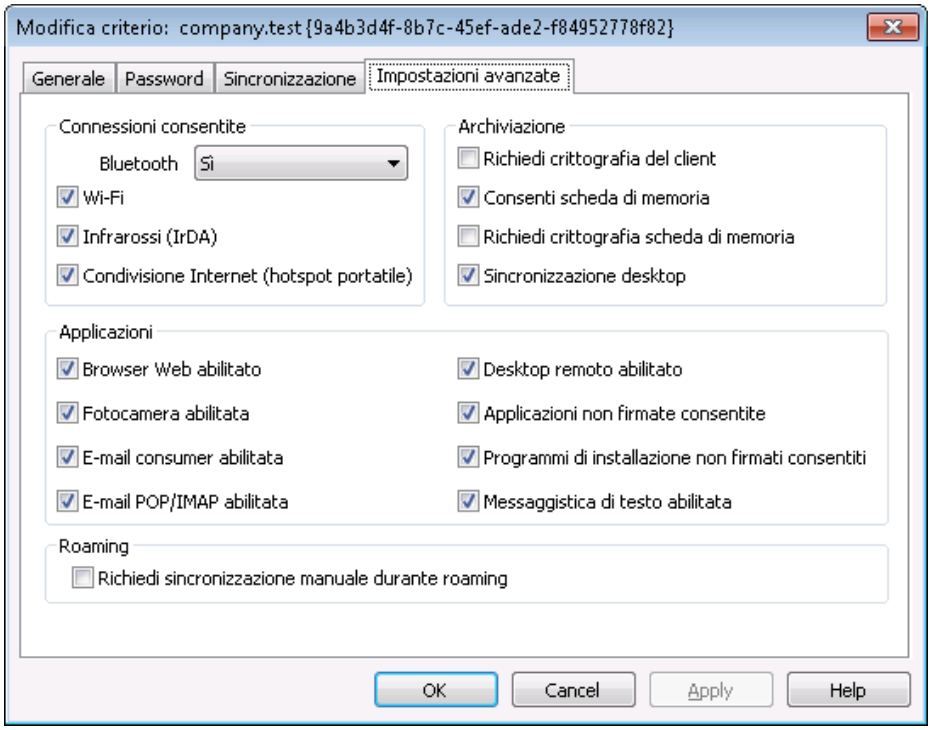
Periodo di tempo massimo per i messaggi e-mail da sincronizzare
Indica la quantità di messaggi e-mail precedenti, per intervallo di date a partire dalla data odierna, che può essere sincronizzata dal dispositivo. Per impostazione predefinita, questa opzione è configurata su "Tutto", ovvero è possibile sincronizzare tutta la posta elettronica, indipendentemente dalla data.

Calendario

Periodo cronologia calendario massimo da sincronizzare
La lunghezza del periodo precedente per cui possono essere sincronizzate le voci di calendario del dispositivo. Per impostazione predefinita, questa opzione è configurata su "Tutto", ovvero è possibile sincronizzare tutte le voci passate, indipendentemente dalla data.

Impostazioni avanzate

Nella scheda Impostazioni avanzate sono disponibili le opzioni per definire i tipi di connessione consentiti, la possibilità di abilitare determinate applicazioni, l'archiviazione, la crittografia e il roaming.



La scheda resta nascosta, a meno che non si attivi l'opzione *Abilita modifica opzioni avanzate criteri*[425], disponibile nella schermata ActiveSync per MDaemon.

Connessioni consentite

Bluetooth

Utilizzare questa opzione per specificare se le connessioni Bluetooth sono consentite o meno per il dispositivo. È possibile scegliere **Sì** per consentire le connessioni Bluetooth, **No** per impedirle o **Viva voce** per limitare la connessione Bluetooth alla sola funzione Viva voce. Per impostazione predefinita, questa opzione è impostata su **Sì**.

WIFI

Consente le connessioni WIFI. L'opzione è abilitata per impostazione predefinita.

Infrarossi (IrDA)

Consente le connessioni a infrarossi (IrDA). L'opzione è abilitata per impostazione predefinita.

Condivisione Internet (hotspot portatile)

L'opzione consente al dispositivo di utilizzare la condivisione Internet (hotspot portatile). L'opzione è abilitata per impostazione predefinita.

Archiviazione

Richiedi crittografia dispositivo
Selezionare questa opzione per richiedere la crittografia sul dispositivo. Non tutti i dispositivi applicano la crittografia. È disabilitata per impostazione predefinita.

Consenti scheda di memoria
Consente di utilizzare una scheda di memoria nel dispositivo. Per impostazione predefinita, questa opzione è abilitata.

Richiedi crittografia scheda di memoria
Selezionare questa opzione per richiedere la crittografia della scheda di memoria. È disabilitata per impostazione predefinita.

Sincronizzazione desktop
Consente di utilizzare ActiveSync per il desktop sul dispositivo. L'opzione è abilitata per impostazione predefinita.

Applicazioni

Browser Web abilitato
Consente l'utilizzo di un browser sul dispositivo. Questa opzione non è supportata su alcuni dispositivi e potrebbe non essere applicabile a browser di terze parti. L'opzione è abilitata per impostazione predefinita.

Videocamera abilitata
Consente l'utilizzo di una videocamera sul dispositivo. L'opzione è abilitata per impostazione predefinita.

E-mail consumer abilitate
Il dispositivo consente all'utente di configurare un account di posta elettronica personale. Se si disattiva questa opzione, i tipi di account di posta elettronica o servizi non consentiti dipendono completamente dal client ActiveSync specifico. L'opzione è abilitata per impostazione predefinita.

Posta POP/IMAP abilitata
Consente l'accesso alla posta elettronica mediante POP e IMAP. L'opzione è abilitata per impostazione predefinita.

Desktop remoto abilitato
Consente al client di utilizzare Desktop remoto. L'opzione è abilitata per impostazione predefinita.

Applicazioni senza firma consentite
Questa opzione consente l'uso di applicazioni senza firma sul dispositivo. Per impostazione predefinita, questa opzione è abilitata.

Programmi di installazione senza firma consentiti
Questa opzione consente l'esecuzione di programmi di installazione senza firma sul dispositivo. Per impostazione predefinita, questa opzione è abilitata.

Messaggi di testo consentiti
Questa opzione consente di utilizzare i messaggi di testo sul dispositivo. I messaggi di testo sono abilitati per impostazione predefinita.

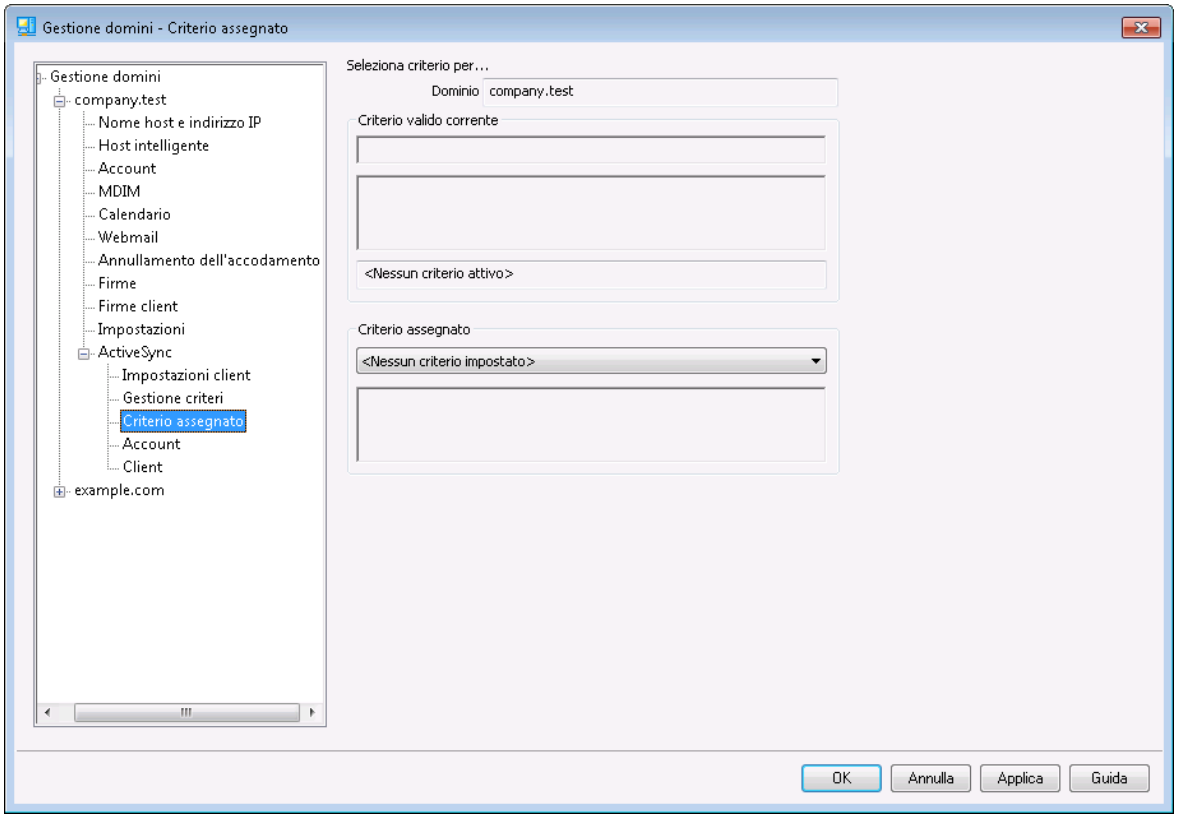
Roaming

Richiedi sincronizzazione manuale in roaming
Utilizzare questa opzione per richiedere la sincronizzazione manuale del dispositivo durante il roaming. La sincronizzazione automatica durante il roaming potrebbe aumentare i costi dei dati per il dispositivo, a seconda del gestore e del piano dati. L'opzione è disabilitata per impostazione predefinita.

Per ulteriori informazioni, vedere:

Domain Manager » Criterio assegnato 236
ActiveSync » Account 461
ActiveSync » Client 470

3.2.11.3 Criterio assegnato



Questa schermata consente di assegnare il criterio ActiveSync 226 predefinito al dominio. Quando un client ActiveSync si connette utilizzando uno degli account del dominio, questo è il criterio che verrà assegnato al client, a meno che non sia stato impostato un criterio alternativo per l'account specifico.

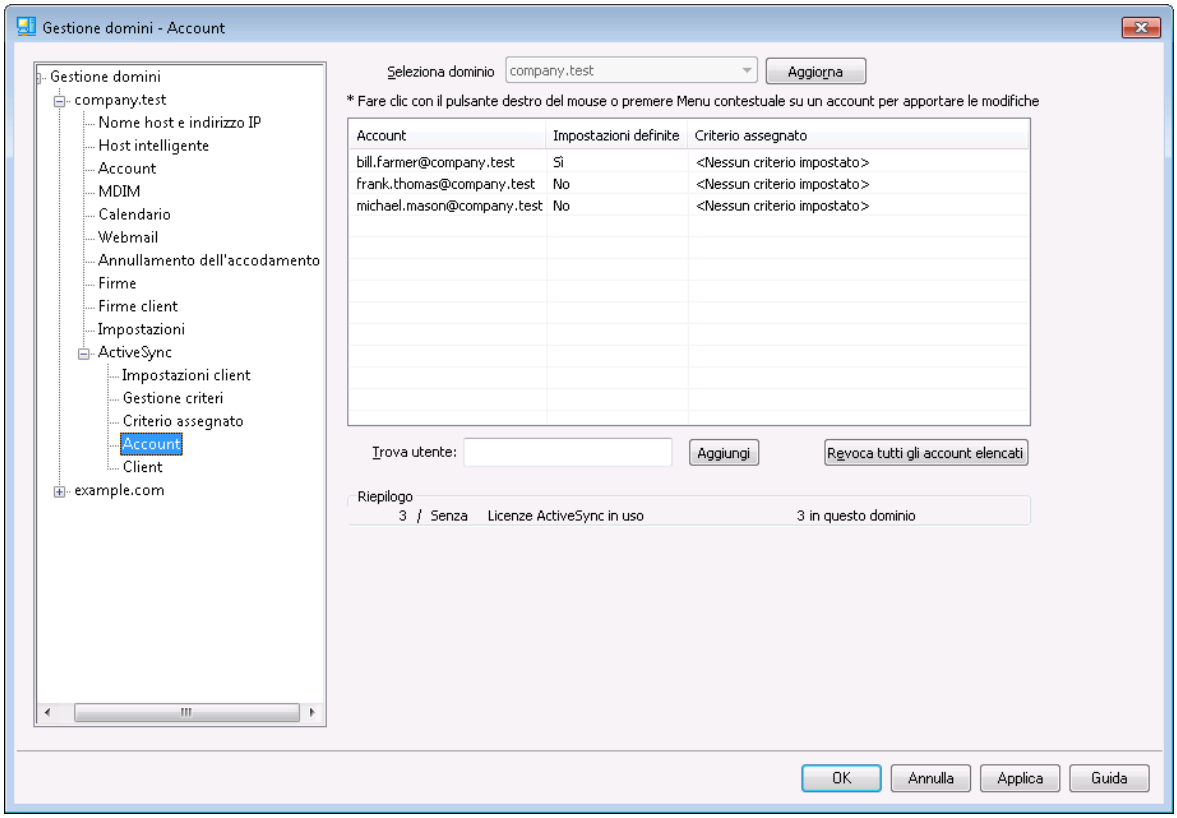
Assegnazione di un criterio ActiveSync predefinito

Per assegnare un criterio ActiveSync predefinito per il dominio, fare clic sull'elenco a discesa **Criterio da assegnare**, selezionare il criterio desiderato e fare clic su **OK**.

Per ulteriori informazioni, vedere:

Domain Manager » Policy Manager 226
ActiveSync » Account 461
ActiveSync » Client 470

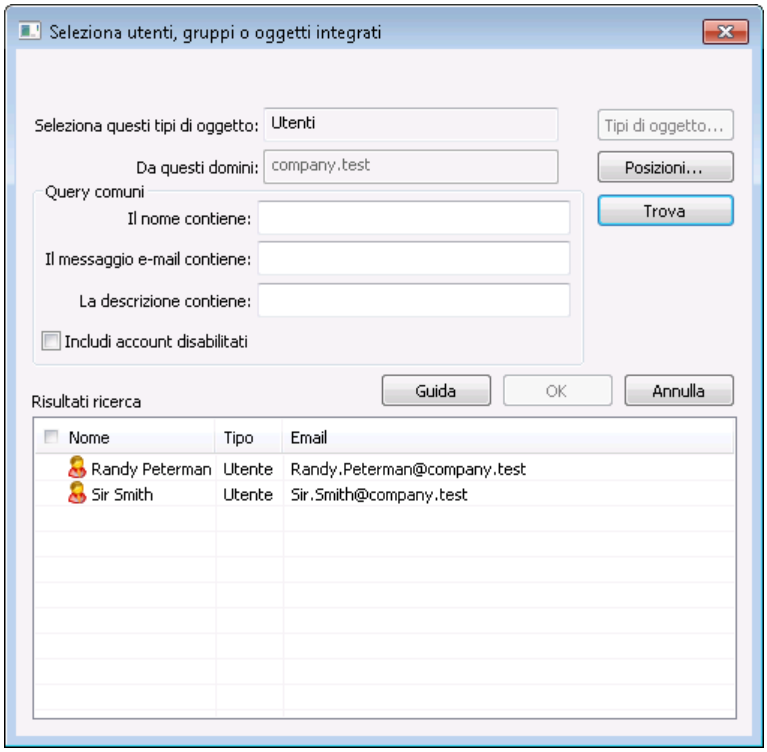
3.2.11.4 Account



Utilizzare questa schermata per designare gli account del dominio autorizzati a utilizzare ActiveSync. Sarà quindi possibile modificare le impostazioni di ciascun client degli account autorizzati e assegnare i criteri di ActiveSync corrispondenti.

Autorizzazione degli account

Fare clic su **Aggiungi** per autorizzare manualmente uno o più degli account del dominio a utilizzare ActiveSync. Viene visualizzata la finestra di dialogo Utenti per la ricerca e la selezione degli account.



Interrogazioni comuni
Utilizzare le opzioni presenti in questa sezione per restringere la ricerca specificando in tutto o in parte nome dell'utente, indirizzo e-mail o i contenuti della Descrizione[729] dell'account. Lasciare i campi vuoti se si desidera che i risultati della ricerca contengano tutti gli utenti che corrispondono alle Posizioni specificate in precedenza.

Includi account disabilitati
Selezionare questa casella di controllo se si desidera includere gli account disabilitati[729] nella ricerca.

Trova
Dopo aver specificato tutti i criteri di ricerca, fare clic su **Trova** per eseguire la ricerca.

Risultati ricerca
Dopo aver eseguito la ricerca, selezionare gli utenti desiderati nei Risultati della ricerca e fare clic su **OK** per aggiungerli all'elenco degli account autorizzati.

Revoca degli account

Per revocare l'autorizzazione all'utilizzo di ActiveSync, selezionarlo dall'elenco e fare clic su **Revoca account selezionato**. Se si desidera revocare tutti gli account, fare clic sul pulsante **Revoca tutti gli account**.

Se si è abilitata l'opzione per *autorizzare tutti gli account al primo accesso tramite il protocollo ActiveSync* 461, la revoca dell'autorizzazione di accesso di un utente lo rimuoverà dall'elenco, ma quando un dispositivo si connetterà nuovamente per l'account, l'autorizzazione verrà concessa nuovamente.

Assegnazione di un criterio ActiveSync

Per assegnare un Criterio 452 all'account:

1. Selezionare un account dall'elenco.
2. Fare clic su **Assegna criterio**. Verrà aperta la finestra di dialogo Applicazione criterio.
3. Fare clic sull'elenco a discesa **Criterio da assegnare** e scegliere il criterio desiderato.
4. Fare clic su **OK**.

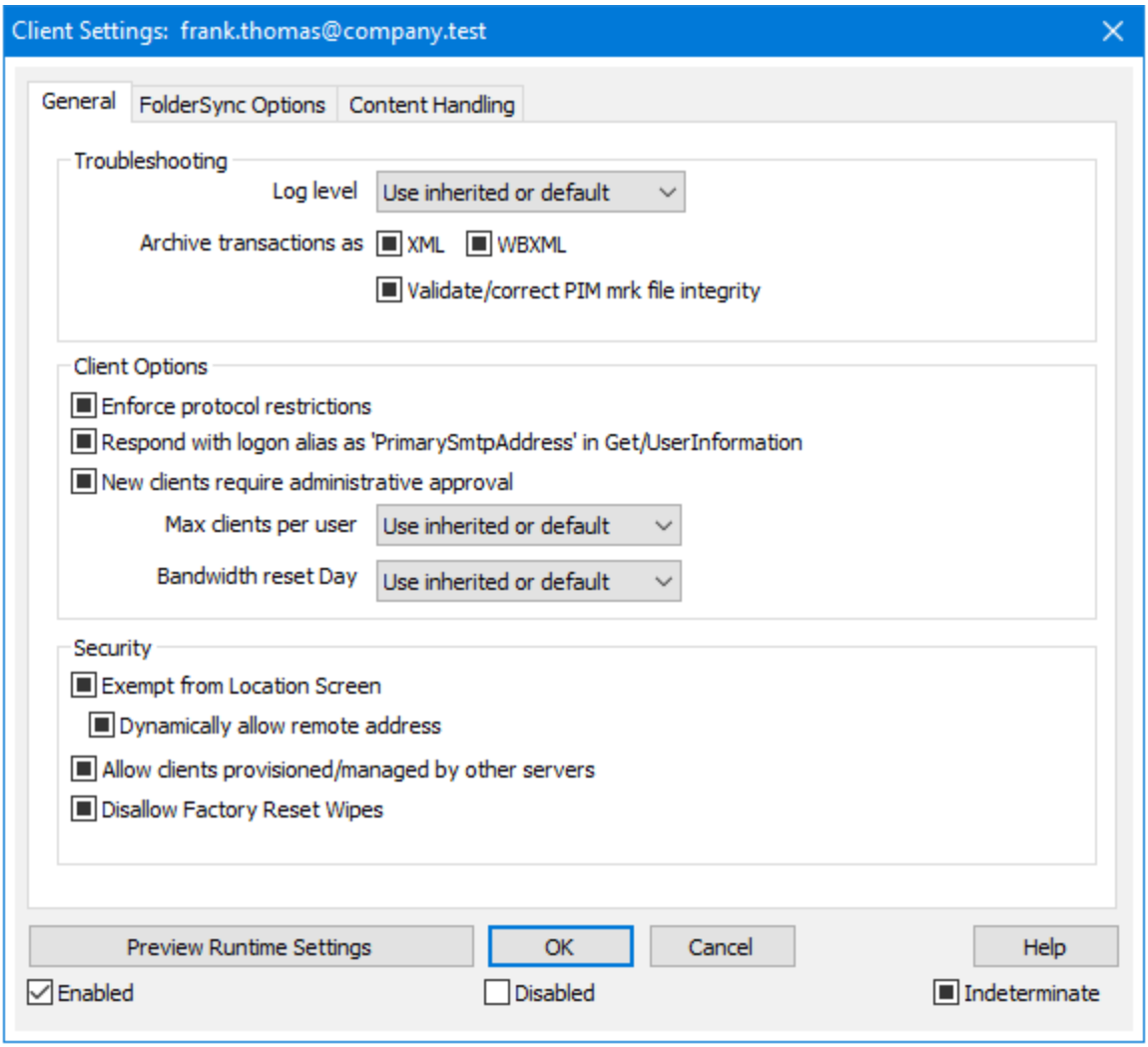
Questo criterio sarà assegnato ai nuovi dispositivi che si connettono per l'account.

Ricerca dell'elenco degli account autorizzati

Se si dispone di un numero elevato di account autorizzati all'uso di ActiveSync, è possibile utilizzare la casella **Trova utente** per cercare l'elenco di un account specifico. Per selezionare l'utente, è sufficiente digitare le prime lettere dell'indirizzo e-mail dell'account.

Impostazioni

Selezionare un account e fare clic su **Impostazioni** per gestire le impostazioni client per l'account. Queste impostazioni saranno applicate ai client ActiveSync che si connettono per l'account.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Impostazioni client del dominio 220. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra. Al contrario, le modifiche apportate in questa schermata sovrascriveranno le impostazioni a livello di dominio per l'account.

Generale

Risoluzione dei problemi

Livello di registrazione

ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei

problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo

modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a

MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche[317] a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca[319] sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche[317] padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise[122] a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise[757] a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client[470] e tipi di client[486] che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

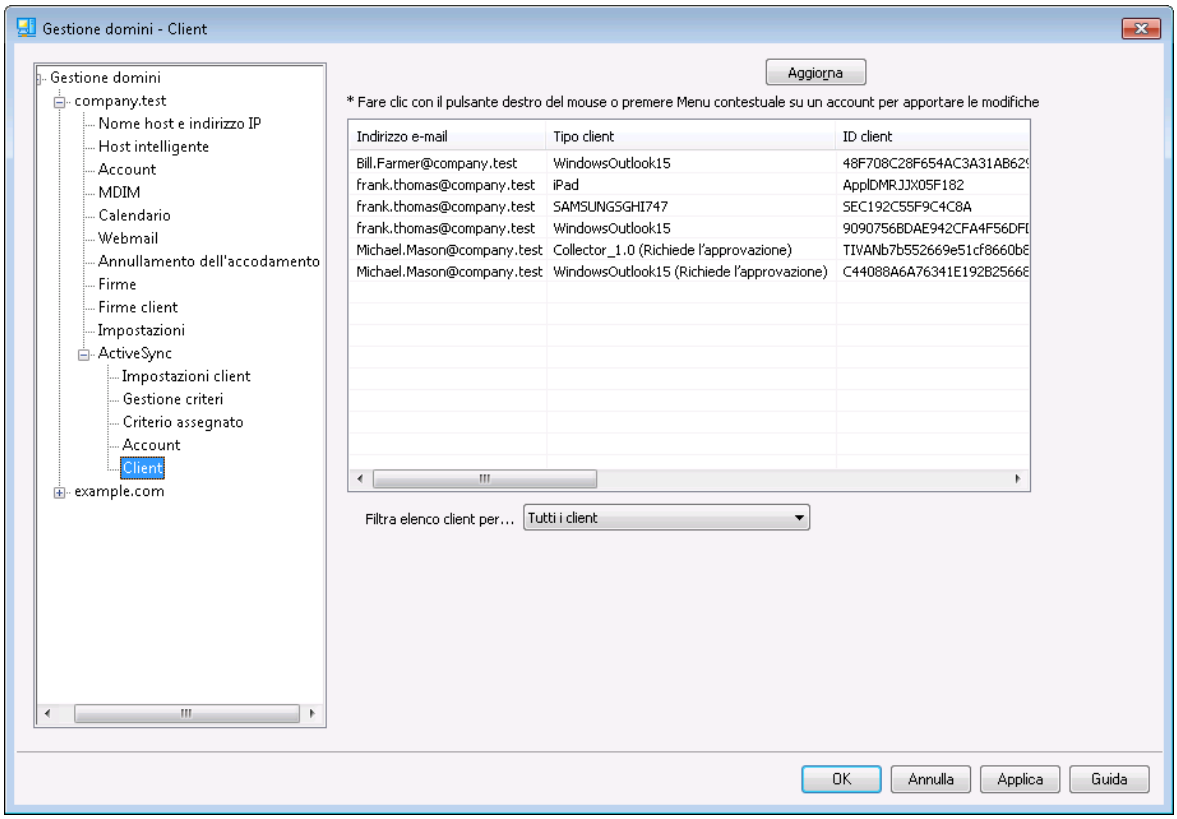
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

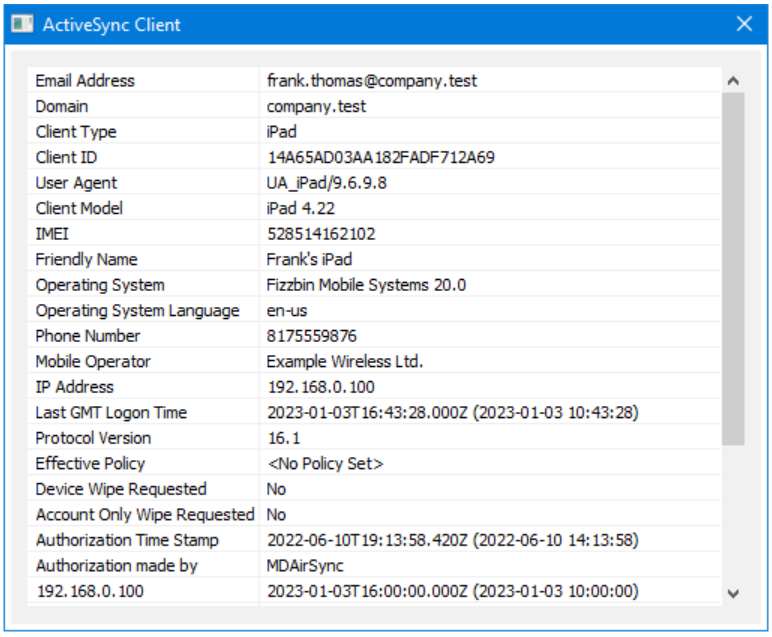
ActiveSync » Impostazioni client 430
ActiveSync » Domini 444
ActiveSync » Client 470

3.2.11.5 Client



Questa schermata include una voce per ciascun dispositivo ActiveSync associato al dominio.

Dettagli client ActiveSync



Fare doppio clic su una voce oppure fare clic con il pulsante destro sulla voce e scegliere **Visualizza dettagli client** per visualizzare la finestra di dialogo Dettagli client. In questa schermata sono riportate informazioni relative al client, come Tipo client, ID client, ora di ultimo accesso e simili.

Impostazioni client

Fare clic con il pulsante destro su un client e scegliere **Personalizza impostazioni client** per gestire le impostazioni del client. Per impostazione predefinita queste impostazioni vengono ereditate da Tipo client, ma si possono modificare secondo necessità. Vedere Gestione delle impostazioni del client di un dispositivo 248 di seguito.

Assegnazione di un criterio ActiveSync

Per assegnare un Criterio 452 al dispositivo:

1. Fare clic con il pulsante destro su un dispositivo nell'elenco.
2. Fare clic su **Applica criterio**. Verrà aperta la finestra di dialogo Applicazione criterio.
3. Fare clic sull'elenco a discesa **Criterio da assegnare** e scegliere il criterio desiderato.
4. Fare clic su **OK**.

Statistiche

Fare clic con il pulsante destro su una voce, quindi su **Visualizza statistiche** per visualizzare la finestra di dialogo Statistiche client, che contiene alcune statistiche sull'uso del client.

Ripristina statistiche

Per azzerare le statistiche di un client, fare clic con il pulsante destro sul client, quindi su **Azzera statistiche**, infine su **OK** per confermare l'azione.

Rimozione di un client ActiveSync

Per rimuovere un client ActiveSync, fare clic con il pulsante destro sul client e scegliere **Elimina**, quindi selezionare **Sì**. In questo modo si rimuove il client dall'elenco e si eliminano tutte le informazioni di sincronizzazione a esso correlate in MDaemon. Ne consegue che, se in futuro l'account utilizzerà ActiveSync per la sincronizzazione dello stesso client, MDaemon tratterà tale client come se non fosse mai stato utilizzato prima sul server; sarà dunque necessario risincronizzare tutti i dati del client con MDaemon.

Cancellazione completa di un client ActiveSync

Quando un criterio 452 è stato applicato a un client ActiveSync selezionato e il client l'ha applicato e ha risposto, per tale client sarà disponibile un'opzione Cancellazione completa. Per effettuare una cancellazione completa, fare clic con il tasto destro del mouse sul client (o selezionarlo se si utilizza MDRA) e fare clic su **Cancellazione completa**. Al successivo collegamento del client, MDaemon imposterà il dispositivo in modo da eliminare tutti i dati o da ripristinare le impostazioni di fabbrica. In base al client, ciò potrebbe comportare la totale rimozione di tutti i dati, app scaricate incluse. Inoltre, finché esisterà la voce ActiveSync del client, MDaemon continuerà a inviare la richiesta di cancellazione ogni volta che il dispositivo si connetterà. Se a un certo punto si desidera eliminare il client, accertarsi di aggiungerlo prima alla Lista bloccati 437, in modo che non possa connettersi di nuovo in futuro. Infine, se un dispositivo eliminato viene recuperato e si desidera consentirgli di connettersi nuovamente, selezionare il dispositivo e fare clic su **Annulla azioni di cancellazione**. Sarà anche necessario rimuoverlo dalla Lista bloccati.

Cancellazione account di un client ActiveSync

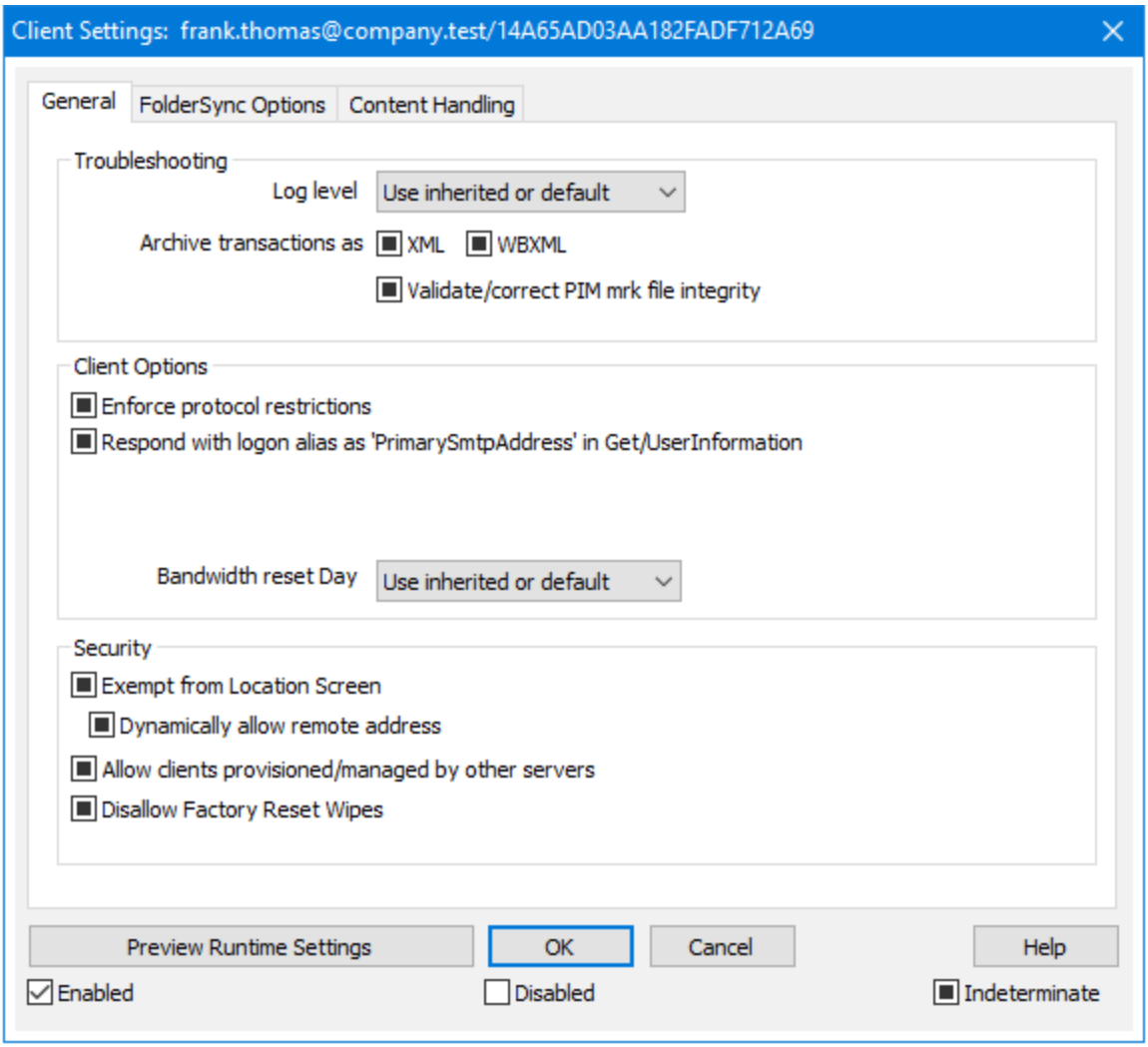
Per cancellare la posta dell'account e i dati PIM dal client o dal dispositivo, fare clic con il pulsante destro e scegliere **Cancella posta e PIM dell'account dal client**. L'opzione *Cancellazione account* è simile all'opzione *Cancellazione completa* descritta sopra, ma invece di eliminare tutti i dati, elimina solo i dati dell'account, come i messaggi di posta elettronica, le voci di calendario, i contatti e così via. Tutto il resto, come applicazioni, foto e musica, viene lasciato dove si trova.

Autorizzazione del client

Se l'opzione "*I nuovi client richiedono l'approvazione dell'amministratore*" nella schermata Impostazioni client ActiveSync 430 è attivata, selezionare un client e fare clic su Approva sincronizzazione client per autorizzarlo alla sincronizzazione con il server.

Gestione delle impostazioni del client di un dispositivo

La schermata Impostazioni client a livello di dispositivo consente di gestire le impostazioni per un dispositivo specifico.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Tipi client Impostazioni client 486. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra. Al contrario, le modifiche apportate in questa schermata sovrascriveranno le impostazioni a livello di tipi di client per il dispositivo.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei

problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo

modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a

MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

ActiveSync » Account 461
ActiveSync » Sicurezza 437

3.3 Gestore gateway

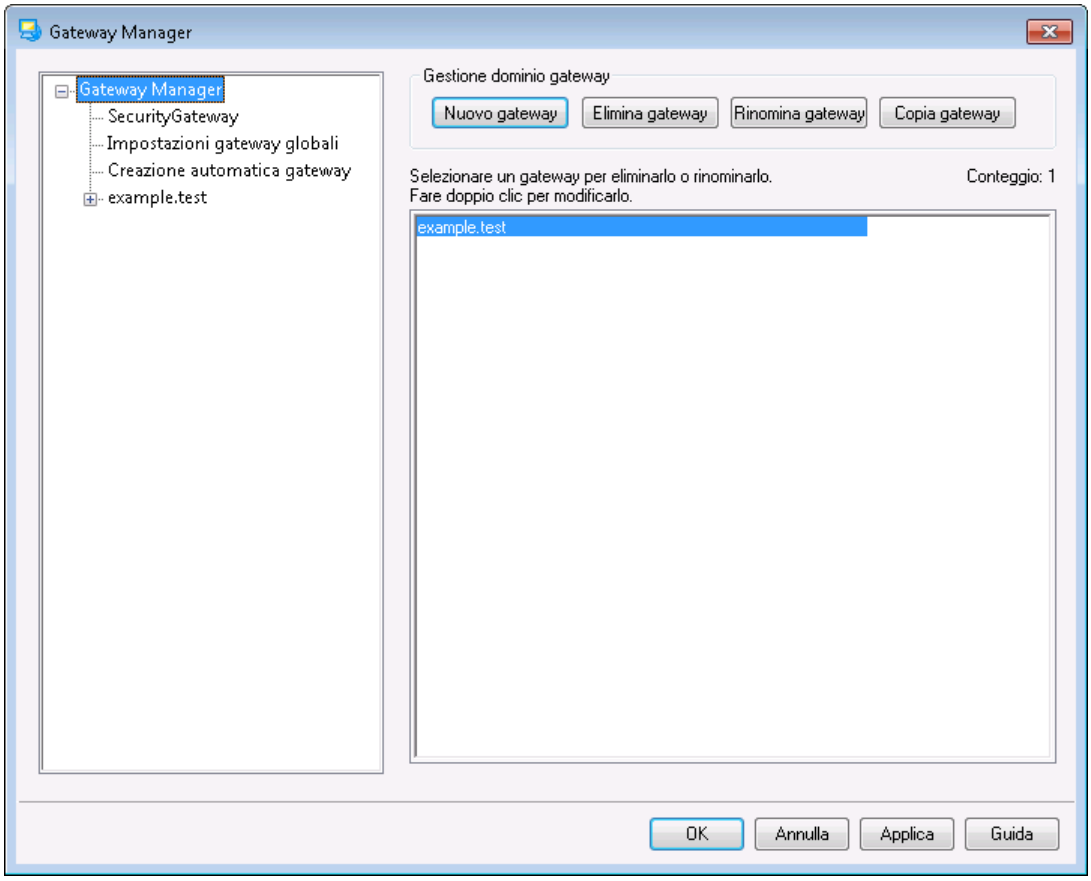
Il Gestore gateway è disponibile mediante la selezione del menu Impostazioni » Gestore gateway.... Questa funzionalità offre un secondo livello di supporto, limitato ma utile, per l'hosting di più domini o come server di posta di backup.

Ad esempio,

> Si supponga di assumere la funzione di server di backup o di mail-drop per conto terzi, ricevendone le e-mail in entrata e memorizzandole in una cartella del server, senza peraltro eseguire l'hosting completo del dominio gestendone i singoli account utente. Il nome di questo dominio di esempio sarà "esempio.com".
>
> La prima cosa da fare è creare il gateway selezionando **Nuovo gateway** in Gestore gateway e quindi specificando "esempio.com" come nome. Ora tutta la posta che MDaemon riceve per il dominio verrà separata dal flusso della posta principale e collocata nella cartella designata nella schermataDominio 262 del gateway, indipendentemente dai destinatari specifici dei messaggi.
>
> Successivamente, è necessario indicare i metodi di raccolta o di consegna desiderati affinché le i messaggi e-mail del dominio pervengano al server di posta effettivo in cui si trovano i relativi account utente. Sono disponibili due metodi per eseguire questa operazione: utilizzare l'opzione *Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota* della schermata Dominio 262 o utilizzare le opzioni di annullamento dell'accodamento 269. Se si desidera, è anche possibile creare un account MDaemon e modificarne la cartella della posta 732 impostandola sulla stessa cartella di memorizzazione 262 utilizzata dal gateway. Questo consentirà a un client di posta di connettersi a MDaemon per raccogliere la posta di esempio.com.
>
> Infine, è probabile che sia necessario modificare le impostazioni DNS di esempio.com in modo da indicare il server MDaemon come host MX del dominio.

Sono disponibili molte altre funzioni e opzioni, ma quello dell'esempio precedente rappresenta un tipico gateway di base. Tuttavia, se si desidera una configurazione atipica può essere necessario eseguire operazioni diverse, ad esempio se si desidera utilizzare un nome di dominio inesistente in Internet come "azienda.mail". La ricezione di messaggi con un nome di dominio altrimenti non valido come questo è possibile, ma è necessario che tale nome sia "nascosto" in un indirizzo di Dominio predefinito 185. Questo metodo consente di creare indirizzi che possano attraversare il dominio predefinito e arrivino al gateway. Se, ad esempio, il dominio predefinito è esempio.com e si dispone di un gateway per azienda.mail, è possibile inviare un messaggio a "bob@azienda.mail" utilizzando l'indirizzo "bob{azienda.mail}@esempio.com". Poiché "esempio.com" è il dominio registrato ospitato da MDaemon, tale messaggio verrà recapitato correttamente ma, dopo aver ricevuto il messaggio in questo formato, MDaemon convertirà l'indirizzo in "bob@azienda.mail" e lo recapiterà alla cartella

specificata per il gateway. Il metodo più semplice consiste, naturalmente, nel registrare un nome di dominio valido per il gateway e quindi indirizzarne il record DNS o MX a `esempio.com`.



Elenco gateway

Nel riquadro di navigazione sul lato sinistro di questa finestra di dialogo è visualizzato l'elenco dei domini, con i collegamenti a ciascuna schermata utilizzata per configurare le diverse impostazioni specifiche del dominio. È inoltre possibile accedere alle Impostazioni gateway globali 258 e alle schermate di Creazione automatica gateway 260. L'elenco sulla destra viene utilizzato per eliminare e rinominare i domini. È possibile fare doppio clic su un gateway dell'elenco per cambiare il dominio e configurarne le impostazioni.

Gestione dei domini gateway

Nuovo gateway

Per creare un nuovo gateway: selezionare **Nuovo gateway**, digitare il nome del nuovo gateway (ad es. esempio.mail) nella finestra di dialogo Crea/rinomina gateway, quindi fare clic su **OK**.

Normalmente, il valore inserito in questo campo corrisponde al nome del dominio Internet registrato che un server DNS trasforma nell'indirizzo IP del sistema locale su cui è in esecuzione il server oppure in un alias qualificato di quel nome. In alternativa, per il nome del gateway è possibile scegliere di utilizzare un nome a uso

interno o non altrimenti valido, ad esempio "company.mail". Questa soluzione richiederebbe comunque di usare il metodo del nome del dominio nidificato illustrato nell'esempio precedente oppure di utilizzare qualche altro schema di filtro dei contenuti per indirizzare correttamente i messaggi.

Elimina gateway
Per eliminare un gateway, selezionare il modello nell'elenco riportato di seguito, fare clic su **Elimina gateway**, quindi fare clic su **Sì** per confermare l'eliminazione.

Rinomina gateway
Per modificare il nome di un gateway: selezionare il gateway dall'elenco, fare clic su **Rinomina gateway**, digitare il nuovo nome nella finestra di dialogo Crea/rinomina gateway, quindi fare clic su **OK**.

Copia gateway
Per creare un nuovo gateway con impostazioni che corrispondono a un altro gateway, selezionare un gateway dall'elenco, fare clic su questo pulsante e specificare un nome per il nuovo gateway.

Gateway Editor

Gateway Editor è utilizzaro per la modifica delle impostazioni di ciascun gateway. Sono disponibili le schermate seguenti:

Dominio 262
Utilizare questa schermata per abilitare/disabilitare il gateway, indicare la cartella da utilizare per archiviare i messaggi del dominio e configurare altre opzioni relative alla consegna e alla gestione degli allegati.

Verifica 264
Se il server del dominio remoto esegue l'aggiornamento di un server LDAP o Active Directory con tutte le caselle postali, tutte le liste di distribuzione e tutti gli alias in esso contenuti o se include un server Minger per la verifica degli indirizzi remoti, è possibile utilizzare questa finestra di dialogo per specificare il server in questione e verificare la validità degli indirizzi dei destinatari dei messaggi in arrivo. Se un indirizzo non è valido, il messaggio viene respinto. Grazie a questo metodo, non è necessario attenersi all'assunto che tutti i destinatari dei messaggi di un dominio siano validi.

Inoltro 268
Questa schermata consente di specificare l'host o l'indirizzo a cui deve essere inoltrata la posta del dominio in arrivo. Sono inoltre disponibili opzioni che consentono di specificare la porta per l'inoltro dei messaggi e di salvare a livello locale una copia dei messaggi.

Annullamento dell'accodamento 269
Le opzioni di questa schermata consentono di specificare se MDaemon deve rispondere alle richieste ETRN e ATRN effettuate per conto del dominio al fine di annullare l'accodamento dei messaggi. È inoltre possibile configurare diverse altre opzioni relative all'annullamento dell'accodamento.

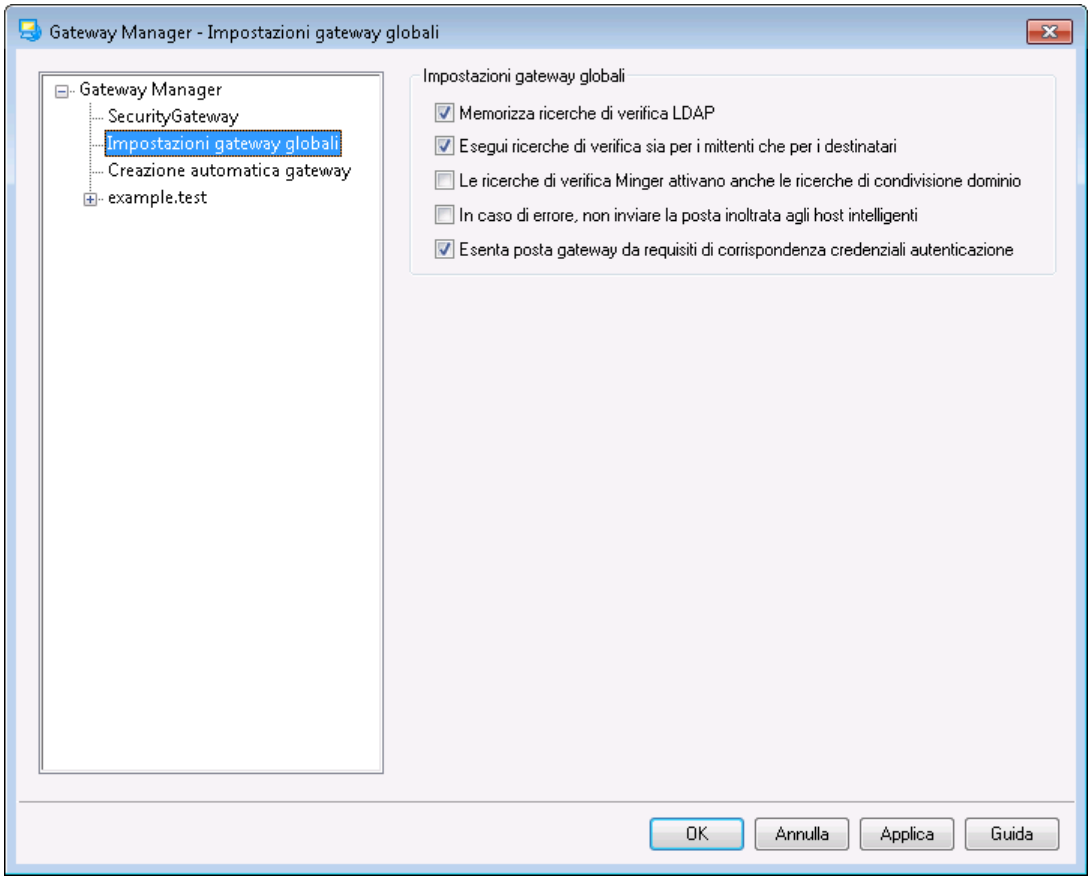
Quote 272
Questa finestra di dialogo consente di impostare i limiti relativi alla quantità di spazio su disco utilizzabile dal dominio e al numero massimo di messaggi memorizzabili.

Impostazioni 274
Questa schermata contiene numerose altre opzioni che verranno applicate al gateway di dominio selezionato. È possibile, ad esempio, abilitare o disabilitare la scansione AntiVirus e AntiSpam per il gateway, specificare se per l'annullamento dell'accodamento della posta è richiesta l'autenticazione, definire la password per l'autenticazione e diverse altre opzioni.

Vedere:

Impostazioni gateway globali 258
Creazione automatica di gateway 260
Gestione domini 185

3.3.1 Impostazioni gateway globali



Impostazioni gateway globali

Le opzioni seguenti sono opzioni globali e non sono limitate a un gateway specifico.

Memorizza ricerche di verifica LDAP
Selezionare questa casella di controllo se si desidera inserire nella cache i risultati delle ricerche di verifica 264 LDAP per i gateway di dominio.

Esegui ricerche di verifica sia per i mittenti che per i destinatari
Per impostazione predefinite, quando le opzioni di verifica 264 dell'indirizzo sono attive per un gateway, MDaemon tenterà di verificare i destinatari e i mittenti dei messaggi del gateway. Disattivare questa opzione se si desidera verificare solo i destinatari.

Le ricerche di verifica Minger attivano anche le ricerche di condivisione dominio
Se si abilita questa opzione e uno dei gateway esegue la verifica degli indirizzi mediante Minger 878, oltre a interrogare l'host Minger indicato nella schermata Verifica 264, MDaemon interroga anche gli host di Condivisione dominio 117. Questa opzione si applica a tutti i gateway impostati per eseguire la verifica degli indirizzi mediante Minger.

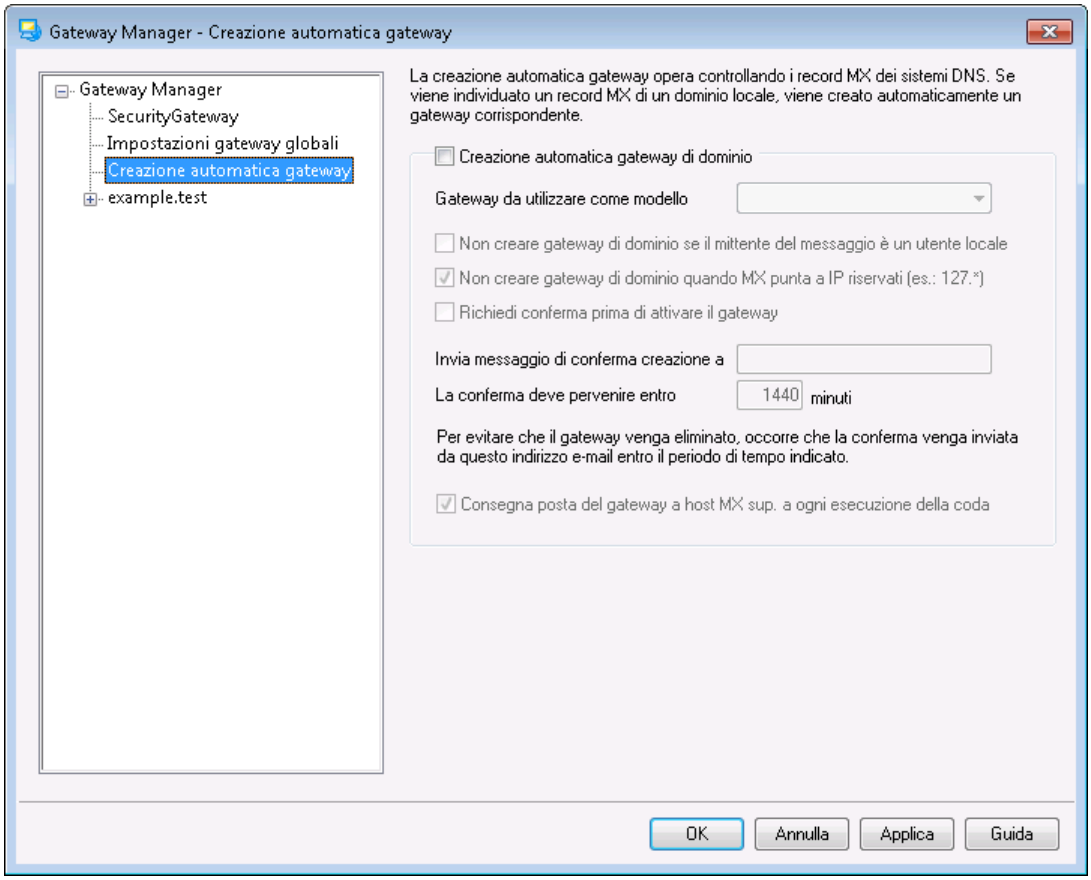
In caso di errore, non inviare la posta inoltrata a un host intelligente
Scegliere questa opzione per evitare l'invio di email inoltrate all'host specificato quando si verificano errori di consegna. L'opzione è disabilitata per impostazione predefinita.

Esenta posta gateway da requisiti di corrispondenza credenziali autenticazione
Per impostazione predefinita la posta gateway è esclusa dalle due seguenti opzioni della schermata Autenticazione SMTP 531: "*Le credenziali utilizzate devono corrispondere a quelle del percorso di ritorno*" e "*Le credenziali utilizzate devono corrispondere a quelle dell'indirizzo nell'intestazione FROM*". Disattivare questa opzione se non si desidera escludere la posta gateway da questi requisiti, ma si consideri che disattivandola si potrebbero causare dei problemi di archiviazione/inoltro della posta del gateway.

Vedere:

Gestore gateway 255
Gateway Editor » Verifica 264
Minger 878
Condivisione dominio 117

3.3.2 Creazione automatica di gateway



Creazione automatica di gateway

Questa funzionalità consente la creazione automatica di un Gateway di dominio 255 relativo a un dominio sconosciuto nel caso in cui un'altra origine tenti di consegnare a MDaemon i messaggi di tale dominio e il risultato di una query DNS indichi la posizione di MDaemon come record MX valido.

Ad esempio:

Si supponga di aver abilitato la creazione automatica di un dominio e che l'indirizzo IP del dominio predefinito MDaemon sia `192.0.2.0`. Quando MDaemon riceve un messaggio via SMTP destinato al dominio sconosciuto `esempio.com`, ricercherà i record MX e A del dominio `esempio.com` per verificare se il proprio indirizzo IP `192.0.2.0` è un host di inoltro della posta conosciuto. Se i risultati delle interrogazioni DNS confermano che l'indirizzo IP di MDaemon è un host MX valido per `esempio.com`, MDaemon crea automaticamente un nuovo gateway di dominio e ne accetta la posta. I messaggi indirizzati a `esempio.com` vengono archiviati in una cartella speciale e, se necessario, accodati in corrispondenza di host MX di livello superiore a ogni intervallo di elaborazione della posta remota. Questa funzione trasforma di fatto il server in un server di backup per un altro dominio, semplicemente configurando il sistema DNS in modo che utilizzi l'indirizzo IP del server come host MX alternativo.

Per garantire la sicurezza di questa funzione, è possibile configurare MDaemon in modo da inviare una richiesta di conferma a un indirizzo e-mail desiderato. Durante l'attesa della conferma, i messaggi per il dominio vengono accettati e memorizzati, ma non consegnati. Le richieste di conferma devono avere riscontro entro un tempo specificato. In caso contrario, il gateway creato automaticamente verrà rimosso e tutti i messaggi archiviati verranno cancellati. Se la conferma viene ricevuta entro il tempo previsto, i messaggi archiviati verranno consegnati normalmente.

È possibile che un utente malintenzionato o "spammer" tenti di sfruttare questa funzione configurando il proprio server DNS in modo che l'indirizzo IP di MDaemon figuri come host MX. La funzione Creazione automatica di gateway deve essere usata con la massima cautela. Per prevenire eventi indesiderati, si consiglia di utilizzare sempre, ove possibile, il comando *Invia messaggio di conferma della creazione a*.

Creazione automatica gateway di dominio
Fare clic su questa casella di controllo se si desidera che i gateway di dominio vengano creati automaticamente in base ai risultati delle interrogazioni DNS.

Gateway da utilizzare come modello
Scegliere un gateway di dominio dall'elenco a discesa per utilizzarne le impostazioni come modello per tutti i gateway che verranno creati automaticamente.

Non creare gateway di dominio se il mittente del messaggio è un utente locale
Abilitare questa opzione per evitare che i messaggi provenienti da utenti locali possano avviare la creazione automatica di gateway.

Non creare gateway di dominio quando MX punta a IP riservati
Selezionare questa casella di controllo per impedire la creazione di un gateway automatico se il record MX punta a un indirizzo IP riservato, ad esempio 127.*, 192.* o simili.

Richiedi conferma prima di attivare il gateway
Se questa opzione è abilitata, MDaemon invia una conferma all'indirizzo e-mail desiderato per determinare se il gateway creato automaticamente è valido. Nonostante continui da accettare i messaggi per il dominio in questione, MDaemon non effettua la consegna finché non viene ricevuta la conferma.

Invia messaggio di conferma creazione a
Immettere l'indirizzo a cui inviare i messaggi di conferma in questa casella di testo.

La conferma deve pervenire entro XX minuti
Immettere il numero di minuti per cui MDaemon attende la conferma. Alla scadenza di questo limite di tempo, il gateway di dominio viene eliminato.

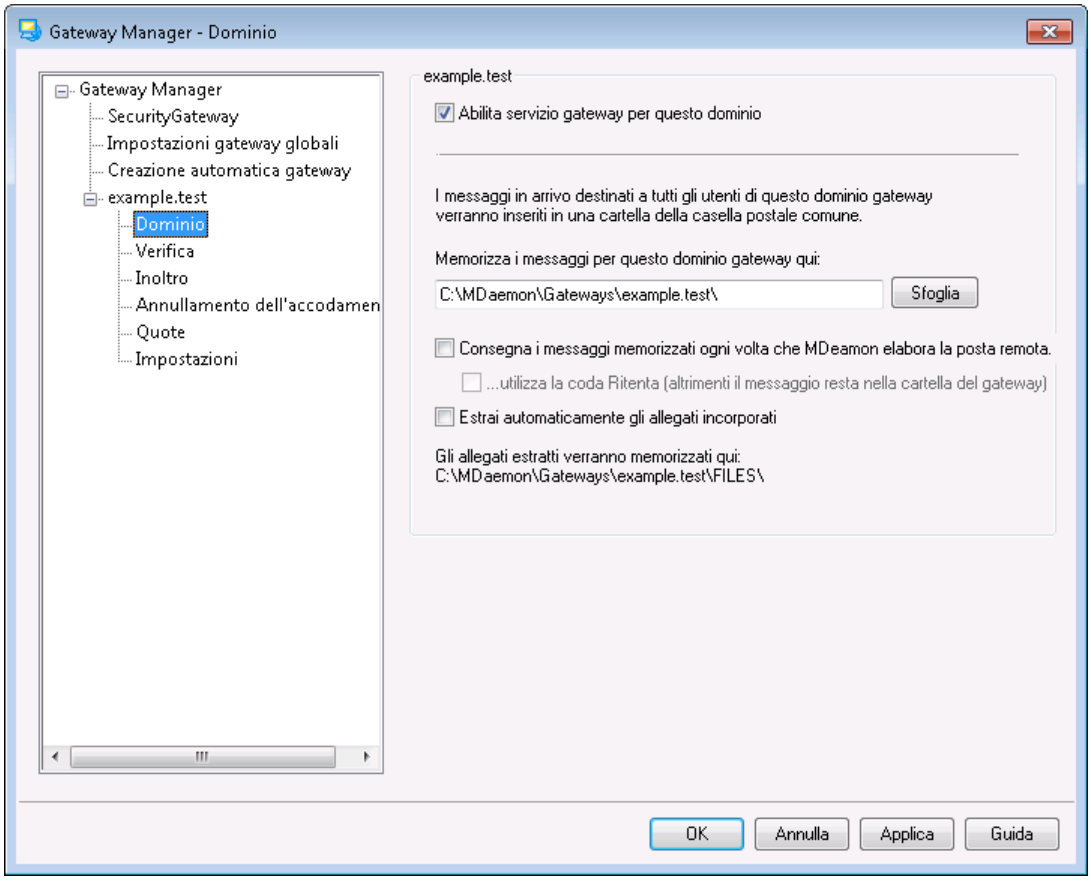
Consegna posta del gateway a host MX superiori a ogni esecuzione della coda
Abilitare questa opzione per specificare che a ogni elaborazione della coda remota i messaggi di questo gateway devono essere consegnati a host MX superiori.

Per ulteriori informazioni, vedere

Gestore gateway 255

3.3.3 Gateway Editor

3.3.3.1 Dominio



Dominio gateway

Attiva servizio gateway per questo dominio
Per attivare il dominio gateway, selezionare questa casella.

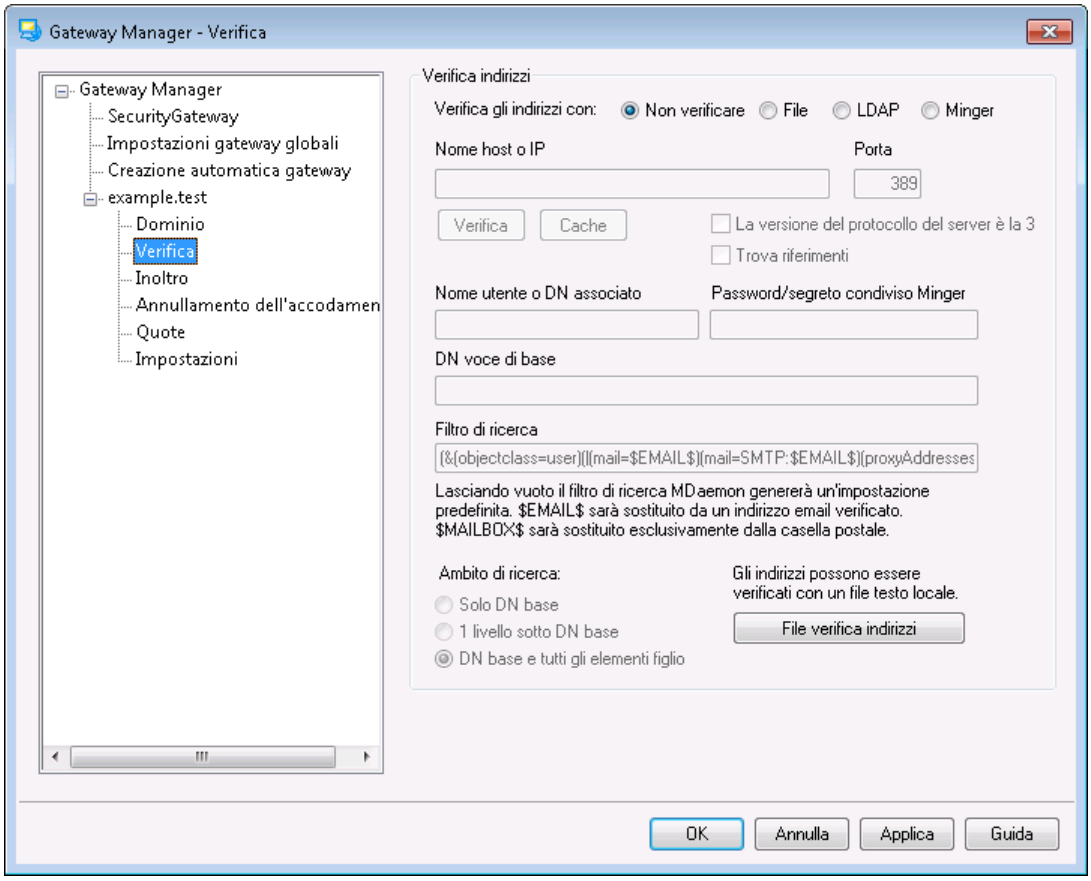
Memorizza i messaggi per il gateway qui:
Inserire la directory nella quale memorizzare la posta in entrata del dominio. Tutti i messaggi verranno memorizzati nella stessa cartella, indipendentemente dai singoli destinatari cui i messaggi sono indirizzati.

Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota
Solitamente, quando MDaemon riceve la posta diretta a uno dei relativi gateway, la memorizza fino a quando il dominio si connette a MDaemon per raccoglierla. In alcune situazioni può essere opportuno che MDaemon tenti di consegnare la posta direttamente via SMTP, senza attendere che venga raccolta dal dominio. Quando questa opzione è abilitata, MDaemon tenta di consegnare i messaggi del dominio ogni volta che viene elaborata la posta remota. La casella postale del gateway opererà temporaneamente come coda remota e verrà eseguito un tentativo di consegna. Tutti i messaggi che non possono essere consegnati rimarranno nella casella postale del gateway finché non vengono raccolti dal dominio oppure verranno consegnati in un secondo momento, ma non saranno spostati né nella coda remota, né nella coda tentativi. Se, tuttavia, il DNS del dominio non è configurato correttamente oppure se la configurazione di MDaemon prevede che trasmetta tutti i messaggi in uscita a un altro host per la consegna, tali messaggi potrebbero rimanere intrappolati in un loop di posta e, successivamente, essere considerati come posta impossibile da consegnare.

Utilizza la coda Ritenta (altrimenti il messaggio resta nella cartella del gateway)
Attivare questa opzione se si desidera utilizzare il meccanismo della coda Ritenta per il recapito della posta. Questa opzione è disattivata per impostazione predefinita, il che significa che la posta del gateway resterà nel gateway per sempre, anche se non può essere recapitata.

Estrai automaticamente gli allegati incorporati
Alcuni sistemi di posta richiedono che i file allegati vengano estratti prima che i messaggi siano sottoposti al flusso di posta. Per facilitare questa operazione, MDaemon è in grado di estrarre automaticamente gli allegati MIME in entrata e di collocarli nella sottocartella `\Files\` della cartella dei messaggi del dominio. Se si desidera l'estrazione automatica degli allegati, abilitare questa casella.

3.3.3.2 Verifica



Un problema diffuso con i gateway di dominio e i servizi di ricezione della posta consiste nel non disporre generalmente di un sistema in grado di stabilire la validità del destinatario del messaggio in entrata. Se, ad esempio, si opera in qualità di gateway per `esempio.com` e arriva un messaggio per `utente01@esempio.com`, non è possibile stabilire se, nel server e-mail di esempio.com, esista effettivamente una casella postale, un alias o una lista di distribuzione corrispondente all'indirizzo. Pertanto, l'unica possibilità consiste nel considerare l'indirizzo valido e accettare il messaggio. Inoltre, poiché in genere gli spammer inviano messaggi a molti indirizzi non validi, questo problema può comportare l'accettazione di una grande quantità di posta indesiderata per il gateway.

MDaemon include un metodo per prevenire questo problema mediante la verifica dell'indirizzo del destinatario. Se il server del dominio remoto esegue l'aggiornamento di un server LDAP o Active Directory con tutte le caselle postali, tutte le liste di distribuzione e tutti gli alias in esso contenuti o se include un server Minger per la verifica degli indirizzi remoti, è possibile utilizzare le opzioni di questa schermata per specificare il server LDAP, Active Directory o Minger nei quali sono memorizzate tali informazioni. In questo modo, all'arrivo di un messaggio per `esempio.com`, è possibile ricercare l'indirizzo del destinatario nell'altro server al fine di stabilirne la validità.

Verifica indirizzi

Verifica gli indirizzi con:

Non verificare
Scegliere questa opzione se non si desidera utilizzare la verifica degli indirizzi email per il gateway di dominio. MDaemon considererà validi tuti gli indirizzi dei destinatari dei messaggi in arrivo per il dominio, poiché non disporrà di alcun metodo per identificare gli indirizzi effettivamente esistenti per il dominio.

File
Scegliere questa opzione se si desidera utilizzare il file `GatewayUsers.dat` come elenco degli indirizzi al fine di verificare la validità dei destinatari dei messaggi in arrivo per il dominio. Si tratta di un elenco globale di indirizzi che viene applicato a tutti i gateway di dominio. Il file viene utilizzato come ulteriore fonte di indirizzi validi anche se si utilizza uno degli altri metodi di verifica disponibili. Se si utilizza l'opzione *File*, tuttavia, il file rappresenta l'unico metodo di verifica utilizzato. È inoltre possibile aprire e modificare l'elenco degli indirizzi validi selezionando il pulsante *File verifica indirizzi*.

LDAP
Scegliere questa opzione per attivare la verifica degli indirizzi remoti mediante LDAP o Active Directory. All'arrivo di un messaggio per un dominio remoto, il server LDAP o Active Directory viene interrogato per verificare la validità dell'indirizzo del destinatario. Se l'indirizzo non è valido, il messaggio verrà respinto. Qualora MDaemon non sia in grado di connettersi al server LDAP o AD, l'indirizzo verrà considerato comunque valido.

Minger
Scegliere questa opzione se si desidera eseguire una ricerca dell'indirizzo del destinatario del dominio nel server Minger del dominio. Qualora MDaemon non sia in grado di connettersi al server, l'indirizzo verrà considerato comunque valido. È inoltre disponibile un'opzione globale in Impostazioni gateway globali 258 che è possibile utilizzare se si desidera che MDaemon esegua una ricerca anche negli della condivisione di dominio 117.

Nome host o IP
Immettere il nome host o l'indirizzo IP del server LDAP/Active Directory del dominio. MDaemon si connetterà a questo server LDAP/Active Directory per verificare la validità dell'indirizzo del destinatario di un messaggio in arrivo relativo al dominio per il quale MDaemon funge da gateway o da server di backup.

Porta
Specificare la porta utilizzata dal server LDAP/AD o Minger del dominio. MDaemon utilizzerà tale porta per la verifica delle informazioni relative all'indirizzo mediante LDAP, Active Directory o Minger.

Verifica
Fare clic su questo pulsante per controllare che le impostazioni per la verifica in remoto dell'indirizzo siano configurate correttamente. MDaemon tenterà semplicemente di connettersi al server LDAP/AD indicato e ne verificherà la corrispondenza con le informazioni specificate.

Cache
Fare clic su questo pulsante per aprire il file cache di LDAP/Minger. È possibile attivare e disattivare la cache in Impostazioni gateway globali[258].

La versione del protocollo del server è la 3
Fare clic su questa casella di controllo se si desidera che la verifica del gateway utilizzi la versione 3 del protocollo LDAP con il server.

Trova riferimenti
A volte un server non dispone dell'oggetto richiesto ma può avere un riferimento incrociato alla relativa posizione a cui può fare riferimento il client. Se si desidera che la verifica del gateway segua questi riferimenti, attivare questa opzione. È disabilitata per impostazione predefinita.

Nome utente o DN associato
Inserire il nome utente o il DN dell'account con accesso di tipo amministrativo al server LDAP/AD del dominio, in modo che MDaemon possa verificare i destinatari dei messaggi in arrivo indirizzati al dominio per il quale agisce da gateway o da server di backup. Questo è il DN che viene usato per l'autenticazione nel procedimento di associazione.

Password/segreto condiviso Minger
La password viene trasmessa al server LDAP/AD del dominio insieme al valore *Associa DN* ai fini dell'autenticazione. Se si utilizza un server Minger, questo valore rappresenta il segreto condiviso o la password.

DN voce di base
Rappresenta il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la verifica dell'account all'interno del server LDAP/AD.

Filtro di ricerca
Rappresenta il filtro di ricerca LDAP/AD utilizzato per la verifica degli indirizzi mediante le ricerche LDAP. MDaemon imposta un filtro di ricerca predefinito, appropriato nella maggior parte dei casi.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche LDAP/AD.

Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca LDAP/AD ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT.

File verifica indirizzi
Fare clic su questo pulsante per aprire l'elenco degli indirizzi e-mail validi del gateway, denominato `GatewayUsers.dat`. Il file include l'elenco degli indirizzi considerati destinatari validi per i messaggi in arrivo indirizzati ai gateway di dominio. MDaemon utilizza questo elenco come ulteriore fonte di indirizzi validi, indipendentemente dall'opzione di verifica impostata. Se si utilizza l'opzione *File*, tuttavia, il file rappresenta il solo e unico metodo di verifica utilizzato.

Uso di più configurazioni per le interrogazioni relative alla verifica LDAP

È possibile specificare più configurazioni LDAP per i domini del gateway. Per specificare insiemi aggiuntivi di parametri LDAP, impostare il primo normalmente, quindi modificare il file `GATEWAYS.DAT` manualmente utilizzando Blocco note.

Il nuovo insieme di parametri deve essere creato in base al formato seguente:

```
LDAPHost1=<nome host>
LDAPPort1=<porta>
LDAPBaseEntry1=<DN della voce di base>
LDAPRootDN1=<DN principale>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

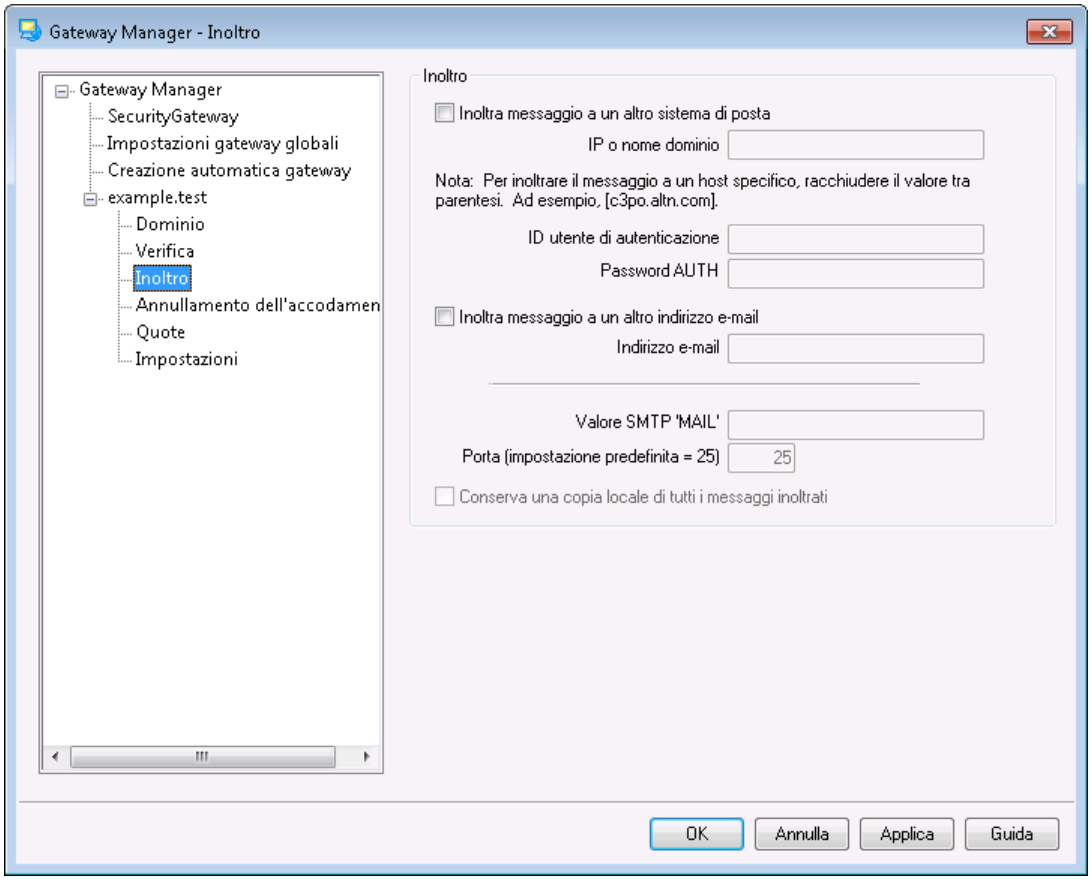
Per ogni nuovo set di parametri, aumentare il numero nel nome di ciascun parametro 1. Ad esempio, nei casi riportati sopra, ogni nome di parametro termina con "1". Per creare un secondo insieme aggiuntivo, terminare ogni nome con "2". Per creare un terzo insieme, terminare ogni nome con "3" e così via.

Quando vengono eseguite le interrogazioni LDAP, MDaemon effettuerà più controlli in sequenza per individuare una corrispondenza. Se viene rilevata una corrispondenza oppure si verifica un errore, non verranno eseguiti ulteriori controlli.

Vedere:

Opzioni di LDAP e della rubrica 844
Minger 878

3.3.3.3 Inoltro



Inoltro

Inoltra messaggio a un altro sistema di posta
In alcuni casi può essere conveniente inoltrare una copia di tutti i messaggi relativi a un dominio non appena questi arrivano. Se si desidera configurare MDaemon in questo modo, immettere il nome o l'indirizzo IP del dominio a cui devono essere inviate le copie della posta in arrivo. Se si desidera inoltrare i messaggi verso un host specifico, racchiuderne il nome tra parentesi quadre, ad esempio `[host1.esempio.com]`. Utilizzare l'opzione Accesso/Password AUTH per immettere le eventuali credenziali di accesso necessarie per il server a cui si desidera inoltrare i messaggi.

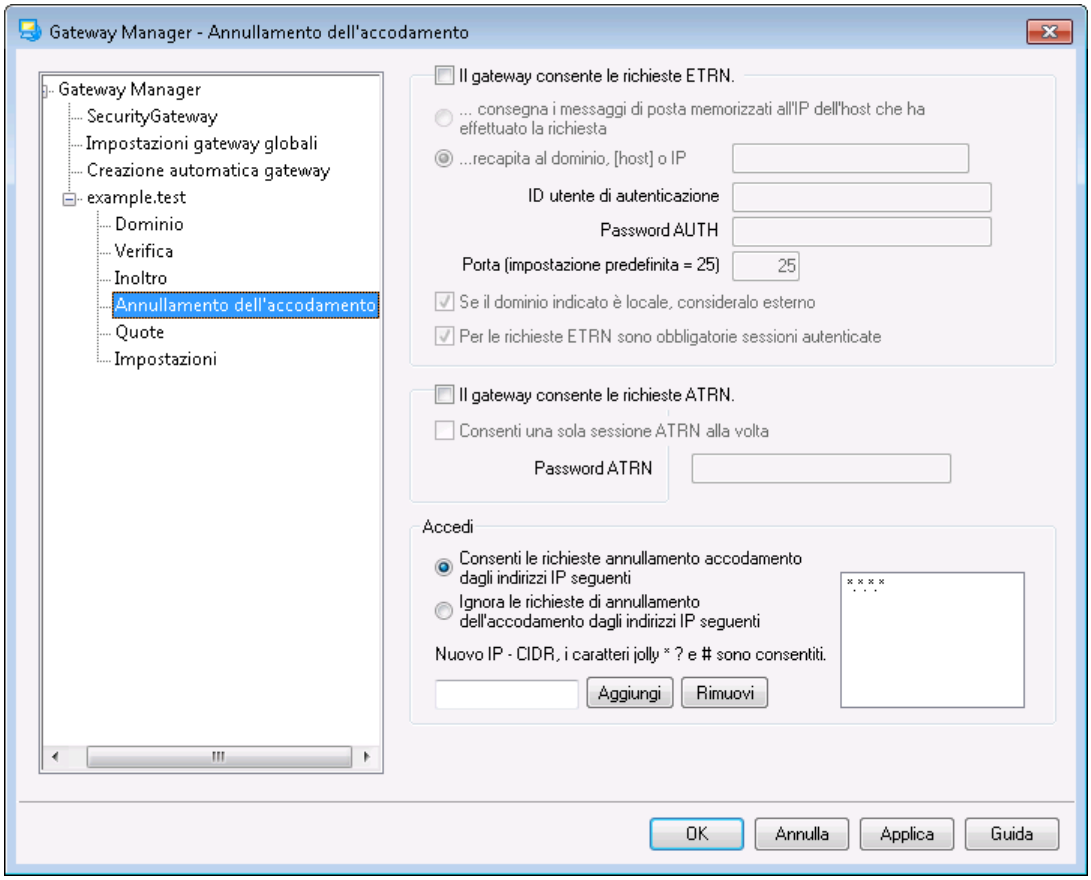
Inoltra messaggio a un altro indirizzo e-mail
Utilizzare questa funzione per inoltrare a un indirizzo e-mail specifico tutti i messaggi e-mail destinati al dominio client.

Valore SMTP 'MAIL'
MDaemon utilizzerà questo indirizzo nella transazione SMTP "Posta da" durante l'inoltro dei messaggi.

Porta (valore predefinito = 25)
MDaemon utilizzerà questa porta durante l'inoltro dei messaggi.

Conserva una copia locale di tutti i messaggi inoltrati
Selezionare questa opzione se si desidera che MDaemon conservi una copia di archiviazione di ciascun messaggio in locale, una volta inoltrato il messaggio.

3.3.3.4 Annullamento dell'accodamento



ETRN

Il gateway consente le richieste ETRN
Quando questa casella di controllo è abilitata, MDaemon risponde alle richieste ETRN effettuate da host qualificati per conto del dominio per cui MDaemon funge da gateway e-mail. Il comando ETRN è un'estensione SMTP che segnala al server nel quale è memorizzata la posta di un particolare dominio di iniziare lo spool. Quando MDaemon riceve una richiesta ETRN per un dominio, inizia immediatamente lo spool della posta memorizzata per la consegna mediante transazioni SMTP successive. La sessione SMTP che emette una richiesta ETRN non coincide con quella che riceve la

posta memorizzata. Per inviare l'eventuale posta memorizzata per il dominio, MDaemon utilizza successive transazioni SMTP indipendenti. In questo modo, viene preservata la busta del messaggio e migliorato il livello di protezione. È opportuno tenere presente che l'host a cui MDaemon invia lo spool dell'eventuale posta memorizzata potrebbe non iniziare immediatamente la ricezione dei messaggi. ETRN infatti garantisce solo che verrà effettuato lo *spool* di consegna per la posta memorizzata, ma il *processo* di consegna vero e proprio è soggetto ad altre limitazioni imposte dall'amministratore e potrebbe essere messo in attesa nella coda della posta in uscita fino all'esecuzione del successivo evento pianificato di elaborazione della posta remota. A causa di queste limitazioni, si consiglia di utilizzare il metodo ODMR (On-Demand Mail Relay) 205 e il relativo comando ATRN anziché ETRN. Si tenga tuttavia presente che questo metodo non è supportato da tutti i client e server e risulta pertanto disponibile solo per i domini client che utilizzano un server compatibile. MDaemon supporta totalmente il metodo ODMR, sia sul lato client che sul lato server.

Per impostazione predefinita MDaemon richiede che l'host di connessione che emette la richiesta ETRN si autentichi prima mediante ESMTP AUTH utilizzando il *Nome dominio* 262 e la *Password ATRN* del Gateway come credenziali di accesso. Se non si desidera richiedere l'autenticazione, è possibile disattivare questa opzione in Impostazioni 274 deselezionando l'opzione *L'annullamento dell'accodamento dei messaggi ETRN richiede l'autenticazione*.

... consegna i messaggi di posta memorizzati all'IP dell'host che ha effettuato la richiesta
Quando questa opzione è selezionata, MDaemon invia l'eventuale posta archiviata all'indirizzo IP del computer da cui proviene la richiesta ETRN. Affinché i messaggi possano essere ricevuti, sul sistema richiedente deve essere in esecuzione un server SMTP.

...recapita al dominio, [host] o IP
Indica il nome dell'host, il nome di dominio o l'indirizzo IP a cui viene inviata l'eventuale posta memorizzata quando una richiesta ETRN viene ricevuta e soddisfatta. Affinché i messaggi possano essere ricevuti, nel sistema ricevente deve essere in esecuzione un server SMTP. Nota: se in questo campo viene specificato il nome di un dominio, è possibile utilizzare i record A e MX a seconda dei risultati DNS ottenuti durante la consegna. Se si desidera consegnare i messaggi a un host specifico racchiuderne il nome tra parentesi quadre (ad esempio, `[host1.esempio.net]`) oppure specificare un indirizzo IP anziché un nome di dominio. Immettere le credenziali *AUTH Logo/Password* necessarie per il recapito in quella posizione.

Porta (valore predefinito = 25)
Utilizzare questa opzione per specificare la porta per lo spooling della posta del dominio.

Se il dominio indicato è locale, consideralo esterno
Attivare questo comando se il dominio è locale ma si desidera che lo spool della posta venga effettuato come se il dominio fosse remoto.

Per le richieste ETRN sono obbligatorie sessioni autenticate
Quando si accettano le richieste ESMTP ETRN, questa opzione verrà utilizzata per impostazione predefinita per richiedere all'host di connessione di autenticarsi prima con il comando ESMTP AUTH. Quando si attiva questa opzione, è necessario designare una password di autenticazione nella casella "Password ATRN".

Deselezionare questa casella di controllo se non si desidera richiedere l'autenticazione di host tramite richieste ETRN.

ATRN

Il gateway risponde alle richieste ATRN.
Abilitare questa opzione se si desidera che MDaemon risponda a comandi `ATRN` provenienti dal dominio del gateway. `ATRN` è un comando ESMTP utilizzato nel metodo ODMR (On-Demand Mail Relay) 205 e rappresenta il miglior metodo di inoltro finora disponibile per l'hosting della posta. ATRN rappresenta una soluzione da preferire a ETRN e ad altri metodi perché richiede l'autenticazione prima che venga annullato l'accodamento della posta, ma non un indirizzo IP statico. Quest'ultimo risulta superfluo perché il flusso di dati tra MDaemon e il dominio client viene invertito immediatamente e, diversamente da `ETRN` che utilizza una connessione separata una volta inviato il comando `ETRN`, lo spool dei messaggi viene annullato senza che debba essere stabilita una nuova connessione. In questo modo, i domini client che utilizzano un indirizzo IP dinamico (non statico) possono raccogliere i messaggi senza utilizzare POP3 o DomainPOP, in quanto la busta SMTP originale viene preservata.

ATRN richiede una sessione autenticata mediante AUTH. È possibile configurare le credenziali di autenticazione nella schermata Impostazioni 274.

Consenti solo una sessione ATRN per volta
Fare clic su questa casella di controllo se si desidera limitare ATRN ad una sessione per volta.

Password ATRN
Quando si utilizza ATRN per la rimozione dalla coda della posta del gateway o quando si richiede l'autenticazione mediante l'opzione *Il decodamento ETRN richiede l'autenticazione* della schermata Impostazioni, specificare qui la password ATRN.

Il dominio per conto del quale MDaemon agisce da gateway e-mail deve utilizzare il proprio nome di dominio come parametro per l'accesso. Ad esempio, se il gateway di dominio è "esempio.com" e si sta utilizzando ATRN per annullare l'accodamento della relativa posta, l'autenticazione verrà effettuata tramite le credenziali di accesso "esempio.com" e la password specificata in questo campo.

Accesso

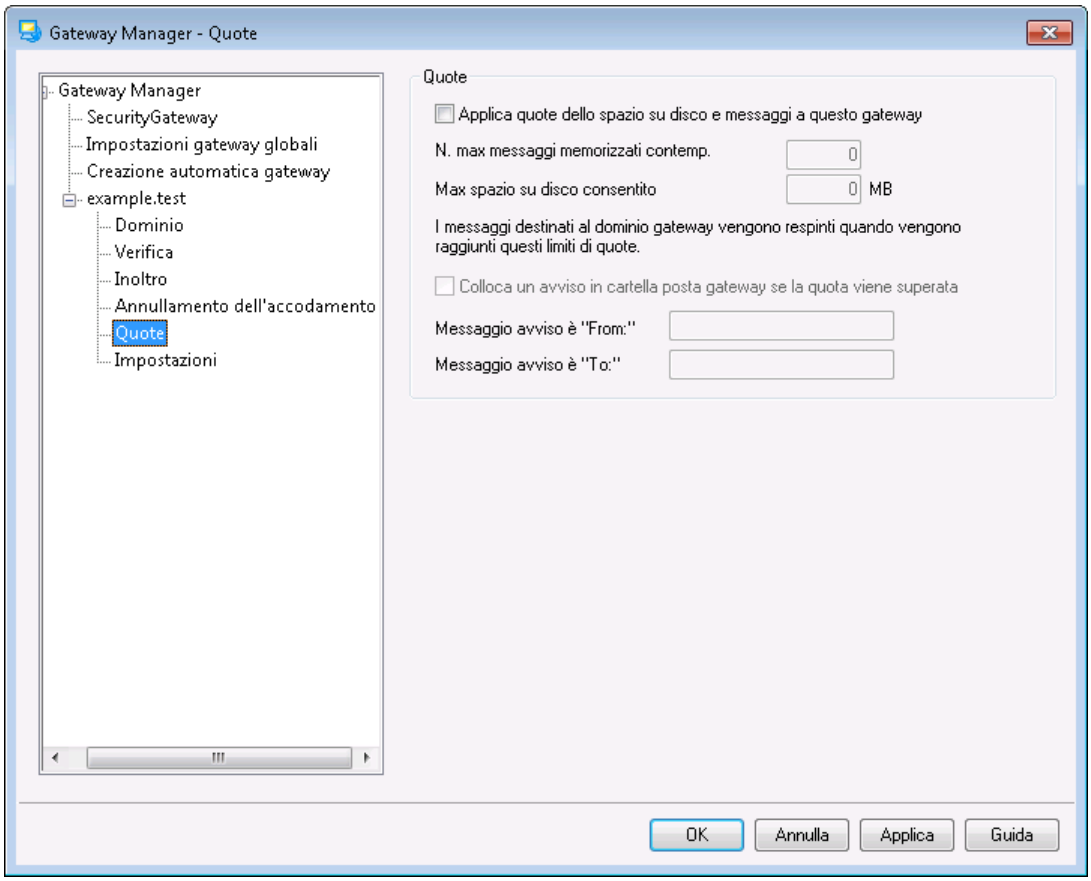
Consenti le richieste di annullamento dell'accodamento dagli indirizzi IP seguenti
Quando questa opzione è selezionata, MDaemon soddisfa ogni richiesta ETRN/ATRN effettuata da un IP presente nell'elenco indirizzi associato.

Ignora le richieste di annullamento dell'accodamento dagli indirizzi IP seguenti
Quando questa opzione è selezionata, MDaemon ignora tutte le richieste ETRN/ATRN effettuate da un IP presente nell'elenco indirizzi associato.

Aggiungi
Per aggiungere un nuovo indirizzo IP all'elenco corrente, è sufficiente inserirlo nella casella di testo e fare clic sul pulsante *Aggiungi*.

Rimuovi
Fare clic su questo pulsante per rimuovere una voce selezionata dall'elenco degli indirizzi IP.

3.3.3.5 Quote



Quote

Applica quote dello spazio su disco e messaggi a questo gateway
Abilitare questa opzione se si desidera specificare il numero massimo di messaggi consentiti per il dominio e la quantità massima di spazio su disco (in kilobyte) utilizzabile, inclusi gli allegati di file codificati che si trovano nella directory Files. Quando la quota viene raggiunta, tutti i messaggi indirizzati al dominio vengono respinti.

Numero massimo di messaggi memorizzati contemporaneamente
Questa casella consente di specificare il numero massimo di messaggi memorizzati per il dominio gateway. Specificare "0" in questa opzione se non si desidera inserire alcuna limitazione di dimensione.

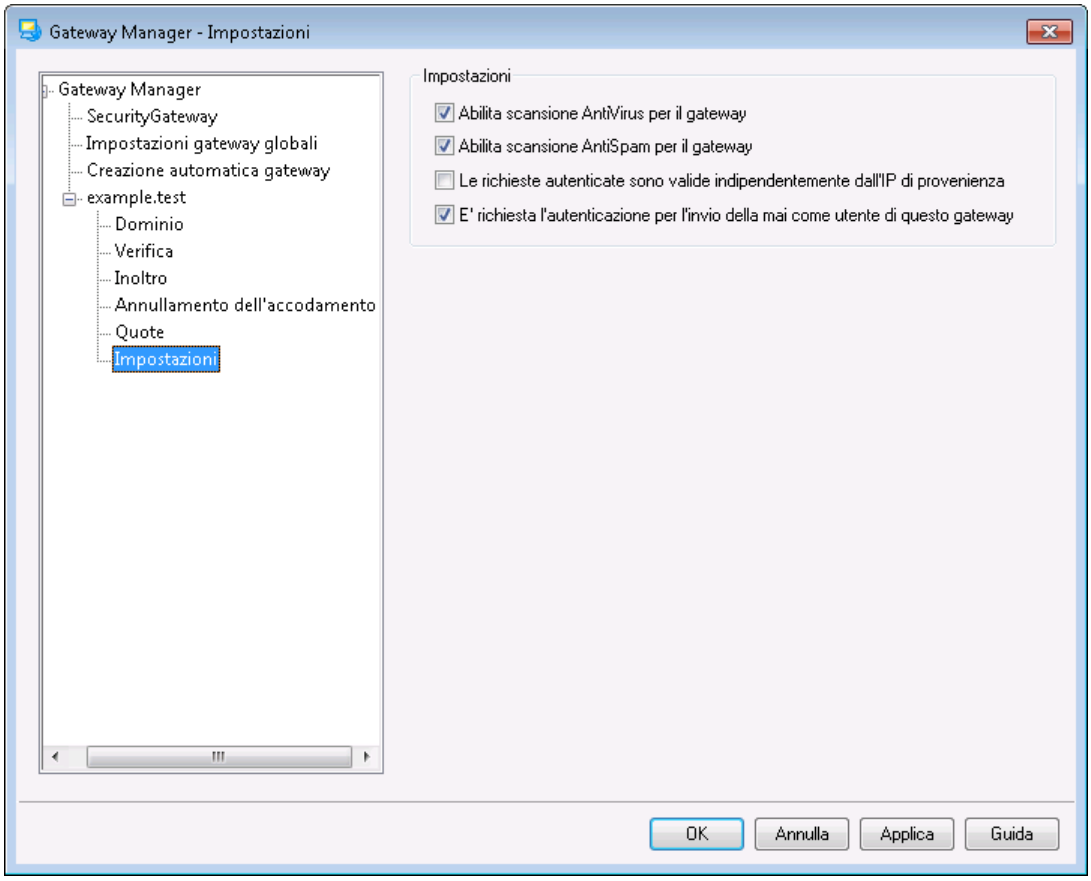
Massimo spazio su disco consentito
Consente di specificare il limite massimo consentito per lo spazio su disco. Se la dimensione dei messaggi memorizzati raggiunge questo limite, tutti i messaggi indirizzati al dominio vengono respinti. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Colloca un avviso in cartella posta gateway se la quota viene superata
Se questa opzione è abilitata e si tenta di consegnare all'account una quantità di posta superiore ai limiti stabiliti per i messaggi e lo spazio su disco, nella directory di posta del gateway di dominio viene collocato un avviso appropriato. Nei campi seguenti è possibile specificare le intestazioni "`From:`" e "`To:`" del messaggio di avviso.

Messaggio avviso è "From:"
Questa opzione consente di specificare l'indirizzo "From:" utilizzato nei messaggi di avviso relativi al superamento della quota.

Messaggio avviso è "To:"
Questa opzione consente di specificare l'indirizzo "To:" utilizzato nei messaggi di avviso relativi al superamento della quota.

3.3.3.6 Impostazioni



Impostazioni

Abilita scansione AntiVirus per il gateway
Selezionare questa opzione se si utilizzano le funzionalità opzionali di MDaemon AntiVirus 658 e si desidera eseguire la scansione dei messaggi del gateway del dominio. Se l'opzione è deselezionata, l'AntiVirus non esegue la scansione dei messaggi di questo gateway.

Abilita scansione AntiSpam per il gateway
Scegliere questa opzione per applicare le impostazioni di Spam Filter ai messaggi del gateway di dominio. In caso contrario, Spam Filter non eseguirà la scansione dei messaggi.

Le richieste autenticate sono valide indipendentemente dall'IP di provenienza
Selezionare questa casella di controllo se si desidera soddisfare le richieste autenticate a prescindere dall'indirizzo IP da cui provengono. Se questa opzione non è abilitata, potranno essere soddisfatte solo le richieste provenienti dagli indirizzi IP specificati nella sezione Accesso.

È richiesta l'autenticazione per l'invio della mail come utente di questo gateway
Selezionare questa casella di controllo se si desidera che per tutti i messaggi che affermano di appartenere al dominio venga richiesta l'autenticazione. Perché un

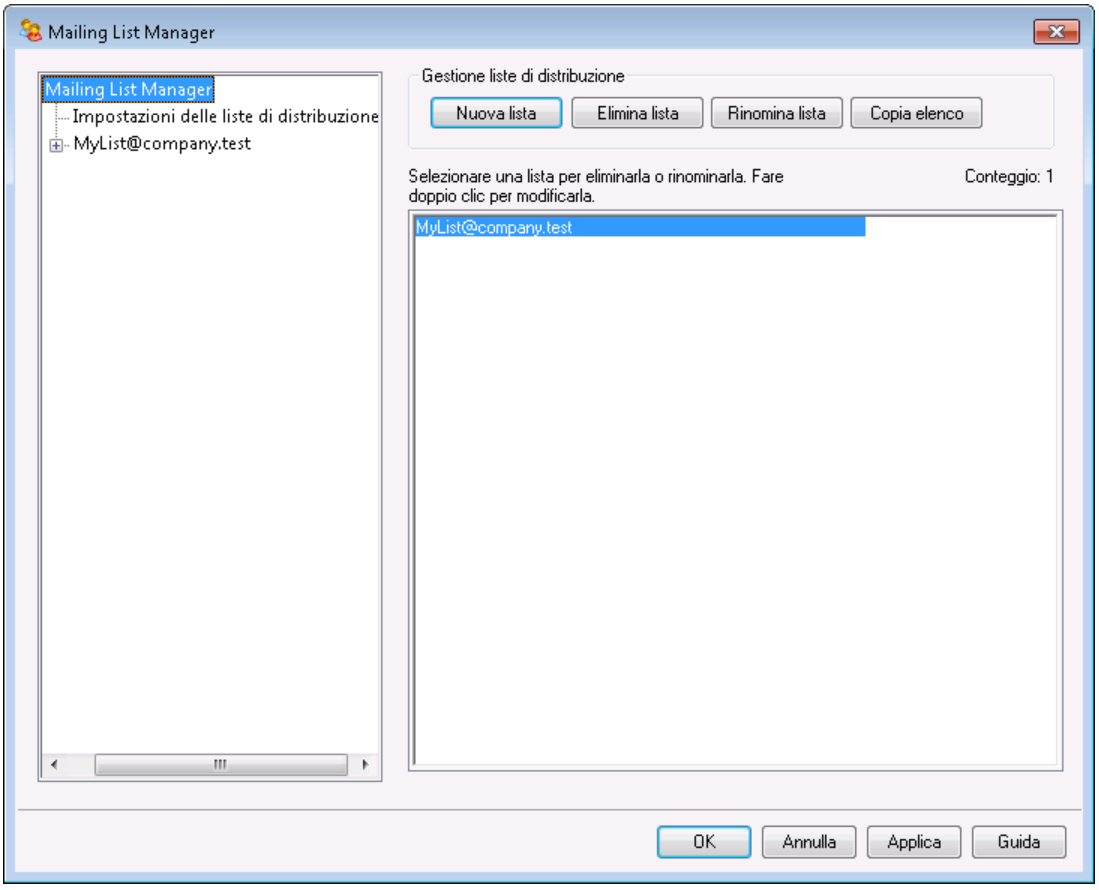
messaggio venga considerato proveniente da questo dominio deve utilizzare una connessione autenticata (o collegarsi da un indirizzo IP accreditato), in caso contrario viene rifiutato. L'opzione è abilitata per impostazione predefinita.

Alla creazione di nuovi gateway di dominio, questa opzione viene attivata per impostazione predefinita. Se si desidera modificare le impostazioni predefinite in modo da disabilitare questa opzione per i nuovi gateway, modificare la seguente chiave nel file `MDaemon.ini`:

```
[Special]
GatewaySendersMustAuth=No (il valore predefinito è Yes)
```

3.4 Mailing List Manager

Le liste di distribuzione (definite anche "mailing list") consentono di inviare messaggi a gruppi di utenti, come se questi condividessero la stessa casella postale. Le copie dei messaggi e-mail inviati alla lista vengono distribuite a ciascun membro. Le liste possono contenere membri con indirizzi di destinazione locale e/o remota, possono essere pubbliche o private, moderate o aperte, possono venire inviate in formato riassunto 297 o normale e così via.

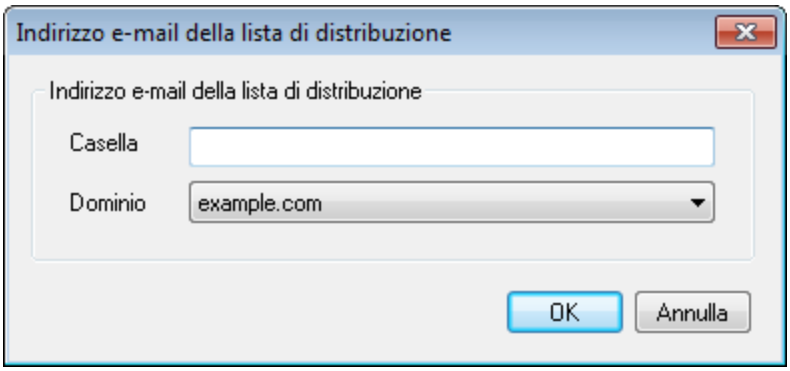


Disponibile nel menu Impostazioni » Mailing List Manager..., la funzione di Mailing List Manager consente di amministrare le liste.

Gestione delle liste di distribuzione

Nel riquadro di navigazione sul lato sinistro di questa finestra di dialogo è disponibile una voce per ciascuna lista di distribuzione, con collegamenti a ogni schermata utilizzata per configurare le diverse impostazioni specifiche della lista. Da qui è inoltre possibile accedere alla schermata Impostazioni lista di distribuzione 278, che consente di configurare diverse opzioni globali correlate alle liste. Le opzioni sul lato destro della finestra di dialogo consentono di creare, eliminare e rinominare le liste. È possibile fare doppio clic su una lista di distribuzione per passare all'editor delle liste e configurare le impostazioni.

Nuova lista
Per creare una nuova lista di distribuzione, fare clic su **Nuova lista** per aprire la finestra di dialogo Indirizzo e-mail della lista di distribuzione. Creare un nome di cassetta postale e selezionare un dominio, ad esempio "ListaMia" ed "esempio.com". L'indirizzo di e-mail della lista di distribuzione sarà ListaMia@esempio.com. I messaggi inviati a questo indirizzo saranno distribuiti ai membri della lista in base alle impostazioni specifiche della stessa. Fare clic su **OK** per creare la lista. Dopo aver creato la lista, è possibile fare doppio clic sulla voce corrispondente per configurarne le impostazioni e aggiungere membri. **Nota:** I nomi di lista non possono contenere i simboli "! " o " | "



Elimina lista
Per eliminare una list di distribuzione: selezionare la lista, fare clic su **Elimina lista** e quindi su **Sì** per confermare la decisione.

Rinomina lista
Per rinominare una lista di distribuzione, selezionare la lista e fare clic su **Rinomina lista** per aprire la finestra di dialogo Indirizzo e-mail della lista di distribuzione. Apportare le modifiche desiderate e fare clic su **OK**.

Copia lista
Per creare una nuova lista di distribuzione con impostazioni che corrispondono a un'altra lista, selezionare la lista dall'elenco, fare clic su questo pulsante e specificare un nome per la casella postale e il dominio per la nuova lista.

Modifica di una lista di distribuzione esistente

Per configurare una lista di distribuzione, fare doppio clic sulla voce corrispondente in Mailing List Manager. Quindi, nel riquadro di navigazione a sinistra, fare clic sulla schermata che si desidera modificare:

Membri 281
Impostazioni 284
Intestazioni 288
Iscrizione 291
Promemoria 295
Moderazione 300
Impostazioni riassunto 297
Instradamento 302
Notifiche 298
File supporto 304
Cartella pubblica 306
Active Directory 307
ODBC 310

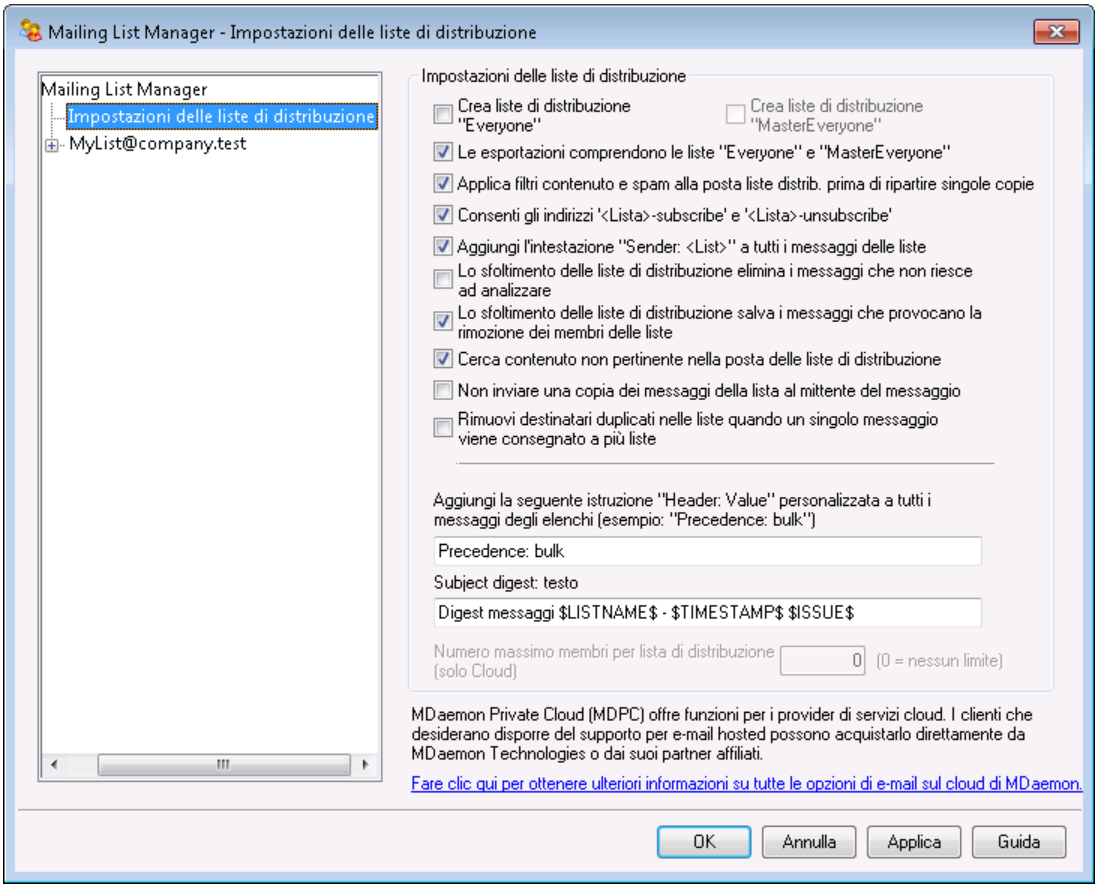
Impostazioni lista di distribuzione

Fare clic su **Impostazioni lista di distribuzione** nel riquadro a sinistra e aprire la schermata Impostazioni lista di distribuzione 278, per configurare delle impostazioni globali correlate alle liste di distribuzione.

Vedere:

Impostazioni lista di distribuzione 278

3.4.1 Impostazioni lista di distribuzione



Impostazioni lista di distribuzione

Crea liste "Everyone"
Abilitare questa casella di controllo per creare e gestire liste di distribuzione "Everyone" per tutti i domini, ad esempio "everyone@esempio.com". Viene creata una lista per ogni dominio, il che consente di inviare un messaggio a tutti gli utenti di un dominio indirizzandolo semplicemente a "everyone@<dominio>". Gli account privati 776 restano nascosti per le liste di distribuzione "Everyone". L'opzione è disabilitata per impostazione predefinita.

Crea lista "MasterEveryone"
Questa opzione consente di ottenere una lista di distribuzione "MasterEveryone". In questo modo, in questa lista saranno inclusi tutti coloro che sono presenti in tutte le liste "Everyone" del dominio specifico. L'opzione è disabilitata per impostazione predefinita.

Le esportazioni comprendono le liste "Everyone" e "MasterEveryone"
Per impostazione predefinita le liste di distribuzione "Everyone" e "MasterEveryone" vengono incluse quando si utilizzano le opzioni "Account » Esportazione..." per esportare le liste. Disattivare questa opzione se non si desidera includerle nelle esportazioni delle liste di distribuzione.

Applica filtri contenuto e spam alla posta liste distrib. prima di ripartire singole copie
Quando si sceglie l'opzione *Consegna singolarmente posta lista a ciascun membro* nella schermata Instradamento 302 dell'editor delle liste di distribuzione, l'abilitazione di questo controllo determina l'applicazione delle regole di Filtro contenuti e di Spam Filter ai messaggi della lista prima che vengano ripartiti e distribuiti ai singoli membri.

Consenti gli indirizzi '<Lista>-subscribe' e '<Lista>-unsubscribe'
Selezionare questa casella di controllo se si desidera che MDaemon riconosca come validi (purché la lista esista) gli indirizzi e-mail con questo formato, al fine di fornire agli utenti un metodo più semplice per iscriversi o ritirarsi dalle liste di distribuzione. Ad esempio: si supponga di avere una lista denominata `NomeLista@esempio.com`. Gli utenti possono iscriversi/ritirarsi dalla lista inviando un messaggio e-mail agli indirizzi `NomeLista-Sottoscrivi@esempio.com` e `NomeLista-Annullasottoscrizione@esempio.com`. Il contenuto dell'oggetto e del corpo del messaggio è irrilevante. Inoltre, quando questa funzione è attiva, MDaemon inserisce in tutti i messaggi della lista l'intestazione seguente:

```
Annulla sottoscrizione lista: <mailto:<Lista>-
Unsubscribe@esempio.com>
```

Alcuni client e-mail sono in grado di convertire automaticamente questa intestazione in un pulsante ANNULLA ISCRIZIONE disponibile agli utenti.

È possibile ignorare questa opzione per le singole liste specificando un valore per le intestazioni List-Subscribe e List-Unsubscribe nelle opzioni **URL lista di distribuzione** presenti nella schermata Moderazione 300 dell'editor delle liste di distribuzione.

Aggiungi intestazione 'Sender: <List>' a tutti i messaggi della lista
Attivare questa opzione se si desidera inserire l'intestazione `Sender` ai messaggi delle liste di distribuzione.

Il programma di sfoltimento della lista di distribuzione elimina i messaggi che non è in grado di analizzare
Quando si attiva questa opzione, MDaemon elimina i messaggi della lista che non contengono indirizzi analizzabili.

Il programma di sfoltimento della lista di distribuzione salva i messaggi che provocano la rimozione di membri della lista
Quando MDaemon è configurato per analizzare i messaggi restituiti alle liste di distribuzione allo scopo di eliminare gli iscritti non raggiungibili, la selezione di questa opzione consente di salvare i messaggi provenienti da iscritti rimossi dalla lista. Per ulteriori informazioni, vedere l'opzione *Rimuovi gli indirizzi di posta elettronica non raggiungibili dai membri della lista...* nella schermata Impostazioni 284.

Cerca contenuto non pertinente nella posta delle liste di distribuzione
Selezionare questa casella di controllo se si desidera scartare i messaggi indirizzati alle liste di distribuzione che in realtà dovrebbero essere indirizzati all'account di

sistema. Ad esempio, per iscriversi a una lista o per annullare l'iscrizione, un utente inserisce all'inizio di un messaggio e-mail il comando Subscribe o Unsubscribe e lo invia all'indirizzo di sistema, ad esempio "mdaemon@esempio.com". Spesso questi messaggi e-mail vengono inviati alla lista stessa per errore. Selezionare questa casella di controllo per evitare l'invio di questi messaggi alla lista.

Non inviare copia del messaggio delle liste al mittente
Quando questa opzione è attivata e un membro della lista invia un messaggio alla lista, il mittente non riceverà una copia del messaggio. L'opzione è disabilitata per impostazione predefinita.

Rimuovi destinatari duplicati nelle liste quando un singolo messaggio viene consegnato a più liste
Quando questa opzione è attivata e un singolo messaggio viene indirizzato a più liste di distribuzione, MDaemon consegnerà una sola copia del messaggio a tutti i destinatari membri[281] di più liste. Se, ad esempio, `franco@esempio.net` è membro di `Lista-A@esempio.com` e `Lista-B@esempio.com` e un messaggio in arrivo viene indirizzato a entrambe le liste, Franco riceverà una sola copia del messaggio anziché due. Questa opzione è applicabile solo alle liste; pertanto, nell'esempio precedente, se il messaggio fosse indirizzato a Franco direttamente, più le due liste, Franco riceverebbe due copie del messaggio anziché tre. L'opzione è disabilitata per impostazione predefinita.

L'utilizzo di questa opzione è generalmente sconsigliato. Le liste di distribuzione possono essere utilizzate e organizzate in diversi modi dagli utenti e non è possibile stabilire quale lista riceverà il messaggio quando viene impostato questo tipo di limitazione per i duplicati. Pertanto, l'utilizzo di questa opzione potrebbe causare, a causa delle preferenze di thread dei messaggi, inutili problemi per alcuni utenti che utilizzano i filtri IMAP[751] per ordinare ad esempio i messaggi in cartelle specifiche.

Aggiungi la seguente "Intestazione: valore" personalizzata a tutti i messaggi della lista
È possibile specificare una combinazione statica intestazione/valore, ad esempio "Precedence: bulk", per tutti i messaggi delle liste di distribuzione.

Testo "Subject:" riassunto
Utilizzare questa opzione per personalizzare l'oggetto utilizzato quando MDaemon invia i messaggi di digest per la lista di distribuzione[297]. L'impostazione predefinita è: "`$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$`" Le macro si possono applicare al nome della lista di distribuzione, all'indicatore di data e ora della creazione del messaggio digest e al numero di pubblicazione.

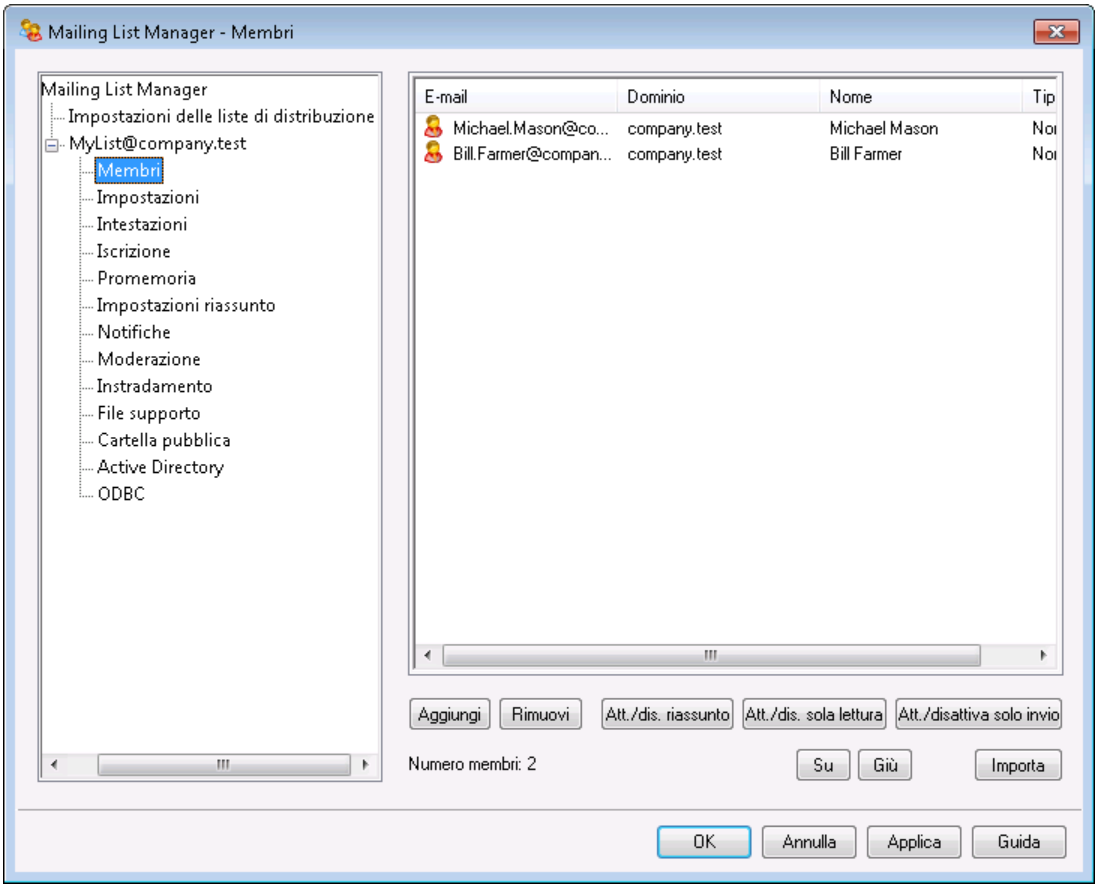
Numero massimo di membri per lista di distribuzione [xx] (0=nessun limite)
Questa opzione consente di impostare il numero massimo di membri consentito per ciascuna lista di distribuzione. È possibile impostare un numero massimo per dominio nella schermata Impostazioni[216] di Domain Manager. L'opzione è disponibile solo in MDaemon Private Cloud.

Vedere:

Mailing List Manager 275

3.4.2 Editor delle liste di distribuzione

3.4.2.1 Membri



In questa schermata vengono visualizzati gli indirizzi e-mail e i nomi di tutti coloro che sono attualmente iscritti alla lista. Per ciascun utente viene indicata la tipologia di iscrizione alla lista: Normale, Riassunto, Solo lettura o Solo invio. Per modificare le impostazioni di un membro, fare doppio clic sulla voce corrispondente.

Aggiungi
Con questo pulsante si apre la schermata Nuovo membro lista per aggiungere dei nuovi membri 283.

Rimuovi
Per rimuovere un iscritto dall'elenco, selezionare la voce desiderata e fare clic su questo pulsante.

Attivazione/disattivazione riassunto
Selezionare un iscritto, quindi fare clic su questo pulsante per designarlo come iscritto di tipo Riassunto[297]. Fare di nuovo clic sul pulsante per riportare l'iscritto alla modalità "normale".

Attivazione/disattivazione sola lettura
Selezionare la voce di un membro e fare clic su questo pulsante per attivare la modalità "Sola lettura". L'utente continuerà a ricevere i messaggi dalla lista, ma non sarà in grado di inviarne. Fare di nuovo clic sul pulsante per riportare l'iscritto alla modalità "normale".

Attiva/disattiva solo invio
Selezionare un iscritto e fare clic su questo pulsante per designarlo come iscritto di tipo "Solo invio". Con questo tipo di appartenenza, è possibile inviare messaggi alla lista, ma non riceverne. Fare di nuovo clic sul pulsante per riportare l'iscritto alla modalità "normale".

Su/Giù
Selezionare uno o più membri e fare clic su questi pulsanti per spostarli in alto o in basso nell'elenco. È inoltre possibile ordinare l'elenco facendo clic sull'intestazione di una colonna. **Nota**: Se si esegue l'ordinamento in base all'intestazione di una colonna, verrà ignorato qualsiasi ordinamento manuale effettuato mediante i pulsanti Su/Giù.

Importa
Per importare gli iscritti alla lista di distribuzione da un file di testo con campi separati (delimitati) da virgole, scegliere questo pulsante. È necessario che esista una voce per ogni riga e che i campi siano delimitati da virgole. Nella prima riga del file, inoltre, deve essere riportato l'elenco dei campi e indicato l'ordine in cui questi vengono visualizzati nelle righe successive. È necessario che uno dei campi sia denominato "**`Email`**" e contenga indirizzi di posta elettronica. Sono disponibili anche due campi opzionali: "**`FullName`**" e "**`Type`**". `FullName` viene utilizzato per il nome del membro della lista. `Type` può avere il valore di: "`Solo lettura`", "`Solo invio`", "`Riassunto`" o "`Normale`". Gli altri campi vengono ignorati dal programma di importazione.

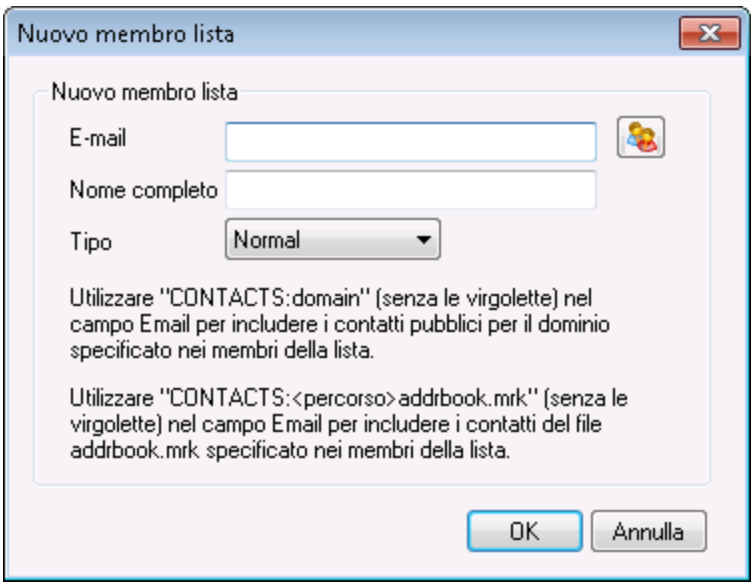
Ad esempio,

```
"Email", "FullName", "Type", "Address", "telephone"
"utente01@altn.com", "Michele Masone", "Riassunto", "Via
Indipendenza 123", "519.555.0100"
```

Gli iscritti importati non ricevono il messaggio di benvenuto alla lista, se previsto, e il programma di importazione non esegue controlli per l'eventuale duplicazione degli iscritti.

Conteggio membri:
Nella parte inferiore della schermata viene visualizzato il numero totale degli iscritti attualmente alla lista.

Aggiunta di nuovi iscritti alla lista



Nuovi membri della lista

Email
Immettere l'indirizzo e-mail da aggiungere alla lista di distribuzione oppure fare clic sull'icona Account per sfogliare gli account e i gruppi di MDaemon da aggiungere alla lista. Gli indirizzi dei membri della lista non possono contenere i simboli "! " o "|".

Per aggiungere tutti gli utenti di uno dei domini o tutti gli utenti che appartengono a un gruppo specifico, è possibile immettere rispettivamente **`ALL_USERS:<dominio>`** oppure **`GROUP:<nome-gruppo>`**, invece di immettere indirizzi e-mail specifici. Ad esempio, l'aggiunta di `ALL_USERS:esempio.com` come membro di una lista equivale ad aggiungere separatamente tutti gli account utente di `esempio.com`.

È anche possibile utilizzare **`CONTACTS:<dominio>`** per includere i contatti pubblici 122 del dominio come membri della lista. Ad esempio, `CONTACTS:esempio.com`.

Nome completo
Inserire in questo campo il nome reale dell'iscritto. Il nome verrà visualizzato nell'intestazione "From:" dei messaggi della lista quando l'opzione "*Sostituisci "Nome visualizzato" nell'intestazione "TO:" con nome membro*" è stata selezionata nella schermata Intestazioni 288.

Tipo
Utilizzare l'elenco a discesa per scegliere il tipo di appartenenza per l'utente:

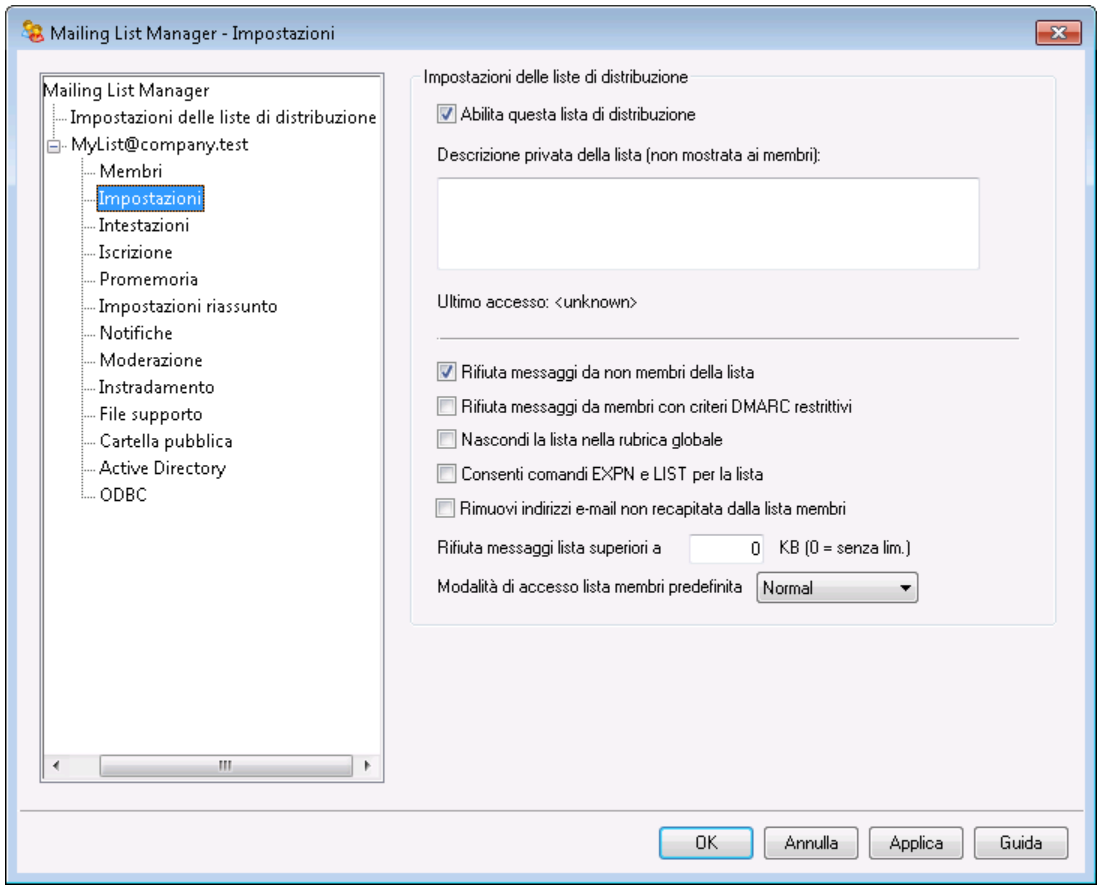
Normale: il membro può inviare e ricevere normalmente i messaggi della lista.

Riassunto: il membro può inviare e ricevere i messaggi della lista, ma i messaggi ricevuti saranno nel formato di un riassunto.

Sola lettura: il membro riceve i messaggi dalla lista ma non può inviare messaggi alla lista.

Solo invio: il membro della lista può inviare messaggi alla lista, ma non riceverne.

3.4.2.2 Impostazioni



Impostazioni lista di distribuzione

Attiva questa lista di distribuzione
Deselezionare questa casella di controllo se si desidera disabilitare temporaneamente la lista di distribuzione. Quando una lista di distribuzione è disattivata, tutti i

messaggi che arrivano via SMTP da o verso tale lista generano un errore temporaneo 451 e vengono rifiutati.

Descrizione privata per questa lista (non visualizzata dai membri)
È possibile immettere qui una descrizione privata della lista. La descrizione è un riferimento personale e non verrà visualizzata dagli altri membri o nelle intestazioni.

Ultimo accesso
Visualizza l'ora dell'ultimo accesso di un utente alla lista. È quindi possibile identificare più facilmente gli elenchi che non vengono più consultati o sono utilizzati di rado.

Rifiuta messaggi da non membri della lista
Quando si abilita questo controllo, la lista viene considerata "privata" e solo gli iscritti possono inviare messaggi. I messaggi provenienti da utenti non iscritti alla lista vengono eliminati.

Rifiuta messaggi da domini con criteri DMARC restrittivi
Attivare questa opzione se si desidera rifiutare un messaggio in arrivo alla lista inviato da un utente proveniente un dominio che applica criteri DMARC 544 restrittivi (ad esempio p=quarantine o p=reject). In generale, non è necessario attivare questa opzione se si utilizza l'opzione "*Sostituire l'indirizzo e-mail "Da:" con l'indirizzo e-mail della lista se il messaggio viene inviato da un dominio che applica criteri DMARC restrittivi*" nella schermata Intestazioni 288.

Se questa opzione e l'opzione "*Sostituire l'indirizzo e-mail "Da:" con l'indirizzo e-mail della lista se il messaggio viene inviato da un dominio che applica criteri DMARC restrittivi* 288" sono disattivate, questo potrebbe causare il rifiuto di alcuni messaggi della lista da parte di alcuni server riceventi e, in alcuni casi, potrebbe determinare la rimozione automatica del destinatario dalla lista dei membri 286. È quindi necessario assicurarsi che almeno una di queste opzioni sia attivata.

Nascondi la lista nella rubrica globale
Selezionare questa opzione per nascondere la lista di distribuzione dalle rubriche pubbliche di Webmail e LDAP.

Attivare i comandi EXPN e LIST per questa lista
Per impostazione predefinita, per garantire la riservatezza dell'appartenenza, MDaemon non accetta i comandi EXPN e LIST per le liste. Se questa opzione è abilitata, l'appartenenza alla lista viene riportata in risposta al comando EXPN o LISTS durante una sessione di posta.

Rimuovi dalla lista indirizzi e-mail non recapitabili
Quando questa funzione è abilitata e si verifica un errore irreversibile permanente durante una consegna, MDaemon rimuove automaticamente il relativo indirizzo dall'elenco degli iscritti. Gli indirizzi vengono rimossi anche quando il relativo

messaggio viene spostato nella coda tentativi[888] e, successivamente, viene considerato scaduto da tale coda.

L'opzione *Rimuovi dalla lista indirizzi e-mail non recapitabili* è un'opzione destinata a essere usata solo in situazioni in cui il server di posta remoto si rifiuta di accettare i messaggi. Questa opzione è operativa solo quando viene selezionata l'opzione "*Consegna singolarmente posta lista a ciascun membro*" nella schermata Instradamento[302]. Se si instradano i messaggi della lista a un host intelligente, per ulteriori informazioni consultare Sfoltimento avanzato della lista[286].

Rifiuta messaggi lista superiori a XX KB
Questo comando pone un limite massimo alla dimensione dei messaggi accettati dalla lista di distribuzione. I messaggi che superano questo limite verranno rifiutati.

Modalità di accesso predefinita del membro della lista
Utilizzare questo elenco a discesa per impostare la modalità di accesso predefinita da utilizzare per i nuovi membri. È possibile modificare la modalità di accesso di ciascun membro nella finestra Membri[281]. Esistono quattro modalità:

Normale: il membro può inviare e ricevere normalmente i messaggi della lista.

Riassunto: il membro può inviare e ricevere i messaggi della lista, ma i messaggi ricevuti saranno nel formato di un riassunto.

Sola lettura: il membro riceve i messaggi dalla lista ma non può inviare messaggi alla lista.

Solo invio: il membro della lista può inviare messaggi alla lista, ma non riceverne.

Sfoltimento avanzato della lista

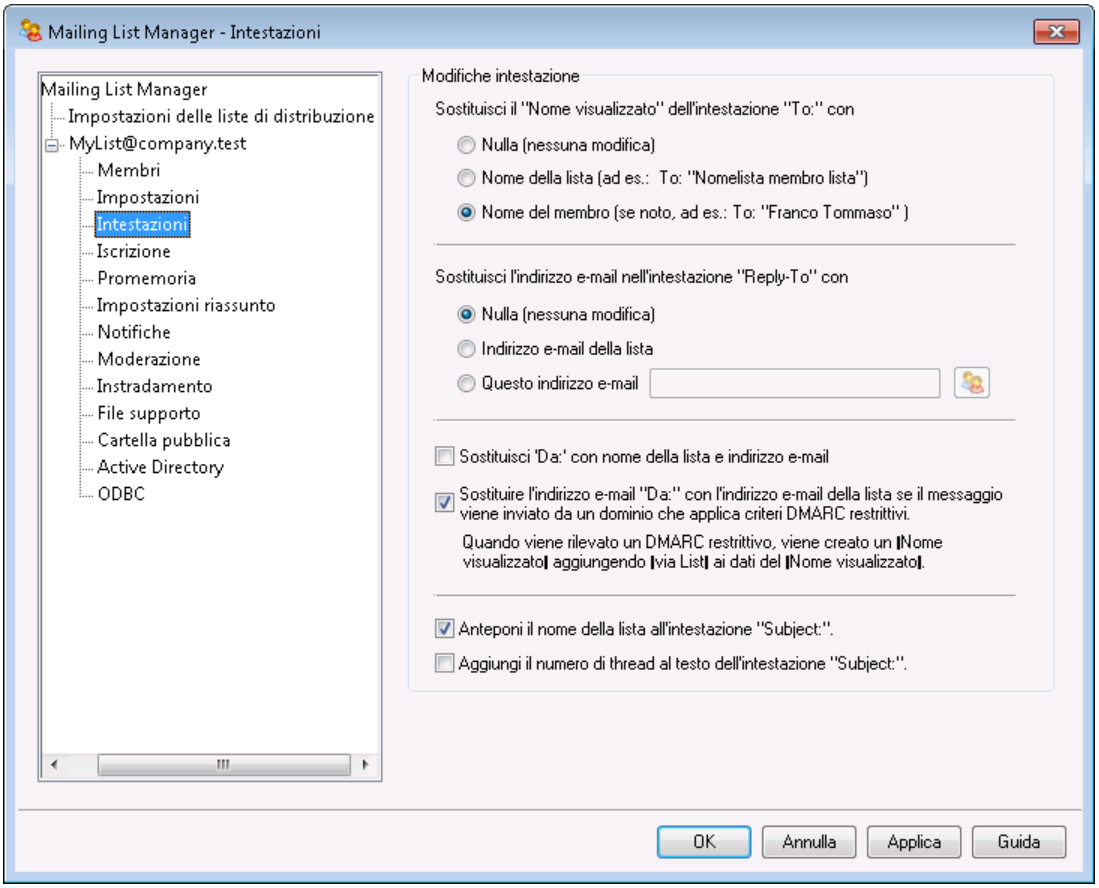
Quando si abilita l'opzione *Rimuovi dalla lista indirizzi e-mail non recapitabili* e si è specificata una casella postale locale come percorso di risposta per i messaggi della lista (vedere l'opzione *Indirizzo di reinvio al mittente SMTP della lista* in Notifiche[298]), ogni giorno a mezzanotte MDaemon tenterà di analizzare i problemi relativi agli indirizzi della posta restituita e rimuoverà i membri che non sono stati raggiunti. In questo modo si sfoltiranno efficacemente gli indirizzi non validi delle liste di distribuzione, in particolare se si instradano i messaggi della lista a un host intelligente anziché consegnarli direttamente.

In Impostazioni lista di distribuzione[278] sono disponibili due opzioni relative a questa funzione. L'opzione *Il programma di sfoltimento della lista di distribuzione elimina i messaggi che non è in grado di analizzare* determina l'eliminazione dei messaggi restituiti che non contengono indirizzi analizzabili, mentre l'opzione *Il programma di sfoltimento della lista di distribuzione salva i messaggi che provocano la rimozione di membri della lista* determina il salvataggio di tutti i messaggi associati a iscritti eliminati dalla lista.

L'impostazione di *Indirizzo di rispedizione SMTP dell'elenco* 298 su un indirizzo dell'utente locale potrebbe causare l'eliminazione dell'e-mail dell'utente come conseguenza delle impostazioni per lo sfoltimento specificate in Impostazioni lista di distribuzione 278.

Quando il recapito a un indirizzo ha come risultato un errore 5xx, l'indirizzo verrà aggiunto al file `BadAddress.txt` presente nella cartella dei registri. Questo può essere d'aiuto, ad esempio, per identificare gli indirizzi non validi nella lista di distribuzione più rapidamente rispetto a cercare nei registri SMTP in uscita. Il file viene rimosso automaticamente ogni notte a mezzanotte per impedire che le dimensioni aumentino troppo.

3.4.2.3 Intestazioni



Modifiche intestazione

Sostituisci il "Nome visualizzato" dell'intestazione "TO:" con
Questa opzione consente di specificare il testo da visualizzare nella parte relativa al nome dell'intestazione TO: quando MDaemon riceve un messaggio indirizzato alla lista.

Nulla (nessuna modifica): selezionando questa opzione, MDaemon non apporta modifiche. Il nome visualizzato e l'indirizzo presenti nell'intestazione TO: vengono visualizzati nella forma in cui sono stati inseriti dal mittente.

Nome della lista: questa opzione consente di sostituire il nome visualizzato con il nome della lista e il "membro della lista". Ad esempio, per una lista di distribuzione denominata "Famiglia" la parte relativa al nome visualizzato dell'intestazione To: includerebbe il testo "Membro lista famiglia".

Nome membro (se noto): con questa opzione, nell'intestazione TO: viene visualizzato il nome, se disponibile, e l'indirizzo del membro della lista al quale è destinato il messaggio.

L'opzione *Nome del membro* può essere selezionata solo se è stata selezionata l'opzione "*Consegna singolarmente posta lista a ciascun membro*" della schermata Instradamento[302]. Quando si seleziona "*Consegna posta lista tramite singoli comandi RCPT per ogni membro*", MDaemon utilizza per impostazione predefinita l'opzione *Nome della lista*.

Sostituisci l'indirizzo e-mail nell'intestazione "Reply-To" con
Questa opzione consente di specificare l'indirizzo e-mail visualizzato nell'intestazione Reply-To: di ciascun messaggio della lista.

Nulla (nessuna modifica)
Selezionare questa opzione se si desidera lasciare invariata l'intestazione Reply-To: rispetto al contenuto presente nel messaggio originale che verrà distribuito alla lista. È consigliabile selezionare questa opzione quando si desidera che le risposte vengano reindirizzate all'utente che ha inviato il messaggio alla lista anziché a tutti i membri della lista.

Indirizzo e-mail della lista
Selezionare questa opzione se si desidera che le risposte vengano indirizzate alla lista anziché a una specifica persona o indirizzo. È consigliabile selezionare questa opzione se si desidera utilizzare la lista come strumento di discussione di gruppo, in cui le risposte vengono inviate a tutti i membri.

Questo indirizzo e-mail
Digitare l'indirizzo e-mail a cui si desidera vengano inviate le risposte oppure selezionare l'icona Account per individuare uno specifico account MDaemon da utilizzare. È possibile utilizzare questa opzione, ad esempio, per una newsletter via e-mail con l'indirizzo di uno specifico contatto a cui inviare le risposte.

Sostituisci “From:” con nome della lista e indirizzo e-mail
Selezionare questa casella di controllo se si desidera sostituire il contenuto dell’intestazione "From:” con il nome e l’indirizzo e-mail della lista di distribuzione.

Sostituire l'indirizzo e-mail "Da:" con l'indirizzo e-mail della lista se il messaggio viene inviato da un dominio che applica criteri DMARC restrittivi
Per impostazione predefinita, quando un messaggio in arrivo alla lista viene inviato da un utente in un dominio che applica criteri DMARC[544] restrittivi (ad esempio p=quarantine o p=reject), MDaemon, prima di inviare il messaggio alla lista, sostituisce l'indirizzo e-mail dell'utente nell'intestazione From: con l'indirizzo della lista. Questa operazione è necessaria per impedire che il messaggio della lista venga rifiutato dai server che accettano i criteri DMARC restrittivi. Oltre a modificare l'indirizzo e-mail dell'intestazione From:, verrà anche modificato il nome visualizzato aggiungendo "Nome lista", per indicare che si tratta di un messaggio inviato dalla lista di distribuzione per conto della persona specificata. Inoltre, ogni volta che l'intestazione "From:" viene modificata da questa funzione, i dati dell'intestazione

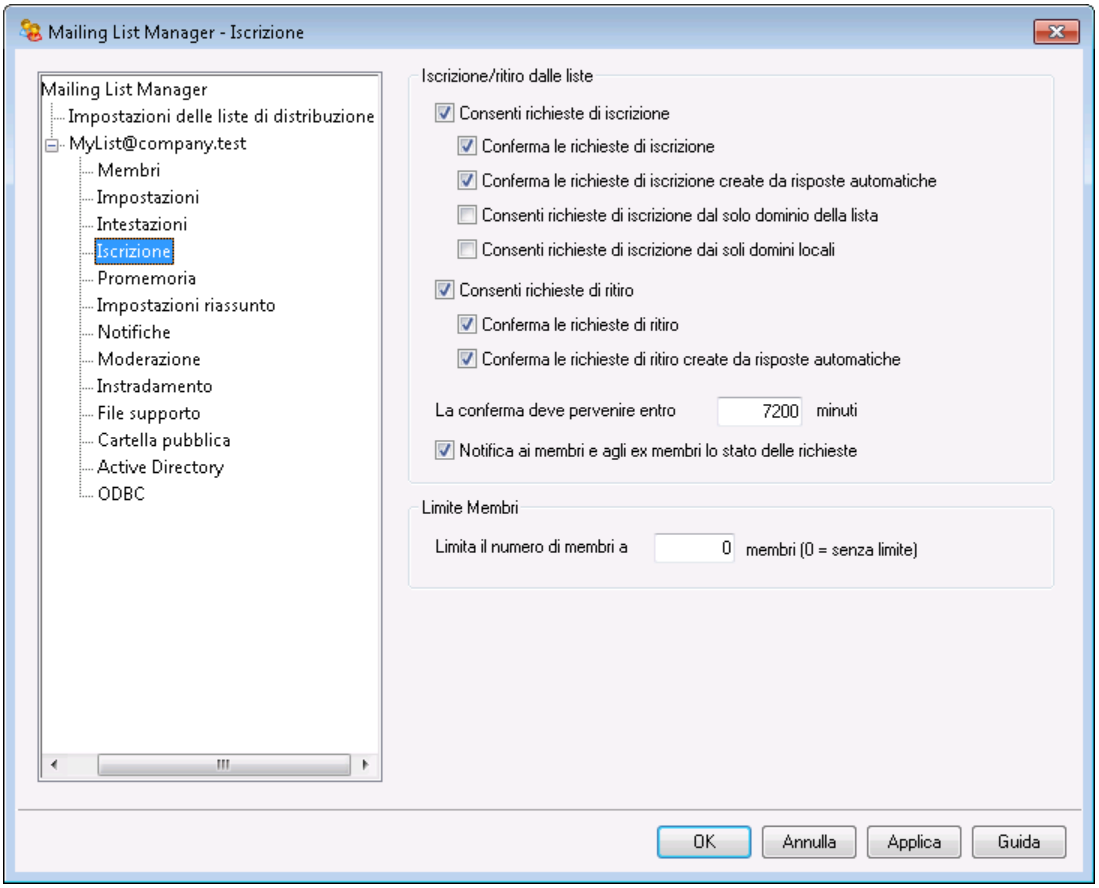
"From" originale vengono spostati nell'intestazione "Reply-To:", ma solo se il messaggio non ha un'intestazione "Reply-To:" e la lista non è configurata per la visualizzazione di un'intestazione "Reply-To:" personalizzata.

È consigliabile disattivare questa opzione solo se necessario e solo se si è pienamente consapevoli delle implicazioni di questa azione. La disattivazione di questa opzione potrebbe causare il rifiuto di alcuni messaggi della lista da parte di alcuni server riceventi e, in alcuni casi, potrebbe determinare la rimozione automatica del destinatario dalla lista dei membri 286. In alternativa, è possibile attivare l'opzione *Rifiuta messaggi da domini con criteri DMARC restrittivi* 284, in modo che i messaggi in arrivo alla lista vengano rifiutati quando provenienti da un domino con criteri DMARC restrittivi.

Anteponi il nome della lista all'intestazione "Subject:"
Mediante questa impostazione, MDaemon racchiude il nome della lista tra parentesi (ad esempio, [Nomelista]) e lo aggiunge all'inizio dell'`oggetto` di tutti i messaggi inviati alla lista. Per impostazione predefinita, questa opzione è abilitata.

Aggiungi il numero di thread al testo dell'intestazione "Subject:"
Questa casella di controllo consente di specificare se visualizzare i numeri di thread nell'intestazione `Subject:` dei messaggi della lista. I numeri vengono apposti tra parentesi alla fine della riga dell'oggetto e utilizzati come numeri di pseudo-thread. Se si ordina la casella della Posta in arrivo in base all'oggetto, i messaggi della lista verranno disposti cronologicamente. L'opzione è disabilitata per impostazione predefinita.

3.4.2.4 Iscrizione



Iscrizione/ritiro dalle liste

Consenti richieste di iscrizione
Questa opzione determina se la lista consente richieste di iscrizione mediante messaggi di posta elettronica appositamente formattati oppure mediante messaggi di risposta automatica. Per ulteriori informazioni, vedere: Iscrizione alle liste di distribuzione 293.

Conferma le richieste di iscrizione
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di iscrizione generando un codice univoco che viene incluso in un messaggio inviato all'indirizzo che ha richiesto di unirsi alla lista. Se la persona risponde al messaggio di conferma, MDaemon aggiunge automaticamente il membro alla lista. I messaggi di conferma hanno validità temporale limitata, ossia è necessario che la risposta dell'utente al messaggio venga ricevuta entro il numero di minuti indicato successivamente. **Nota:** Il contenuto del messaggio di conferma è inserito nel file `SubConf.dat` che si trova nella cartella "`MDaemon\app\`".

Conferma le richieste di ritiro create da risposte automatiche
Quando si seleziona questa casella di controllo, MDaemon tenta di confermare le richieste di iscrizione generate automaticamente tramite l'opzione di risposta

automatica 739 "*Aggiungi mittente a lista distribuzione*". Analogamente a quanto avviene con l'opzione precedente, MDaemon genera un codice univoco e lo include in un messaggio inviato all'indirizzo in attesa di essere aggiunto alla lista. Se la persona risponde al messaggio di conferma, MDaemon aggiunge automaticamente il membro alla lista. Anche questi messaggi di conferma hanno validità temporale limitata, pertanto richiedono una risposta entro il numero di minuti indicato successivamente.

Consenti richieste di iscrizione dal solo dominio della lista
Selezionare questa opzione se si desidera consentire le richieste di iscrizione solo da parte degli utenti che appartengono al dominio della lista. Ad esempio, per la lista "MyList@example.com", solo gli utenti "@example.com" avrebbero l'autorizzazione per iscriversi alla lista.

Consenti richieste di iscrizione dai soli domini locali
Selezionare questa opzione se si desidera consentire le richieste di iscrizione solo da parte degli utenti che appartengono a uno dei domini locali del server di MDaemon.

Ritiro dell'iscrizione

Consenti richieste di ritiro
Questa opzione determina se la lista consente richieste di annullamento iscrizione o ritiro mediante messaggi di posta elettronica appositamente formattati oppure mediante messaggi di risposta automatica. Per ulteriori informazioni, vedere: Iscrizione alle liste di distribuzione 293.

Conferma le richieste di ritiro
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di ritiro di un membro dalla lista, generando un codice univoco che viene incluso in un messaggio inviato all'indirizzo che ha richiesto di annullare l'iscrizione alla lista. Se la persona risponde al messaggio di conferma, MDaemon ritira automaticamente il membro dalla lista. I messaggi di conferma hanno validità temporale limitata, ossia è necessario che la risposta dell'utente al messaggio venga ricevuta entro il numero di minuti indicato successivamente. **Nota:** Il contenuto del messaggio di conferma è inserito nel file `UnSubConf.dat` che si trova nella cartella "`MDaemon\app\`".

Conferma le richieste di ritiro create da risposte automatiche
Quando si seleziona questa casella di controllo, MDaemon tenta di confermare le richieste di ritiro generate automaticamente tramite l'opzione di risposta automatica 739 "*Rimuovi mittente da lista distribuzione*". Analogamente a quanto avviene con l'opzione *Conferma le richieste di ritiro*, MDaemon genera un codice univoco e lo include in un messaggio inviato all'indirizzo in attesa di essere rimosso dalla lista. Se la persona risponde al messaggio di conferma, MDaemon rimuove automaticamente il membro. Anche questi messaggi di conferma hanno validità temporale limitata, pertanto richiedono una risposta entro il numero di minuti indicato successivamente.

La conferma deve pervenire entro XX minuti
Questo valore indica il numero di minuti disponibili prima della scadenza del messaggio di conferma di iscrizione o di ritiro. Se questo limite viene superato prima che MDaemon riceva il messaggio di risposta, l'indirizzo non viene aggiunto o rimosso dalla lista. È necessario, quindi, che l'utente invii nuovamente la richiesta di iscrizione o di ritiro dalla lista. L'impostazione predefinita per questa opzione è di 7200 minuti, ossia cinque giorni.

Si tratta di un valore globale applicato a tutte le liste di distribuzione, non solo alla lista in corso di modifica.

Notifica ai membri e agli ex membri lo stato delle richieste
Quando questa casella di controllo è selezionata, MDaemon invierà un messaggio di notifica completo all'utente che si è iscritto o ritirato dalla lista di distribuzione.0

Il contenuto di un file denominato UnSubUser.dat (se esistente) sarà aggiunto all'e-mail inviata agli utenti quando annullano l'iscrizione alle liste.

Limite membri

Limita il numero di membri a [xx] membri (0 = senza limite))
Questa funzione consente di definire il numero massimo di persone autorizzate a iscriversi alla lista di distribuzione. Se non si desidera specificare alcun limite, immettere il valore zero.

Tale limite viene applicato solo agli indirizzi che si sono iscritti mediante i metodi e-mail descritti in *Iscrizione alle liste di distribuzione* 293. Non viene applicato, invece, agli iscritti inseriti manualmente nella schermata Membri 281, né alle richieste di iscrizione pervenute tramite posta elettronica nel caso esista una Password elenco 300.

Vedere:

Iscrizione alle liste di distribuzione 293
Risposta automatica 739

3.4.2.4.1 Iscrizione alle liste di distribuzione

Iscrizione/ritiro mediante comandi e-mail

Per iscriversi o ritirarsi da una lista di distribuzione, inviare un messaggio e-mail indirizzato a `MDaemon` o a un suo alias appropriato presso il dominio che effettua

l'hosting della lista di distribuzione e inserire il comando `Subscribe` o `Unsubscribe` come prima riga del corpo del messaggio. Ad esempio, esiste una lista di distribuzione denominata `MD-Support` che risiede sull'host `mdaemon.com`. È possibile iscriversi alla lista componendo un messaggio indirizzato a "`mdaemon@mdaemon.com`" e inserendo il valore: `SUBSCRIBE MD-Support@mdaemon.com` nella prima riga del corpo del messaggio. L'oggetto del messaggio è irrilevante e può essere lasciato vuoto.

Per informazioni più esaurienti su questo e altri messaggi di comando, vedere: Controllo remoto del server via e-mail 912.

Talvolta gli utenti tentano di iscriversi o ritirarsi dalle liste via e-mail inviando i comandi alla lista stessa anziché all'account del sistema MDaemon. A seguito di questa azione, il comando viene inviato alla lista anziché all'utente che sta tentando di iscriversi o ritirarsi. Per prevenire la registrazione di tali messaggi nelle liste di distribuzione, esiste un'opzione situata in Impostazioni » Preferenze » Sistema 501, denominata "*Cerca contenuto non pertinente nella posta delle liste di distribuzione*." L'opzione è abilitata per impostazione predefinita.

Iscrizione/ritiro mediante indirizzi e-mail

L'opzione "*Accetta indirizzi "<Lista>-subscribe" e "<Lista>-unsubscribe"*" disponibile in Impostazioni » Mailing List Manager » Impostazioni liste di distribuzione 278, consente agli utenti di iscriversi o di annullare l'iscrizione alle liste di distribuzione inviando un messaggio a un indirizzo e-mail speciale, anziché richiedere l'uso dei comandi e-mail descritti in *Iscrizione/annullamento dell'iscrizione mediante i comandi e-mail*. Per iscriversi o ritirarsi da una lista utilizzando questo metodo, è sufficiente inviare un messaggio all'indirizzo della lista, aggiungendo "`-subscribe`" o "`-unsubscribe`" alla parte dell'indirizzo relativa alla casella postale. Se, ad esempio, il nome della lista è "franco`-lista@esempio.com`", è possibile iscriversi alla lista inviando un messaggio a "`franco-lista-subscribe@esempio.com`". Per ritirarsi, inviare il messaggio a "`franco-lista-unsubscribe@esempio.com`". In entrambi i casi, il contenuto dell'oggetto e del corpo del messaggio è irrilevante. Inoltre, quando questa funzione è attiva, MDaemon inserisce in tutti i messaggi della lista l'intestazione seguente:

```
List-Unsubscribe: <mailto:<Lista>-Unsubscribe@esempio.com>
```

Alcuni client e-mail sono in grado di convertire automaticamente questa intestazione in un pulsante ANNULLA ISCRIZIONE disponibile agli utenti.

Iscrizione/ritiro mediante funzioni di risposta automatica

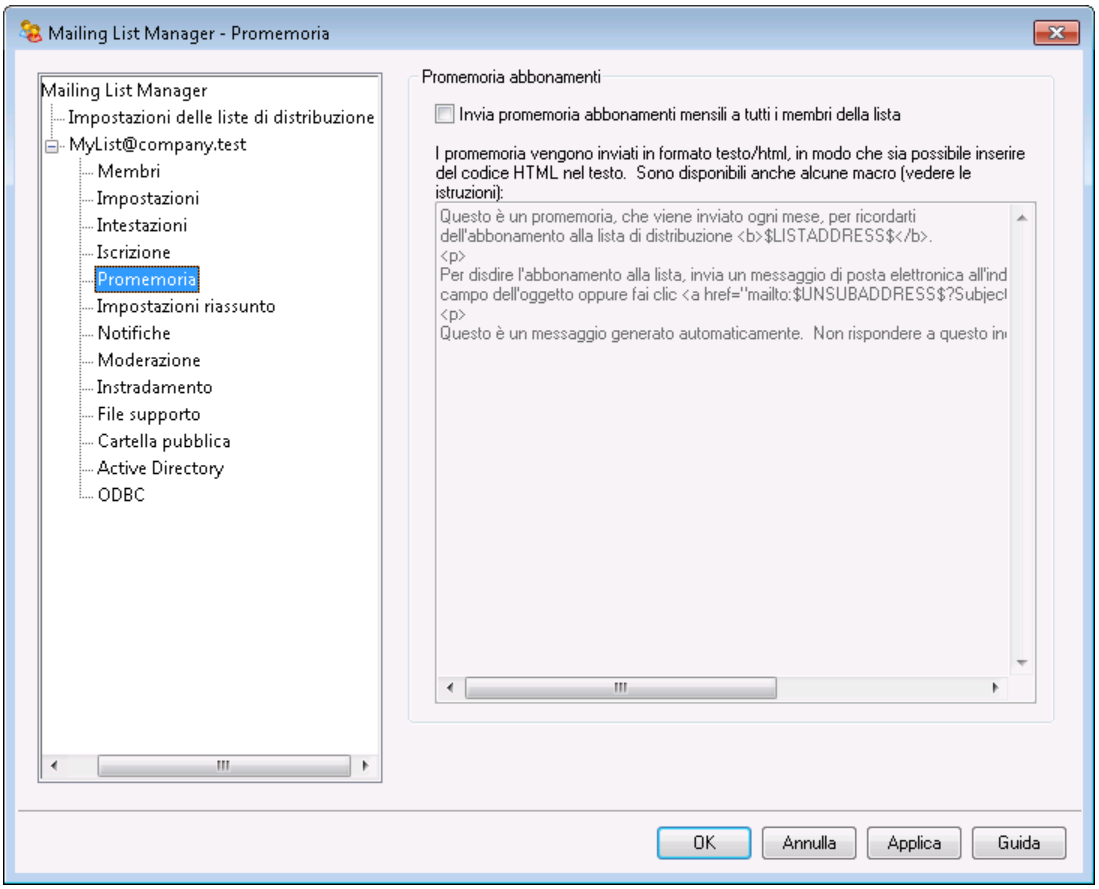
Per l'iscrizione o il ritiro automatico di membri dalla lista, è possibile utilizzare anche le funzioni di risposta automatica 739. A questo scopo, è necessario creare uno o più account di MDaemon il cui unico obiettivo sia quello di aggiungere o rimuovere automaticamente gli indirizzi che hanno inviato un messaggio a tali account, mediante le funzioni di risposta automatica espressamente configurate. Se, ad esempio, esiste una lista di distribuzione denominata "`franco-lista@esempio.com`", è possibile creare un account di MDaemon con il seguente indirizzo: "`join-franco-lista@esempio.com`".

È necessario quindi configurare una risposta automatica per l'account che aggiunga a "franco-lista@esempio.com" eventuali indirizzi dai quali abbia ricevuto un messaggio. Così, per unirsi alla lista, è sufficiente inviare un e-mail a "join-franco-lista@esempio.com". Questa rappresenta una soluzione semplice, in quanto non è necessario che gli utenti ricordino i particolari comandi e-mail necessari con il metodo *Iscrizione/ritiro mediante comandi e-mail*.

Vedere:

Iscrizione 291
Controllo remoto del server via e-mail 912
Risposta automatica 739
Preferenze » Sistema 501
Preferenze » Varie 511

3.4.2.5 Promemoria



Promemoria abbonamenti

Invia promemoria abbonamenti mensili a tutti i membri della lista
Attivare questa opzione per inviare il contenuto della casella di testo fornita come messaggio di promemoria abbonamento a tutti i membri della lista il primo giorno di ogni mese. Il messaggio promemoria viene inviato come testo/html, in modo che sia possibile, se necessario, utilizzare del codice HTML nel testo. Sono disponibili le seguenti macro da utilizzare all'interno del messaggio di promemoria:

$LISTADDRESS$ - Estende all'indirizzo di posta elettronica della lista di distribuzione (ad esempio, mialista@esempio.com).

$LISTNAME$ - Estende alla parte locale dell'indirizzo di posta elettronica della lista di distribuzione (ad esempio, mialista).

$UNSUBADDRESS$ - Estende all'indirizzo di annullamento dell'iscrizione della lista (l'indirizzo del sistema MDaemon, ad esempio mdaemon@esempio.com).

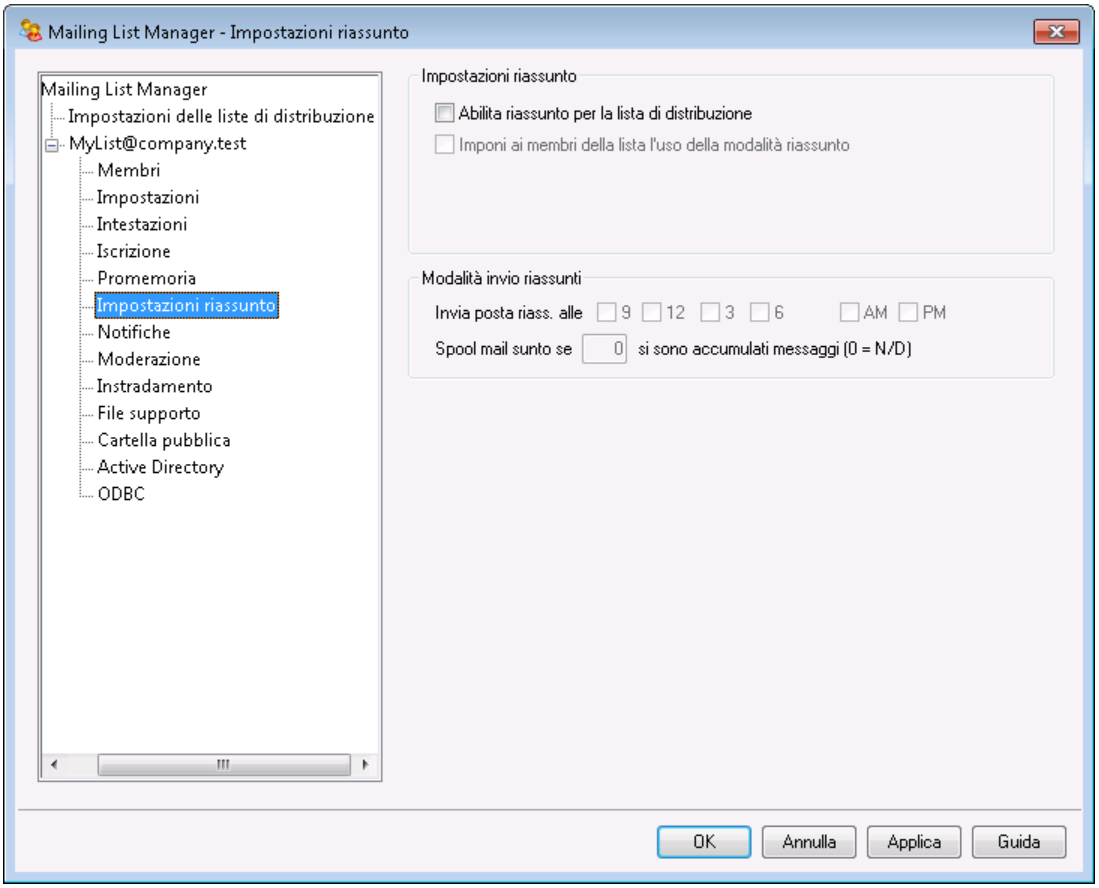
$MEMBERADDRESS$ - Estende all'indirizzo di posta elettronica del membro della lista che riceve il promemoria (ad esempio, franco.tommaso@esempio.com).

Per inviare i promemoria un altro giorno del mese, impostare la seguente chiave nel file MDaemon.ini:

```
[Special]
ListReminderDay=X
```

Impostare "X" a un numero compreso tra 1 e 28, a rappresentare il giorno del mese in cui si desidera inviare i promemoria.

3.4.2.6 Impostazioni riassunto



Riassunti

Abilita riassunto per la lista distribuzione
Per consentire il supporto dell'attivazione/disattivazione riassunti per la lista di distribuzione, abilitare questa casella. Quando viene attivato il supporto riassunti, una copia di ogni messaggio inviato alla lista di distribuzione viene archiviata in modo che agli iscritti il cui tipo di appartenenza 281 sia impostato su *Riassunto* vengano periodicamente inviati gruppi di messaggi archiviati in formato indicizzato compatto e non i singoli messaggi.

Imponi a tutti i membri della lista di usare la modalità riassunto
Per impostazione predefinita, i membri della lista possono scegliere se ricevere il traffico della lista in formato riassunto o normale. Se si abilita questa casella, verrà utilizzata la modalità riassunto, a prescindere dalla selezione dell'utente.

Modalità invio riassunti

Le seguenti opzioni determinano la frequenza e le circostanze in cui gli iscritti alla lista, le cui impostazioni lo prevedono, riceveranno la posta in formato riassunto. Le opzioni operano tutte in modo indipendente le une dalle altre, così che l'invio di un riassunto può essere determinato da alcune o da tutte le impostazioni.

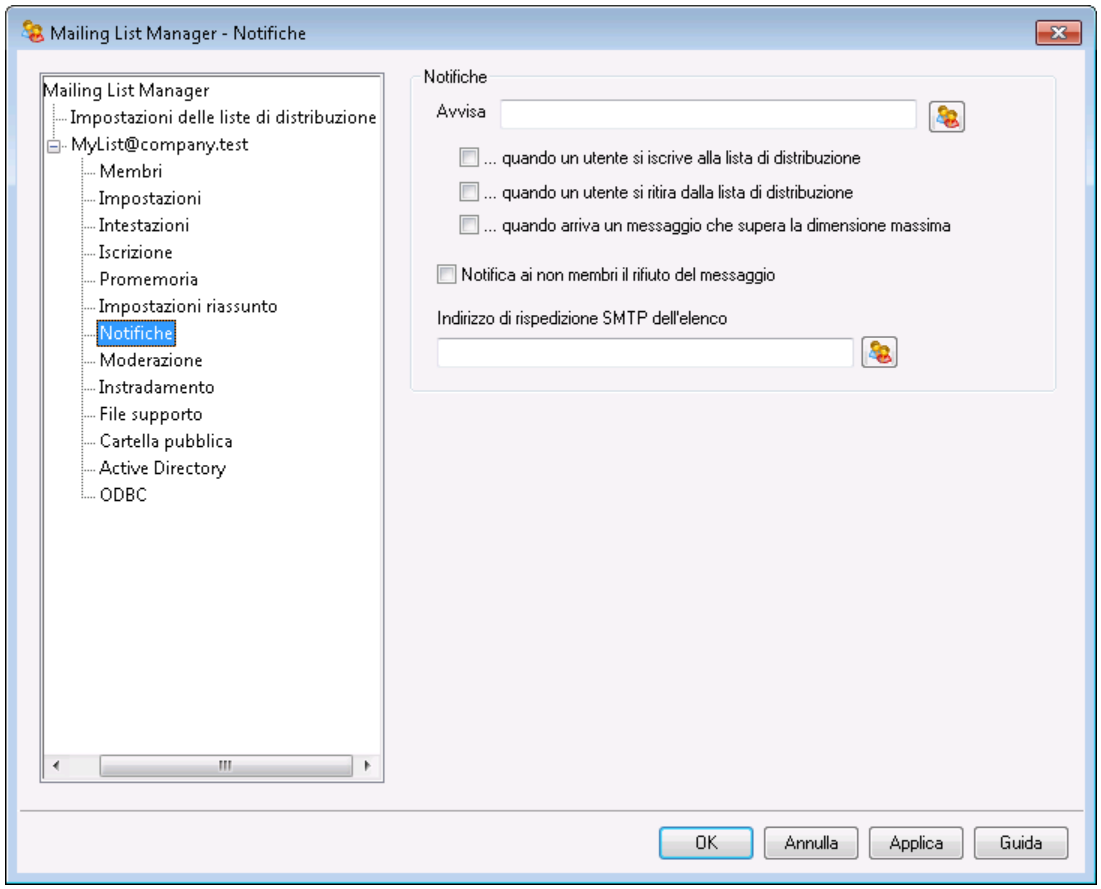
Invia posta riass. alle 9, 12, 3, 6 am e/o pm
Questa opzione consente di pianificare la frequenza di invio dei riassunti. Abilitando tutte le caselle di questa opzione, i riassunti verranno inviati ogni tre ore oltre che in base agli eventi attivati dalle opzioni successive.

Spool mail sunto se si sono accumulati [XX] messaggi (0 = N/D)
Se si desidera che i riassunti vengano inviati automaticamente quando si supera la soglia di un determinato numero di messaggi, specificarne il numero. Inserire "0" se non si desidera usufruire di questa opzione. "0" è l'impostazione predefinita.

Vedere:

Membri 281
Controllo remoto del server via e-mail 912

3.4.2.7 Notifiche



Notifiche

Notifica
Questa opzione consente di specificare un indirizzo a cui inviare una notifica quando si verificano gli eventi selezionati.

... quando un utente si iscrive alla lista di distribuzione
Abilitare questa casella per inviare una nota all'indirizzo indicato per ogni iscrizione alla lista di distribuzione.

... quando un utente si ritira dalla lista di distribuzione
Abilitare questa casella per inviare una nota all'indirizzo indicato per ogni ritiro dalla lista di distribuzione.

... quando arriva un messaggio che supera la dimensione massima
Abilitando questa casella è possibile inviare una nota all'indirizzo indicato ogni volta che alla lista di distribuzione viene inviato un messaggio superiore al limite *Rifiuta messaggi lista superiori a XX KB* indicato in Impostazioni 284.

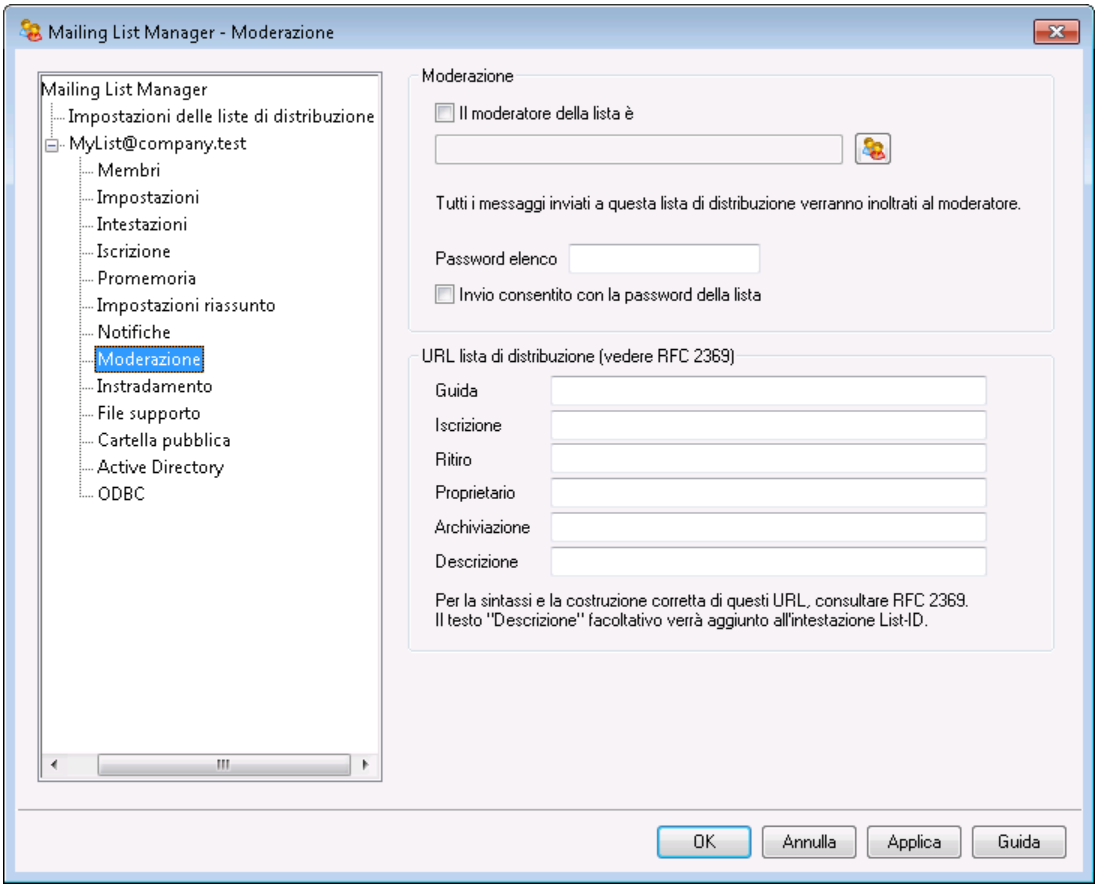
Notifica ai non membri il rifiuto del messaggio
Se questa opzione è abilitata, quando gli utenti inviano messaggi a una lista privata di cui non fanno parte, ricevono un apposito avviso da MDaemon, nonché istruzioni per un'eventuale iscrizione alla lista. Per definire una lista privata, utilizzare l'opzione *Invio posta alla lista consentito solo ai membri* di Impostazioni 284.

Posta restituita

Indirizzo di rispedizione SMTP dell'elenco
Questa opzione consente di specificare l'indirizzo di rispedizione della posta o dei messaggi sullo stato di consegna generati dal traffico della lista. Ad esempio, una lista di distribuzione con 100 destinatari può includere dieci indirizzi a cui non è possibile recapitare i messaggi perché l'indirizzo è cambiato, il server è fuori servizio o per altri motivi. Il sistema SMTP genera un messaggio per notificare tale impossibilità di consegna e lo invia al mittente del messaggio. Questa opzione consente di indicare l'indirizzo che riceverà questi messaggi relativi alle liste di distribuzione. È anche possibile indicare che nessuno li riceva. In questo caso MDaemon inserirà i messaggi della lista nel flusso di posta, in modo che non sia possibile inviare un messaggio di risposta. L'indirizzo NON può coincidere con l'indirizzo della lista di distribuzione.

L'impostazione di *Indirizzo di rispedizione SMTP dell'elenco* su un indirizzo dell'utente locale potrebbe causare l'eliminazione dell'e-mail dell'utente come conseguenza delle impostazioni per lo sfoltimento specificate in Impostazioni lista di distribuzione 278. Prestare attenzione prima di impostare questa opzione sull'indirizzo di un utente locale. Per ulteriori informazioni, vedere Sfoltimento avanzato della lista 286.

3.4.2.8 Moderazione



Moderazione

Il moderatore della lista è
Se si desidera che la lista venga moderata da un determinato utente, abilitare questa casella e indicare un account. Tutti messaggi delle liste con moderatore vengono inviati al moderatore stesso. Solo il moderatore può sottoporre o inoltrare i messaggi alla lista.

Password elenco
Fare clic per assegnare una password alla lista di distribuzione. Le password delle liste possono essere utilizzate con l'opzione *Invio consentito con la password della lista* oppure per sovrascrivere l'opzione *Limite membri* della schermata Iscrizione 291. Consentono, inoltre, di accedere alle numerose funzioni descritte nella sezione *Controllo remoto del server via e-mail* 912.

Invio consentito con la password della lista
Se alla lista viene assegnata una password e si abilita questa opzione, per scrivere alla lista è necessario inserire la password all'inizio dell'oggetto del messaggio, anche se alla lista è associato un moderatore qualora questo sia diverso dal mittente.

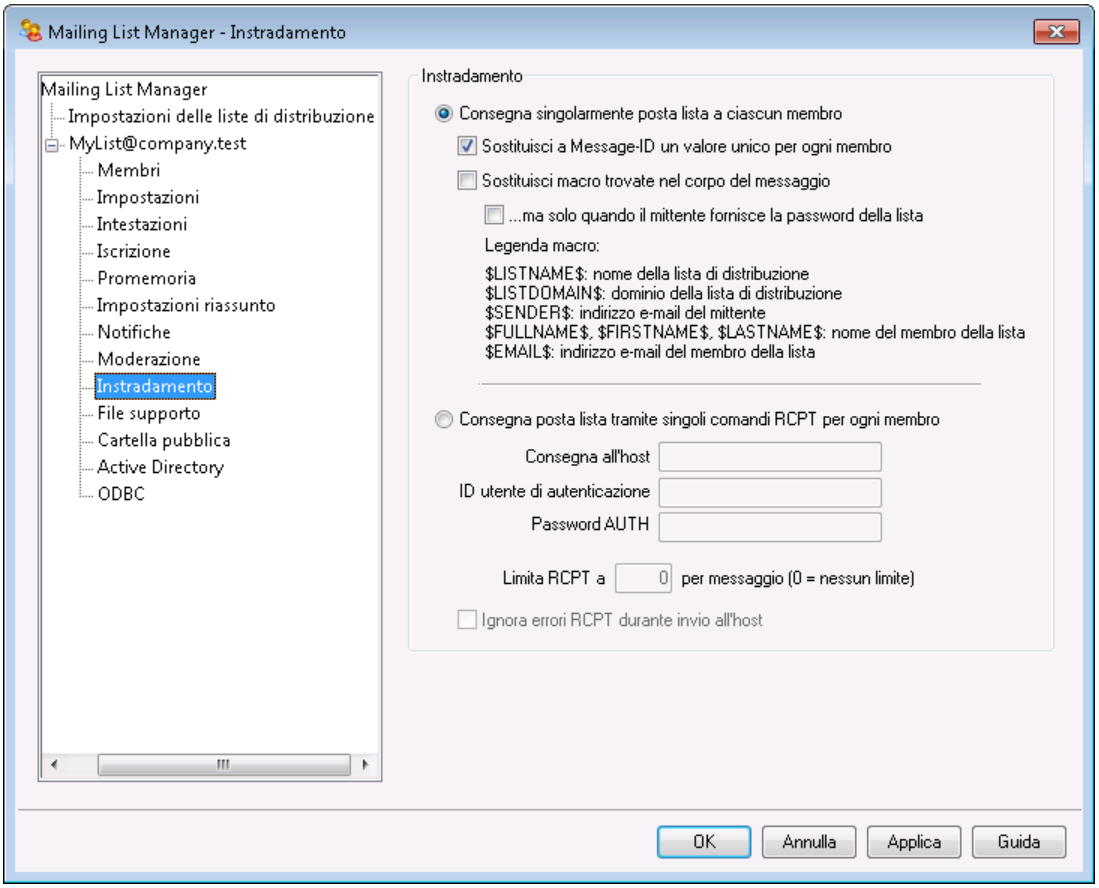
URL lista di distribuzione (vedere RFC 2369)

MDaemon può aggiungere ai messaggi di una lista di distribuzione tutti i sei campi intestazione specificati in RFC 2369: *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. Le sei intestazioni sono: **List-Help**, **List-Subscribe**, **List-Unsubscribe**, **List-Post**, **List-Owner** e **List-Archive**. Per utilizzare le intestazioni nei messaggi di una lista, immettere il valore desiderato dell'intestazione in uno dei campi specificati di seguito. I valori delle intestazioni devono essere formattati in base alle specifiche riportate in RFC 2369 (ad esempio, `<mailto:elenco@esempio.com?subject=help>`). Per alcuni esempi di ognuna delle intestazioni, vedere il documento collegato. MDaemon non apporta modifiche a questi dati quindi, se i dati non sono formati in modo corretto, non sarà possibile ottenere i risultati desiderati.

Descrizione (usata nell'intestazione List-ID:)
Immettere una breve descrizione della lista di distribuzione se si desidera aggiungerla all'intestazione `List-ID:` inclusa nei messaggi inviati alla lista. La descrizione e l'identificatore della lista saranno inclusi nell'intestazione (ad esempio `List-ID: "lista di distribuzione personale di Franco" <nome lista.esempio.com>`) L'identificatore della lista corrisponde all'indirizzo della lista di distribuzione con il carattere "." utilizzato in sostituzione del simbolo "@" per garantire la conformità alla specifica List-ID -. Se si lascia vuota l'opzione *Descrizione*, l'intestazione List-ID: conterrà solo l'identificatore della lista (ad esempio `List-ID: <nome lista.esempio.com>`). Se un messaggio in arrivo indirizzato all lista contiene un'intestazione List-ID: preesistente, MDaemon sostituirà la precedente intestazione con quella appropriata per la lista.

Le intestazioni List-Subscribe e List-Unsubscribe vengono incluse per impostazione predefinita in tutti i messaggi della lista di distribuzione quando si attiva l'opzione "*Consenti gli indirizzi "<List>-subscribe" e "<List>-subscribe"*" option nella schermata Preferenze » Varie 511. Per ignorare tale opzione per questa lista, utilizzando valori di intestazione diversi rispetto a quelli aggiunti automaticamente dall'opzione, immettere qui i valori desiderati. Se si disattiva l'opzione, non viene aggiunta alcuna intestazione List-Subscribe e List-Unsubscribe ai messaggi della lista, a meno che non si specifichi il relativo valore qui.

3.4.2.9 Instradamento



Instradamento

Consegna singolarmente posta lista a ciascun membro
Se si seleziona questa opzione, viene creata una copia distinta dei messaggi ricevuti per la distribuzione alla lista che viene, poi, recapitata ai singoli membri. Ciò determina la creazione di numerosi messaggi che si riflette sulle prestazioni del server in base alla dimensione della lista e al carico del server. Questa opzione è selezionata per impostazione predefinita.

Sostituisci a Message-ID un valore unico per ogni membro
Se si imposta MDaemon per la creazione di una copia distinta di ogni messaggio per i singoli membri, con questa casella di controllo è possibile assegnare a tutti i messaggi un ID univoco. Questa opzione è disattivata per impostazione predefinita ed è sconsigliata a meno che non sia necessaria in alcune particolari circostanze.

Sostituisci macro trovate nel corpo del messaggio
Attivare questa opzione se si desidera consentire l'uso di macro speciali nei messaggi delle liste di distribuzione. Quando viene trovata una macro, MDaemon la sostituisce con il valore corrispondente rappresentato dalla macro, separatamente per ciascun messaggio prima di inviarlo a ciascun membro della lista.

...ma solo quando il mittente fornisce la password della lista
Quando si consente l'uso delle macro all'interno del corpo dei messaggi, selezionare quest'opzione se si desidera richiedere la password della lista 300 perché l'utente sia autorizzato a usare le macro nei messaggi. Quando questa opzione è disattivata, tutti gli utenti in grado di inviare un messaggio alla lista potranno utilizzare le macro.

Macro:

$LISTNAME$	Il nome della lista o la parte "casella postale" dell'indirizzo della lista (ad es. "MyList" per MyList@example.com).
$LISTDOMAIN$	Il dominio della lista (ad es. "example.com" per MyList@example.com).
$SENDER$	L'indirizzo e-mail del mittente del messaggio.
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	Il nome completo, il nome o il cognome del membro della lista (se disponibile).
$EMAIL$	L'indirizzo e-mail del membro della lista.

Consegna posta lista tramite singoli comandi RCPT per ogni membro
Se questa casella di controllo è selezionata, anziché inviare messaggi ai singoli membri, MDaemon instrada una sola copia di ciascun messaggio della lista all'host intelligente specificato. Durante la sessione SMTP con l'host specificato, questo metodo utilizza più istruzioni `RCPT TO`.

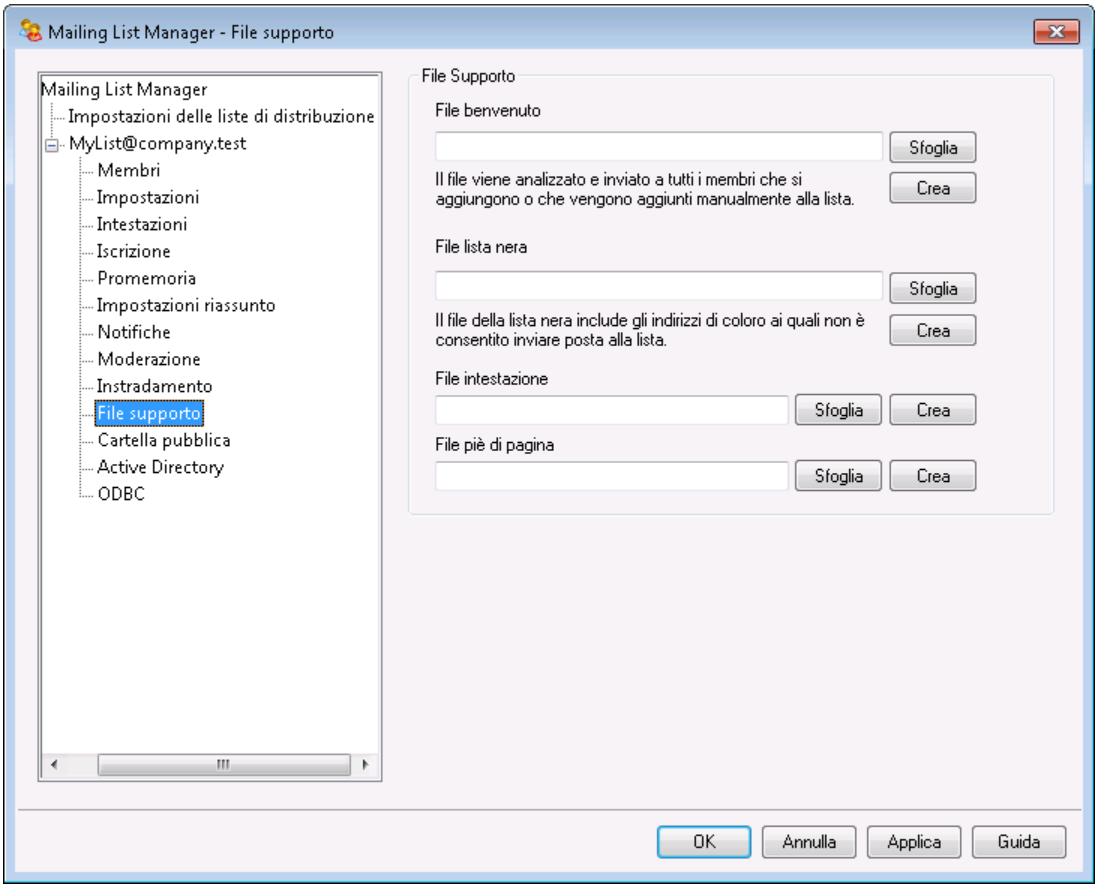
Consegna all'host
Consente di indicare l'host intelligente al quale trasmettere tutti i messaggi della lista da consegnare, utilizzando istruzioni RCPT TO per ogni membro.

Accesso/Password AUTH
Le credenziali di accesso richieste dall'host.

Limita RCPT a XX per messaggio (0=nessun limite)
Alcuni host stabiliscono un limite sul numero di istruzioni `RCPT TO` che si possono utilizzare per l'instradamento di una singola copia del messaggio. Se si specifica tale limite in questo campo, MDaemon crea delle copie supplementari del messaggio e suddivide la lista in gruppi più ridotti. Quindi, consegna il messaggio a tali gruppi, evitando così di superare il limite specificato. Questa opzione è simile alla precedente *Consegna singolarmente posta lista a ciascun membro*, ma crea un numero di copie inferiore e invia ogni copia a un gruppo di indirizzi, anziché generare copie distinte per ogni membro.

Ignora errori RCPT durante invio all'host
Poiché per determinati domini alcuni host intelligenti rifiutano di collocare la posta nella coda o di eseguirne lo spool, la consegna alla lista mediante instradamento potrebbe generare numerosi inconvenienti. A causa di un codice di errore restituito dall'host intelligente come risultato del rifiuto, di solito MDaemon abbandona il tentativo di consegna. Selezionando questa opzione, MDaemon ignora i codici di errore restituiti dall'host intelligente durante la consegna della posta della lista instradata consentendo, così, ai membri accettati di ricevere il messaggio della lista.

3.4.2.10 File di supporto



File di supporto

File benvenuto
Se indicato, il file presente in questo campo viene elaborato e il suo contenuto inviato a tutti i nuovi membri subito dopo l'iscrizione. Nel file di benvenuto per un nuovo iscritto è possibile utilizzare le seguenti macro:

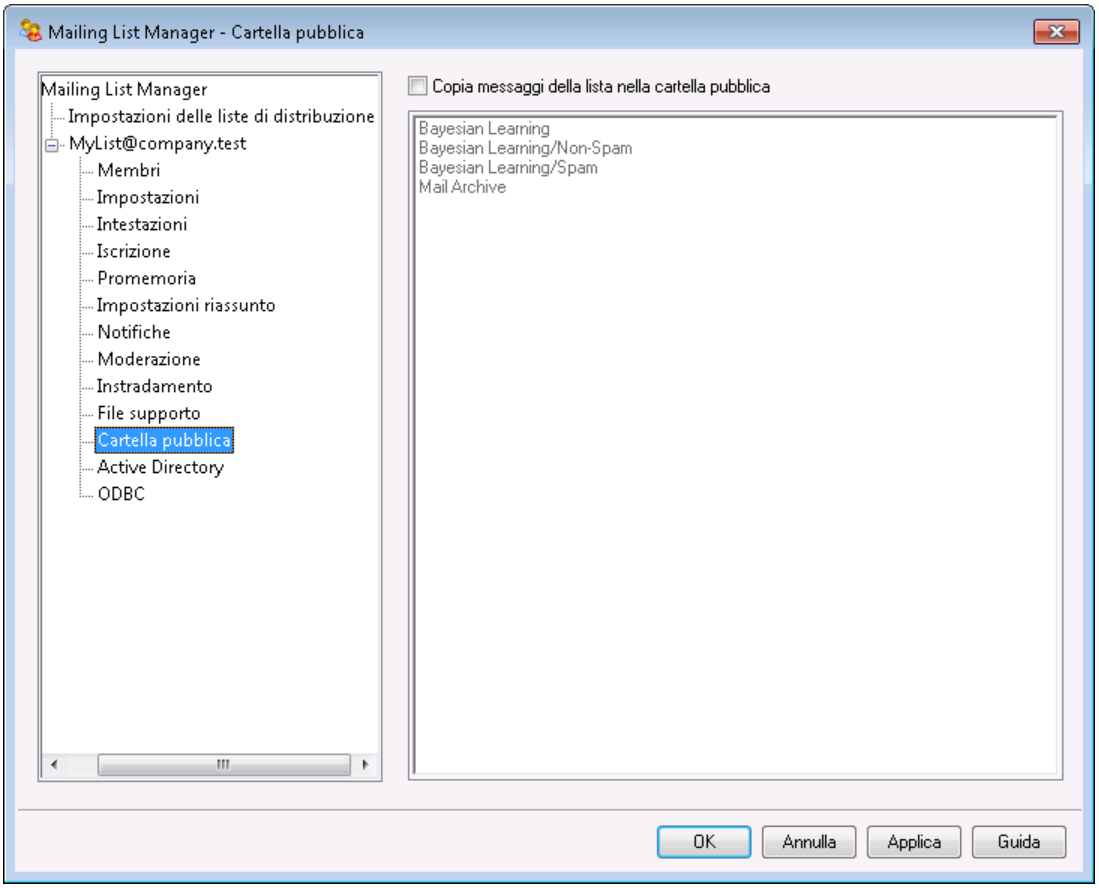
$PRIMARYDOMAIN$	Questa macro viene estesa al nome di dominio predefinito di MDaemon, che è designato nel Domain Manager 185.
$PRIMARYIP$	La macro restituisce l'indirizzo IPv4 associato all'indirizzo del Dominio predefinito 185 di MDaemon.
$PRIMARYIP6$	Questa macro restituisce l'indirizzo IPv6 associato al dominio predefinito 185 di MDaemon.
$DOMAINIP$	Questa macro restituisce l'indirizzo IPv4 associato al dominio.
$DOMAINIP6$	Questa macro restituisce l'indirizzo IPv6 associato al dominio.
$MACHINENAME$	Questa macro restituisce il contenuto dell'opzione FQDN indicata nello schermo Dominio.
$LISTEMAIL$	Questa macro consente di visualizzare l'indirizzo di posta elettronica della lista. Esempio: `NomeLista@esempio.com`
$LISTNAME$	Questa macro consente di visualizzare il nome della lista di distribuzione. Esempio: `NomeLista`
$LISTDOMAIN$	Questa macro restituisce il dominio della lista di distribuzione. Esempio: `esempio.com`
%SETSUBJECT%	Questa macro consente di indicare un oggetto alternativo per il messaggio di benvenuto. Il testo dell'oggetto specificato può includere altre macro di elenco come `$LISTEMAIL$`. Esempio: `%SetSubject%=Benvenuto in $LISTNAME$.`

File lista bloccati
Se indicato, il file presente in questo campo viene utilizzato per sopprimere i messaggi inviati da utenti specifici.

File intestazione/piè di pagina
Il contenuto dei file specificati in questi campi viene utilizzato sotto forma di intestazione e/o piè di pagina per i messaggi della lista.

Crea
Per creare un nuovo file, fare clic sul pulsante *Crea* corrispondente al file da creare, specificare un nome e, quindi, fare clic su *Apri*. In tal modo, il file di nuova creazione viene aperto in Blocco note e può essere modificato.

3.4.2.11 Cartella pubblica

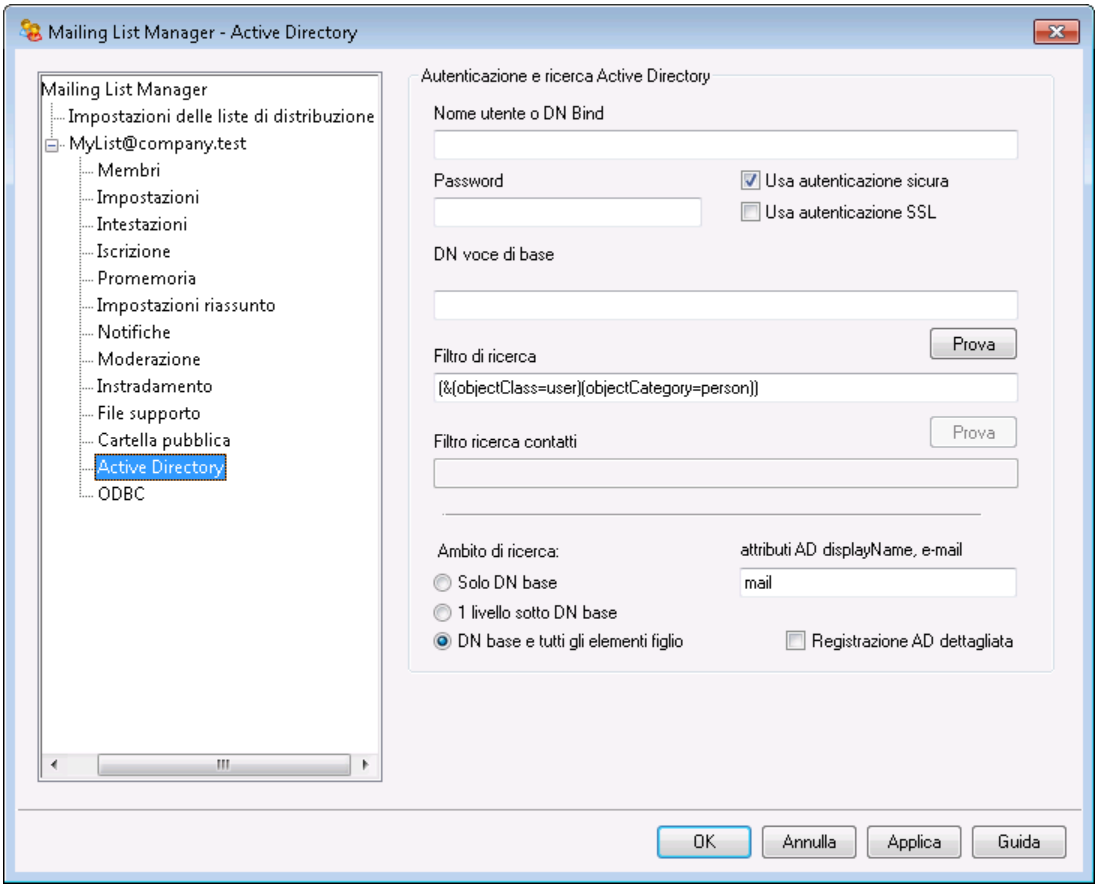


MDaemon consente di utilizzare le Cartelle IMAP pubbliche[120] con le liste di distribuzione. Le cartelle pubbliche sono cartelle aggiuntive che, diversamente dalle cartelle IMAP personali di solito accessibili a un solo utente, possono essere utilizzate da più utenti IMAP (Internet Message Access Protocol). Utilizzando le opzioni di questa schermata, tutti i messaggi indirizzati alla lista di distribuzione vengono automaticamente copiati in una delle cartelle pubbliche.

Copia messaggi della lista nella cartella pubblica
Abilitare questo comando se si desidera che i messaggi della lista vengano copiati in una delle cartelle pubbliche, oltre a essere consegnati alla lista.

Seleziona cartella pubblica
Selezionare la cartella pubblica che si desidera associare ai messaggi della lista.

3.4.2.12 Active Directory



Utilizzare le opzioni di questa schermata se si desidera recuperare gli indirizzi dei membri dell'elenco da Active Directory.

Autenticazione e ricerca Active Directory

Nome utente o DN associato
ID utente dell'account Windows o il DN che MDaemon utilizzerà per l'associazione ad Active Directory mediante LDAP. Per l'associazione, Active Directory consente l'uso di un account Windows o di un UPN.

> Quando si utilizza un DN invece di un ID utente Windows per questa opzione, è necessario disattivare/deselezionare l'opzione "*Usa autenticazione sicura*" riportata di seguito.

Password
Password corrispondente al DN o all'ID utente Windows indicato nell'opzione *DN associato*.

Usa autenticazione sicura
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione sicura durante l'esecuzione di ricerche in Active Directory. Non è possibile utilizzare questa opzione se nell'opzione *DN associato* indicata in precedenza viene specificato un DN anziché un ID utente Windows.

Usa autenticazione SSL
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione SSL durante l'esecuzione di ricerche in Active Directory.

L'utilizzo di questa opzione richiede la presenza di un server e di un'infrastruttura SSL nella rete Windows e in Active Directory. Se non si è certi dell'impostazione della rete o per ulteriori informazioni sulla possibilità di attivare questa opzione, rivolgersi al proprio reparto IT.

DN voce di base
Specificare il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la ricerca degli indirizzi di Active Directory. È possibile utilizzare "`LDAP://rootDSE`" in questa opzione per eseguire la ricerca a partire dalla directory principale DSE, che rappresenta la voce di livello più alto nella gerarchia di Active Directory. L'indicazione di un punto iniziale più accurato e prossimo alla posizione degli account utente o del gruppo desiderato di indirizzi nella struttura di Active Directory può ridurre il tempo richiesto dalla ricerca nella struttura DIT. Lasciare vuoto questo campo se non si desidera recuperare alcun indirizzo della lista dalla Active Directory.

Filtro di ricerca
Rappresenta il filtro di ricerca LDAP utilizzato per le ricerche in Active Directory. Utilizzare questo filtro per consentire a MDaemon di localizzare con maggiore accuratezza gli account utente desiderati o gli indirizzi che si desidera considerare come iscritti alla lista.

Test
Usare questi pulsanti per testare le impostazioni del filtro di ricerca.

---

attributi AD displayName, e-mail
È necessario utilizzare questo campo per specificare l'attributo in cui sarà inserito l'indirizzo e-mail utilizzato dalla lista. Ad esempio, se si specifica "`Mail`" in questo campo, ogni account Active Directory da considerare membro della lista deve avere l'attributo "`Mail`" e l'attributo deve contenere un indirizzo e-mail. È possibile anche immettere un attributo di Active Directory nel campo nel nome completo dei membri della lista prima dell'attributo dell'indirizzo e-mail, separato da una virgola. É ad esempio possibile immettere: "`displayName, mail`" invece di "`mail`" in questa opzione. Il primo è l'attributo di Active Directory in cui si trova il nome completo e il secondo è l'attributo e-mail.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche Active Directory.

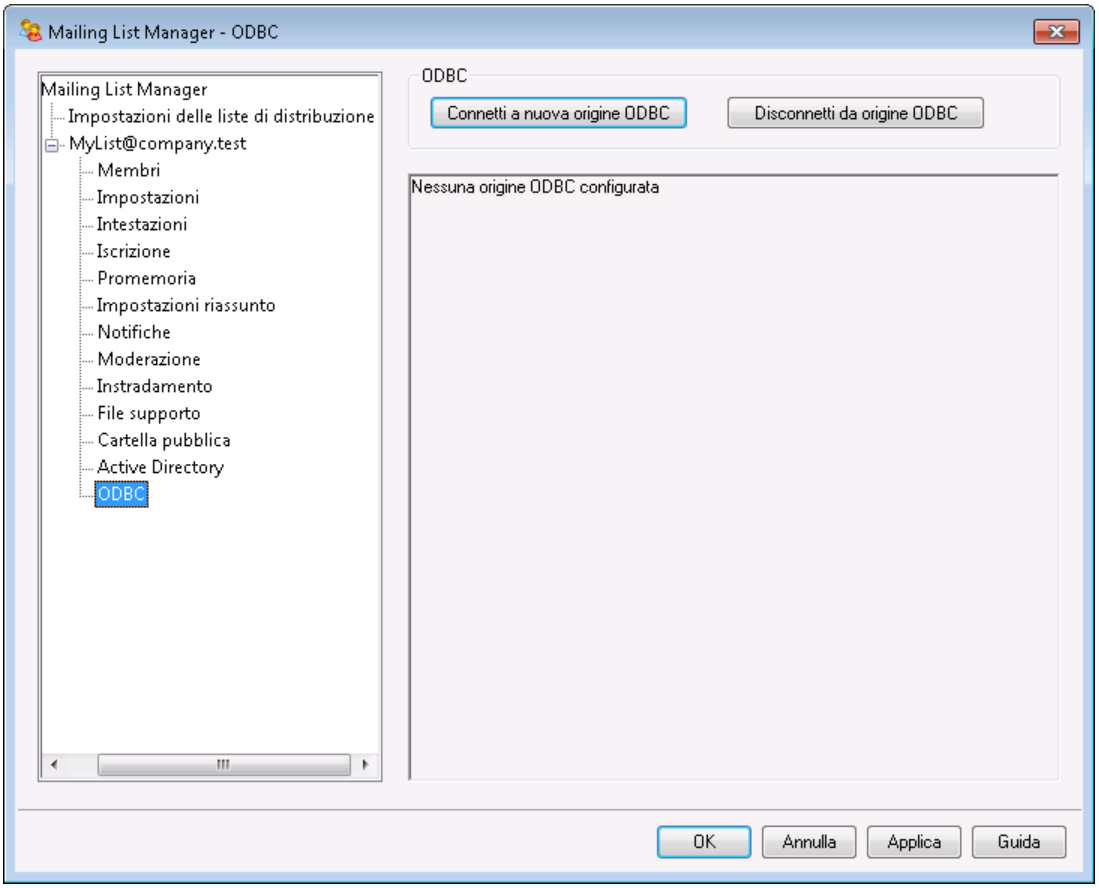
Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca nella struttura DIT di Active Directory ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT.

Registrazione AD dettagliata
Per impostazione predefinita, MDaemon utilizzerà la registrazione dettagliata per gli eventi di Active Directory. Deselezionare questa casella di controllo se si desidera utilizzare una modalità di registrazione Active Directory meno dettagliata.

3.4.2.13 ODBC



Questa funzionalità consente di gestire l'elenco degli appartenenti alle liste di distribuzione mediante un database compatibile con ODBC. La schermata ODBC dell'editor delle liste di distribuzione consente di selezionare la corrispondenza con origini dati, tabelle e campi per il collegamento alla lista. Quando arriva un messaggio per la propria lista, vengono eseguite automaticamente una o più interrogazioni SQL e gli indirizzi e-mail risultanti vengono considerati come appartenenti alla lista.

È inoltre possibile aggiungere, rimuovere e modificare i membri della lista presenti nel database con qualsiasi applicazione di database compatibile con ODBC.

ODBC

In questa sezione vengono visualizzate le proprietà ODBC impostate per la lista di distribuzione. Vengono inoltre riportate le corrispondenze tra i campi del database e le interrogazioni SQL configurate per indicare lo stato di appartenenza di ogni membro: modalità Normale, Solo invio, Solo lettura e/o Riassunto.

Connetti a nuova origine ODBC
Questo pulsante consente di avviare Selezione guidata ODBC per la scelta dell'origine dati di sistema da utilizzare per la lista di distribuzione.

Disconnetti da origine ODBC
Fare clic su questo pulsante per scollegare la lista dall'origine dati ODBC elencata.

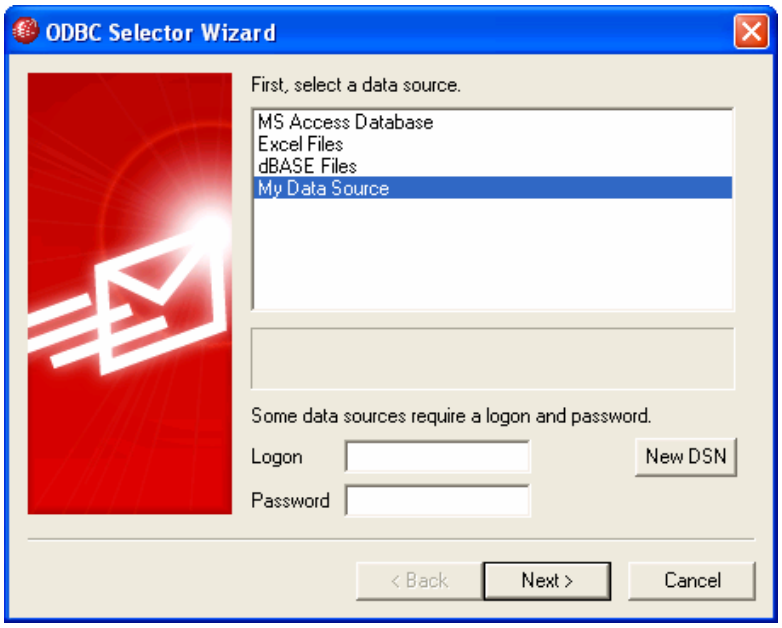
Vedere:

[Configurazione di un'origine dati di sistema ODBC per una lista di distribuzione](#) 311
[Creazione di una nuova origine dati di sistema](#) 313

3.4.2.13.1 Configurazione di un'origine dati ODBC

Per utilizzare un database ODBC con una lista di distribuzione, procedere come segue.

1. Nella schermata ODBC 310 dell'editor delle liste di distribuzione, fare clic su **Connetti a nuova origine ODBC** per aprire Selezione guidata ODBC.

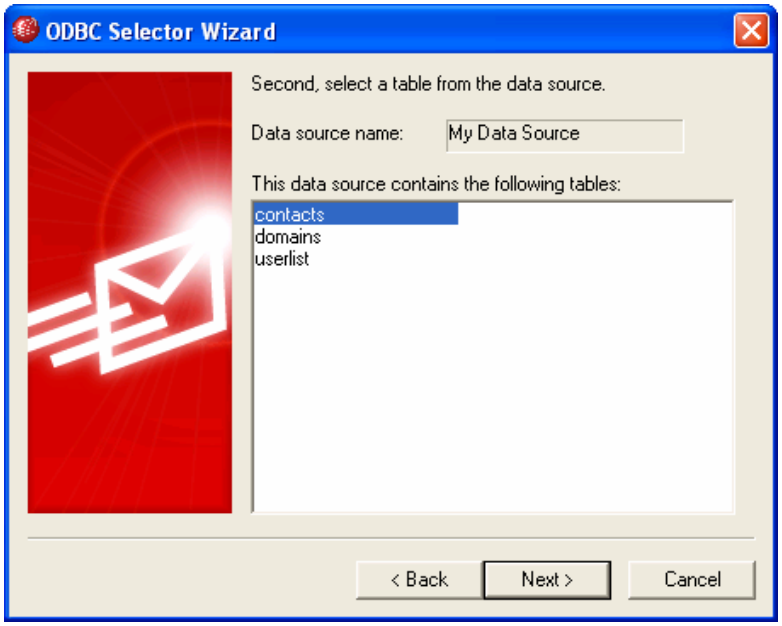


2. Selezionare l'**origine dati** desiderata per la lista di distribuzione. Se questa non è presente nell'elenco, fare clic su **Nuovo DSN** e seguire le indicazioni fornite in [Creazione di una nuova origine dati ODBC](#) 313.

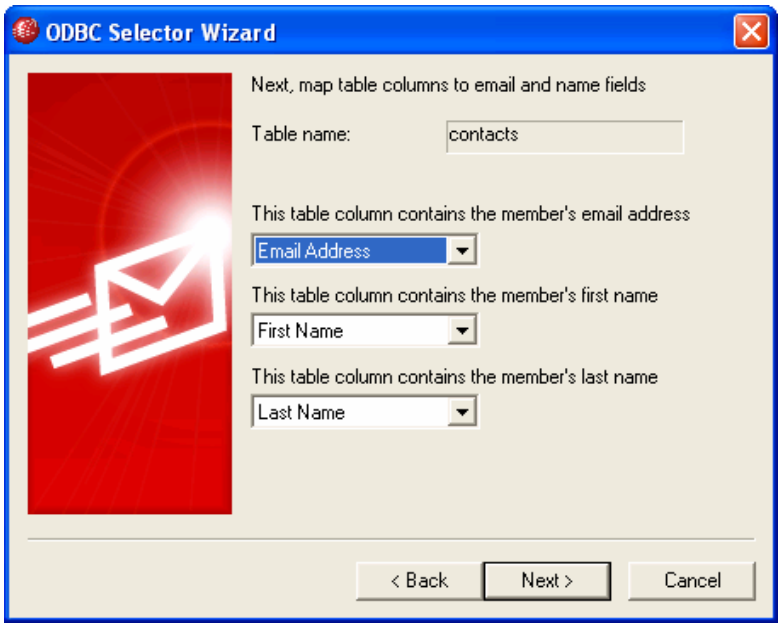
3. Se necessario, inserire l'**ID accesso** e la **Password** dell'origine dati.

4. Scegliere **Avanti**.

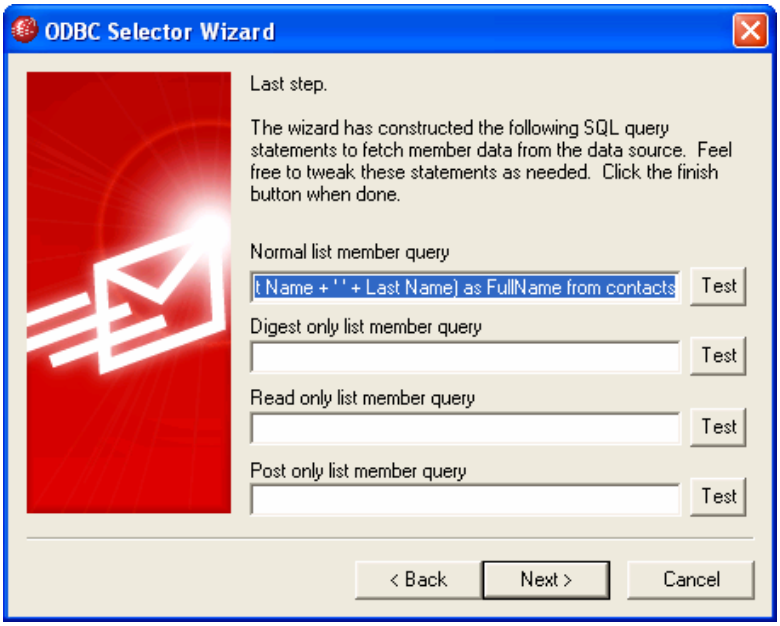
5. Nell'origine dati deve essere presente almeno una tabella contenente i campi relativi all'indirizzo di posta elettronica e al nome. Se sono disponibili più tabelle di qualificazione, selezionare quella desiderata e scegliere **Avanti**. Altrimenti, scegliere **Annulla** per uscire dalla Selezione guidata ODBC e, prima di proseguire, aggiungere una tabella al database in questione utilizzando l'applicazione di database.



6. Nelle caselle di riepilogo a discesa indicare i campi della tabella che corrispondono all'**indirizzo di posta elettronica**, al **nome** e al **cognome**. Scegliere **Avanti**.



7. Selezione guidata ODBC crea un'istruzione di interrogazione SQL in base a quanto selezionato nel **passaggio 6**. I risultati verranno utilizzati per recuperare i dati dei membri della lista normale dal database. È possibile modificare questa istruzione nel modo desiderato, nonché includere altre istruzioni di interrogazione nei controlli rimanenti per consentire ai membri di ricevere i messaggi in modalità Riassunto e per indicare quale membri siano in modalità Solo lettura o Solo invio. Accanto a ogni controllo è presente un pulsante **Test**, che consente di esaminare le istruzioni di interrogazione per verificare che recuperino i dati desiderati. Al termine della configurazione delle istruzioni di interrogazione, fare clic su **Avanti**.



8. Scegliere **Fine**.

Vedere:

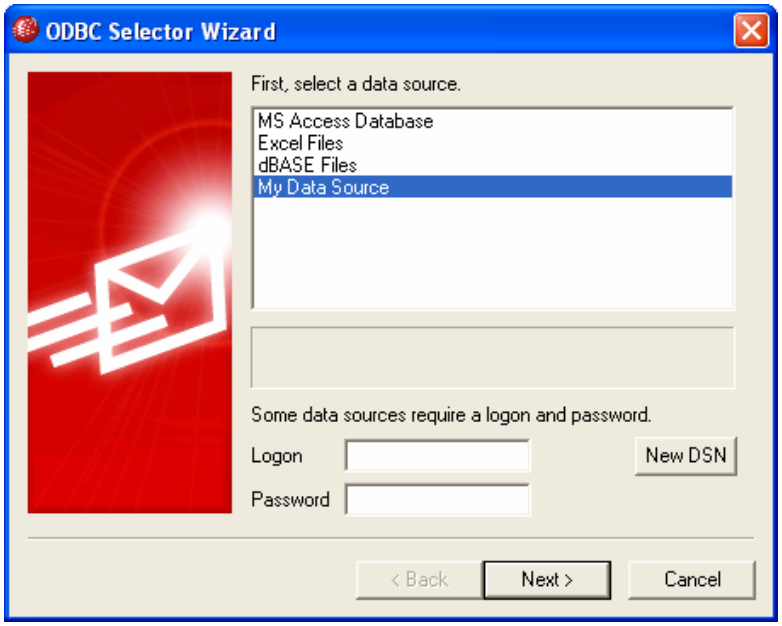
Editor Liste di distribuzione » ODBC 310
Creazione di una nuova origine dati ODBC 313

3.4.2.13.2 Creazione di una nuova origine dati ODBC

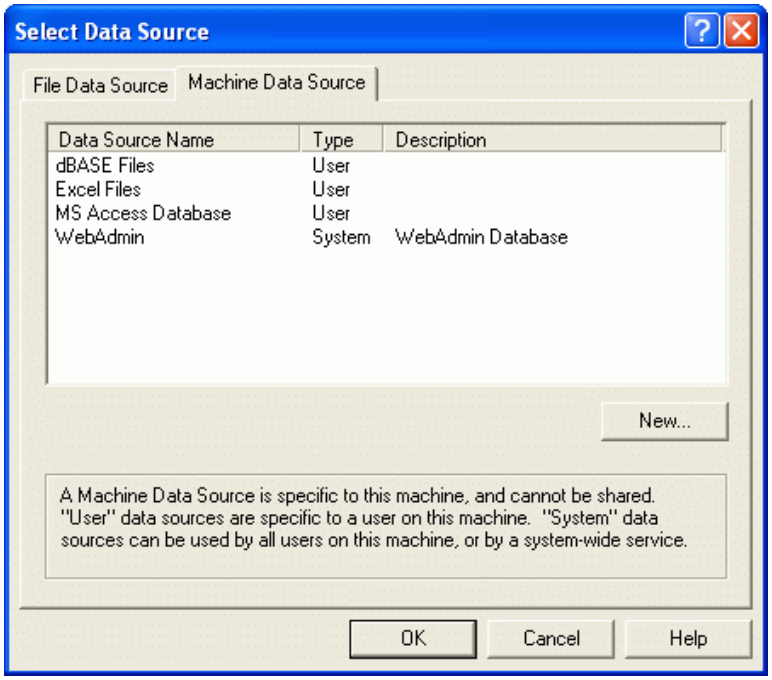
Per creare una nuova origine dati di sistema ODBC da utilizzare per la lista di distribuzione, procedere come segue.

1. Nella schermata ODBC 310 dell'editor delle liste di distribuzione, fare clic su **Connetti a nuova origine ODBC** per aprire Selezione guidata ODBC.

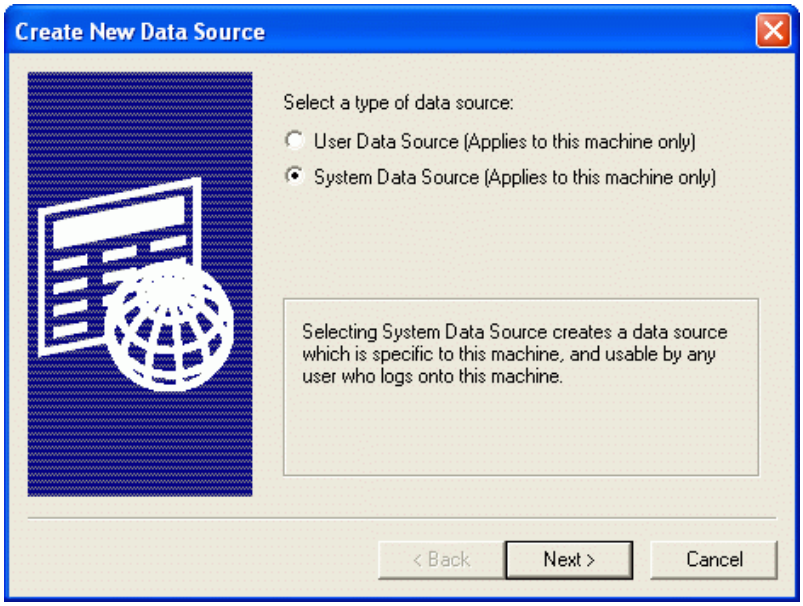
2. Fare clic su **Nuovo DSN** per aprire la finestra di selezione dell'origine dati.



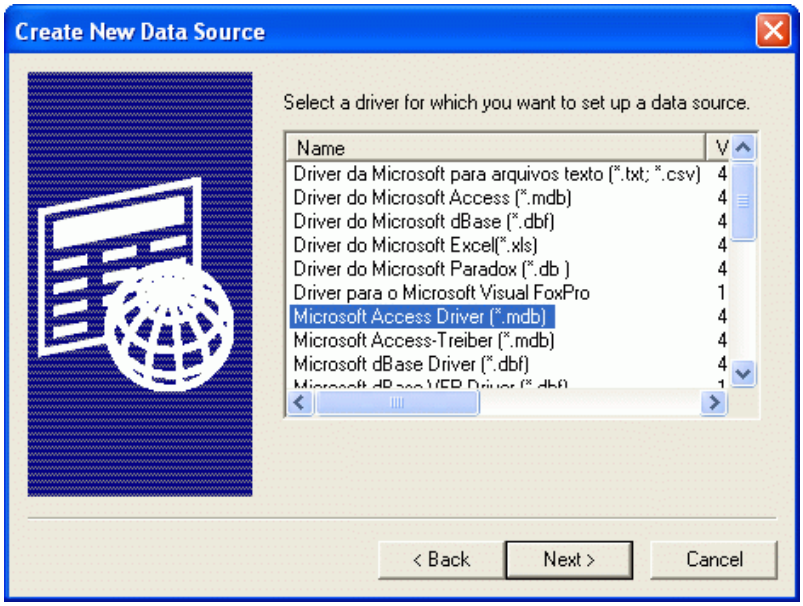
3. Passare alla scheda **Origine dati computer** e fare clic su **Nuova** per aprire la finestra di dialogo Crea nuova origine dati.



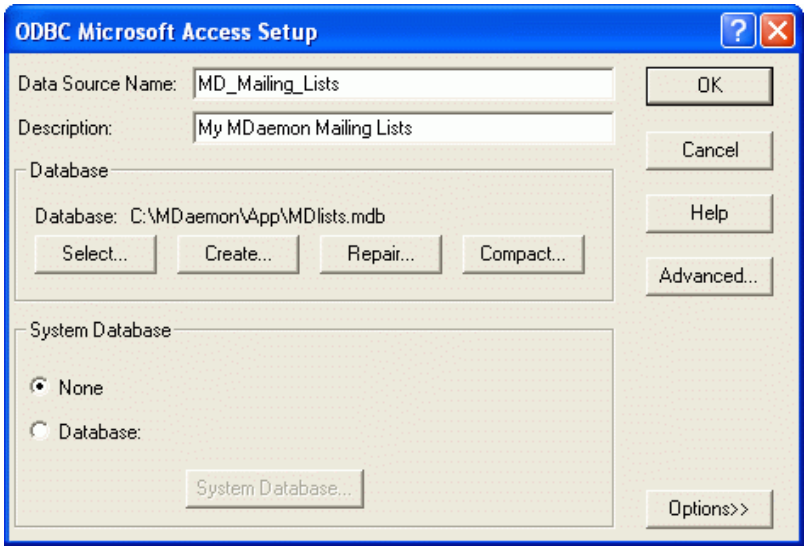
4. Selezionare **Origine dati di sistema** e fare clic su **Avanti**.



5. Selezionare il **driver** di **database** per il quale si desidera configurare l'origine dati, quindi fare clic su **Avanti**.



6. Fare clic su **Fine** per visualizzare la finestra di dialogo per l'impostazione del driver specifico. L'aspetto di questa finestra di dialogo varia a seconda del driver selezionato. Quella visualizzata di seguito è la finestra di dialogo relativa alle impostazioni di accesso Microsoft.



7. Indicare un valore per la nuova origine nel campo **Nome origine dati** e fornire le altre informazioni richieste dalla finestra di dialogo relativa allo specifico driver, quali la creazione o l'indicazione di un database, la scelta di una directory o di un server e così via.

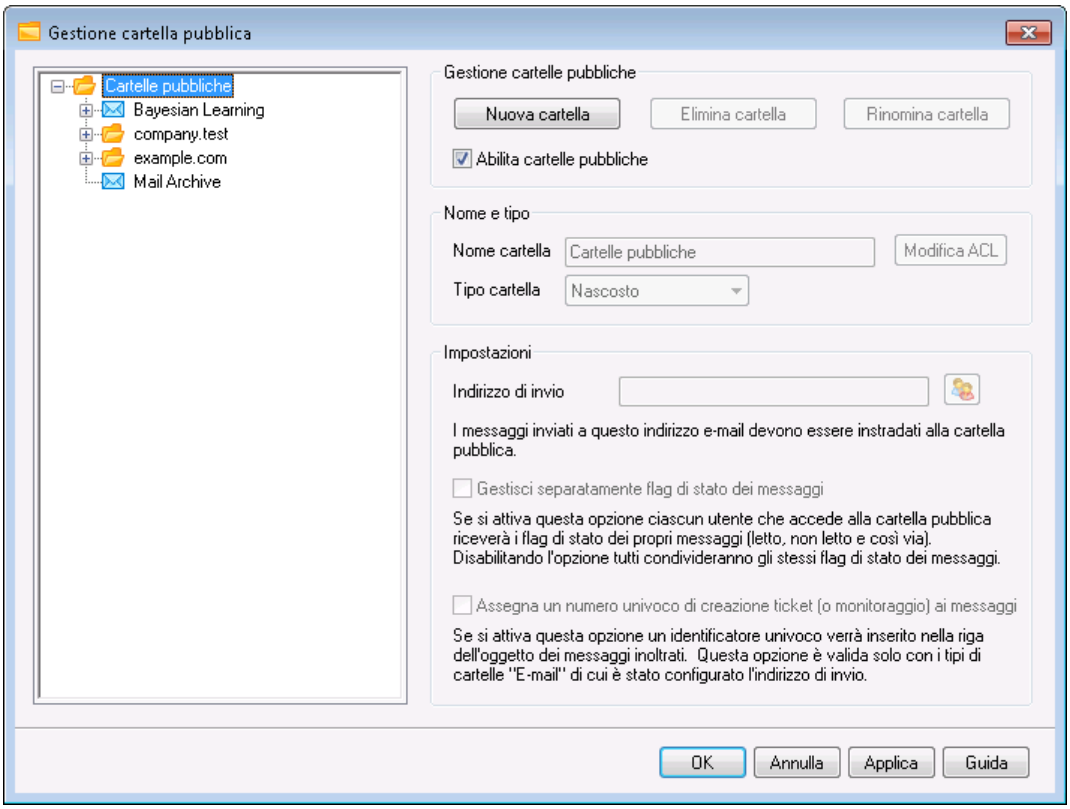
8. Fare clic su **OK** per chiudere la finestra di dialogo del driver.

9. Fare clic su **OK** per chiudere la finestra di dialogo per la selezione dell'origine dati.

Per ulteriori informazioni, vedere:

ODBC - Liste di distribuzione 310
Configurazione di un'origine dati di sistema ODBC per una lista di distribuzione 311

3.5 Gestione cartelle pubbliche



Utilizzare questa schermata per gestire le cartelle pubbliche[120]. Per accedere a Gestione cartelle pubbliche, fare clic su "Impostazioni » Gestione cartelle pubbliche...".

Gestione cartelle pubbliche

Nuova cartella

Per creare una nuova cartella pubblica, selezionare la cartella nell'elenco che si desidera scegliere come principale e fare clic su *Nuova cartella*. Digitare un nome per la cartella, scegliere il tipo di cartella e fare clic su *OK*.

Elimina cartella
Per rimuovere dall'elenco una cartella pubblica, selezionarla e fare clic sul pulsante *Elimina cartella*.

Rinomina cartella
Per rinominare una cartella pubblica, selezionarla e fare clic su *Rinomina cartella*. Digitare un nuovo nome e fare clic su *OK*.

Abilita cartelle pubbliche
Fare clic su questa casella di controllo per consentire agli utenti di accedere alle cartelle pubbliche. Gli utenti autorizzati ad accedere a tali cartelle e il livello di accesso accordato vengono controllati selezionando una cartella e facendo clic sul pulsante *Modifica ACL*.

Nome e tipo

Nome cartella
Nella casella viene visualizzato il nome della cartella selezionata nell'elenco. Le altre opzioni della schermata si applicano alla cartella selezionata.

Tipo cartella
Utilizzando l'elenco a discesa, indicare il tipo di cartella: Posta, Contatti, Calendario e così via.

Modifica ACL
Selezionare una cartella e fare clic su questo pulsante per aprire la finestra di dialogo Elenco controllo accessi 319 per la cartella. Utilizzare la finestra di dialogo Elenco controllo accessi per specificare gli utenti o i gruppi a cui sarà consentito accedere alla cartella, nonché le rispettive autorizzazioni.

Impostazioni

Indirizzo di invio
Immettere un indirizzo e-mail locale o scegliere un account MDaemon specifico da associare alla cartella condivisa, in modo che i messaggi destinati a quell'*Indirizzo di invio* siano automaticamente instradati alla cartella condivisa. Tuttavia, solo gli

utenti a cui sia stata accordata l'autorizzazione a inviare nella cartella sono in grado di effettuare invii a tale indirizzo.

Gestisci separatamente flag di stato dei messaggi
Fare clic su questa casella di controllo se si desidera impostare i flag dei messaggi della cartella (letto, non letto, risposto a, inoltrato e così via) a livello di singolo utente anziché a livello globale. Ciascun utente visualizza lo stato dei messaggi nella cartella condivisa in base alla propria interazione personale. Un utente che non abbia letto un messaggio lo visualizzerà contrassegnato come 'non letto' mentre un utente che lo abbia letto lo visualizzerà come 'letto'. Se questa opzione è disabilitata, tutti gli utenti visualizzano lo stesso stato. Pertanto, una volta che un utente ha letto un messaggio, anche tutti gli altri lo visualizzano come 'letto'.

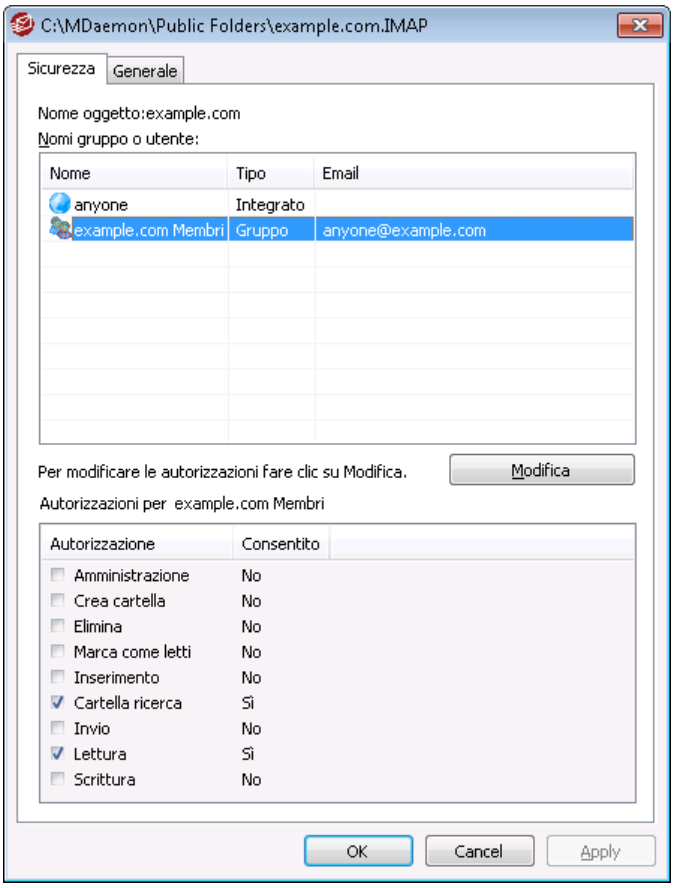
Assegna un numero univoco di creazione ticket (o monitoraggio) ai messaggi
Utilizzare questa opzione per configurare la cartella pubblica come cartella pubblica per la creazione di ticket come messaggi. Il *nome della cartella* e un identificatore univoco vengono aggiunti automaticamente all'oggetto dei messaggi inviati all'*indirizzo di invio* della cartella pubblica. Tutti i messaggi in uscita con questo oggetto in formato speciale avranno l'indirizzo Da modificato nell'indirizzo di invio della cartella pubblica e una copia del messaggio in uscita verrà collocata in una sottocartella pubblica denominata "Risposta inviata". Inoltre, tutti i messaggi in entrata con questo oggetto in formato speciale verranno reindirizzati automaticamente alla cartella pubblica, indipendentemente dall'indirizzo del destinatario del messaggio.

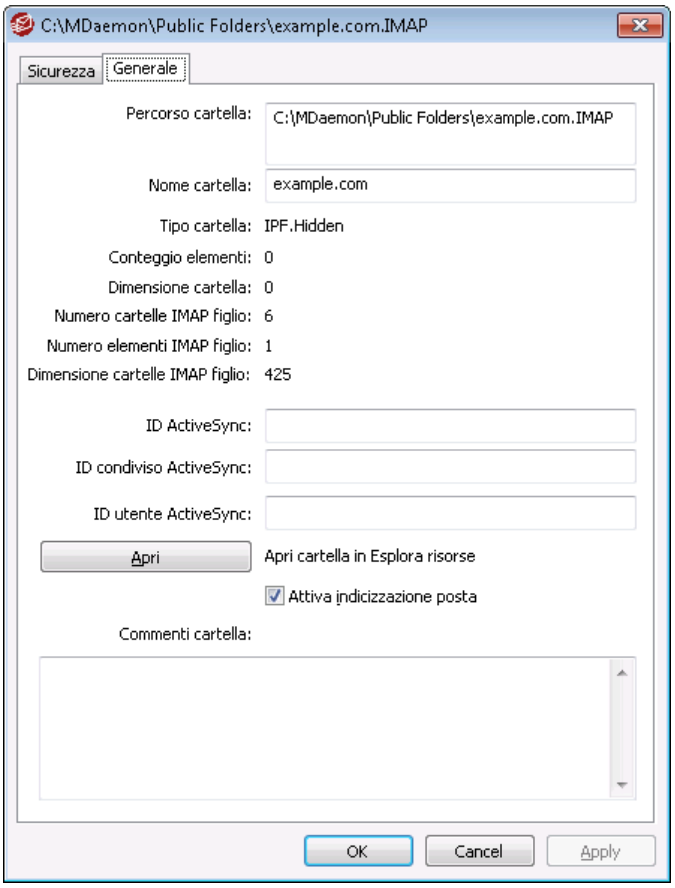
Vedere:

Elenco controllo accessi 319
Panoramica sulle cartelle pubbliche 120
Cartelle pubbliche e condivise 122
Account Editor » Cartelle condivise 757
Lista distribuzione » Cartelle pubbliche 306

3.5.1 Elenco controllo accessi

L'Elenco controllo accessi (ACL) viene utilizzato per impostare le autorizzazioni di accesso di utenti o gruppi alle cartelle pubbliche e condivise 120. È possibile accedervi mediante il pulsante *Modifica ACL* in Gestione cartelle pubbliche 317 o mediante il pulsante *Modifica elenco controllo accessi* nella schermata Cartelle condivise 757 di Account Editor.





Sicurezza

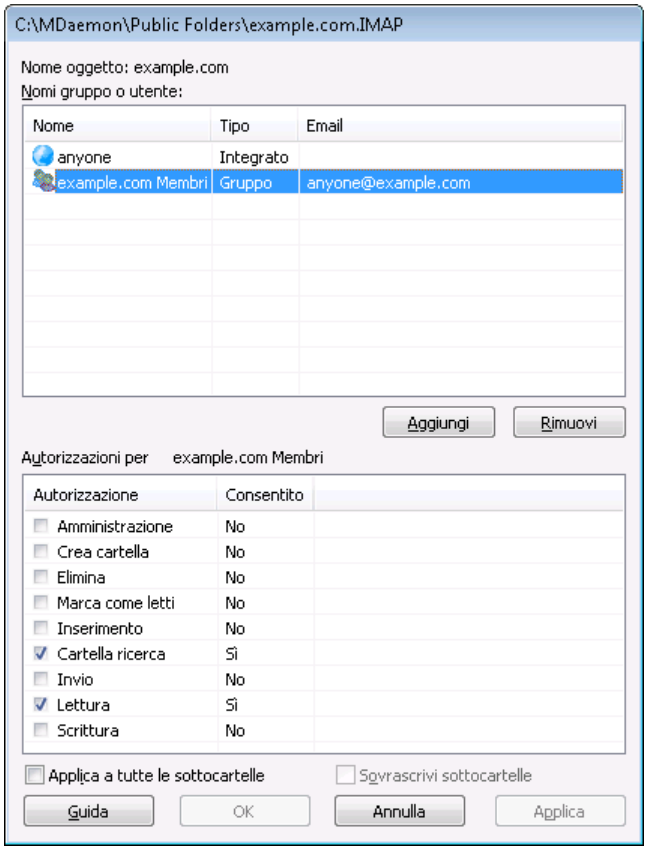
Questa scheda consente di visualizzare l'elenco di gruppi o utenti associati alla cartella e le autorizzazioni di accesso specifiche concesse a ciascuno di essi. Selezionare un gruppo o un utente nell'elenco per visualizzare le relative autorizzazioni 322 ed esaminarle nella finestra Autorizzazioni riportata di seguito. Per modificare le autorizzazioni, fare clic su **Modifica** 321.

Generale

Questa scheda consente di visualizzare le proprietà delle cartelle, come percorso, nome, tipo, dimensioni e così via.

Editor ACL

Fare clic su **Modifica** nella scheda Sicurezza dell'ACL per aprire l'Editor ACL per la modifica delle autorizzazioni di accesso.



Nome oggetto
Nome dell'oggetto o della cartella alla quale si applicano le autorizzazioni per l'ACL.

Nomi gruppo o utente
Sono i gruppi o gli utenti ai quali possono essere state concesse autorizzazioni di accesso di specifici livelli. Selezionare un gruppo o un utente per visualizzare le relative autorizzazioni nella finestra *Autorizzazioni per <gruppo o utente>* riportata di seguito. Selezionare la casella situata accanto alle autorizzazioni di accesso che si desidera concedere all'utente o al gruppo.

Aggiungi
Per concedere le autorizzazioni di accesso a un gruppo o un utente non presente nell'elenco, fare clic su **Aggiungi**323.

Rimuovi
Per rimuovere un gruppo o un utente, selezionare la voce nell'elenco riportato sopra e fare clic su **Rimuovi**.

Autorizzazioni per <gruppo o utente>
Selezionare la casella situata accanto alle autorizzazioni di accesso che si desidera concedere all'utente o al gruppo selezionato sopra.

È possibile concedere le autorizzazioni di controllo dell'accesso seguenti:

Amministrazione - L'utente è in grado di amministrare l'ACL (Access Control List) relativo alla cartella.

Creazione - L'utente è in grado di creare delle sottocartelle della cartella.

Eliminazione - L'utente è in grado di eliminare elementi dalla cartella.

Contrassegno come letto - L'utente è in grado di modificare lo stato letto/non letto dei messaggi presenti nella cartella.

Inserimento - L'utente è in grado di allegare e copiare i messaggi nella cartella.

Ricerca cartella - L'utente è in grado di visualizzare la cartella nel proprio elenco personale di cartelle IMAP.

Invio - L'utente è in grado di inviare la posta direttamente alla cartella, se quest'ultima lo consente.

Lettura - L'utente è in grado di aprire la cartella e visualizzarne il contenuto.

Scrittura - L'utente è in grado di modificare i flag applicati ai messaggi della cartella.

Applica a tutte le sottocartelle
Selezionare questa casella per applicare le autorizzazioni di controllo accessi della cartella a tutte le sottocartelle in essa contenute. In questo modo si aggiungeranno le autorizzazioni dell'utente o del gruppo alle sottocartelle, sostituendole in caso di eventuali conflitti. Non si elimineranno tuttavia altre autorizzazioni di utenti o gruppi che hanno attualmente accesso a tali cartelle.

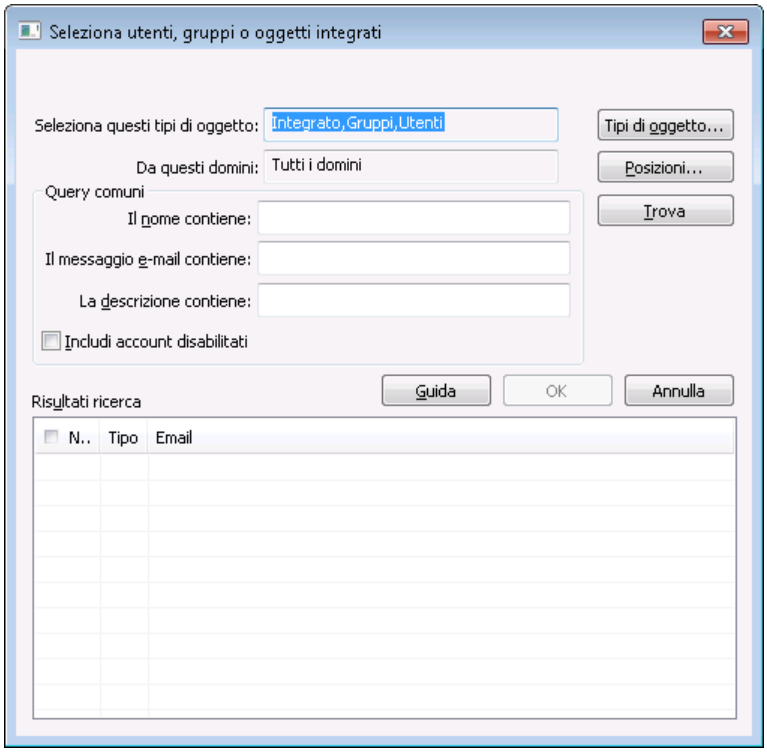
Esempio:

La cartella principale concede determinate autorizzazioni all'`Utente_A` e all'`Utente_B`. La sottocartella concede autorizzazioni all'`Utente_B` e all'`Utente_C`. Questa opzione consente di aggiungere le autorizzazioni dell'`Utente_A` alla sottocartella, sostituire le autorizzazioni dell'`Utente_B` della sottocartella con quelle della cartella principale e lasciare inalterate le autorizzazioni dell'`Utente_C`. Pertanto la sottocartella disporrà delle autorizzazioni per l'`Utente_A`, l'`Utente_B` e l'`Utente_C`.

Sovrascrivi sottocartelle
Selezionare questa casella se si desidera sostituire tutte le autorizzazioni di accesso della sottocartella con le autorizzazioni di accesso della cartella principale. Le autorizzazioni della sottocartella saranno quindi identiche a quelle della cartella principale.

Aggiunta di un gruppo o di un utente

Fare clic su **Aggiungi** nell'Editor ACL se si desidera aggiungere un altro utente o un altro gruppo all'elenco controllo accessi. Viene quindi aperta la schermata Aggiunta gruppo o utente che è possibile utilizzare per cercare e aggiungere utenti e gruppi.



Selezionare questi tipi di oggetti
Fare clic su **Tipi di oggetto...** per selezionare i tipi di oggetto all'interno dei quali si desidera cercare i gruppi o gli utenti da aggiungere. È possibile selezionare: Integrati, Gruppi e Utenti.

Da queste posizioni
Fare clic su **Posizioni...** per selezionare i domini nei quali si desidera cercare. È possibile selezionare tutti i domini MDaemon o domini specifici.

Interrogazioni comuni
Utilizzare le opzioni presenti in questa sezione per restringere la ricerca specificando in tutto o in parte nome dell'utente, indirizzo e-mail o i contenuti della Descrizione 729 dell'account. Lasciare vuoti questi campi se si desidera che i risultati della ricerca contengano tutti i gruppi e gli utenti corrispondenti ai Tipi di oggetto e alle Posizioni specificati sopra.

Includi account disabilitati
Selezionare questa casella di controllo se si desidera includere gli account disabilitati 729 nella ricerca.

Trova
Dopo aver specificato tutti i criteri di ricerca, fare clic su **Trova** per eseguire la ricerca.

Risultati ricerca
Dopo aver eseguito la ricerca, selezionare gli utenti o i gruppi desiderati nei Risultati della ricerca e fare clic su **OK** per aggiungerli all'ACL.

I diritti di accesso vengono controllati mediante le funzioni di supporto ACL (Access Control List) di MDaemon. Queste funzioni sono un'estensione del protocollo Internet Message Access Protocol (IMAP4) che consente di creare un elenco di accesso per ogni cartella di messaggi IMAP disponibile, accordando diritti di accesso a tali cartelle anche agli altri utenti che dispongono di un account sullo stesso server di posta. Se il client e-mail in uso non supporta ACL, è comunque possibile impostare le autorizzazioni mediante i comandi di questa finestra di dialogo.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo http://www.rfc-editor.org/rfc/rfc2086.txt.

Vedere:

Gestione cartelle pubbliche 317
Panoramica sulle cartelle pubbliche 120
Cartelle pubbliche e condivise 122
Account Editor » Cartelle condivise 757
Lista distribuzione » Cartelle pubbliche 306

3.6 Web e Servizi IM

3.6.1 Webmail

3.6.1.1 Panoramica

MDaemon Webmail è una soluzione e-mail basata su Web inclusa in MDaemon, progettata per offrire agli utenti funzionalità di client e-mail tramite il browser Web preferito. Webmail offre tutte le funzioni di un qualsiasi client di posta tradizionale, nonché un prezioso vantaggio aggiuntivo: consente agli utenti di accedere e utilizzare la posta elettronica ovunque e in qualsiasi momento, disponendo di Internet o di una connessione di rete. Poiché, inoltre, tutte le cartelle e-mail, i contatti, i calendari e così via risiedono nel server anziché nel computer locale, gli utenti dispongono di un accesso completo come se si trovassero alla propria scrivania.

MDaemon Webmail offre numerosi vantaggi agli amministratori di posta elettronica. Poiché Webmail non dipende da una workstation, è possibile configurare tutto mediante il server, a differenza di molte applicazioni client. In tal modo, non è necessario configurare e gestire i singoli client e-mail. È possibile inoltre personalizzare le immagini

grafiche e le pagine HTML utilizzate con Webmail in modo che soddisfino le specifiche esigenze dell'azienda o dei clienti. Inoltre, è possibile risparmiare tempo consentendo agli utenti di conservare le impostazioni del proprio account. In questo modo, l'amministratore di rete può decidere di accordare agli utenti una maggiore o minore responsabilità di gestione.

Infine, oltre ai vantaggi di un client basato sul Web, esistono molte altre funzioni utili per gli utenti, quali: funzionalità e-mail estese, interfaccia lato client disponibile in quasi 30 lingue, rubriche personali e globali, gestione di cartelle e filtri di posta, invio/ricezione di file allegati, numerosi "temi" grafici per l'interfaccia, temi per dispositivi mobili, funzioni di calendario, funzioni GroupWare, un'applicazione di messaggistica istantanea integrata da scaricare e installare sul desktop e molto altro ancora.

Funzioni di calendario e pianificazione

MDaemon è dotato di un sistema di collaborazione completo. È possibile creare appuntamenti, pianificare riunioni e gestire rubriche direttamente da Webmail. Sono pienamente supportate le funzioni dedicate agli appuntamenti ricorrenti, che possono essere descritti dettagliatamente tramite campi appositi. Inoltre, i contatti, i calendari e i dati sulle attività vengono archiviati sotto forma di cartelle IMAP nelle directory di coda principali degli utenti. Tramite Webmail, gli utenti possono accedere a queste cartelle personali e controllare quali altri utenti vi hanno accesso. In tutti i temi di Webmail sono disponibili modelli che consentono di presentare le cartelle dei contatti, del calendario, delle note e delle attività in modo più logico e intuitivo.

Grazie all'integrazione del sistema di calendario, è possibile creare notifiche e-mail per appuntamenti, anche pianificati da terze parti. Ogni volta che una terza parte pianifica un appuntamento per l'amministratore, questi riceve un messaggio e-mail di riepilogo. Al riguardo delle riunioni, ciascun partecipante riceve un messaggio e-mail che indica la data, l'ora e l'argomento della riunione e fornisce un elenco completo dei partecipanti. Inoltre, se nel calendario di un partecipante è previsto un evento in conflitto con la fascia oraria della riunione, viene inviato un messaggio di avviso per notificare l'impegno e la sovrapposizione di orario. L'organizzatore riceve un messaggio di riepilogo contenente tutti i dettagli della riunione e un elenco dei partecipanti (con e senza conflitti di orario).

Il sistema di calendario è inoltre dotato del supporto per Internet Calendar (iCal), utilizzato da Microsoft Outlook e da altri programmi e-mail compatibili con iCalendar ed è in grado di rilevare ed elaborare le informazioni di iCalendar inviate agli utenti e di utilizzarle per aggiornare i calendari. All'apertura di un allegato iCalendar da Webmail, le informazioni contenute nell'allegato vengono riprodotte nel calendario Webmail dell'utente. Inoltre, quando gli utenti creano dei nuovi appuntamenti o delle nuove riunioni, possono specificare uno o più indirizzi e-mail a cui desiderano sia inviato un messaggio e-mail iCalendar. I singoli utenti possono impostare questa funzione nelle opzioni Webmail.

MDaemon Instant Messenger

MDaemon Instant Messenger (MDIM) è il client di messaggistica istantanea protetta e applet della barra delle applicazioni di MDaemon che consente l'accesso rapido alle funzioni e-mail di Webmail. MDIM può essere scaricato da ciascun utente di Webmail e successivamente installato nei singoli computer locali. Poiché viene preconfigurato per

l'utente specifico al momento dello scaricamento, non richiede un livello approfondito di configurazione manuale.

MDIM, che viene eseguito in background, controlla l'account per l'eventuale presenza di nuovi messaggi interrogando direttamente il server Webmail. In questo modo, non è più necessario aprire un browser e mantenerlo aperto durante il controllo della posta. MDIM verifica se sono presenti nuovi messaggi e, in caso affermativo, ne trasmette notifica all'utente con un segnale acustico o visivo. In MDIM viene inoltre visualizzato un elenco delle cartelle di posta insieme al numero e al tipo di messaggi (nuovi, non letti e letti) contenuti in ognuna. Può essere inoltre utilizzato per avviare il browser e spostarlo immediatamente in una cartella di posta specifica.

MDIM è anche dotato di un client di messaggistica istantanea completo. È possibile visualizzare l'elenco dei contatti MDIM con il relativo stato (ad esempio, se online, disconnesso o assente), nonché avviare una conversazione con un singolo utente o un gruppo, impostare il proprio stato online e visualizzare le conversazioni precedenti in una cartella ordinata cronologicamente.

Per istruzioni più dettagliate, consultare la Guida in linea di MDaemon Instant Messenger.

Sistema di messaggistica istantanea di MDaemon Instant Messenger

MDIM è dotato di un client di messaggistica istantanea (IM) che utilizza il server XMPP 381 di MDaemon. Questa funzionalità consente di aggiungere altri utenti che condividono il dominio (e a scelta altri domini ospitati sul server MDaemon) all'elenco contatti MDIM e quindi di comunicare con essi immediatamente. È possibile impostare lo stato online, visualizzare lo stato dei contatti, utilizzare emoticon, impostare il colore del testo, inviare file, impostare il suono delle notifiche e controllare altre preferenze. Si può inoltre avviare una conversazione di gruppo coinvolgendo diversi contatti contemporaneamente. Le funzioni IM sono disponibili tramite il menu di scelta rapida dell'icona delle applicazioni e dalla finestra MDIM.

Al sistema IM di MDaemon Instant Messenger è inoltre possibile applicare gli script, in modo da creare un'interfaccia con eventuali programmi personalizzati. Grazie alla creazione di file semaforo (`SEM`) nella cartella \MDaemon\WorldClient\, un'applicazione esterna è in grado di inviare messaggi IM agli utenti di MDIM. Di seguito è riportato il formato del file SEM:

`A: utente1@esempio.com`	Indirizzo e-mail dell'utente di MDIM.
`Da: utente2@esempio.com`	Indirizzo e-mail del mittente del messaggio istantaneo.
`<riga vuota>`	
`Testo del messaggio istantaneo.`	Testo inviato come messaggio istantaneo.

Il nome del file `SEM` deve iniziare con i caratteri "`IM-`", seguiti da un valore numerico univoco. Ad esempio, "`IM-0001.SEM`". Le applicazioni devono creare un file corrispondente denominato "`IM-0001.LCK`" per bloccare il file `SEM`. Una volta completato il file `SEM`, rimuovere il file `LCK` per avviare l'elaborazione del file `SEM`. MDaemon utilizza questo metodo di script per inviare dei promemoria IM relativi ad appuntamenti e riunioni imminenti.

Il sistema Filtro contenuti è dotato di un'azione che invia i messaggi istantanei avvalendosi di questo metodo di script. Inoltre, le regole che utilizzano questa azione possono includere nel messaggio istantaneo le macro di Filtro contenuti. È possibile, ad esempio, creare una regola per l'invio di una regola di messaggio istantaneo con righe come quelle riportate di seguito:

```
Messaggio e-mail da $SENDER$.
Subject: $SUBJECT$
```

Questa regola rappresenta un modo efficace per inviare avvisi di nuovi messaggi mediante MDIM.

Molti amministratori non si avvalgono pienamente dei sistemi di messaggistica istantanea in azienda a causa dell'assenza di una gestione centralizzata e dell'impossibilità di monitorare il traffico IM nei client IM tradizionali e più diffusi. Il sistema di messaggistica istantanea di MDIM è stato progettato per ridurre al minimo queste limitazioni. Innanzitutto, il sistema non è di tipo peer-to-peer: i singoli client MDIM non si connettono direttamente l'uno all'altro per messaggi istantanei. Inoltre, poiché ogni messaggio istantaneo passa per il server, viene registrato in una posizione centrale accessibile all'amministratore di MDaemon. In questo modo, è possibile conservare una registrazione di tutte le conversazioni e garantire la sicurezza sia dell'azienda che degli utenti. L'attività IM è registrata in un file denominata `XMPPServer-<date>.log` posizionato nella directory`MDaemon\LOGS\`.

La funzione di messaggistica istantanea agisce a livello di singolo dominio. Il controllo globale per l'attivazione di messaggi istantanei è disponibile nella schermata MDIM 340 della finestra di dialogo di Webmail (Impostazioni » Web e servizi IM» Webmail » MDIM). È disponibile una schermata analoga in Domain Manager 194 che consente di attivare e disattivare questa funzione per domini specifici.

Skin di MDaemon Instant Messenger

L'interfaccia di MDIM è compatibile con gli skin *msstyles*, facilmente reperibili via Internet. Comprende numerosi stili, ma per installarne uno nuovo è necessario scaricare il file `*.msstyles` e inserirlo nella cartella `\Styles\` di MDIM, in una sottocartella che abbia lo stesso nome del file. Se, ad esempio, il file è stato denominato `Red.msstyles` il percorso sarà: "`\.\Styles\Red\Red.msstyles`"

Integrazione con Dropbox

È stata aggiunta una nuova schermata a Ctrl+W|Webmail|Dropbox. In questa schermata sono disponibili i controlli in cui è possibile inserire "Chiave app" e "Segreto app" di Dropbox nonché il testo di informativa sulla privacy. Sono tutti necessari per attivare il servizio integrato e vengono resi disponibili quando ci si registra a MDaemon Webmail come "app" Dropbox visitando il sito Web di Dropbox. L'operazione deve essere necessariamente eseguita dall'utente ma una sola volta. Consultare l'articolo 1166 della Knowledge Base per istruzioni complete su come registrare Webmail come app con Dropbox.

Dopo aver configurato "Chiave app" e "Segreto app", Webmail sarà in grado di connettere i relativi account all'account Dropbox. La prima volta che un utente accede al tema WorldClient o al tema LookOut, visualizzerà un menu a discesa nella parte superiore della pagina. L'utente ha tre opzioni, visualizzare il menu a discesa al

successivo accesso, non visualizzarlo mai più oppure andare alla nuova vista Opzioni | App Cloud. Nella vista Opzioni | App Cloud, l'utente può fare clic sul pulsante Configura Dropbox. Verrà visualizzato un menu a comparsa OAuth 2.0. Il menu a comparsa specifica in dettaglio ciò a cui l'utente si connette e le autorizzazioni richieste da Webmail. È anche disponibile un collegamento all'informativa sulla privacy e il pulsante "Connetti a Dropbox". Dopo aver fatto clic sul pulsante "Connetti a Dropbox", si passerà alla pagina di Dropbox. Se l'utente non è registrato a Dropbox, verrà visualizzato un sito in cui è possibile eseguire l'accesso o creare un account. Dopo aver completato questo passaggio, verrà visualizzata un'altra pagina Dropbox in cui viene chiesto se si desidera che Webmail abbia accesso completo all'account. Facendo clic su "Consenti", l'utente tornerà a Webmail e verrà informato se l'autorizzazione è riuscita o meno. L'autorizzazione è valida per una settimana dopo ogni visualizzazione della schermata e il token di accesso ricevuto viene utilizzato per la settimana successiva. Dopo aver completato l'autorizzazione, l'utente vedrà l'icona di Dropbox accanto a ciascun allegato del messaggio. Sarà sufficiente fare clic sull'icona perché l'allegato venga salvato nell'account Dropbox dell'utente nella cartella /WorldClient_Attachments.

Nella vista di composizione dei temi WorldClient e LookOut, gli utenti potranno scegliere i file dagli account Dropbox facendo clic sull'icona Dropbox nella barra degli strumenti dell'editor (in alto a sinistra). Questa funzione non richiede agli utenti di configurare l'accesso agli account in uso tramite la vista Opzioni | App Cloud e OAuth 2.0 ma solo "Chiave app" e "Segreto app".

Il supporto Dropbox è disattivato per impostazione predefinita ma è possibile riattivarlo nella schermata Dropbox 345 di MDaemon. Se si desidera attivare o disattivare Dropbox in base al singolo utente, è possibile eseguire l'operazione aggiungendo "DropboxAccessEnabled=Yes " al file User.ini.

Utilizzo di Webmail

Avvio di Webmail

Sono disponibili tre modi per avviare/arrestare il server Webmail:

1. Nella scheda Statistiche presente nel riquadro sinistro della GUI di MDaemon, fare clic con il pulsante destro del mouse sulla voce Webmail e scegliere l'opzione *Attiva/Disattiva* dal menu di scelta rapida.
2. Nell'interfaccia principale, fare clic su "File » Abilita server Webmail".
3. Selezionare "Impostazioni » Web e Servizi IM" nell'interfaccia principale, quindi fare clic su *Webmail in esecuzione con server Web incorporato* nella schermata Server Web.

Accesso a Webmail

1. Aprire mediante il browser la pagina `http://esempio.com:NumeroPortaWebmail`. NumeroPortaWC viene definito nella schermata Server Web 330 della sezione relativa a Webmail. Se si configura Webmail affinché utilizzi la porta Web predefinita (porta 80), non è necessario indicare il numero di porta nell'URL di accesso. In questo caso, è sufficiente specificare `www.esempio.com` invece di `www.esempio.com:3000`.
2. Digitare il nome utente e la password dell'account MDaemon.
3. Fare clic su Entra.

Modifica delle impostazioni della porta di Webmail

1. Selezionare "Impostazioni » Web e Servizi IM" sulla barra dei menu.
2. Digitare il numero della porta desiderata nella casella *Esegui il server Webmail su questa porta TCP.*
3. Fare clic su OK.

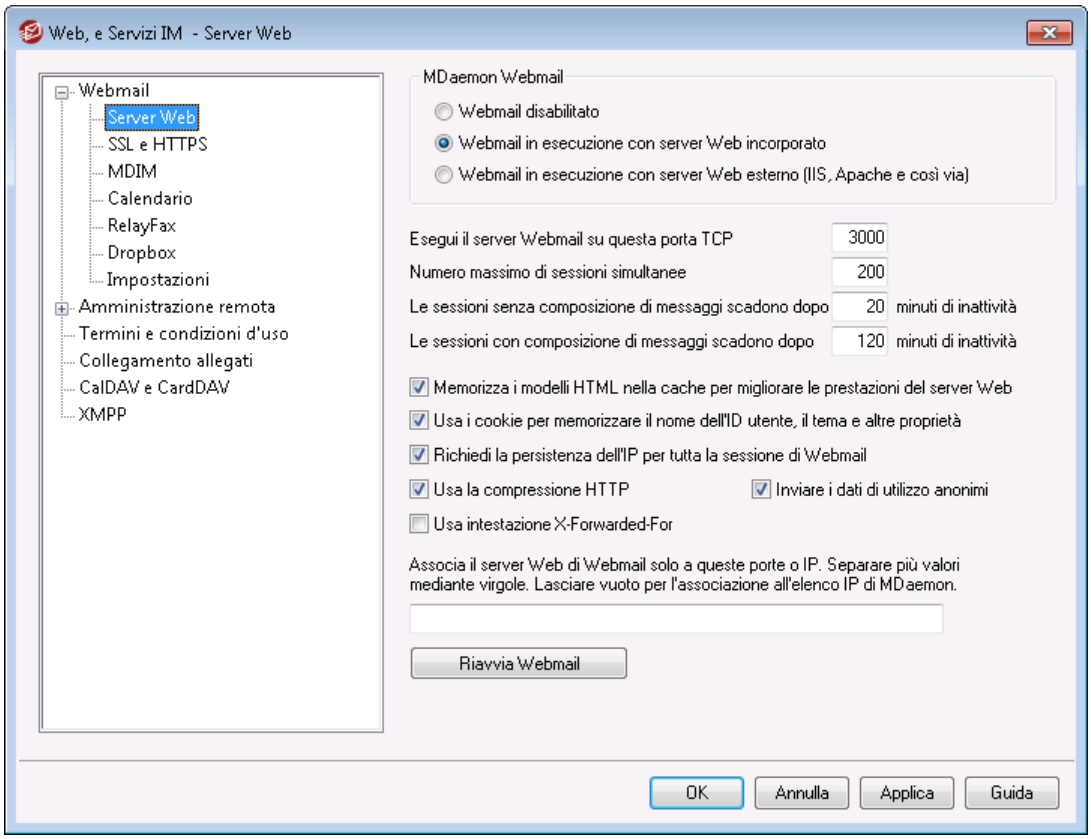
Guida del client

Webmail viene fornito con una guida completa delle funzioni lato client. Per informazioni sulle funzioni e sulle caratteristiche del client, consultare la Guida in linea di Webmail.

Per informazioni sulle altre opzioni della rubrica, vedere:

Webmail » MDIM 340
LDAP 844

3.6.1.2 Server Web



In questa schermata sono incluse diverse impostazioni globali a livello di server che consentono di controllare la configurazione e il comportamento di Webmail, a prescindere dagli utenti o dai relativi domini di appartenenza.

MDaemon Webmail

Webmail è disabilitato
Scegliere questa opzione per disabilitare Webmail. Il server Webmail può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon.

Per utilizzare la funzione Collegamento allegati 373, è necessario che Webmail sia attivo.

Webmail in esecuzione con server Web incorporato
Scegliere questa opzione per eseguire Webmail utilizzando il server Web incorporato di MDaemon. Il server Webmail può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon.

Webmail utilizza server Web esterni (IIS, Apache e così via)
Scegliere questa opzione se si desidera eseguire Webmail in Internet Information Server (IIS) o in un altro server Web diverso dal server incorporato di MDaemon. In questo modo, è possibile impedire l'accesso a elementi della GUI che potrebbero entrare in conflitto con il server alternativo.

Per ulteriori informazioni, vedere Esecuzione di Webmail con IIS 333

Avviare il server Webmail su questa porta TCP
È la porta da cui Webmail riceve le richieste di connessione provenienti dai browser degli utenti.

Numero massimo di sessioni simultanee
È il numero massimo di sessioni che possono connettersi contemporaneamente a Webmail.

Le sessioni senza composizione di messaggi scadono dopo xx minuti di inattività
Si tratta dell'intervallo di tempo durante il quale la sessione può rimanere inattiva (un utente ha effettuato l'accesso a Webmail ma non compone alcun messaggio di posta) prima che Webmail la chiuda.

Le sessioni con composizione di messaggi scadono dopo xx minuti di inattività
Questo timer stabilisce per quanto tempo la sessione dell'utente rimarrà aperta mentre viene composto il messaggio (e la sessione risulta inattiva). È buona norma impostare il timer su valori superiori rispetto a quelli definiti per le *sessioni in cui non vengono composti messaggi*, in quanto l'intervallo di inattività è normalmente superiore durante la composizione di un messaggio. La composizione di un messaggio non richiede infatti alcun tipo di comunicazione con il server finché il messaggio non viene inviato.

Memorizza i modelli HTML nella cache per migliorare le prestazioni del server Web
Selezionare questa casella di controllo se si desidera che Webmail memorizzi i modelli nella cache anziché leggerli ogni volta che è necessario accedervi. In questo modo è

possibile aumentare sensibilmente le prestazioni del server. Tuttavia, è necessario riavviare Webmail se si apportano delle modifiche a uno dei file di modello.

Usa i cookie per memorizzare il nome dell'ID utente, il tema e altre proprietà
Selezionare questa opzione se si desidera che Webmail memorizzi un cookie con il nome dell'ID utente, il tema e altre proprietà nel computer locale in uso. Questa funzione consente di offrire agli utenti un accesso più "personalizzato", a condizione che nei loro browser sia abilitato il supporto per i cookie.

Richiedi la persistenza dell'IP per tutta la sessione di Webmail
Come misura di sicurezza aggiuntiva, è possibile selezionare questa casella di controllo affinché Webmail limiti ciascuna sessione utente all'indirizzo IP da cui l'utente si è connesso all'inizio della sessione. Poiché è richiesta la persistenza dell'IP, nessuno può "appropriarsi" della sessione dell'utente. Questa configurazione è più sicura ma può causare problemi agli utenti che utilizzano un server proxy o una connessione Internet con assegnazione e modifica dinamiche degli indirizzi IP.

Usa intestazione X-Forwarded-For
Fare clic su questa casella di controllo per consentire l'uso dell'intestazione `X-Forwarded-For` che viene in alcuni casi aggiunta dai server proxy. L'opzione è disabilitata per impostazione predefinita. Attivarla solo se il server proxy inserisce questa intestazione.

Usa la compressione HTTP
Selezionare questa casella di controllo per utilizzare la compressione HTTP nelle sessioni Webmail.

Inviare i dati di utilizzo anonimi
Per impostazione predefinita Webmail invia i seguenti dati in forma anonima e destinati esclusivamente al miglioramento del prodotto: sistema operativo utilizzato, versione del browser utilizzata, lingua e così via. Questi dati vengono utilizzati da MDaemon Technologies per migliorare il funzionamento di Webmail. Se non si desidera inviare i dati di utilizzo, disabilitare questa opzione.

Associa il server Web di Webmail solo a questi IP/porte
Per limitare l'associazione del server Webmail solo a determinati indirizzi IP o porte, specificare gli indirizzi o le porte in questa casella separandoli con virgole. Utilizzare il formato: "`Indirizzo_IP:Porta`" per indicare la porta, ad esempio, `192.0.2.0:80`. Se non si include una porta, saranno utilizzate la porta TCP predefinita specificata sopra e la porta HTTPS predefinita specificata nella schermata SSL e HTTPS 336 . Se si desidera che Webmail rimanga in ascolto su tutte le porte, utilizzare "`*`". Ad esempio, indicando "`*,*:80`" Webmail rimane in attesa di connessioni da tutti gli indirizzi IP sulle porte predefinite specificate (3000 e 443), nonché di connessioni da tutti gli indirizzi IP sulla porta 80. Se si lascia vuoto questo campo, Webmail controlla tutti gli indirizzi IP specificati per i Domini 185.

Riavvia Webmail (se cambiano porte o parametri di IIS)
Fare clic su questo pulsante per riavviare il server Webmail. Nota: dopo la modifica delle impostazioni della porta di Webmail, è necessario riavviare Webmail per rendere effettive le nuove impostazioni.

3.6.1.2.1 Esecuzione di Webmail con IIS6

Poiché in Webmail è incorporato un server Web, Internet Information Server (IIS) non è richiesto. Webmail supporta comunque IIS e può pertanto funzionare come DLL ISAPI. Le informazioni riportate di seguito sulla configurazione di Webmail per il funzionamento con IIS6 sono state estratte dall'articolo #01465 della Knowledge Base di MDaemon sul sito www.mdaemon.com:

1. Aprire la console di gestione di IIS (Internet Information Services).
2. Fare clic con il pulsante destro del mouse su **Pool applicazioni**.
3. Fare clic su **Nuovo/Pool applicazioni**.
4. Assegnare al pool il nome **Alt-N** e scegliere il pulsante **OK**.
5. Fare clic con il pulsante destro del mouse su **Alt-N**.
6. Fare clic su **Proprietà**.
7. Fare clic sulla scheda **Prestazioni**.
8. Deselezionare le opzioni **Chiudi processi di lavoro dopo un periodo di inattività di (in minuti):** e **Limite massimo per la coda di richieste al kernel (numero di richieste)**.
9. Fare clic sulla scheda **Identità**.
10. Nell'elenco a discesa Predefinito scegliere **Servizio locale**.
11. Fare clic sul pulsante **OK**.
12. Fare clic con il pulsante destro del mouse su **Siti Web**.
13. Scegliere **Nuovo**.
14. Fare clic su **Siti Web**. Verrà avviata una procedura guidata.
15. Fare clic sul pulsante **Avanti**.
16. Digitare il nome del sito, ad esempio **Webmail**.
17. Fare clic sul pulsante **Avanti**.
18. Fare nuovamente clic sul pulsante **Avanti**.
19. Selezionare la home directory, corrispondente a **C:\MDaemon\WorldClient\HTML** nel caso di un'installazione predefinita.
20. Fare clic sul pulsante **Avanti**.
21. Accertarsi che siano selezionate le opzioni **Lettura**, **Esecuzione script** ed **Esecuzione**.
22. Fare clic sul pulsante **Avanti**.
23. Fare clic sul pulsante **Fine**.
24. Fare clic con il pulsante destro del mouse sul sito Web appena creato **(Webmail)**.
25. Scegliere **Proprietà**.
26. Fare clic sulla scheda **Documenti**.
27. Rimuovere tutti i documenti elencati.
28. Aggiungere **WorldClient.dll**.

29. Selezionare la scheda **Home directory**.
30. Nell'elenco a discesa Pool applicazioni, scegliere **Alt-N**.
31. Fare clic sul pulsante **OK**.
32. Fare clic su **Estensioni servizio Web**.
33. Abilitare **tutte le estensioni ISAPI sconosciute** o creare una nuova estensione relativa a **WorldClient.DLL**.

È necessario assegnare all'account Internet Guest, ossia a **IUSER_<SERVER_NAME>**, le autorizzazioni NTFS **Controllo completo** relative alla directory MDaemon e a tutte le relative sottodirectory.

1. Fare clic con il pulsante destro del mouse sulla directory MDaemon. (C:\MDaemon)
2. Scegliere **Proprietà**.
3. Selezionare la scheda **Sicurezza**.
4. Fare clic sul pulsante **Aggiungi**.
5. Fare clic sul pulsante **Avanzate**.
6. Fare clic sul pulsante **Trova**.
7. Selezionare **IUSER_<SERVER_NAME>** (in cui "<SERVER_NAME>" è il nome del computer locale).
8. Fare clic sul pulsante **OK**.
9. Fare clic sul pulsante **OK**.
10. Selezionare la casella **Controllo completo**.
11. Fare clic sul pulsante **OK**.

È necessario seguire questa procedura per tutte le directory da utilizzare con MDaemon.

Durante gli aggiornamenti di MDaemon successivi all'impostazione Web:

1. Aprire la console di gestione di IIS (Internet Information Services).
2. Aprire l'elenco **Pool applicazioni**.
3. Fare clic con il pulsante destro del mouse su **Alt-N**.
4. Scegliere **Arresta**.
5. Chiudere MDaemon.
6. Installare l'aggiornamento.
7. Al termine dell'installazione, riavviare MDaemon.
8. Nella console di gestione di IIS, fare clic con il pulsante destro del mouse su **Alt-N**.
9. Scegliere **Avvia**.

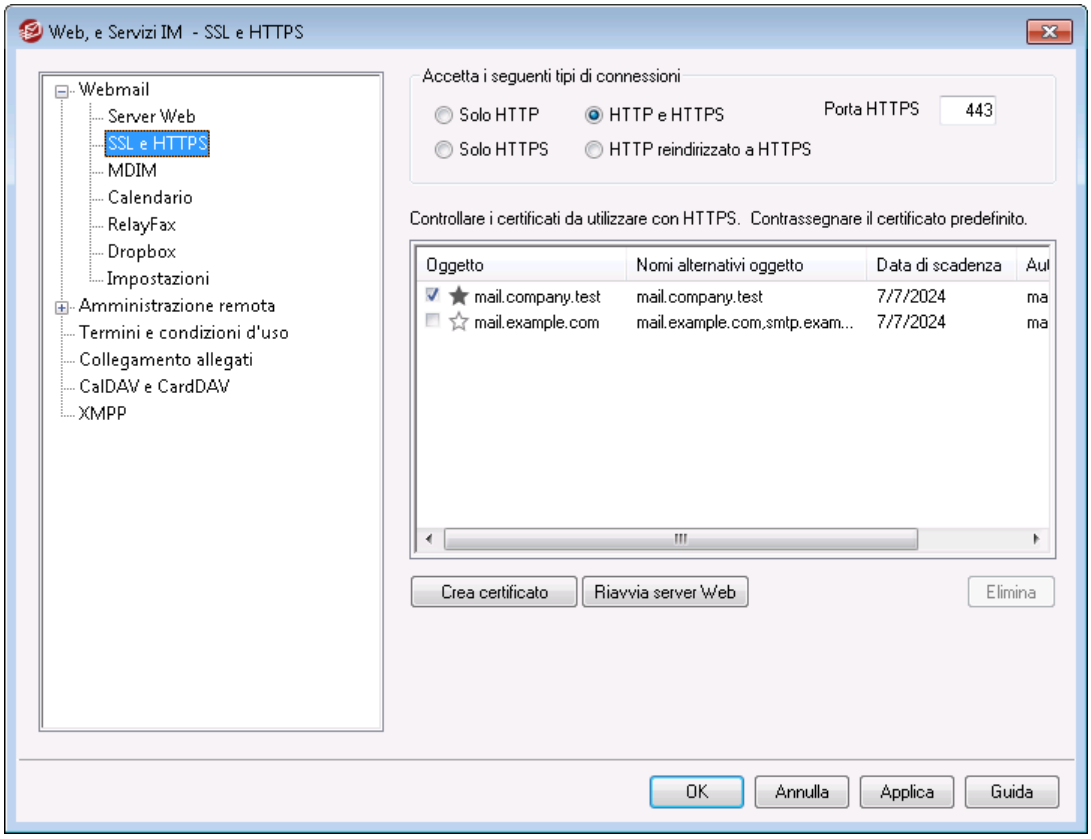
Se la procedura precedente è stata seguita correttamente, avviene quanto riportato di seguito.

1. Dopo l'arresto di **Pool applicazioni**, viene visualizzato un messaggio che informa che il **servizio non è disponibile**.
2. La procedura descritta riduce al minimo l'eventualità di dover riavviare il computer dopo un aggiornamento di MDaemon.

La configurazione di questo programma con IIS NON è supportata dall'assistenza tecnica e i clienti che decidono di eseguire Webmail con IIS devono essere consapevoli di tutti i problemi di sicurezza e delle implicazioni dell'esecuzione delle applicazioni con IIS. Prima di installare Webmail come estensione ISAPI è consigliabile installare tutte le correzioni e gli aggiornamenti di IIS.

Quando viene eseguito con IIS, Webmail non può essere avviato e chiuso dall'interfaccia di MDaemon. È necessario utilizzare gli strumenti forniti con IIS.

3.6.1.3 SSL/HTTPS



Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). SSL è il metodo standard per la protezione delle comunicazioni Web tra server e client. e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare Webmail per l'utilizzo di HTTPS si trovano nella schermata SSL & HTTPS accessibile da Impostazioni » Web e Servizi IM » Webmail". Per comodità, tuttavia, queste opzioni sono anche riportate in "Sicurezza » Security Manager » SSL & TLS » Webmail".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 585

Questa finestra di dialogo è valida per Webmail solo quando si utilizza il server Web incorporato di MDaemon. Se si configura Webmail per l'uso con un altro server Web come IIS, queste opzioni non saranno utilizzate. Il supporto SSL/HTTPS dovrà essere configurato utilizzando gli altri strumenti per i server

web.

Accetta i seguenti tipi di connessioni

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a Webmail. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in Webmail e non si desidera imporre agli utenti di Webmail l'utilizzo di HTTPS. Webmail rimane in attesa di connessioni sulla porta HTTPS indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta TCP di Webmail definita nella schermata Server Web 330 di Webmail.

Solo HTTPS
Scegliere questa opzione se si desidera che HTTPS sia il protocollo richiesto al momento della connessione a Webmail. Se si attiva questa opzione, Webmail risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da Webmail per le connessioni SSL. Il valore predefinito della porta SSL è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di Webmail (vale a dire, "https://example.com" è equivalente a "https://example.com:443").

Questa porta è diversa dalla porta di Webmail definita nella scheda Server Web 330. Se le connessioni HTTP a Webmail sono consentite, devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

Seleziona certificato da usare per HTTPS/SSL

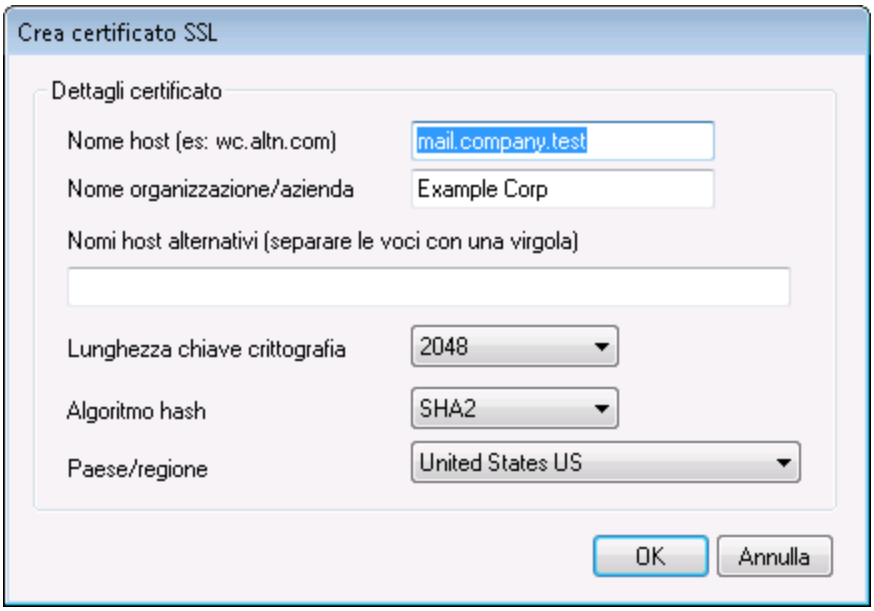
Questa casella consente di visualizzare i certificati SSL. Selezionare la casella di controllo accanto ai certificati che si intende attivare. Fare clic sulla stella accanto a quello che si desidera impostare come certificato predefinito. MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito. Fare doppio clic su un certificato per aprirlo nella finestra di dialogo Certificato di Windows e visualizzarne i dettagli (funzionalità

disponibile solo nell'interfaccia dell'applicazione, non nell'amministrazione remota basata su browser).

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Crea certificato

Fare clic su questo pulsante per aprire la finestra di dialogo Crea certificato SSL.



Dettagli certificato

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà

> i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto. Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Algoritmo hash
Scegliere l'algoritmo hash che si desidera utilizzare: SHA1 o SHA2. L'impostazione predefinita è SHA2.

Riavvia server Web

Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare un nuovo certificato, è necessario riavviare il server Web.

Utilizzo di Let's Encrypt per la gestione del certificato

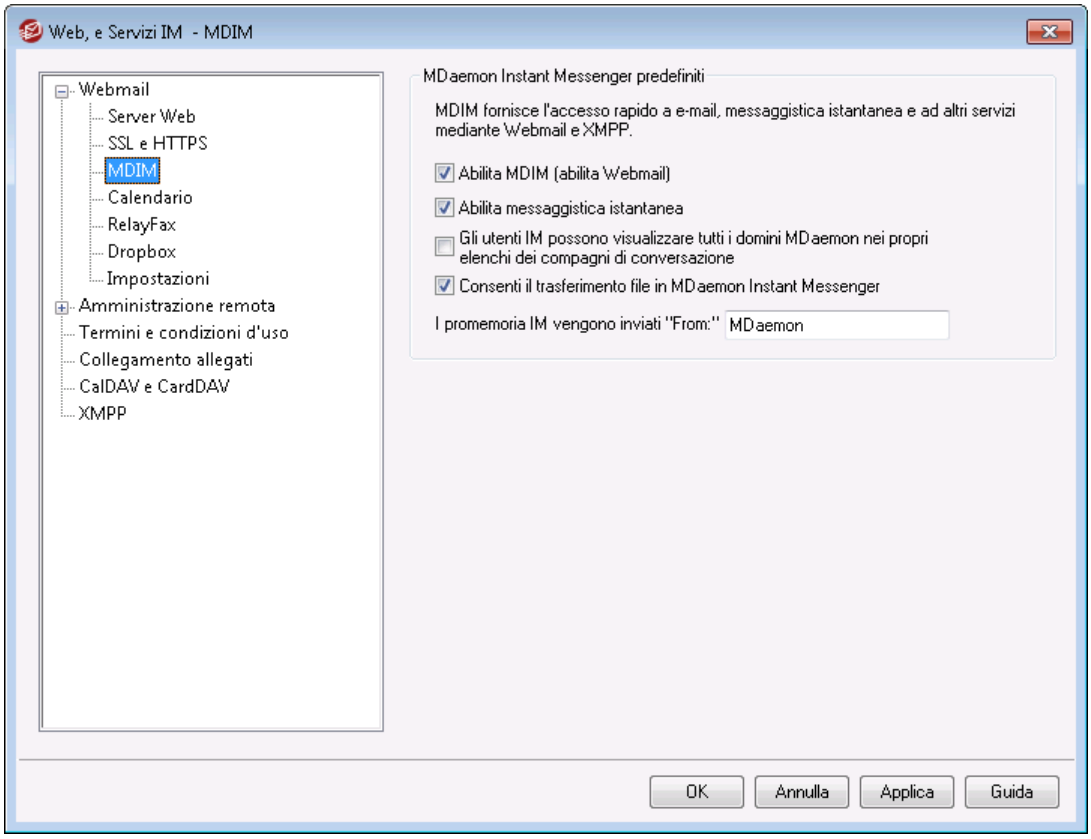
Let's Encrypt è un'autorità di certificazione (CA) che fornisce certificati gratuiti mediante un processo automatizzato che si pone la finalità di eliminare i processi più complessi di creazione, convalida, firma, installazione e rinnovo manuali dei certificati per i siti Web sicuri.

Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un certificato, è disponibile la schermata Let's Encrypt 605 che consente di configurare ed eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP 188 del dominio predefinito 185 come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica. Vedere l'argomento Let's Encrypt 605 per ulteriori informazioni.

Vedere:

SSL e certificati 585
Creazione e uso dei certificati SSL 928

3.6.1.4 MDIM



Questa schermata consente di controllare le impostazioni predefinite dei nuovi domini per MDaemon Instant Messenger (MDIM) 326. È possibile modificare le impostazioni di specifici domini nella schermata MDIM 194 di Domain Manager. È possibile abilitare o disabilitare i servizi MDaemon Instant Messenger per account o gruppi specifici tramite le schermate Servizi Web 735 e Proprietà gruppo 798.

Impostazioni predefinite di MDaemon Instant Messenger

Abilita MDIM (abilita Webmail)
Attivare questa opzione se si desidera rendere disponibile MDaemon Instant Messenger per il download da Webmail per impostazione predefinita. L'utilità può essere scaricata dalla pagina *Opzioni » MDaemon Instant Messenger*. Il file di installazione scaricato viene personalizzato automaticamente in base all'account di ciascun utente, così da facilitare l'installazione e la configurazione. Questa opzione rende possibile per MDIM l'uso delle funzionalità delle cartelle My Mail, consentendo all'utente di controllare la presenza di nuovi messaggi e aprire Webmail direttamente dal menu di scelta rapida di MDIM. MDIM è attivato per impostazione predefinita.

Abilita messaggistica istantanea
Per impostazione predefinita, gli account possono utilizzare MDIM e i client XMPP 381 di terze parti per scambiare messaggi istantanei con altri membri del dominio. Se non si desidera consentire l'uso di messaggi istantanei, deselezionare questa casella di controllo.

Gli utenti IM vedono tutti i domini MDaemon nei propri elenchi amici
Fare clic su questa opzione se si desidera consentire agli utenti di aggiungere contatti nei propri elenchi amici da tutti i domini MDaemon. Quando questa opzione è disattivata, i contatti devono essere nello stesso dominio. Ad esempio, se MDaemon esegue l'hosting della posta di esempio.com ed esempio.org, attivando questa opzione gli utenti potranno aggiungere i contatti di messaggistica istantanea da entrambi i domini. Disattivare l'opzione significa invece che gli utenti esempio.com possono aggiungere solo altri utenti di esempio.com e gli utenti esempio.org aggiungere solo utenti di esempio.org. L'opzione è disabilitata per impostazione predefinita. È disponibile un'opzione equivalente in Domain Manager 194 che consente di attivare e disattivare questa funzione per domini specifici.

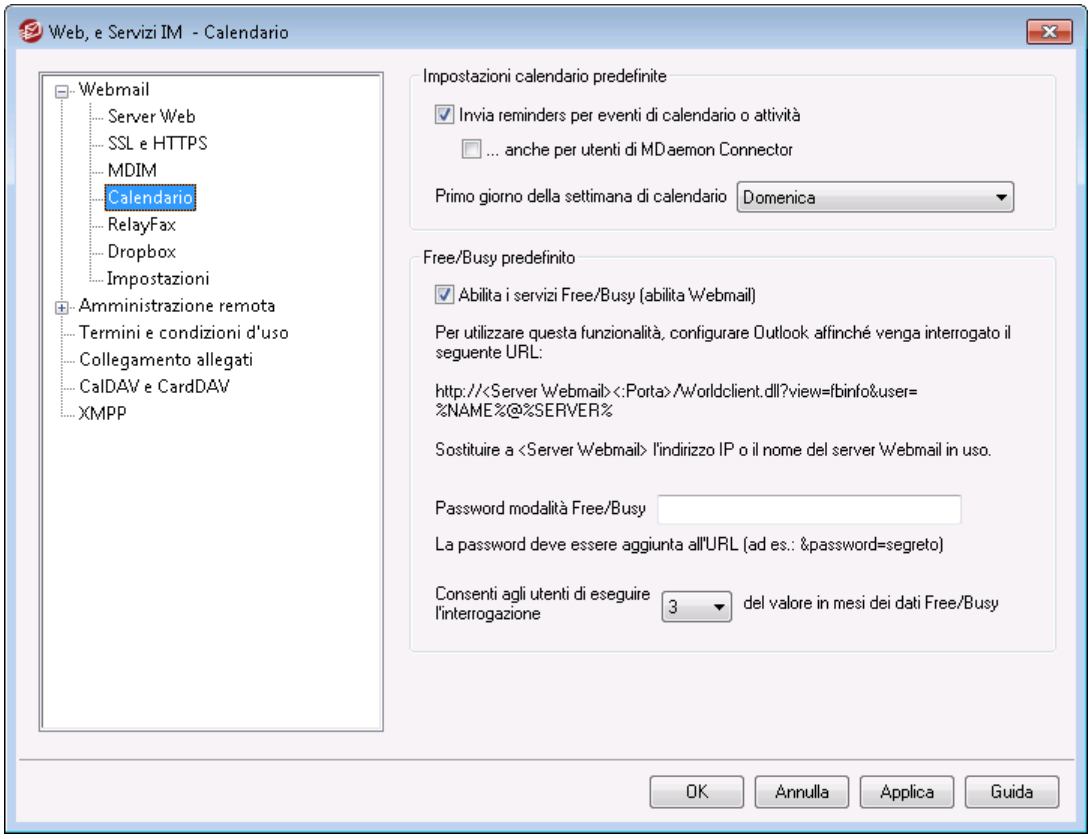
Consenti trasferimenti file in MDaemon Instant Messenger
Per impostazione predefinita, gli utenti MDIM possono trasferire file ai contatti MDIM. Deselezionare questa casella di controllo se non si desidera consentire l'utilizzo di MDIM per trasferire file.

Promemoria IM inviati con 'From:'
Quando sul calendario di un utente di Webmail è pianificato un appuntamento, l'evento può essere impostato per inviare un promemoria all'utente a un'ora specifica. Se per il dominio dell'utente il sistema IM è attivo, il promemoria verrà inviato in un messaggio istantaneo all'utente. Utilizzare questa casella di testo per specificare che si desidera che il messaggio compaia come proveniente dall'indirizzo indicato nel campo "`Da:`". Questa è l'impostazione predefinita per i nuovi domini. È possibile cambiarla per domini specifici tramite la schermata MDaemon Instant Messenger 194.

Vedere:

Domain Manager » MDaemon Instant Messenger 194
Account Editor » Servizi Web 735
Proprietà gruppo 798

3.6.1.5 Calendario



Questa schermata consente di controllare le impostazioni predefinite per le funzioni di calendario di MDaemon. È possibile controllare le impostazioni di specifici domini nella schermata Calendario[196] di Gestione domini.

Impostazioni calendario predefinite

Invia reminder per eventi di calendario o attività
Selezionare questa casella di controllo per consentire l'invio agli utenti del calendario e dei promemoria delle attività di Webmail tramite posta elettronica e MDaemon Instant Messenger.

...anche a utenti MDaemon Connector
Se l'opzione "*Invia promemoria per eventi di calendario o attività*" è attivata, selezionare questa opzione se si desidera attivare i promemoria anche per gli utenti MDaemon Connector[395].

Primo giorno della settimana
Scegliere un giorno dall'elenco a discesa. La selezione verrà visualizzata nei calendari come primo giorno della settimana.

Free/Busy predefinito

MDaemon include un server Free/Busy che consente a un pianificatore di riunioni di visualizzare la disponibilità dei potenziali partecipanti. Per accedere a questa

funzione, fare clic su Pianificazione in Webmail quando si crea un nuovo appuntamento. Viene aperta la finestra Pianificazione che contiene l'elenco dei partecipanti e una griglia calendario con codifica cromatica che presenta una riga per ciascuno dei partecipanti. La riga di ciascun partecipante è contraddistinta da un colore specifico a indicare gli orari in cui questi sarà disponibile per una riunione. Ai colori corrispondono le modalità Occupato, Incerto, Fuori sede e Nessuna informazione. Con il pulsante Passa al successivo è inoltre possibile interrogare il server a proposito della successiva fascia oraria in cui tutti i partecipanti potrebbero essere disponibili. Al termine della creazione dell'appuntamento, verrà inviato un invito a tutti i partecipanti che potranno quindi accettarlo o declinarlo.

Il server Free/Busy di Webmail è inoltre compatibile con Microsoft Outlook. Per utilizzarlo, configurare Outlook affinché venga interrogato il seguente URL per cercare dati relativi alla disponibilità. Ad esempio, in Outlook 2002 le opzioni Free/Busy si trovano in "Strumenti » Opzioni » Opzioni calendario... » Opzioni disponibilità..."

URL del server Free/Busy per Outlook:

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Sostituire "<Webmail>" con l'indirizzo IP o il nome dominio del server Webmail e "<:Port>" con il relativo numero di porta se non si utilizza la porta Web predefinita. Ad esempio,

```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Per ulteriori informazioni sull'utilizzo delle funzioni di Free/Busy di Webmail per la pianificazione degli appuntamenti, vedere la Guida in linea di Webmail.

Abilita i servizi Free/Busy
Fare clic su questa opzione se si desidera consentire l'accesso alle funzioni del server Free/Busy agli utenti.

Password modalità Free/Busy
Per richiedere una password agli utenti che tentano di accedere alle funzioni del server Free/Busy tramite Outlook, inserire la password in questo campo. È necessario aggiungere la password all'URL (nel formato: "&password=FBServerPass") quando vengono configurate le impostazioni di disponibilità in Outlook. Ad esempio,

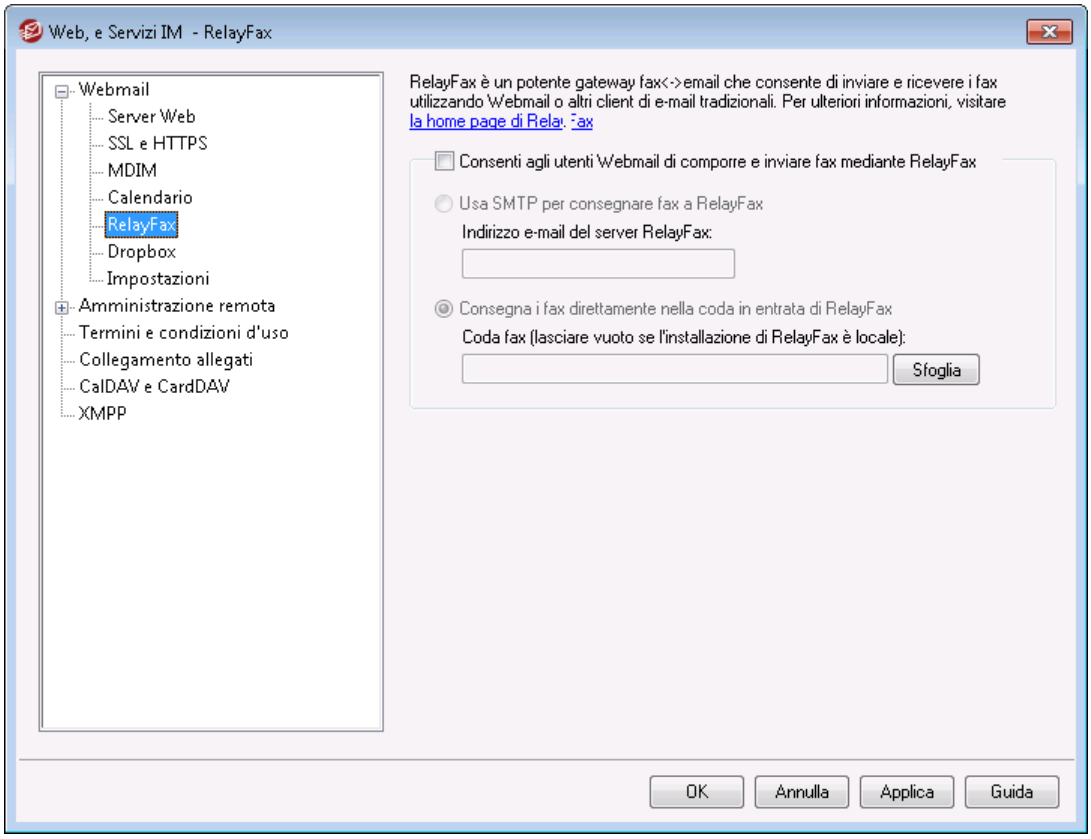
```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

Consenti agli utenti di eseguire l'interrogazione del valore in mesi dei dati Free/Busy
Utilizzare questa opzione per specificare l'intervallo dei dati relativi alla disponibilità che è possibile interrogare, espresso in numero di mesi.

Vedere:

Gestione domini » Calendario 196

3.6.1.6 RelayFax



Il server RelayFax di MDaemon Technologies è un gateway e-mail verso fax o fax verso e-mail, che può essere efficacemente integrato con Webmail per offrire servizi agli utenti. Quando questa funzionalità è abilitata, gli utenti di Webmail possono accedere a una serie di risorse per la composizione e l'invio di fax dalle schermate del client Webmail. Per ulteriori informazioni, visitare la sezione RelayFax del sito www.mdaemon.com.

Opzioni di integrazione di RelayFax

Consenti all'utente Webmail di creare e inviare fax con RelayFax
Selezionare questa opzione per integrare RelayFax con Webmail. Una volta attivato il server RelayFax, nelle pagine di Webmail vengono visualizzati il comando Componi fax e altre funzioni correlate.

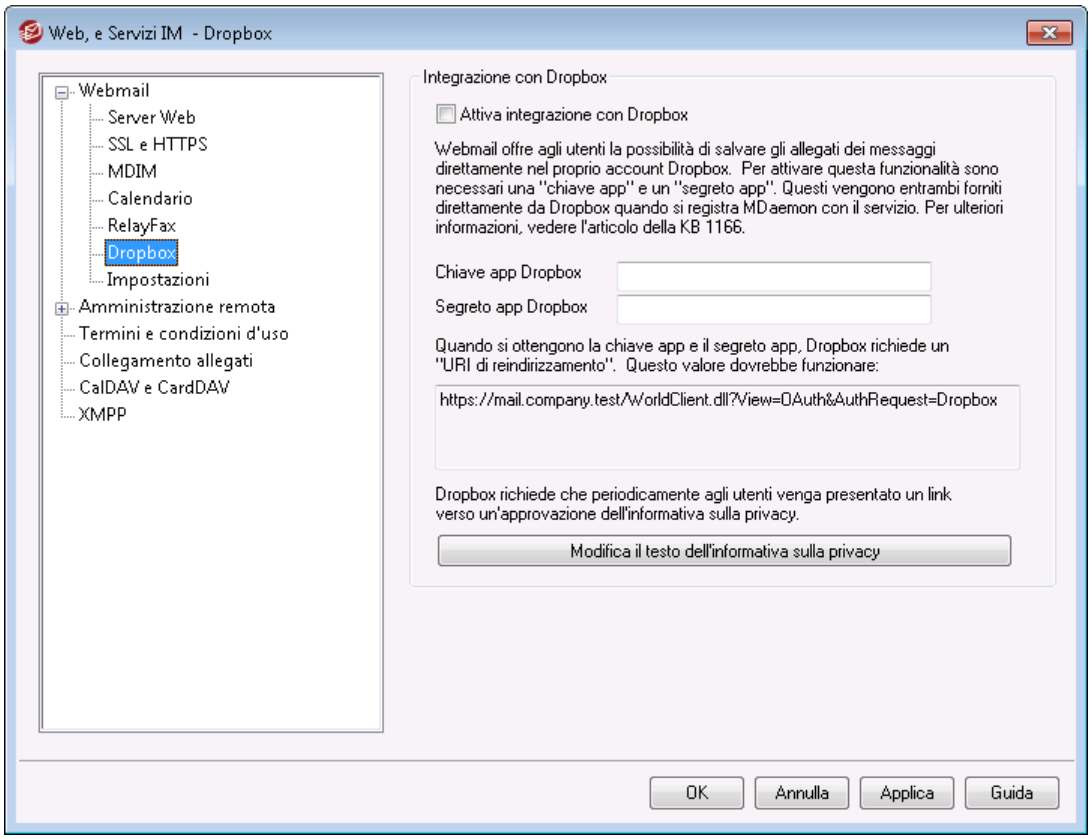
Usa SMTP per consegnare fax a RelayFax
Il server RelayFax controlla una specifica casella postale per verificare la presenza di messaggi in entrata da trasmettere via fax. Selezionare questa opzione affinché MDaemon invii tali messaggi all'indirizzo della casella postale in questione mediante il normale processo di trasmissione SMTP. Questa opzione è utile quando il server RelayFax controlla una casella postale non situata nella rete LAN in uso. Se il server RelayFax è installato nella rete in uso, è possibile impostare MDaemon affinché trasmetta i messaggi direttamente alla coda di posta del server RelayFax, saltando l'intero processo di trasmissione SMTP. Per ulteriori informazioni, vedere *Consegna i fax direttamente nella coda in entrata di RelayFax* più avanti in questo capitolo.

Indirizzo e-mail del server RelayFax
In questo campo viene specificato l'indirizzo e-mail a cui consegnare i messaggi trasmessi via fax. Il valore deve corrispondere all'indirizzo specificato in RelayFax per il monitoraggio di questo tipo di messaggi.

Consegna i fax direttamente nella coda in entrata di RelayFax
Se il server RelayFax è residente sulla LAN in uso, per la distribuzione dei messaggi da inviare via fax è possibile scegliere questo metodo anziché la trasmissione SMTP. Quando il server MDaemon riceve un messaggio destinato a RelayFax, lo consegna direttamente nella coda in entrata di RelayFax, anziché trasmetterlo via SMTP.

Coda fax
Se il server RelayFax è installato nello stesso sistema su cui è in esecuzione il server MDaemon, il campo del percorso del file può essere lasciato vuoto; in caso contrario, è necessario specificare il percorso di rete della directory \app\ del server RelayFax.

3.6.1.7 Dropbox



Webmail dispone di supporto diretto per Dropbox, che consente agli utenti di salvare allegati di file nei relativi account Dropbox e di inserire collegamenti diretti ai file Dropbox nei messaggi in uscita. Per fornire questa funzione agli utenti Webmail, è necessario impostare Webmail come app Dropbox sulla Guida degli sviluppatori della

piattaforma Dropbox. Si tratta di un processo semplice che richiede solo di registrarsi a un account Dropbox, di creare un nome univoco per una app con l'accesso Dropbox completo, di specificare l'URI di reindirizzamento a Webmail e di modificare un'impostazione predefinita. Si dovranno quindi copiare e incollare la Chiave app e il Segreto app di Dropbox nelle opzioni della schermata associata in MDaemon. Dopodiché gli utenti saranno in grado di collegare gli account Dropbox a Webmail quando accedono a Webmail. Per le istruzioni dettagliate su come creare la app Dropbox e il collegamento a Webmail vedere: Creazione e collegamento alla app Dropbox 347 di seguito.

Quando si crea la app Dropbox lo stato iniziale sarà "Sviluppo". Ciò consente a un massimo di 500 utenti Webmail di collegare gli account Dropbox all'app. Secondo Dropbox, comunque, "dopo che l'app ha collegato 50 utenti Dropbox, per due settimane si potrà richiedere e ricevere l'approvazione allo stato Produzione prima che venga bloccata all'app la possibilità di collegare altri utenti Dropbox indipendentemente da quanti collegamenti compresi tra 0 e 500 abbia già eseguito". Ciò significa che finché non si riceve l'approvazione per la produzione, l'integrazione con Dropbox continuerà a funzionare ma nessun altro utente sarà in grado di collegare il proprio account. Dopo aver ricevuto l'approvazione per la produzione, sarà semplice accertarsi che l'app sia conforme alle linee guida e ai termini di servizio di Dropbox. Per ulteriori informazioni, vedere la sezione Approvazione per la produzione della Guida dello sviluppatore per piattaforma Dropbox.

Dopo aver creato e configurato correttamente la app Webmail, ciascun utente Webmail avrà la possibilità di connettere il proprio account all'account Dropbox quando accede a Webmail. All'utente viene richiesto di accedere a Dropbox e di concedere alla app l'autorizzazione di accesso all'account Dropbox. A questo punto l'utente verrà reindirizzato a Webmail tramite un URI trasferito a Dropbox durante il processo di autenticazione. Per motivi di sicurezza all'URI dovrà corrisponda uno degli URI di reindirizzamento (vedere di seguito) specificati nella pagina di informazioni dell'app all'indirizzo Dropbox.com. Infine, Webmail e Dropbox si scambieranno un codice e un token di accesso, il che consentirà a Webmail di connettersi all'account Dropbox dell'utente in modo che quest'ultimo possa salvare gli allegati in questa posizione. Il token di accesso scambiato scade ogni sette giorni, quindi l'utente periodicamente dovrà riautorizzare l'account all'uso di Dropbox. Inoltre gli utenti possono disconnettere manualmente i propri account da Dropbox o riautorizzarli se necessario, dalla schermata delle opzioni App Cloud in Webmail.

Integrazione con Dropbox

Attiva integrazione con Dropbox

Dopo aver creato la app Dropbox e averla collegata a Webmail, fare clic su questa casella di controllo per consentire agli utenti Webmail di collegarsi agli account Dropbox. Se si desidera, è possibile attivare o disattivare Dropbox in base al singolo utente aggiungendo "`DropboxAccessEnabled=Yes` (o `No`)" al file `User.ini`.

Chiave app e Segreto app di Dropbox

Chiave app e Segreto app si trovano nella pagina di informazioni dell'app all'indirizzo Dropbox.com. Inserire qui il collegamento Webmail alla app Dropbox.

URI di reindirizzamento

È necessario specificare un URI di reindirizzamento nella pagina di informazioni dell'app all'indirizzo Dropbox.com. MDaemon visualizza automaticamente in questo

campo un URI che l'utente dovrebbe essere in grado di utilizzare. Tuttavia è possibile aggiungere più URI di reindirizzamento. Pertanto è possibile aggiungere un URI per ciascun dominio e anche uno per l'host locale che può essere utilizzato per accedere a Webmail dal computer su cui il server è in esecuzione.

Ad esempio:

```
https://mail.company.test/WorldClient.dll?
    View=OAuth&AuthRequest=Dropbox

https://example.com/WorldClient.dll?
    View=OAuth&AuthRequest=Dropbox

https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
```

Dropbox richiede che gli URI di reindirizzamento siano protetti, pertanto HTTPS 336 deve essere attivato per Webmail.

Modifica il testo dell'informativa sulla privacy
Fare clic su questo pulsante per modificare il file di testo contenente l'informativa sulla privacy della app Webmail. Poiché Dropbox richiede che una informativa sulla privacy approvata venga presentata periodicamente agli utenti, è disponibile un collegamento "Informativa sulla privacy" ai contenuti di questo file nella pagina **Connetti a Dropbox** visualizzata dagli utenti. Il collegamento visualizza una piccola finestra contenente il testo e un pulsante Scarica su cui gli utenti possono fare clic per scaricare il file. Utilizzare il codice HTML nel file se si desidera formattare il testo se si desidera includere eventuali collegamenti.

Creazione e collegamento alla app Dropbox

Istruzioni dettagliate per la creazione dell'app Dropbox e il collegamento a Webmail.

1. Nel browser passare alla Piattaforma Dropbox
2. Accedere all'account Dropbox
3. Scegliere **API Dropbox**
4. Scegliere **Dropbox complesso**
5. Assegnare all'app un nome univoco
6. Fare clic su **Crea app**.
7. Fare clic su **Abilita utenti aggiuntivi** e quindi su **OK**
8. Cambiare **Consenti concessione implicita** in **Non consentire**
9. Inserire uno o più URI di reindirizzamento facendo clic su **Aggiungi** dopo ciascuno di essi. Devono essere URL sicuri a Webmail (HTTPS deve essere attivato in Webmail).

   Ad esempio:

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

10. Lasciando il browser aperto sulla pagina di informazioni dell'app, aprire la GUI di MDaemon
11. Fare clic su **Impostazioni**
12. Fare clic su **Web e servizi IM**
13. Fare clic su **Dropbox** in **Webmail**
14. Copiare/incollare **Chiave app** e **Segreto app** dal browser nella schermata **Dropbox** di MDaemon.
15. Fare clic su **Applica**
16. Fare clic su **OK**

Per istruzioni sul collegamento di un account utente Webmail all'account Dropbox dell'utente, vedere la Guida in linea di Webmail o l'articolo 1166 della Knowledge Base.

3.6.1.8 Google Drive

Questa pagina è disponibile solo nell'interfaccia Web di MDaemon Remote Administration 359 (MDRA).

Integrazione con Google Drive

MDaemon Webmail può offrire agli utenti la possibilità di salvare gli allegati dei messaggi direttamente nel proprio account di Google Drive e di modificare e lavorare con i documenti che archiviano. Per attivare questa funzionalità, sono necessari **chiave API**, **ID del client** e **segreto client**. Tutti questi dati si ottengono direttamente da Google creando un'app con la Google API Console e registrando il proprio MDaemon presso l'apposito servizio. Di questa app fa parte un componente di autenticazione OAuth 2.0, che consente agli utenti di accedere a Webmail e di autorizzare quindi l'accesso degli utenti ai rispettivi account Google Drive mediante MDaemon. Una volta autorizzati, gli utenti possono visualizzare le cartelle e i file archiviati su Google Drive. Inoltre, gli utenti possono caricare, scaricare, spostare, copiare, rinominare ed eliminare file, nonché copiare/spostare file da e verso le cartelle di documenti locali. Per modificare un documento, l'utente può fare clic sull'opzione per visualizzare il file in Google Drive e modificarlo in base alle autorizzazioni impostate in Google Drive. Il processo di configurazione di Google Drive è simile all'Integrazione Dropbox 345 di MDaemon e alle funzionalità di integrazione MultiPOP OAuth 146.

Attiva integrazione con Google Drive
Fare clic su questa casella di controllo per attivare l'integrazione con Google Drive. Vedere: **Configurazione dell'integrazione con Google Drive** di seguito.

Chiave API Google Drive:
Questa è la chiave API univoca che verrà generata nella console Google Drive API durante la creazione dell'app.

ID client Google Drive
È l'ID client univoco assegnato all'app Google Drive quando questa viene creata nella console API di Google. Dopo aver creato l'app, copiare il relativo ID client e incollarlo qui.

Segreto client Google Drive
È il segreto client univoco assegnato all'app Google Drive quando questa viene creata nella console API di Google. Dopo aver creato l'app, copiare il relativo Segreto client e incollarlo qui.

URI di reindirizzamento
Quando si crea l'app Google Drive è necessario specificare uno o più URI di reindirizzamento. L'URI di reindirizzamento di esempio è costruito a partire dal nome host SMTP del dominio predefinito 185 *** 188, che dovrebbe funzionare per gli utenti di quel dominio che accedono a Webmail. È necessario aggiungere altri URI di reindirizzamento all'app per qualsiasi altro dominio MDaemon che gli utenti utilizzano per accedere a Webmail. Ad esempio, "`https://mail.esempio.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" funziona per tutti gli utenti che utilizzano `mail.esempio.com` per accedere a Webmail. Vedere: **Creazione e collegamento dell'app Google Drive** di seguito per ulteriori informazioni.

Modifica il testo dell'informativa sulla privacy
L'integrazione con Google Drive impone di presentare periodicamente ai propri utenti un collegamento verso un'informativa sulla privacy approvata. Fare clic su questo pulsante per modificare l'informativa sulla privacy.

Creazione e collegamento dell'app Google Drive

Istruzioni dettagliate per la creazione e il collegamento dell'app Google Drive.

Attenersi alla procedura riportata di seguito per creare un'app Google che consenta agli utenti di accedere a Google Drive dall'interno di Webmail nella pagina **Documenti**.

1. Accedere a MDaemon Remote Administration 359 e passare alla pagina Google Drive (sotto la voce Principale » Impostazioni Webmail), quindi attivare l'opzione **Attiva integrazione con Google Drive**.
2. In una scheda del browser separata, accedere al proprio account Google e passare alla sezione Console API Google.
3. Dall'interno dell'elenco dei progetti, fare clic su **NUOVO PROGETTO** oppure, dalla pagina di gestione delle risorse, fare clic su **(+) CREA PROGETTO**.
4. Digitare un **nome del progetto,** ad esempio "Google Drive per MDaemon", quindi fare clic su **Modifica** per modificare l'ID del progetto oppure lasciarlo impostato sul valore predefinito. **Nota:** l'ID del progetto non può essere modificato dopo la creazione.
5. Se si dispone di una risorsa organizzazione, selezionarla in **Posizione**. In caso contrario, lasciare il campo impostato su "Nessuna organizzazione".
6. Dopo il caricamento, fare clic su **+ ABILITA API E SERVIZI**.

7. Nel campo di ricerca digitare "Google Drive", scegliere **Google Drive API** e fare clic su **Abilita**.
8. Nel riquadro a sinistra, sotto **API e servizi**, fare clic su **Credenziali**.
9. Fare clic su **+ Crea credenziali** all'inizio della pagina e selezionare **Chiave API** nel menu a discesa.
10. Copiare **la propria chiave API** (accanto alla chiave è disponibile l'icona Copia negli Appunti).
11. Passare alla scheda MDaemon del browser e incollare la chiave nel campo **Chiave API Google Drive** della pagina Google Drive in MDaemon (oppure salvarla altrove se si desidera eseguire questa operazione in un secondo momento).
12. Nel riquadro a sinistra, sotto **API e servizi**, fare clic sulla **schermata consenso OAuth**.
13. In Tipo Utente, selezionare **Esterno** e fare clic su **Crea**. **Nota:** se si dispone di una Risorsa organizzazione oppure a seconda dello stato di pubblicazione dell'app, la scelta di Interno potrebbe essere una scelta migliore. Per ulteriori informazioni, vedere la nota Stato di pubblicazione 351 riportata di seguito.
14. Immettere il **nome dell'app** (ad esempio Google Drive per Webmail), un **indirizzo email per l'assistenza** che gli utenti possono contattare, quindi un **indirizzo e-mail dello sviluppatore** che Google può contattare per richiedere modifiche al progetto. Questo è tutto ciò che viene richiesto in questa pagina per la configurazione ma, a seconda dell'organizzazione o dei requisiti di verifica, è possibile inserire anche il logo dell'azienda e i collegamenti ai termini e condizioni del servizio 372 e all'informativa sulla privacy (come sopra descritto). I campi dei **domini autorizzati** saranno popolati automaticamente quando si aggiungono gli *URI di reindirizzamento* nella fase successiva riportata di seguito. **Nota:** queste informazioni vengono utilizzate per la schermata di consenso che verrà visualizzata dagli utenti per autorizzare Webmail ad accedere all'account Google Drive.
15. Fare clic su **Salva e continua**.
16. Fare clic su **AGGIUNGI O RIMUOVI AMBITI**, quindi copiare/incollare gli URI (anche tutti insieme) nella casella sotto "Aggiungi ambiti manualmente". Fare quindi clic su **AGGIUNGI A TABELLA**.

```
https://www.googleapis.com/auth/userinfo.email
https://www.googleapis.com/auth/drive.file
https://www.googleapis.com/auth/documents
https://www.googleapis.com/auth/drive
https://www.googleapis.com/auth/drive.readonly
https://www.googleapis.com/auth/drive.metadata
https://www.googleapis.com/auth/drive.photos.readonly
https://www.googleapis.com/auth/drive.activity.readonly
https://www.googleapis.com/auth/spreadsheets
```

17. Fare clic su **Salva e continua**.
18. In Utenti di prova, fare clic su **AGGIUNGI UTENTI**, immettere ciascun account Google a cui Google Drive per MDaemon accederà mediante questa app e fare

clic su **AGGIUNGI** (vedere la nota di seguito relativa allo stato di pubblicazione[351] dell'app).

19. Fare clic su **Salva e continua**.
20. In Riepilogo, fare clic su **TORNA ALLA DASHBOARD** in fondo alla pagina.
21. Fare clic su **Credenziali** nel riquadro a sinistra, scegliere **(+) Crea credenziali**, quindi selezionare **ID client OAuth**.
22. Nella casella di riepilogo a discesa "Tipo applicazione" selezionare **Applicazione Web** e in "URI di reindirizzamento autorizzati" selezionare **+ AGGIUNGI URI**. Immettere gli URI di reindirizzamento. L'URI di reindirizzamento visualizzato nella pagina di Google Drive in MDaemon è un esempio costruito a partire dal nome dell'host SMTP del dominio predefinito[185] ***[188], che dovrebbe funzionare per gli utenti di quel dominio che accedono a Webmail. È necessario aggiungere altri URI di reindirizzamento all'app per qualsiasi altro dominio MDaemon che gli utenti utilizzano per accedere a Webmail. Ad esempio, "`https://mail.esempio.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" funziona per tutti gli utenti che utilizzano `mail.esempio.com` per accedere a Webmail. Se si ospita anche un dominio denominato, "`mail.azienda.test`", sarà necessario immettere anche un URI di reindirizzamento per quel dominio, vale a dire "`https://mail.azienda.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`".
23. Fare clic su **CREA**.
24. Copiare i valori di **ID client** e **Segreto client** nelle caselle *ID client Google Drive* e *Segreto client Google Drive* nella pagina Google Drive di MDaemon. È anche possibile immettere la chiave API di Google Drive, se non già immessa.

Stato di pubblicazione - Queste istruzioni riguardano la creazione di un'app Google con lo Stato di pubblicazione impostato su "**Prova**". A tale scopo è necessaria l'aggiunta di ogni specifico account Google che utilizzerà l'app per accedere a Google Drive ed è previsto un limite di 100 utenti. Inoltre, in Webmail, quando agli utenti viene chiesto di autorizzare MDaemon ad accedere a Google, viene visualizzato un messaggio di avviso "per confermare che l'utente dispone dell'accesso in prova al progetto, ma deve considerare i rischi associati alla concessione a un'applicazione non verificata dell'autorizzazione all'accesso ai propri dati". Inoltre, l'autorizzazione scade dopo sette giorni, quindi ogni utente dovrà riautorizzare l'accesso a Google ogni settimana.

Per eliminare questi requisiti e limitazioni, è necessario modificare lo stato in "**In produzione**", operazione che potrebbe richiedere o meno la modifica del Tipo utente da esterno a interno, il passaggio attraverso un processo di verifica dell'app o entrambe le operazioni. Per ulteriori informazioni sulla verifica delle app e sullo stato di pubblicazione, consultare i seguenti articoli di Google:

Impostazione della schermata di consenso OAuth e FAQ sulla verifica dell'API OAuth.

Autorizzazione di Google Drive in Webmail

Una volta creata l'app Google Drive e configurata la pagina Google Drive di MDaemon secondo le istruzioni sopra riportate, ogni utente che intende accedere al proprio account di Google Drive da Webmail deve prima autorizzare l'accesso. A tal fine l'utente deve:

1. Accedere a Webmail.
2. Fare clic sull'icona **Opzioni** nell'angolo superiore destro, quindi scegliere **App cloud**.
3. Fare clic su **Configura Google Drive** (si aprirà una pagina **OAuth 2.0**).
4. Fare clic su **Connetti a Google Drive**.
5. Se non è stato ancora effettuato l'accesso, Google Drive chiederà di fornire le informazioni di accesso o di scegliere un account.
6. Potrebbe essere visualizzato il messaggio di avviso: "Google non ha verificato questa app". Ti è stato concesso l'accesso a un'app in fase di prova. Procedi solo se conosci lo sviluppatore che ti ha invitato". Fare clic su **Continua**.
7. Selezionare le funzionalità di Google Drive a cui Webmail potrà accedere, quindi fare clic su **Continua**.
8. Verrà visualizzata una pagina finale per informare che MDaemon è ora connesso a Google Drive. Gli utenti possono chiudere questa finestra.
9. Per accedere a Google Drive dovranno quindi utilizzare la pagina **Documenti** di Webmail.

Vedere:

MultiPOP OAuth 146
Integrazione con Dropbox 345

3.6.1.9 Categorie

Le opzioni Categorie sono disponibili nell'interfaccia di Remote Administration di MDaemon in: **Principale » Impostazioni Webmail » Categorie**.

Webmail supporta le categorie per e-mail, eventi, note e attività nei temi LookOut e WorldClient. Gli utenti possono aggiungere la colonna Categorie alla lista dei messaggi in "**Opzioni » Colonne**" selezionando "**Categorie**" nella sezione Lista messaggi.

Per impostare le categorie per uno o più messaggi all'interno della lista, selezionare i messaggi e fare clic con il pulsante destro del mouse su uno dei messaggi selezionati. Per impostare la categoria utilizzare il menu contestuale. In alternativa, è possibile aprire un messaggio e impostare una categoria utilizzando l'opzione presente nella barra degli strumenti.

Categorie

Nella pagina Categorie dell'interfaccia Remote Administration di MDaemon è possibile impostare le categorie di dominio, ovvero un elenco fisso di categorie che tutti gli utenti possono visualizzare, ma non modificare o eliminare, in Webmail. È inoltre possibile creare un elenco predefinito di categorie personali che verranno visualizzate dai nuovi utenti.

Categorie di dominio

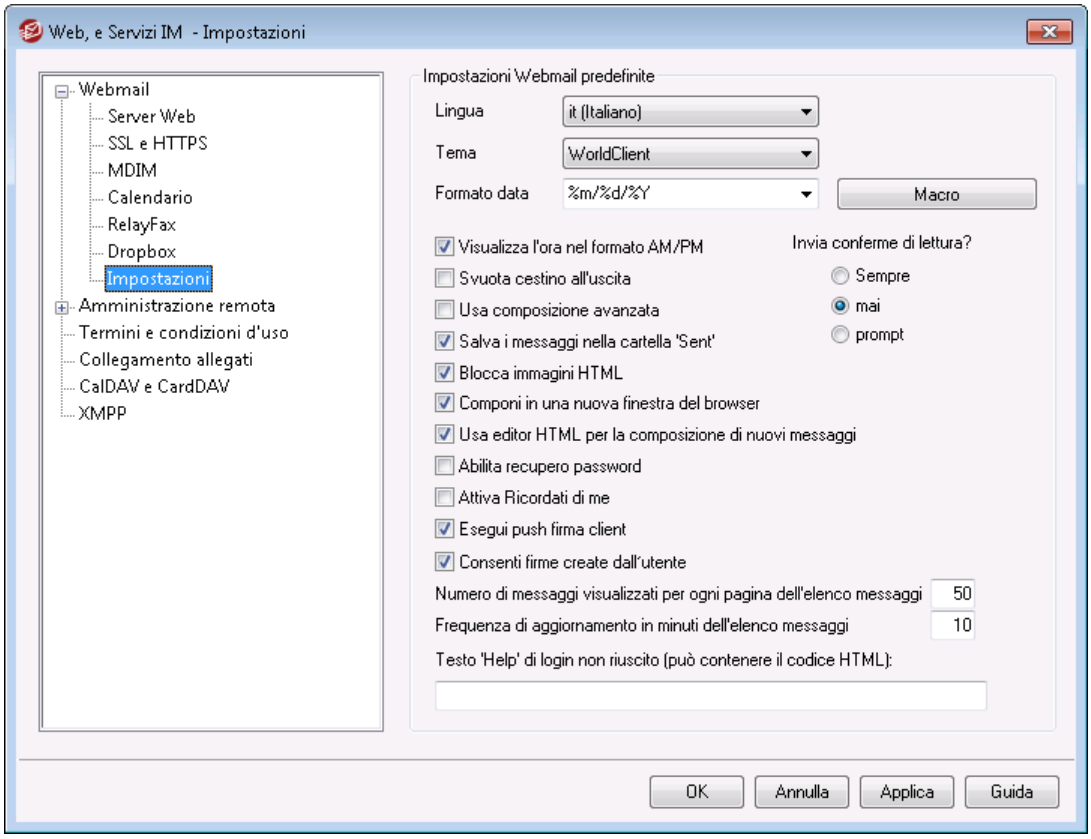
Le categorie di dominio sono categorie fisse che non possono essere riordinate, modificate o eliminate dagli utenti. Quando si attiva l'opzione *Attiva categorie di dominio*, l'elenco corrispondente viene visualizzato all'inizio dell'elenco di categorie dell'utente in Webmail. È possibile riordinare, modificare, eliminare o creare nuove categorie di dominio utilizzando le opzioni corrispondenti.

Categorie personali

È l'elenco predefinito delle categorie che verranno copiate negli account dei nuovi utenti di Webmail. Gli utenti possono controllare in modo completo l'elenco delle categorie personali. Possono infatti riordinare, modificare o eliminare le categorie, oltre a poterne creare di nuove. Se, tuttavia, si utilizzano anche le categorie di dominio, queste vengono riportate all'inizio dell'elenco di tutti gli utenti, che non possono modificarle o duplicarle. Le eventuali categorie personali con nomi che corrispondono a quelli di categorie di dominio saranno nascoste. Se non si desidera consentire l'uso di categorie personali, deselezionare **Gli utenti possono modificare le categorie personali**. In questo caso vengono visualizzate solo le categorie di dominio. Se anche l'opzione Categorie di dominio è disattivata, gli utenti non potranno utilizzare alcuna categoria.

Per informazioni più approfondite sui file di MDaemon in cui si gestiscono le categorie e le relative traduzioni, vedere: `MDaemon\WorldClient\CustomCategories.txt`.

3.6.1.10 Impostazioni



In questa schermata è possibile configurare le impostazioni predefinite per la schermata Impostazioni Webmail[198] di Domain Manager. Quando un utente accede a Webmail, queste opzioni regolano il modo in cui le varie funzioni di Webmail operano all'inizio per l'utente. Molte di queste impostazioni sono personalizzabili dall'utente tramite le pagine Opzioni di Webmail.

Impostazioni Webmail predefinite

Lingua
Utilizzare questa casella di riepilogo a discesa per scegliere la lingua predefinita con cui l'interfaccia di Webmail viene visualizzata agli utenti durante la prima registrazione al dominio selezionato. Gli utenti possono modificare le impostazioni personali della lingua mediante la pagina di accesso a Webmail e mediante un'opzione di Opzioni » Personalizza in Webmail.

Tema
Questa casella di riepilogo a discesa consente di indicare il tema predefinito di Webmail da utilizzare per il primo accesso degli utenti. È possibile personalizzare l'impostazione del tema mediante Opzioni » Personalizza in Webmail.

Formato data
Utilizzare questa casella di testo per specificare la formattazione delle date in Webmail. Fare clic sul pulsante *Macro* per visualizzare un elenco di codici macro utilizzabili in questa casella di testo. Sono disponibili le seguenti macro:

%A — Nome completo del giorno

%B — Nome completo del mese

%d — Giorno del mese (visualizzato nel formato "01-31")

%m — Mese (visualizzato nel formato "01-12")

%y — Anno nel formato a 2 cifre

%Y — Anno nel formato a 4 cifre

Ad esempio, la data "`%d/%m/%Y`" può essere in Webmail nel modo seguente "`25/12/2011`".

Macro
Fare clic su questo pulsante per visualizzare un elenco di codici macro utilizzabili in *Formato data*.

Invia conferme di lettura
Questa opzione determina la risposta di Webmail ai messaggi in arrivo che contengono una richiesta di conferma di lettura.

sempre
Selezionando questa opzione, MDaemon invia una notifica di avvenuta lettura al mittente. All'utente di Webmail che ha ricevuto il messaggio non viene segnalato che è stata richiesta o soddisfatta una conferma di lettura.

mai
Questa opzione indica a Webmail di ignorare le richiesta di conferma di lettura.

prompt
Con questa opzione, agli utenti di Webmail viene richiesto se inviare una conferma di lettura ogni volta che viene aperto un messaggio che lo richiede.

Visualizza l'ora nel formato AM/PM
Selezionare questa opzione se si desidera che in Webmail l'ora del dominio selezionato venga visualizzata nel formato orario basato su 12 ore (AM/PM). Deselezionare questa casella di controllo per utilizzare il formato basato su 24 ore. I singoli utenti possono modificare questa impostazione mediante l'opzione "*Visualizza gli orari in formato AM/PM*" situata nella pagina Opzioni » Calendario in Webmail.

Svuota cestino all'uscita
Se si seleziona questa opzione, il cestino dell'utente verrà svuotato all'uscita da Webmail. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Personalizza in Webmail.

Usa composizione avanzata
Selezionare questa casella se si desidera che, per impostazione predefinita, gli utenti visualizzino la schermata Composizione avanzata di Webmail, anziché la normale schermata Componi. I singoli utenti possono modificare questa impostazione in Opzioni » Componi in Webmail.

Salva i messaggi nella cartella 'Sent'
Selezionare questa opzione se si desidera che una copia di ogni messaggio inviato venga salvata nella cartella *Posta inviata*. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi in Webmail.

Blocca immagini HTML
Questa casella di controllo consente di impedire la visualizzazione automatica di immagini remote durante la visualizzazione di messaggi di posta elettronica HTML con Webmail. Per visualizzare le immagini, è necessario selezionare la barra visualizzata al di sopra del messaggio nella finestra del browser. Si tratta di una funzione anti spam, perché molti messaggi spam contengono immagini con particolari URL che identificano l'indirizzo di posta elettronica dell'utente che ha visualizzato le immagini, confermando così al mittente che si tratta di un indirizzo valido e operativo. L'opzione è abilitata per impostazione predefinita.

Componi in una nuova finestra del browser
Selezionare questa casella se si desidera che per la composizione dei messaggi venga aperta una nuova finestra del browser. In caso contrario, si passerà dalla finestra principale alla schermata di composizione. Deselezionare la casella se non si desidera che venga aperta una finestra separata. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi in Webmail.

Usa editor HTML per la composizione di nuovi messaggi
Abilitare questa casella se si desidera che, per impostazione predefinita, gli utenti possano visualizzare l'editor di composizione HTML di Webmail. Gli utenti possono modificare questa impostazione in Opzioni » Componi in Webmail.

Abilita recupero password
Se si attiva questa opzione, gli utenti autorizzati a modificare la propria password 735 potranno immettere un indirizzo di posta elettronica alternativo in Webmail, a cui potrà essere inviato un collegamento per il ripristino di una password dimenticata. Per impostare questa funzionalità, gli utenti devono immettere sia l'indirizzo di posta elettronica per il recupero della password che la propria password corrente in Webmail, nella pagina Opzioni » Sicurezza. Dopo aver configurato questa impostazione, quando un utente tenta di accedere a Webmail con una password non corretta, viene visualizzato il collegamento "password dimenticata?". Il collegamento porta alla pagina in cui viene richiesto di confermare l'indirizzo di posta elettronica per il recupero della password. Se immette l'indirizzo di posta elettronica corretto, l'utente riceverà un messaggio e-mail con un collegamento alla pagina per la modifica della password. Questa funzione è disabilitata per impostazione predefinita.

È possibile abilitare o disabilitare l'opzione per ogni singolo utente, aggiungendo il seguente codice al file `user.ini` dell'utente di Webmail (ad esempio `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (oppure "=No" per disabilitare l'opzione
per l'utente)
```

Consenti l'autenticazione a due fattori Ricordati di me (valido anche per Remote Admin)
Quando si utilizza l'autenticazione a due fattori (2FA) per accedere a Webmail o Remote Admin, nella pagina di autenticazione 2FA è di norma disponibile l'opzione Ricordati di me, che impedisce al server di richiedere nuovamente la 2FA per tale utente per un determinato numero di giorni (vedere l'opzione "*Consenti memorizzazione autenticazione*" di seguito). Deselezionare questa casella di controllo se non si desidera visualizzare l'opzione Ricordati di me della 2FA, in modo che tutti gli utenti con 2FA attivato debbano immettere un codice 2FA a ogni accesso. **Nota:** l'opzione è disponibile solo nell'interfaccia Web di MDaemon Remote Administration (MDRA) 359.

Attiva Ricordati di me
Selezionare questa casella se si desidera che nella pagina di accesso di MDaemon Webmail sia presente una casella di controllo *Ricordati di me* quando gli utenti si connettono attraverso la porta https 336. Se gli utenti selezionano questa casella all'accesso, le rispettive credenziali saranno ricordate per il dispositivo utilizzato. Quindi ogni volta che useranno quel dispositivo per connettersi a Webmail in futuro accederanno automaticamente fino a quando non eseguiranno la disconnessione manuale dall'account o il token di Ricordati di me scadrà.

Per impostazione predefinita, le credenziali dell'utente restano memorizzate per un massimo di 30 giorni prima che l'utente sia obbligato a eseguire di nuovo l'accesso. Se si desidera spostare la data di scadenza, è possibile modificare il valore dei token *Scadenza Ricordati di me dopo questo numero di giorni* nell'interfaccia Web MDaemon Remote Administration (MDRA) 359. È anche possibile cambiarla modificando la chiave `RememberUserExpiration=30` nella sezione `[Default:Settings]` del file `Domains.ini`, che si trova nella cartella `\MDaemon\WorldClient\`. Il valore della scadenza può essere impostato su massimo 365 giorni. **Nota:** L'autenticazione a due fattori 735 (2FA) ha una propria chiave per la scadenza di Ricordati di me (`TwoFactorAuthRememberUserExpiration=30`), che si trova nella sezione `[Default:Settings]` del file `Domains.ini` nella cartella `\MDaemon\WorldClient\`. Pertanto l'autenticazione 2FA sarà nuovamente richiesta all'accesso quando il token di Ricordati di me di 2FA scadrà, anche se il normale token è ancora valido.

L'opzione*Ricordati di me* è disabilitata per impostazione predefinita e si applica a tutti i domini dell'utente. Per ignorare questa impostazione su domini specifici, utilizzare l'impostazione *Ricordati di me* nella schermata Webmail 198 di Domain Manager.

Dato che l'opzione *Ricordati di me* consente agli utenti di avere un accesso permanente su più dispositivi, agli utenti deve essere ricordato che l'uso di Ricordati di me su reti pubbliche può essere pericoloso. Inoltre, se si sospetta una violazione della sicurezza per un account, in MDRA è disponibile un pulsante *Ripristina Ricordati di me* che è possibile utilizzare per reimpostare i token Ricordati di me per tutti gli utenti.

> Questo richiederà a tutti gli utenti di eseguire di nuovo l'accesso con le proprie credenziali.

Esegui push firma client
Selezionare questa casella di controllo per eseguire il push della firma predefinita del client[141] agli utenti di Webmail. In Webmail questa selezione provocherà la creazione di una firma denominata "Sistema" nelle opzioni per la firma in: **Opzioni » Componi**. Gli utenti potranno quindi scegliere di inserire automaticamente questa firma nella vista della composizione durante la redazione di un nuovo messaggio. Per personalizzare oppure abilitare/disabilitare la firma del client per domini specifici, utilizzare le opzioni Firme client[211] e Webmail[198] di Domain Manager.

Consenti firme create dall'utente
Selezionare questa casella di controllo per consentire agli utenti di creare le proprie firme personalizzate in Webmail. Gli utenti potranno quindi scegliere quale firma inserire automaticamente nella vista della composizione durante la redazione dei messaggi. Quando non si consente la creazione delle firme create dall'utente, ma si attiva l'opzione *Esegui push firma client*, è possibile inserire automaticamente solo la firma del client[141] (vale a dire, la firma "Sistema" di Webmail). In Webmail le opzioni per la firma sono disponibili in: **Opzioni » Componi**.

Consenti agli utenti di modificare i nomi alias visualizzati
Selezionare questa casella di controllo per consentire agli utenti di modificare il nome alias visualizzato associato al proprio account. Per modificare il nome alias, gli utenti possono utilizzare l'opzione *Modifica nomi alias visualizzati*, disponibile nel tema Pro di Webmail, in Impostazioni » Componi. L'opzione è disabilitata per impostazione predefinita. **Nota:** l'opzione è disponibile solo nell'interfaccia Web di MDaemon Remote Administration (MDRA)[359].

Numero di messaggi visualizzati per ogni pagina dell'elenco messaggi
Indica il numero di messaggi che vengono visualizzati su ciascuna pagina dell'elenco dei messaggi per ogni cartella di posta. Se in una cartella è contenuto un numero di messaggi superiore a quello specificato in questo campo, sopra e sotto l'elenco verranno visualizzati dei comandi che consentono di passare alle altre pagine. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza di WorldClient.

Frequenza di aggiornamento in minuti dell'elenco messaggi
Indica per quanti minuti Webmail attende prima di aggiornare automaticamente l'elenco dei messaggi. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza in Webmail.

Testo 'Guida' errore di accesso (può contenere codice HTML)
Questa opzione consente di specificare una frase testuale, in testo semplice o HTML, da visualizzare nella schermata di registrazione di Webmail quando si verifica un problema di accesso. Il testo viene visualizzato al di sotto del seguente testo predefinito: "*Accesso errato, riprovare. Se è necessaria assistenza, contattare l'amministratore della posta elettronica*". Il testo può essere utilizzato per dirigere gli utenti a una data pagina o per ottenere informazioni relative all'accesso a Webmail.

Personalizzazione delle cartelle dei mittenti consentiti e dei mittenti bloccati

Sono disponibili diverse funzionalità standard di Webmail personalizzabili modificando determinati file nella cartella `MDaemon\WorldClient\`:

È possibile nascondere per impostazione predefinita le cartelle Mittenti consentiti e Mittenti bloccati per gli utenti di Webmail. Per eseguire questa operazione, aprire `MDaemon\WorldClient\Domains.ini` e in `[Default:UserDefaults]` modificare il valore "`HideWhiteListFolder=`" o "`HideBlackListFolder=`" da"`No`" in "`Yes`". È possibile nascondere o mostrare queste cartelle a utenti specifici modificando quelle stesse chiavi nel file `User.ini` nella sezione `[User]`.

Vedere:

Domain Manager » Impostazioni Webmail 198

3.6.1.11 Branding

Per personalizzare le immagini del banner di Webmail che vengono visualizzate nella pagina di accesso e nella barra di spostamento laterale, accedere alla pagina Branding in nell'interfaccia Web Remote Administration 359 di MDaemon.

Per utilizzare le proprie immagini personalizzate:

1. Fare clic su **Usa immagini personalizzate** nella sezione Personalizzazione.
2. Nella sezione Immagine pagina di accesso utilizzare l'opzione **Scegli file** o **Sfoglia** (in base al browser installato) e selezionare il file da caricare. In questa sezione sono inoltre elencate le dimensioni predefinite per l'immagine della pagina di accesso.
3. Fare clic su **Carica immagine personalizzata**.
4. Ripetere i passaggi 2 e 3 per l'immagine della barra di spostamento laterale e l'immagine della barra di spostamento laterale invertita.

Le immagini caricate saranno visualizzate nei riquadri corrispondenti e utilizzate in luogo delle immagini predefinite di Webmail.

3.6.2 Remote Administration

L'interfaccia Web di MDaemon Remote Administration (MDRA) è stata progettata per consentire agli utenti di amministrare MDaemon in remoto mediante un browser Web. Remote Administration è un'applicazione server progettata per essere eseguita in background sullo stesso computer nel quale è in esecuzione MDaemon. Per accedere a Remote Administration, aprire il browser e specificare l'URL e il numero di porta presso cui risiede il server di amministrazione (ad esempio, `www.example.com:1000`). Una volta fornite le credenziali appropriate, l'utente avrà accesso ai controlli e alle impostazioni di MDaemon. Il tipo e il numero delle impostazioni che possono essere gestite dipendono dal livello di accesso fornito, esistono tre livelli di accesso per gli utenti di amministrazione remota: Globale, Dominio o Utente.

Amministratori globali - Si tratta di utenti per cui sono abilitate autorizzazioni di accesso globale nelle relative impostazioni di account in MDaemon. Se usufruisce di accesso globale, l'utente può visualizzare e configurare tutte le impostazioni e tutti i controlli accessibili via Remote Administration. Gli amministratori globali possono aggiungere, modificare ed eliminare utenti, domini e liste di distribuzione. Grazie al completo controllo amministrativo, sono inoltre in grado di modificare i file INI dei prodotti, specificare altri utenti come amministratori di dominio, gestire le password e altro.

Amministratori di dominio: analogamente agli amministratori globali, anche quelli di dominio hanno il controllo su tutti gli utenti e le impostazioni accessibili via Remote Administration. Tuttavia, tale controllo è limitato ai domini a cui hanno accesso e alle autorizzazioni specificate nella schermata Servizi Web 735. Gli amministratori di dominio e i domini sui quali esercitano il controllo vengono specificati all'interno di Remote Administration da un amministratore globale o da un altro amministratore di dominio che ha accesso ai domini in questione.

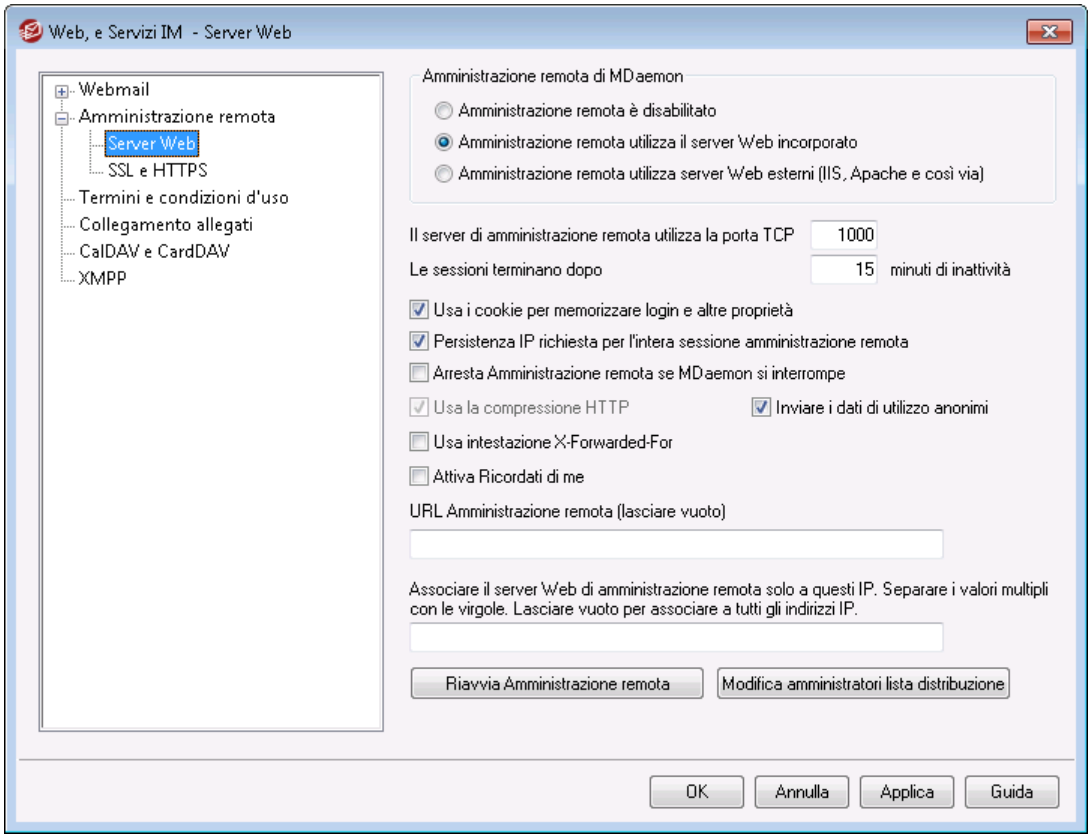
Utenti - Il livello minimo previsto per l'accesso a Remote Administration è l'accesso utente. Gli utenti MDaemon, ad esempio, possono accedere all'interfaccia di amministrazione remota e visualizzare le proprie impostazioni di account, nonché modificare le voci MultiPOP, i filtri applicati alla posta, le risposte automatiche e così via. Il tipo e il numero delle impostazioni modificabili si basano sulle autorizzazioni fornite nelle impostazioni di account di ciascun utente.

Qualunque utente che abbia l'autorizzazione ad accedere sia a Webmail che a Remote Administration, può accedere a quest'ultimo da Webmail, piuttosto che accedere separatamente a entrambi. È possibile aprire Remote Administration in una finestra separata del browser da Webmail facendo clic sul collegamento "Impostazioni avanzate" in "Opzioni".

Vedere:

Remote Administration » Server Web 361
Remote Administration » HTTPS 364
Gestione modelli » Servizi Web 814
Account Editor » Servizi Web 735
Esecuzione di Remote Administration in IIS 368

3.6.2.1 Server Web



MDaemon Remote Administration

Remote Administration è disabilitato
Scegliere questa opzione per disabilitare Remote Administration. Il server Remote Administration può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon

Remote Administration in esecuzione con server Web incorporato
Scegliere questa opzione per eseguire WebAdmin utilizzando il server Web incorporato di MDaemon. Il server Remote Administration può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon

Remote Administration utilizza server Web esterni (IIS, Apache e così via)
Scegliere questa opzione se si desidera eseguire WebAdmin in Internet Information Server (IIS) o in un altro server Web diverso dal server incorporato di MDaemon. In questo modo, è possibile impedire l'accesso a elementi della GUI che potrebbero entrare in conflitto con il server alternativo.

Per ulteriori informazioni, vedere Esecuzione di Remote Administration con IIS 368.

Il server Remote Administration utilizza la porta TCP
Si tratta della porta da cui Il server Remote Administration rileverà le connessioni provenienti dal browser Web. La porta predefinita è 1000.

Le sessioni terminano dopo XX minuti di inattività
Una volta ottenuto l'accesso a Remote Administration, le sessioni possono rimanere inattive per il tempo specificato in questo campo prima di essere chiuse. Il valore predefinito è di 15 minuti.

Impostazioni varie

Usa i cookie per memorizzare login e altre proprietà
Per impostazione predefinita l'interfaccia di Remote Administration utilizza dei cookie, in modo che il browser dell'utente ricordi il nome di accesso dell'utente e altre proprietà. Se non si desidera utilizzare i cookie, deselezionare questa casella di controllo. Questa funzione consente di offrire agli utenti un accesso più "personalizzato", purché nel browser sia abilitato il supporto per i cookie.

Richiedi la persistenza dell'IP per tutta la sessione di Remote Administration
Come misura di sicurezza aggiuntiva, è possibile selezionare questa casella di controllo in modo che Remote Administration limiti ciascuna sessione utente all'indirizzo IP da cui si è connesso l'utente all'inizio della sessione. Poiché è richiesta la persistenza dell'IP, nessuno potrà "appropriarsi" della sessione dell'utente. Questa configurazione è più sicura ma può generare problemi quando si utilizza un server proxy o una connessione Internet che assegna e modifica dinamicamente gli indirizzi IP.

Arresta Remote Administration se MDaemon si interrompe
Fare clic su questa opzione se si desidera chiudere Remote Administration quando viene chiuso MDaemon. In caso contrario, Remote Administration continua ad essere eseguito in background.

Usa la compressione HTTP
Fare clic su questa casella di controllo per utilizzare la compressione HTTP nelle sessioni di Remote Administration.

Inviare i dati di utilizzo anonimi
Per impostazione predefinita il client Web di MDaemon Remote Administration invia i seguenti dati in forma anonima e destinati esclusivamente al miglioramento del prodotto: sistema operativo utilizzato, versione del browser utilizzata, lingua e così via. Questi dati vengono utilizzati da MDaemon Technologies per migliorare il funzionamento di Remote Administration. Se non si desidera inviare i dati di utilizzo, disabilitare questa opzione.

intestazione X-Forwarded-For
Fare clic su questa casella di controllo per consentire l'uso dell'intestazione `X-Forwarded-For` che viene in alcuni casi aggiunta dai server proxy. L'opzione è disabilitata per impostazione predefinita. Attivarla solo se il server proxy inserisce questa intestazione.

Attiva Ricordati di me
Selezionare questa casella se si desidera che nella pagina di accesso di Remote Administration sia presente una casella di controllo *Ricordati di me* quando gli utenti si connettono attraverso la porta https 364. Se gli utenti selezionano questa casella all'accesso, le rispettive credenziali saranno ricordate per il dispositivo utilizzato. Quindi ogni volta che useranno quel dispositivo per connettersi in futuro accederanno automaticamente fino a quando non eseguiranno la disconnessione manuale dall'account o il token di Ricordati di me scadrà.

Per impostazione predefinita, le credenziali dell'utente restano memorizzate per un massimo di 30 giorni prima che l'utente sia obbligato a eseguire di nuovo l'accesso. Se si desidera spostare la data di scadenza, è possibile modificare il valore dei token *Scadenza Ricordati di me dopo questo numero di giorni* nell'interfaccia Web MDaemon Remote Administration (MDRA). È anche possibile cambiarla modificando la chiave `RememberUserExpiration=30` nella sezione `[Default:Settings]` del file `Domains.ini`, che si trova nella cartella `\MDaemon\WorldClient\`. Il valore della scadenza può essere impostato su massimo 365 giorni. **Nota:** L'autenticazione a due fattori 735 (2FA) ha una propria chiave per la scadenza di Ricordati di me (`TwoFactorAuthRememberUserExpiration=30`), che si trova nella sezione `[Default:Settings]` del file `Domains.ini` nella cartella `\MDaemon\WorldClient\`. Pertanto l'autenticazione 2FA sarà nuovamente richiesta all'accesso quando il token di Ricordati di me di 2FA scadrà, anche se il normale token è ancora valido.

L'opzione *Ricordati di me* è disabilitata per impostazione predefinita.

Dato che l'opzione *Ricordati di me* consente agli utenti di avere un accesso permanente su più dispositivi, agli utenti deve essere ricordato che l'uso di Ricordati di me su reti pubbliche può essere pericoloso. Inoltre, se si sospetta una violazione della sicurezza per un account, in MDRA è disponibile un pulsante *Ripristina Ricordati di me* che è possibile utilizzare per reimpostare i token Ricordati di me per tutti gli utenti. Questo richiederà a tutti gli utenti di eseguire di nuovo l'accesso con le proprie credenziali.

URL Remote Administration
Questo è l'URL che Webmail utilizza internamente quando gli utenti fanno clic sul collegamento Impostazioni avanzate per modificare le impostazioni del proprio account mediante Remote Administration. Lasciare vuoto questo campo se Remote Administration viene eseguito con il server Web incorporato. Se si utilizza un server Web alternativo come l'IIS e Remote Administration è stato configurato per essere eseguito in un URL o in un indirizzo IP alternativi, specificare l'URL in questo campo.

Associa il server Web di Remote Administration solo a questi IP
Per limitare l'associazione del server Remote Administration solo a determinati indirizzi IP, specificare tali indirizzi in questa casella separandoli con virgole. Se si lascia vuoto questo campo, Remote Administration controlla tutti gli indirizzi IP specificati per i Domini 185..

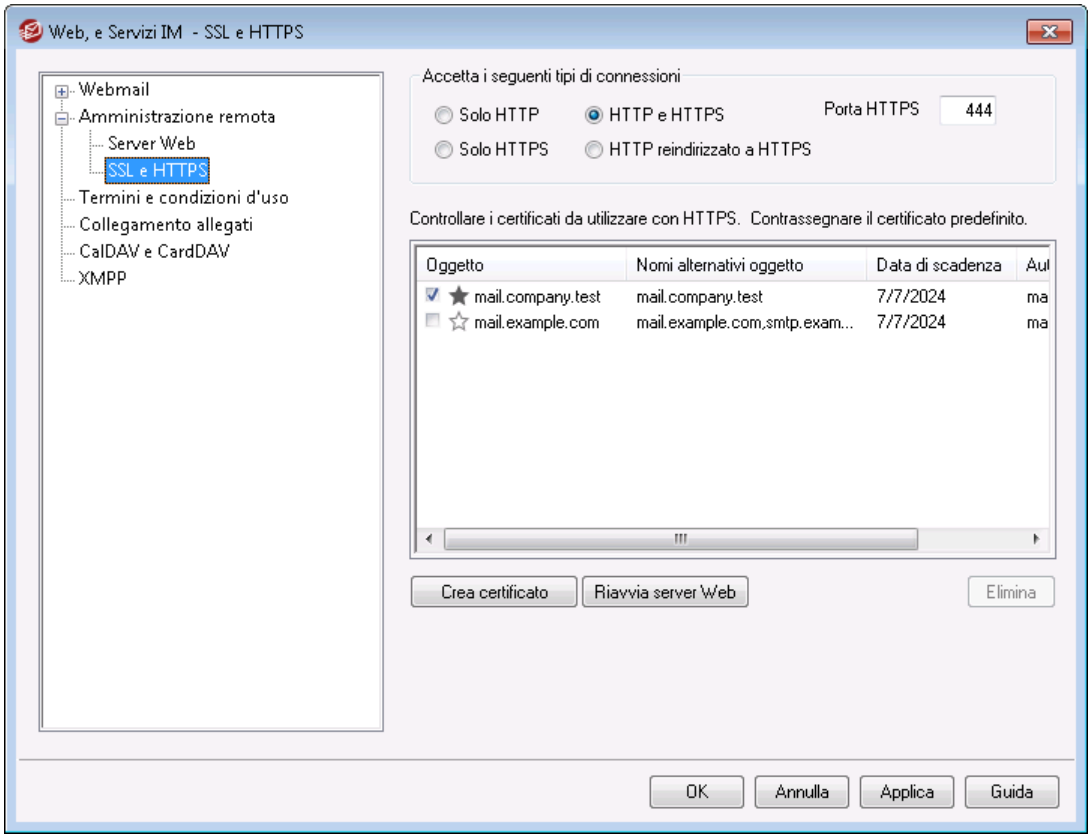
Riavvia Remote Administration (se cambiano porte o parametri di IIS)
Fare clic su questo pulsante per riavviare il server Remote Administration. Nota: dopo la modifica delle impostazioni della porta, per applicare le nuove impostazioni è necessario riavviare Remote Administration.

Modifica amministratori lista distribuzione
Fare clic su questo pulsante per aprire il file degli amministratori della lista di distribuzione per visualizzarlo o modificarlo.

Vedere:

Remote Administration 359
Remote Administration » HTTPS 364
Esecuzione di Remote Administration in IIS 368
Gestione modelli » Servizi Web 814
Account Editor » Servizi Web 735

3.6.2.2 SSL/HTTPS



Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). SSL è il metodo standard per la protezione delle comunicazioni Web tra server e client. e offre funzioni per l'autenticazione server, la crittografia dei

dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare Remote Administration per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in Impostazioni » Web e Servizi IM » Remote Administration. Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » Remote Administration".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 585

Questa schermata è valida per Remote Administration solo quando si utilizza il server Web incorporato di MDaemon. Se si configura Remote Administration per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Accetta i seguenti tipi di connessioni

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a Remote Administration. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in Remote Administration e non si desidera imporre agli utenti di Remote Administration l'utilizzo di HTTPS. Remote Administration rileva le connessioni sulla porta HTTPS designata di seguito, ma risponde comunque alle normali connessioni http sulla porta TCP di Remote Administration della schermata Server Web 361.

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a Remote Administration. Se si attiva questa opzione, Remote Administration risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da Remote Administration per le connessioni SSL. La porta SSL predefinita è 444. Se si utilizza la porta SSL predefinita, non sarà necessario includere il numero di porta nell'URL di Remote Administration per la connessione via HTTPS (ovvero, "https://esempio.com" equivale a https://esempio.com:444").

Non si tratta della stessa porta di Remote Administration designata nella schermata Server Web 361. Se consentite, le connessioni HTTP a Remote Administration devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

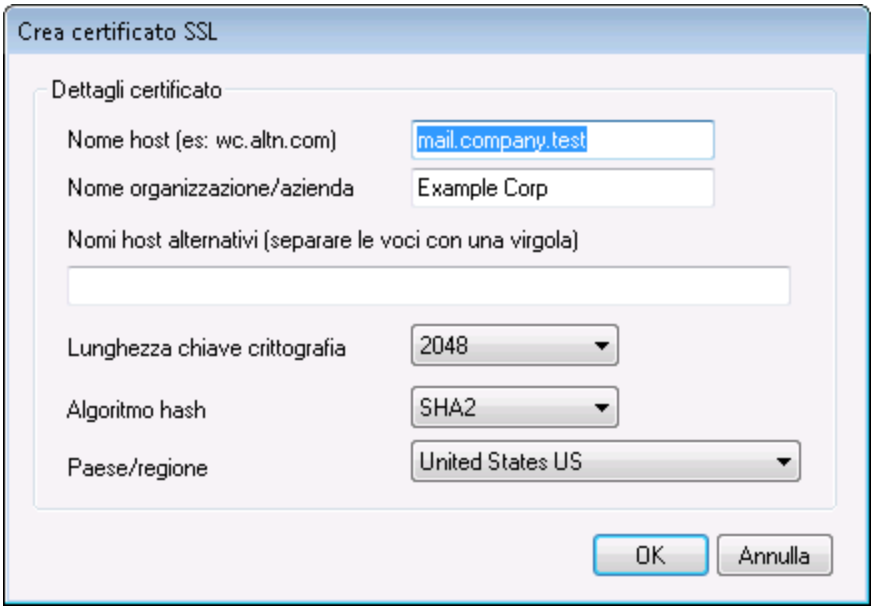
Seleziona certificato da usare per HTTPS/SSL

Questa casella consente di visualizzare i certificati SSL. Selezionare la casella di controllo accanto ai certificati che si intende attivare. Fare clic sulla stella accanto a quello che si desidera impostare come certificato predefinito. MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito. Fare doppio clic su un certificato per aprirlo nella finestra di dialogo Certificato di Windows e visualizzarne i dettagli (funzionalità disponibile solo nell'interfaccia dell'applicazione, non nell'amministrazione remota basata su browser).

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Crea certificato

Fare clic su questo pulsante per aprire la finestra di dialogo Crea certificato SSL.



Dettagli certificato

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto. Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Algoritmo hash
Scegliere l'algoritmo hash che si desidera utilizzare: SHA1 o SHA2. L'impostazione predefinita è SHA2.

Riavvia server Web

Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare un nuovo certificato, è necessario riavviare il server Web.

Utilizzo di Let's Encrypt per la gestione del certificato

Let's Encrypt è un'autorità di certificazione (CA) che fornisce certificati gratuiti mediante un processo automatizzato che si pone la finalità di eliminare i processi più complessi di creazione, convalida, firma, installazione e rinnovo manuali dei certificati per i siti Web sicuri.

Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un certificato, è disponibile la schermata Let's Encrypt 605 che consente di configurare ed

eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP[188] del dominio predefinito[185] come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica. Vedere l'argomento Let's Encrypt[605] per ulteriori informazioni.

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere:

Esecuzione di Remote Administration in IIS[368]
SSL e certificati[585]
Creazione e uso dei certificati SSL[928]

Per ulteriori informazioni su Remote Administration, vedere:

Configurazione remota[359]
Remote Administration » Server Web[361]
Valori predefiniti di accesso Web[814]
Account Editor » Accesso Web[735]

3.6.2.3 Esecuzione dell'amministrazione remota in IIS

Poiché in MDaemon è incorporato un server Web, per Remote Administration non è necessario l'utilizzo di Internet Information Server (IIS). WebAdmin supporta comunque IIS e può pertanto funzionare come DLL ISAPI.

Per configurare il funzionamento con IIS 5:

1. Interrompere l'esecuzione di Remote Administration. A questo scopo, fare clic con il pulsante destro del mouse sulla voce Remote Administration di *Server* nel riquadro sinistro della GUI di MDaemon e fare clic su **Attiva/Disattiva**.

2. Aprire il programma di gestione IIS mediante **Start→ Impostazioni→ Pannello di controllo→ Strumenti di amministrazione→ Gestione servizio Internet**.

3. Fare clic con il pulsante destro del mouse su**Sito Web predefinito** e selezionare **Nuovo→ Directory virtuale**.

4. Attenersi alla procedura guidata che illustra passo dopo passo il processo di creazione di una directory virtuale. Di seguito vengono suggeriti nomi e percorsi per i dati da digitare nella procedura guidata, che possono comunque variare in base all'installazione di MDaemon e alla posizione del componente Remote Administration di MDaemon.

a. Alias: "WebAdmin". Scegliere **Avanti**.
b. Directory: "c:\mdaemon\webadmin\templates". Scegliere **Avanti**.
c. Fare clic su **Avanti**.
d. Fare clic su **Fine**.

5. Impostare le autorizzazioni di esecuzione su **Solo script**.
6. Impostare il livello di protezione dell'applicazione su **Basso (Processo IIS)**.
7. Fare clic sul pulsante **Configurazione** nella sezione Impostazioni applicazione della scheda Directory virtuale.
8. Nella scheda **Mapping**, fare clic su **Aggiungi**.
9. Nel campo **Eseguibile** inserire "c:\mdaemon\webadmin\templates\WebAdmin.dll". Nota: nel campo non possono essere inseriti spazi. Se il percorso contiene uno spazio, è necessario convertirlo nel formato 8.3. Il comando `dir /x` consente di visualizzare il nome del file o della directory nel formato 8.3.
10. Nel campo **Estensione** inserire ".wdm" e selezionare il pulsante di opzione per **Tutti i verbi**.
11. Fare clic sulla casella **Modulo script**.
12. Fare clic su **OK**.
13. Se si desidera, rimuovere le altre mappature, quindi scegliere **OK**.
14. Nella scheda **Documenti** aggiungere `login.wdm` come documento predefinito e rimuovere tutte le altre voci dall'elenco.
15. In MDaemon, passare a **Impostazioni→ Web e servizi IM→ Remote Administration** e fare clic su **Remote Administration utilizza server Web esterni**.
16. In **URL Remote Administration** inserire "/WebAdmin/login.wdm".
17. Fare clic su **OK**.

Per configurare il funzionamento con IIS 6:

Creare un nuovo pool di applicazioni per Remote Administration:

1. Interrompere l'esecuzione di Remote Administration. A questo scopo, fare clic con il pulsante destro del mouse sulla voce Remote Administration di *Server* nel riquadro sinistro della GUI di MDaemon e fare clic su **Attiva/Disattiva**.
2. Aprire il programma di gestione IIS mediante **Start→ Impostazioni→ Pannello di controllo→ Strumenti di amministrazione→ Gestione servizio Internet**.

3. Fare clic con il pulsante destro del mouse su **Pool applicazioni**.
4. Fare clic su **Nuovo→ Pool applicazioni**.
5. Nel campo dell'ID del pool di applicazioni inserire "Alt-N" e fare clic su **OK**.
6. Fare clic con il pulsante destro del mouse su **Alt-N**
7. Scegliere **Proprietà**.
8. Fare clic sulla scheda **Prestazioni.**
9. Deselezionare "**Chiudi processi di lavoro dopo un periodo di inattività di**" e "**Limite massimo per la coda di richieste al kernel**".
10. Fare clic sulla scheda **Identità**.
11. Nell'elenco a discesa Predefinito, scegliere **Sistema locale**.
12. Fare clic su **OK**.

Creare una directory virtuale per Remote Administration:

1. Aprire il programma di gestione IIS mediante **Start→ Impostazioni→ Pannello di controllo→ Strumenti di amministrazione (Gestione servizio Internet)**).
2. Fare clic con il pulsante destro del mouse sul sito Web, quindi selezionare Nuovo (Directory virtuale).
3. Specificare un alias per la directory virtuale (ad esempio "WebAdmin").
4. Nel campo Percorso, digitare il percorso della directory dei modelli di Remote Administration, ad esempio "C:\Programmi\Alt-N Technologies\WebAdmin\Templates".
5. Lasciare selezionate le opzioni **Lettura** ed **Esecuzione script**.
6. Completare la procedura guidata e fare clic con il pulsante destro del mouse sulla directory virtuale creata.
7. Scegliere **Proprietà**.
8. Nella scheda Home Directory modificare il pool di applicazioni in Alt-N.
9. Fare clic sul pulsante Configurazione.
10. Scegliere **Aggiungi** per aggiungere una mappatura con estensione ISAPI.
11. Nel campo Eseguibile inserire il percorso del file WebAdmin.dll. Ad esempio: "C:\Programmi\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll".

12. Nel campo Estensione inserire ".wdm".
13. Selezionare le caselle **Modulo script** e **Verifica esistenza file**.
14. Fare clic su **OK**.
15. Se si desidera, rimuovere le altre mappature, quindi scegliere **OK**.
16. Selezionare la scheda **Documenti**.
17. Verificare che l'opzione **Abilita pagina contenuto predefinita** sia selezionata.
18. Accertarsi che l'elenco includa solo la voce "login.wdm".
19. Fare clic su **OK** e uscire dalla finestra di dialogo delle proprietà della directory virtuale.

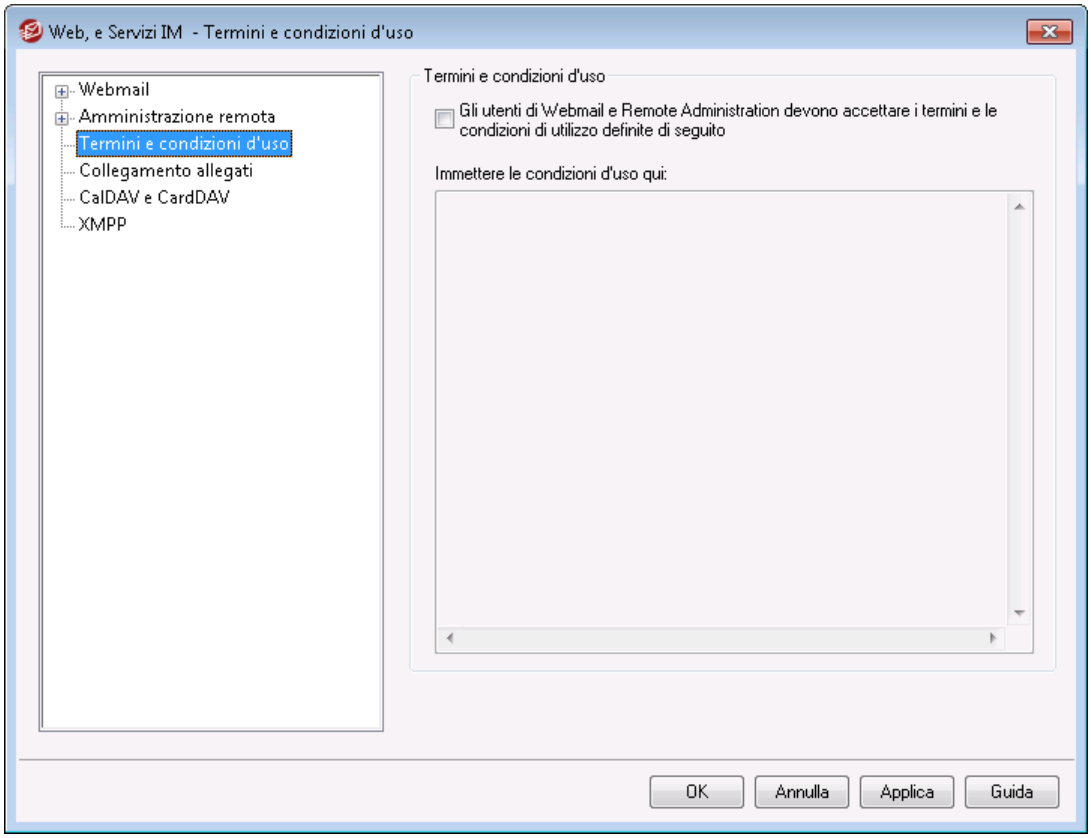
Aggiungere .WDM all'elenco delle estensioni Web consentite:

1. Fare clic sulla cartella **Estensioni servizi Web** di IIS MMC.
2. Fare clic su **Aggiungi nuova estensione servizio Web**.
3. Nel campo Estensione inserire "WebAdmin".
4. Fare clic su **Aggiungi**, quindi selezionare l'estensione ISAPI WebAdmin. Ad esempio: C:\Programmi\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll.
5. Selezionare **Imposta stato estensione su consentito**.
6. Fare clic su **OK**.
7. In MDaemon, passare a **Impostazioni→Web e servizi IM→Remote Administration** e fare clic su **Remote Administration utilizza server Web esterni**.
8. In **URL Remote Administration** inserire "/WebAdmin/login.wdm".
9. Fare clic su **OK**.

Per ulteriori informazioni su Remote Administration, vedere:

Remote Administration 359
Remote Administration » Server Web 361
Remote Administration » SSL/HTTPS 364
Gestione modelli » Servizi Web 814
Account Editor » Servizi Web 735

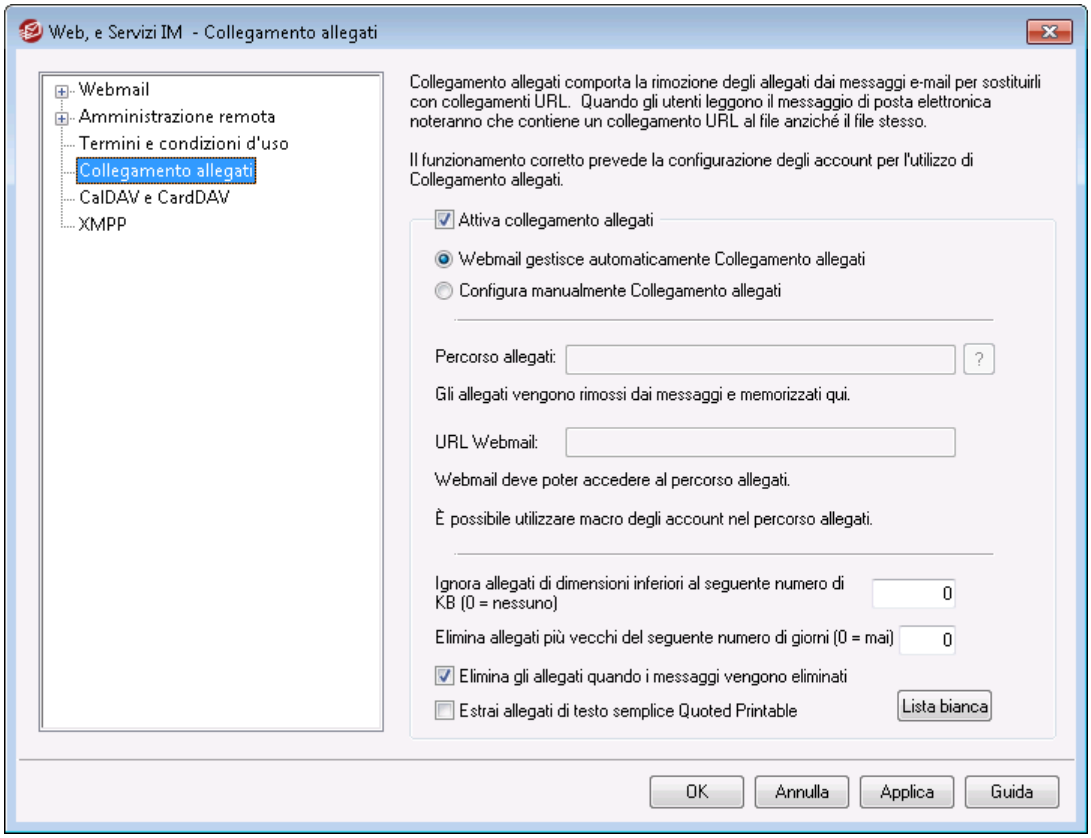
3.6.3 Termini e condizioni d'uso



Gli utenti Webmail e Remote Administration devono accettare i termini e le condizioni di utilizzo definite di seguito

Selezionare questa casella e immettere i propri Termini e condizioni d'uso nello spazio disponibile se si desidera richiedere agli utenti di Webmail e Remote Administration di accettare tali Termini e condizioni d'uso a ogni accesso.

3.6.4 Collegamento allegati



Collegamento allegati (Impostazioni » Web e Servizi IM » Collegamento allegati) è una funzione che consente di rimuovere tutti gli allegati dai messaggi di posta in arrivo, di memorizzarli nella posizione indicata e di inserire collegamenti URL ai file nei messaggi dai quali sono stati estratti. I destinatari possono quindi selezionare i collegamenti per scaricare i file. Grazie a questa funzione, è possibile velocizzare l'elaborazione della posta elettronica, in particolare quando gli utenti ricevono messaggi o sincronizzano le proprie cartelle di posta, perché vengono eliminati gli allegati di grandi dimensioni. La funzione offre inoltre una maggiore sicurezza e un accresciuto livello di protezione perché gli allegati possono essere memorizzati in una posizione centralizzata, soggetta al controllo dell'amministratore, e non vengono scaricati direttamente da client di posta elettronica che potrebbero eseguirli automaticamente. Inoltre, se si seleziona l'opzione "*Gestione automatica di Webmail del Collegamento allegati*", le posizioni dei file e gli URL di Webmail sono gestiti automaticamente. Con la gestione manuale di Collegamento allegati, è possibile specificare la posizione nella quale memorizzare i file e renderla dinamica mediante particolari macro. Per un corretto funzionamento di Collegamento allegati, è necessario aver attivato tale funzione a livello globale mediante l'opzione di questa schermata e aver configurato espressamente ogni account desiderato nella schermata Allegati 749 di Account Editor. Nella stessa schermata, è disponibile un'opzione che consente di applicare la funzione Collegamento allegati anche ai messaggi in uscita; i messaggi in uscita dell'account verranno estratti e sostituiti con un collegamento ai file memorizzati. I collegamenti inseriti da MDaemon nei messaggi non contengono i percorsi diretti dei file agli allegati. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura GUID è memorizzata nel file `AttachmentLinking.dat`.

Collegamento allegati tenterà di utilizzare il nome del file fornito nelle intestazioni MIME (se disponibili). Se il nome del file contiene più di 50 caratteri, verranno utilizzati solo gli ultimi 50 caratteri. Se al nome del file manca l'estensione, verrà aggiunta l'estensione ".att".

Per impostazione predefinita, la funzionalità Collegamento allegati attualmente inserisce il testo "MDaemon ha sostituito i file seguenti con questi collegamenti:" in alcune e-mail. Se si desidera modificare il testo, aggiungere la chiave seguente al file MDaemon.ini che si trova nella cartella \app\ e riavviare MDaemon:

```
[AttachmentLinking]
HeaderText=Questo è il mio testo.
```

Attiva collegamento allegati
Questa casella di controllo consente di attivare Collegamento allegati per tutti gli account espressamente configurati a questo scopo nella schermata Allegati[749] di Account Editor. Quando si attiva l'opzione globale, viene richiesto se si desidera anche attivare l'opzione specifica per tutti gli account di MDaemon. Se si seleziona "Sì", Collegamento allegati viene abilitato per tutti gli account e viene attivata anche l'opzione corrispondente nel modello Nuovo account[828]. Se si sceglie "No", la funzione Collegamento allegati viene abilitata, ma sarà necessario attivare manualmente l'estrazione degli allegati per ogni account. Quando è attivato il Collegamento allegati, il server Webmail deve rimanere attivo.

Gestione automatica di Webmail del Collegamento allegati
Questa è l'opzione predefinita quando si attiva Collegamento allegati. Utilizzare questa opzione se si desidera che il Collegamento allegati venga gestito automaticamente da Webmail. I file estratti vengono memorizzati in: "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\".

Configura manualmente Collegamento allegati
Questa opzione consente di indicare la cartella nella quale memorizzare gli allegati. Quando si seleziona questa opzione, è necessario indicare sia il percorso degli allegati che l'URL di Webmail.

Percorso allegati
Questa casella di testo consente di indicare la cartella in cui memorizzare gli allegati estratti. È possibile impostare un percorso statico o utilizzare le macro di modello[810] e script[857] per rendere il percorso dinamico. Ad esempio, con "$ROOTDIR$\Attachments\$DOMAIN$\" tutti gli allegati vengono raggruppati in una sottocartella denominata in base al dominio cui appartiene l'utente, contenuta in un'altra sottocartella denominata "Attachments" che si trova nella cartella principale di MDaemon, in genere C:\MDaemon\. Di conseguenza, nel caso di "utente1@esempio.com" già citato, gli allegati estratti vengono collocati nella sottocartella, "C:\MDaemon\Attachments\esempio.com\". Per definire ulteriormente la

posizione di memorizzazione degli allegati, è possibile aggiungere la macro di modello "$MAILBOX$" all'esempio precedente. In tal modo, i file di utente1 verranno memorizzati nella sottocartella di "\esempio.com\" denominata "utente1". Il nuovo percorso pertanto sarà: "C:\MDaemon\Attachments\esempio.com\utente1\".

URL Webmail
Immettere l'URL di Webmail (ad es. "http://mail.example.com:3000/WorldClient.dll"). MDaemon utilizza tale URL per inserire i collegamenti nei messaggi dai quali sono estratti gli allegati.

Ignora allegati di dimensioni inferiori al seguente numero di KB (0 = nessuno)
Rappresenta la dimensione minima richiesta perché un allegato venga estratto da un messaggio. Utilizzare questa opzione se non si desidera estrarre allegati di minori dimensioni. Se questa opzione è impostata su "0", la funzione Collegamento allegati estrarrà tutti gli allegati, indipendentemente dalla dimensione.

Elimina allegati più vecchi del seguente numero di giorni (0 = mai)
Questa opzione consente di impostare un limite al numero di giorni per cui gli allegati verranno memorizzati. Durante l'evento di pulizia giornaliero, MDaemon rimuoverà qualsiasi allegato memorizzato con data anteriore al limite specificato, se gli allegati sono contenuti nella cartella predefinita degli allegati o in una delle relative sottocartelle. La cartella predefinita è la seguente: "<MDaemonRoot>\Attachments\...". Gli allegati non vengono rimossi se si configura la cartella degli allegati in modo che faccia riferimento a un'altra posizione. Questa opzione è disabilitata per impostazione predefinita ("0").

Elimina gli allegati quando i messaggi vengono eliminati
Selezionare questa opzione per eliminare dal server gli allegati estratti quando i messaggi a cui sono associati vengono eliminati.

Se l'opzione è attivata e un utente raccoglie la posta con un client POP3 non configurato in modo da lasciare i messaggi nel server, tutti gli allegati estratti andranno persi. Se questa opzione non è attivata, non si perderà alcun allegato, ma è possibile che i file degli allegati non più necessari occupino inutilmente una notevole quantità di spazio su disco. Tutti i client POP consentono di lasciare i messaggi nel server.

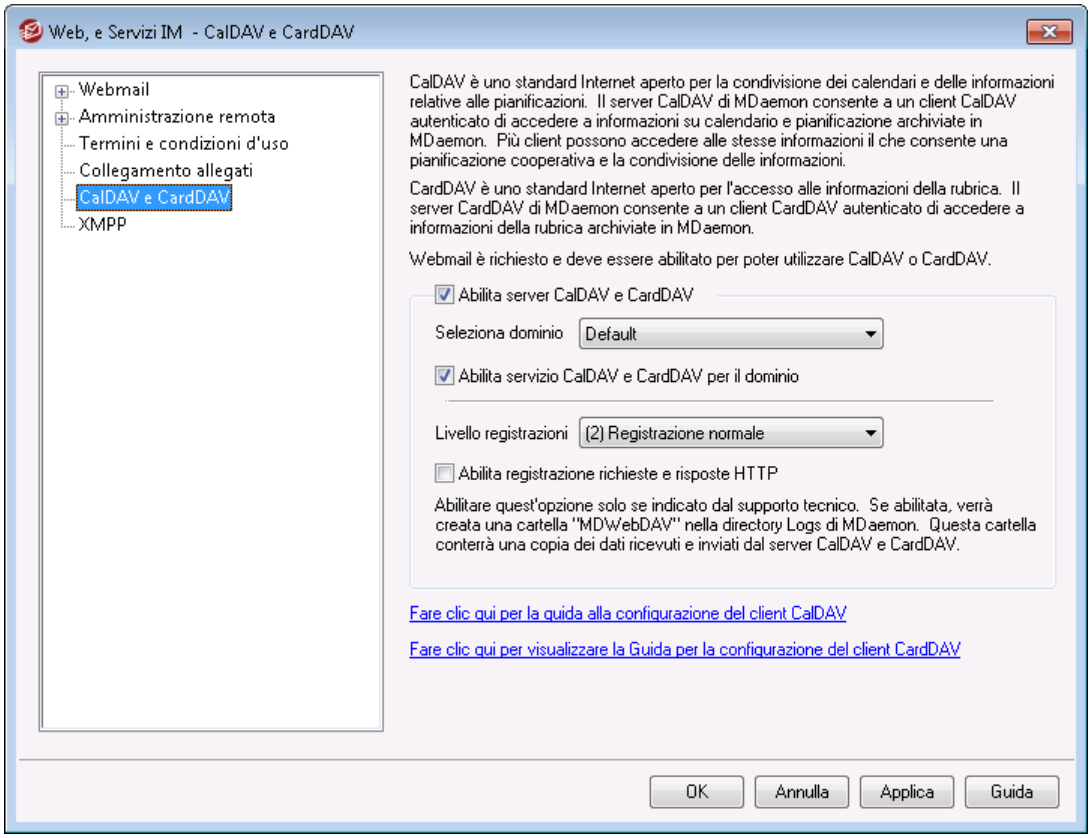
Estrai allegati di testo semplice Quoted Printable
Per impostazione predefinita, gli allegati di testo semplice Quoted Printable non vengono estratti. Selezionare questa casella di controllo se si desidera estrarre automaticamente questo tipo di allegato.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni di Collegamento allegati. Includere tutti i nomi di file che non si desidera estrarre dai messaggi. Il file Winmail.dat viene incluso in questo elenco per impostazione predefinita.

Vedere:

Modello Nuovi account 808
Account Editor » Allegati 749
Macro dei modelli 810
Macro degli script 857

3.6.5 CalDAV e CardDAV



CalDAV è uno standard Internet per la gestione e la condivisione delle informazioni relative a calendari e pianificazioni. Il supporto di CalDAV di MDaemon rende possibile l'utilizzo da parte degli account di un qualsiasi client che supporti CalDAV per accedere e gestire calendari e attività personali. I client possono anche accedere a qualsiasi calendario o attività pubblica 317 o condivisa 757 in base ai rispettivi diritti di accesso 319. CardDAV è uno standard per l'accesso alle informazioni su contatti/rubrica. Il server CardDAV consente a un client CardDAV autenticato di accedere alle informazioni di contatto memorizzate in MDaemon.

Abilita il server CalDAV e CardDAV
Il supporto CalDAV/CardDAV è abilitato per impostazione predefinita. Tuttavia, è richiesto Webmail e pertanto deve essere abilitato 330 per poterlo utilizzare. Se non si desidera CalDAV o CardDAV, disabilitare questa opzione. Per l'attivazione/disattivazione dei singoli domini, utilizzare le opzioni riportate di seguito.

Modifica delle impostazioni CalDAV/CardDAV predefinite per i domini
Inizialmente, tutti i domini di MDaemon avranno CalDAV/CardDAV attivato o disattivato in base alla selezione *predefinita* nell'elenco a discesa *Seleziona dominio*. Per modificare l'impostazione predefinita:

1. Nell'elenco a discesa *Seleziona dominio* selezionare **Predefinito**.
2. Selezionare la casella accanto a**Abilita servizio CalDAV e CardDAV per il dominio** se si desidera che CalDAV/CardDAV sia attivato per tutti i domini per impostazione predefinita o deselezionarla se si desidera sia disattivato per impostazione predefinita.
3. Fare clic su **OK**.

Attivazione/disattivazione di CalDAV/CardDAV per domini specifici
Per sovrascrivere l'impostazione CalDAV/CardDAV *predefinita* per i singoli domini:

1. Selezionare un dominio specifico nell'elenco a discesa *Seleziona dominio*.
2. Selezionare la casella accanto a **Abilita servizio CalDAV e CardDAV per il dominio** se si desidera che CalDAV/CardDAV sia attivato per il dominio o deselezionarla se si desidera sia disattivato.
3. Fare clic su **OK**.

Registrazione

Livello di registrazione
Questo elenco a discesa consente di specificare il livello di dettaglio utilizzato per registrare le attività CalDAV/CardDAV. Sono disponibili sei possibili livelli di registrazione: 1 - registrazione debug; 2 - registrazione normale (predefinita); 3 - solo avvisi e errori; 4 - solo errori; 5 - solo errori critici; 6 - nessuna registrazione. Si tratta di un'impostazione globale che non può essere applicata a specifici domini

Abilita richiesta HTTP e registrazione risposta
Se abilitata, questa opzione creerà una cartella `MDWebDAV` nella cartella dei registri di MDaemon. Tutti i dati inviati e ricevuti dal server CalDAV/CardDAV verranno registrati in tale cartella. Normalmente questa opzione sarebbe utilizzata solo per la diagnostica e non dovrebbe essere abilitata a meno che non venga richiesto dal Supporto tecnico.

Configurazione dei client CalDAV

Per configurare i client che supportano RFC 6764 (Individuazione dei servizi per le estensioni dei calendari per WebDAV (CalDAV)), dovrebbero essere richiesti solo il server, nome utente e password. È possibile configurare i record DNS perché indirizzino

il client all'URL corretto. Quando un record DNS non è stato configurato, l'utente può immettere uno speciale "URL ben conosciuto" sul client: "hostname/.well-known/caldav". Ad esempio: `http://example.com:3000/.well-known/caldav`. Il server Web integrato di Webmail supporta questo ben noto URL.

I client che non supportano l'individuazione automatica del servizio CalDAV, come Mozilla Thunderbird via il plug-in Lightning, richiederanno un URL completo per ciascun Calendario ed elenco di Attività. Gli URL CalDAV di MDaemon sono strutturati in questo modo:

Calendari e Attività
Calendario o elenco attività predefinite dell'utente:

`http://[host]/webdav/calendar`
(ad es. `http://esempio.com:3000/webdav/calendar`)

`http://[host]/webdav/tasklist`
(ad es. `http://esempio.com/webdav/tasklist`)

Calendario o elenco attività dell'utente:

`http://[host]/webdav/calendar/[nome-calendario]`
(ad es. `http://esempio.com/webdav/calendar/personal`)

`http://[host]/webdav/tasklist/[nome-elencoattività]`
(ad es. `http://esempio.com/webdav/tasklist/todo`)

Calendario o elenco attività personalizzato dell'utente:

http://[host]/webdav/calendar/[folder]/[nome-calendario]
(ad es. `http://esempio.com/webdav/calendar/my-stuff/personal`)

http://[host]/webdav/tasklist/[folder]/[nome-elencoattività]
(ad es. `http://esempio.com/webdav/tasklist/my-stuff/todo`)

Calendari e Attività condivisi
Calendario o elenco attività predefinite di un altro utente:

`http://[host]/webdav/calendars/[dominio]/[utente]`
(ad es. `http://esempio.com/webdav/calendars/example.net/frank`)

`http://[host]/webdav/tasks/[dominio]/[utente]`
(ad es. `http://esempio.com/webdav/tasks/example.net/frank`)

Calendario o elenco attività personalizzato di un altro utente:

`http://[host]/webdav/calendars/[dominio]/[utente]/[nome-calendario]`
(ad es.
`http://esempio.com/webdav/calendars/example.net/frank/personal`)

`http://[host]/webdav/tasks/[dominio]/[utente]/[nome-elencoattività]`
(ad es. `http://esempio.com/webdav/tasks/example.net/frank/todo`)

Calendari e Attività pubblici
Calendario o elenco attività predefinite del dominio:

`http://[host]/webdav/public-calendars/[dominio]`
(ad es. `http://esempio.com/webdav/public-calendars/example.com`)

`http://[host]/webdav/public-tasks/[dominio]`
(ad es. `http://esempio.com/webdav/public-tasks/example.com`)

Calendario o elenco attività nella cartella radice della gerarchia Cartella pubblica:

`http://[host]/webdav/public-calendars/[nome-calendario]`
(ad es. `http://esempio.com/webdav/public-calendars/holidays`)

`http://[host]/webdav/public-tasks/[nome-elencoattività]`
(ad es. `http://esempio.com/webdav/public-tasks/projects`)

è necessario prestare particolare attenzione quando si eseguono i test del client OutlookDAV. Se esistono più profili MAPI, si è notato che il client invia al server comandi di eliminazione per tutte le voci di calendario restituite dal server. OutlookDAV supporta solo il profilo MAPI predefinito.

Per ulteriori informazioni sull'impostazione dei client CalDAV, cercare "CalDav" nel sito Web della Knowledge Base di MDaemon.

Configurazione dei client CardDAV

Per configurare i client che supportanoRFC 6764 (Ricerca dei servizi per CalDAV (Calendaring Extensions to WebDAV) e CardDAV (vCard Extensions to WebDAV)), sono necessari solo l'indirizzo del server, il nome utente e la password. La rubrica Apple e iOS supportano questo standard. I record DNS possono essere impostati affinché indichino al client l'URL corretto. Quando un record DNS non è stato configurato, i client interrogano un "URL conosciuto", che nel caso di CardDAV è `/.well-known/carddav`. Il server Web integrato di Webmail supporta questo ben noto URL. I client che non supportano la ricerca automatica del servizio CardDAV necessitano di un URL completo.

I client CardDAV rilevanti sono i contatti Apple (inclusi in Mac OS X), Apple iOS (iPhone) e Mozilla Thunderbird tramite il plugin SOGO.

A partire da OS X 10.11 (EL Capitan), l'applicazione dei contatti Apple supporta un'unica raccolta/cartella. Quando il server CardDAV rileva l'applicazione dei contatti Apple, restituirà solo la cartella dei contatti predefiniti dell'utente autenticato. Inoltre, OS X 10.11 (EL Capitan) presenta un

problema noto che impedisce l'aggiunta di un account CardDAV utilizzando la vista "Avanzate" della finestra di dialogo.

Accesso alle rubriche
Il percorso "addressbook" è un collegamento alla propria rubrica predefinita.

`http://[host]/webdav/addressbook` - cartella dei contatti predefiniti.

`http://[host]/webdav/addressbook/friends` - cartella dei contatti "amici".

`http://[host]/webdav/addressbook/myfolder/personal` - cartella dei contatti "personali" presenti in una sottocartella denominata "myfolder".

Accesso alle cartelle condivise di un altro utente alle quali si ha accesso
Il percorso "contacts" è un collegamento alle cartelle dei contatti condivisi.

`http://[host]/webdav/contacts/example.com/user2` - cartella dei contatti predefiniti di utente2@example.com

`http://[host]/webdav/contacts/example.com/user2/myfolder` - cartella dei contatti "myfolder" di utente2@esempio.com

Accesso alle cartelle pubbliche alle quali si ha accesso
Il percorso "public-contacts" è un collegamento alle cartelle dei contatti pubblici.

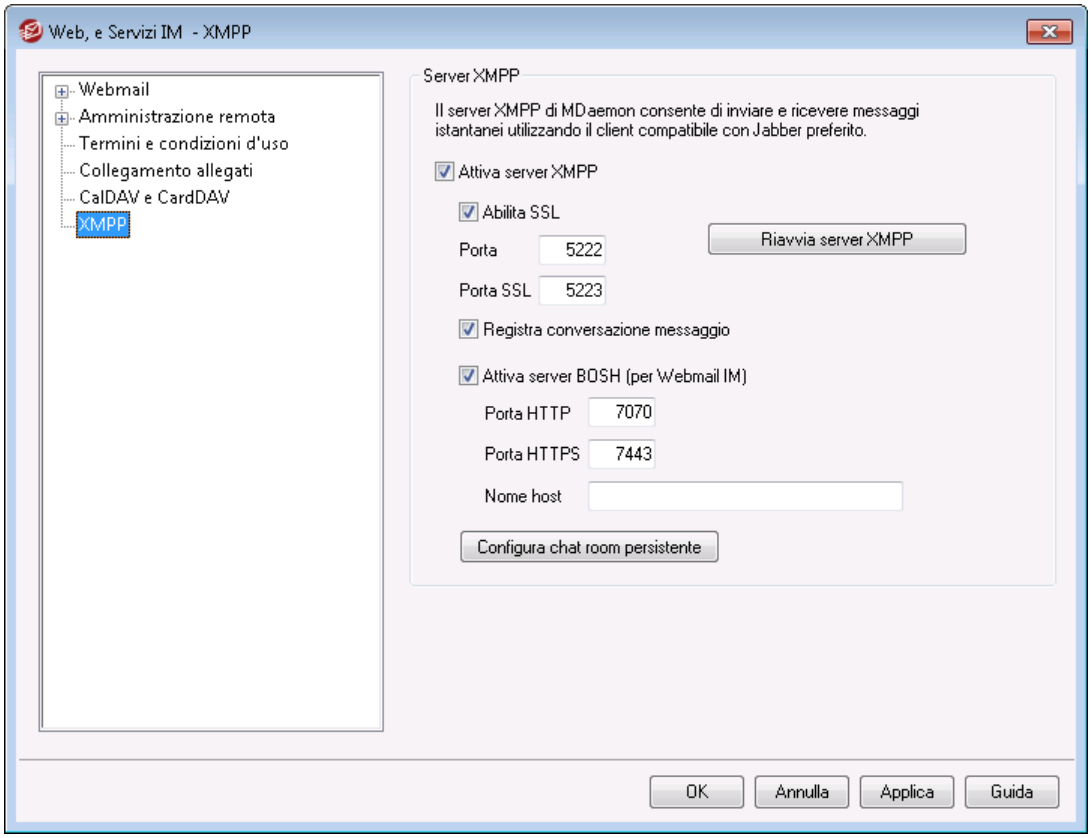
`http://[host]/webdav/public-contacts/example.com` - cartella dei contatti predefiniti di esempio.com

`http://[host]/webdav/public-contacts/foldername` - cartella dei contatti "foldername" nella radice della gerarchie di cartelle pubbliche

è necessario prestare particolare attenzione quando si eseguono i test del client OutlookDAV. OutlookDAV supporta solo il profilo MAPI predefinito. Se esistono più profili MAPI, il client potrebbe inviare al server comandi di eliminazione per tutte le voci restituite dal server.

Per ulteriori informazioni sull'impostazione dei client CardDAV, cercare "CardDAV" nel sito Web della Knowledge Base di MDaemon.

3.6.6 XMPP



MDaemon è dotato di un server XMPP (Extensible Messaging and Presence Protocol), talvolta definito server Jabber. Questo consente agli utenti di inviare e ricevere messaggi istantanei mediante MDaemon Instant Messenger 326 e client XMPP di terze parti, come Pidgin, Gajim, Swift e moti altri. I client sono disponibili per la maggior parte delle piattaforme dei dispositivi mobili e sistemi operativi.

Il server XMPP è installato come servizio Windows e le porte server predefinite sono la 5222 (SSL tramite STARTTLS) e 5223 (SSL dedicata). Il server XMPP utilizzerà la configurazione SLL di MDaemon se attivata in MDaemon. Inoltre, alcuni client XMPP utilizzano il record DNS SRV per il rilevamento automatico dei nomi host. Per ulteriori informazioni, visitare il sito http://wiki.xmpp.org/web/SRV_Records.

Gli utenti accedono attraverso il client XMPP preferito utilizzando indirizzo e-mail e password. Tuttavia alcuni client richiedono che l'indirizzo e-mail venga suddiviso in componenti separati per l'accesso. Ad esempio, anziché "`franco@esempio.com`", alcuni client richiedono "`franco`" come nome utente/accesso e "`esempio.com`" come dominio.

Per il servizio chat multiutente/gruppo, i client di solito mostrano "room" o "conference". Quando si desidera avviare una sessione chat di gruppo, creare una room/conference (assegnare un nome) e inviare gli altri utenti a tale chat room. Gran parte dei client non richiede di immettere una posizione server per la conferenza in quanto è sufficiente inserire un nome. Nel momento in cui viene richiesta questa operazione utilizzare comunque "`conference.<dominio>`" come posizione (ovvero. `conference.esempio.com`). Alcuni client richiedono di inserire il nome e la posizione

insieme nel modulo: "room@conference.<dominio>" (ovvero Room01@conference.esempio.com).

Alcuni client (ad esempio Pidgin) supportano il servizio di ricerca utenti consentendo agli utenti la ricerca del server mediante nome o indirizzo e-mail, il che rende molto più semplice aggiungere i contatti. Di solito non è necessario fornire una posizione di ricerca, se tuttavia viene richiesto utilizzare "search.<dominio>" (ad es. search.esempio.com). Durante la ricerca, è possibile utilizzare il simbolo % come carattere jolly. Pertanto è possibile utilizzare "%@esempio.com" nel campo dell'indirizzo e-mail per visualizzare un elenco di tutti gli utenti il cui indirizzo e-mail termina con "@esempio.com."

Server XMPP

Attiva server XMPP
Fare clic su questa opzione per abilitare il server XMPP. Per consentire la messaggistica istantanea è necessario accertarsi che l'opzione **Abilita messaggistica istantanea** sia attivata nella schermata MDIM 340.

Abilita SSL
Fare clic su questa opzione per supportare SSL per il server XMPP, utilizzando la *porta SSL* specificata di seguito. **Nota:** quanto detto vale anche per l'opzione *Porta HTTPS* del server BOSH riportata di seguito.

Porta
La porta predefinita per XMPP è la 5222, che supporta SSL tramite STARTTLS.

Porta SSL
La porta SSL dedicata di XMPP è la 5223.

Riavvia server XMPP
Fare clic su questo pulsante per riavviare il server XMPP.

Registra conversazione messaggio
Per impostazione predefinita tutte le conversazioni di messaggistica istantanea vengono registrate in un file denominato XMPPServer-<date>.log, ubicato nella cartellaMDaemon\Logs\. Se non si desidera registrare le conversazioni, deselezionare questa casella di controllo.

Attiva server BOSH (per Webmail IM)
Fare clic su questa opzione per attivare il server BOSH e consentire l'uso della messaggistica istantanea in MDaemon Webmail.

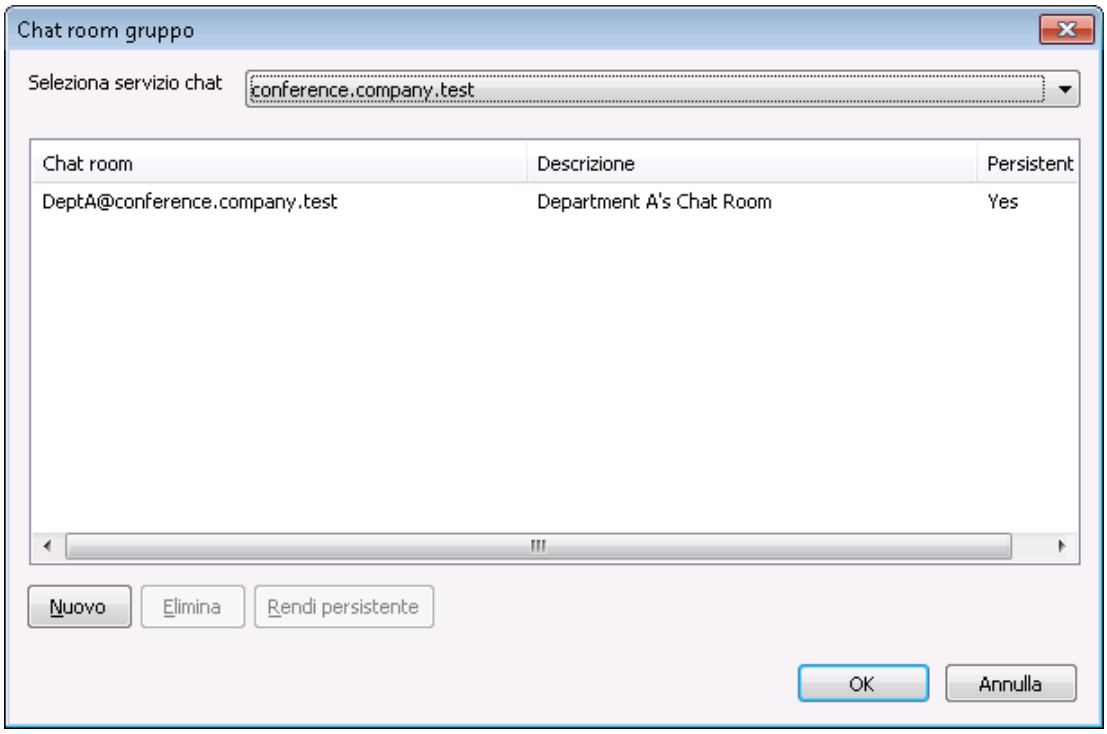
Porta HTTP
Per impostazione predefinita il server BOSH utilizza la porta HTTP 7070.

Porta HTTPS
Il server BOSH utilizza questa porta HTTPS quando si attiva l'opzione *Abilita SSL* sopra descritta. La porta predefinita è 7443.

Nome host
Utilizzare questa opzione per specificare, se necessario, un nome host.

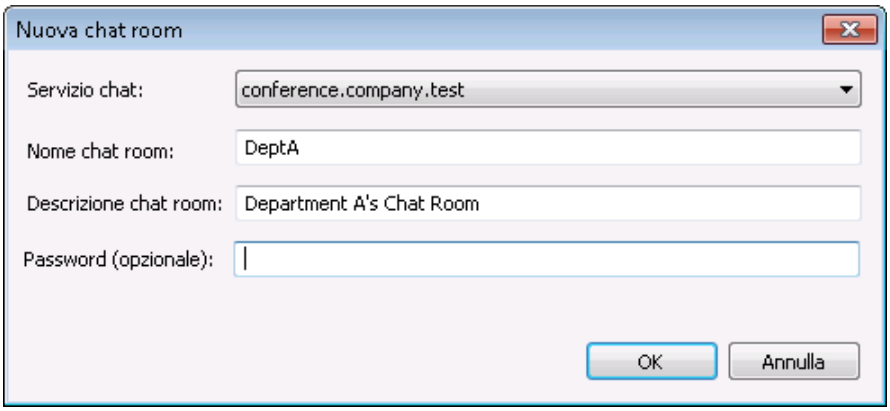
Configura chat room persistenti

Fare clic su questo pulsante per visualizzare la finestra di dialogo Chat room di gruppo. In genere, quando un utente crea una chat room, questa viene eliminata non appena l'ultima persona partecipante esce dalla chat room, ma è possibile utilizzare queste opzioni per creare chat room persistenti che restano attive anche se vuote. È inoltre possibile eliminare le chat room e convertire quelle temporanee già esistenti in persistenti.



Seleziona servizio chat
Selezionare il servizio chat per visualizzare le chat room di tale dominio.

Nuova
Fare clic su questo pulsante per aggiungere una chat room persistente.



Seleziona servizio chat
Selezionare il servizio chat per la chat room.

Nome chat room
Digitare un nome per la chat room, senza inserire spazi.

Descrizione chat room
Immettere qui una descrizione della chat room. Gli utenti visualizzeranno questo testo quando selezioneranno la chat room a cui partecipare.

Password (facoltativa)
Per richiedere l'immissione di una password per accedere alla chat, immettere qui la password.

Elimina
Per rimuovere una chat room, selezionare la chat room e fare clic su questo pulsante per eliminarla.

Rendi persistente
Quando una chat room è già presente nell'elenco, selezionare la chat room e fare clic su questo pulsante per renderla persistente.

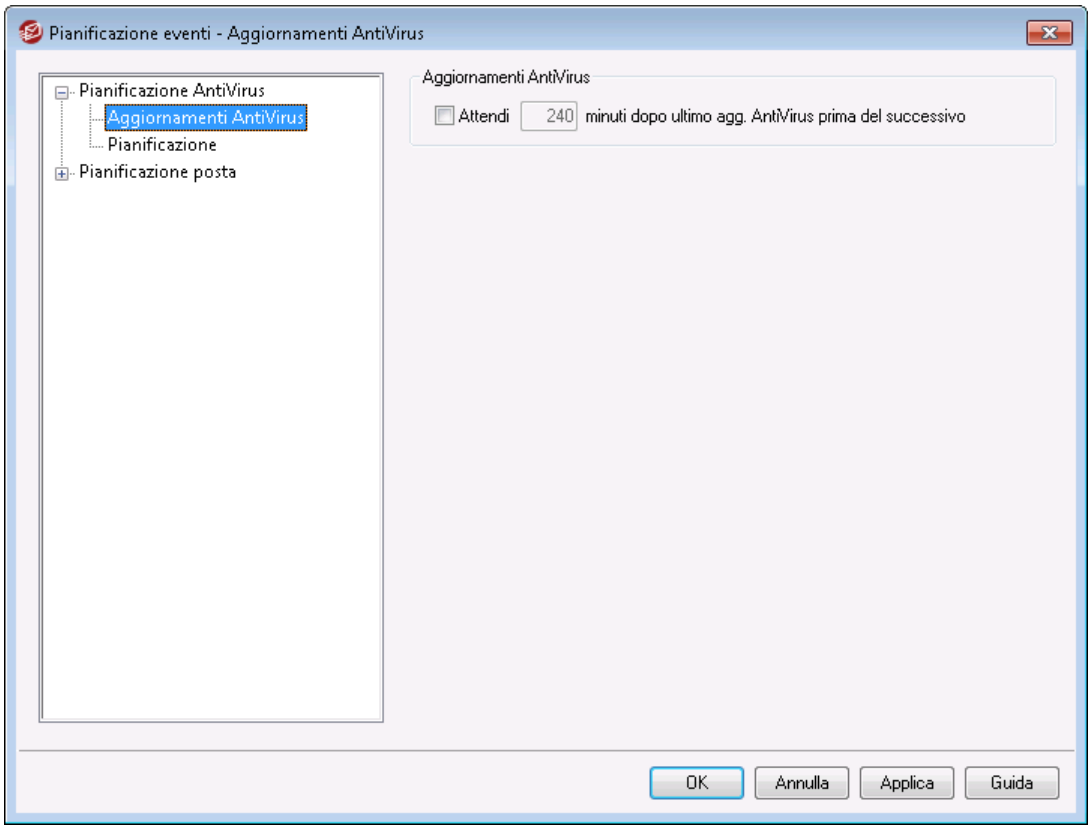
Vedere:

Webmail » MDIM 340

3.7 Pianificazione eventi

3.7.1 Pianificazione AntiVirus

3.7.1.1 Aggiornamenti AntiVirus



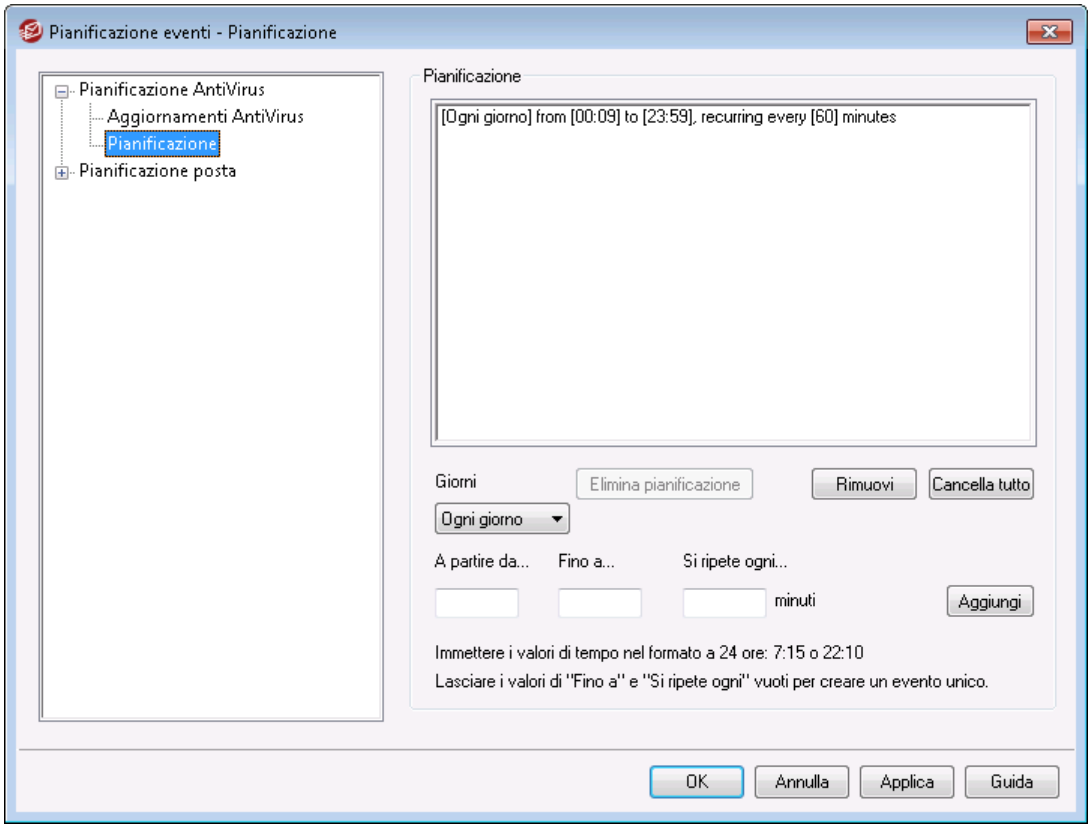
Aggiornamenti AntiVirus

Attendi XX minuti dopo ultimo agg. AntiVirus prima del successivo
Fare clic su questa casella di controllo e specificare il numero di minuti per cui si desidera che AntiVirus attenda prima di verificare la presenza di nuovi aggiornamenti delle definizioni dei virus. In realtà si tratta del numero di minuti per cui AntiVirus *tenterà* di attendere dopo l'ultima ricerca di un aggiornamento, sia effettuata manualmente che attivata da una funzione di pianificazione. Gli aggiornamenti eseguiti manualmente o da un'utilità di pianificazione hanno la precedenza su questa impostazione. Di conseguenza, al verificarsi di uno di questi aggiornamenti di AntiVirus, il contatore viene azzerato. In altri termini, se l'opzione è impostata per verificare la disponibilità di aggiornamenti ogni 240 minuti e dopo 100 minuti si cerca manualmente un aggiornamento, il contatore verrà reimpostato su 240 minuti.

Per ulteriori informazioni, vedere:

Pianificazione degli aggiornamenti AntiVirus 386
AntiVirus 684
Utilità di aggiornamento AntiVirus 688

3.7.1.2 Pianificazione



La pianificazione degli aggiornamenti AntiVirus consente di indicare orari specifici nei quali controllare gli aggiornamenti di AntiVirus. La pianificazione è disponibile in: Impostazioni » Pianificazione eventi » Aggiornamenti AntiVirus » Pianificazione.

Pianificazione

Rimuovi
Per rimuovere un evento dall'elenco, selezionare la voce desiderata e fare clic su questo pulsante.

Cancella tutto
Con questo pulsante vengono rimosse tutte le voci della pianificazione.

Creazione di eventi pianificati

Giorni
Quando si crea un nuovo evento pianificato, è necessario selezionare innanzitutto in quali giorni si desidera che si verifichi il controllo dell'aggiornamento. È possibile selezionare: tutti i giorni, giorni feriali (da lunedì a venerdì), fine settimana (sabato e domenica) oppure determinati giorni della settimana.

Ora inizio
Inserire l'ora in cui si desidera che abbia inizio il controllo degli aggiornamenti. Il valore dell'ora deve essere in formato 24 ore e compreso tra le 00:00 e le 23:59. Se si desidera che l'evento sia isolato anziché ricorrente, inserire solo questo valore, lasciando vuote le opzioni *Ora fine* e *Ogni*.

Ora fine
Inserire l'ora in cui si desidera che termini il controllo degli aggiornamenti. Il formato dell'orario deve essere di 24 ore, dalle 00:01 alle 23:59 e il valore deve essere successivo a quello di *Ora inizio*. Se, ad esempio, il valore di *Ora inizio* è "10:00", questo valore deve essere compreso tra le "10:01" e le "23:59". Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Ogni [xx] minuti
Questa è la frequenza con cui AntiVirus controllerà la presenza di aggiornamenti tra gli orari designati *Dalle...* e *Alle...*. Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

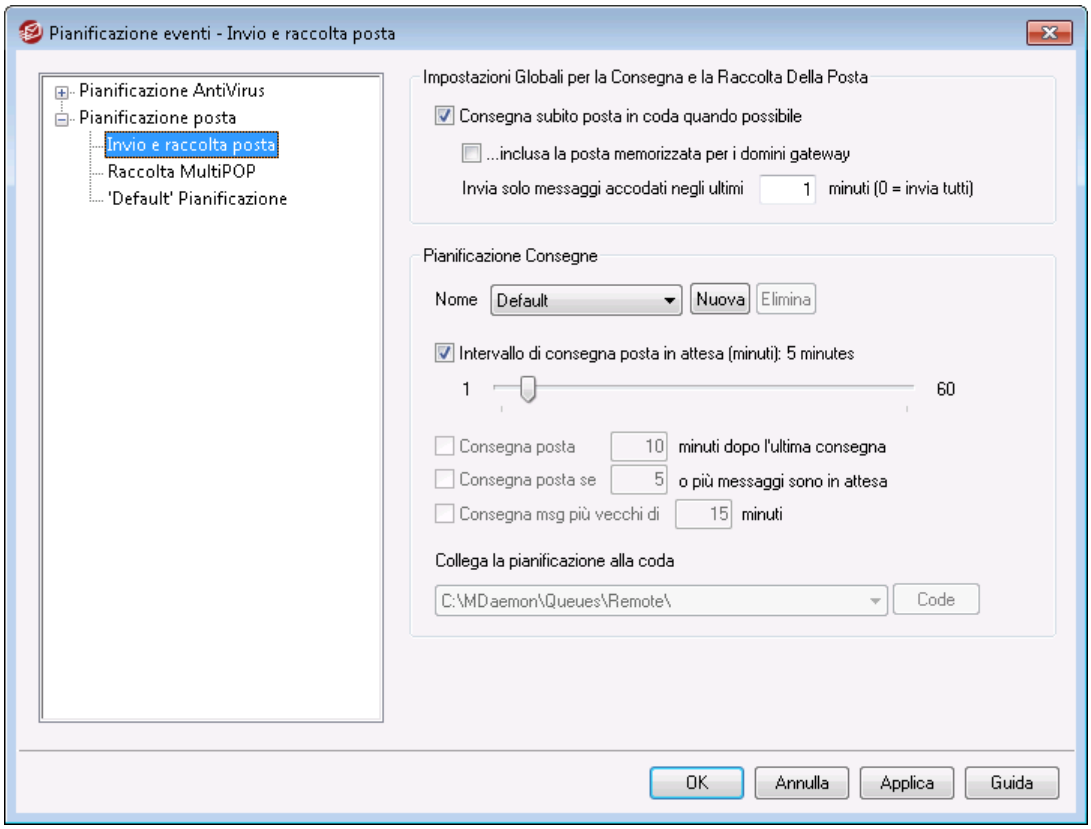
Aggiungi
Dopo aver indicato i *Giorni* e l'*Ora inizio*, l'*Ora fine* facoltativa e il valore *Ogni*, aggiungere l'evento alla pianificazione con questo pulsante.

Vedere:

Aggiornamenti AntiVirus
AntiVirus 684
Utilità di aggiornamento AntiVirus 688

3.7.2 Pianificazione della posta

3.7.2.1 Invio e raccolta della posta



Fare clic su Impostazioni » Pianificazione eventi per aprire la pianificazione venti di MDaemon. In questa schermata è possibile pianificare gli eventi di elaborazione della posta remota di MDaemon, in modo semplice o avanzato, a seconda delle esigenze. È possibile utilizzare un contatore per elaborare la posta a intervalli regolari oppure si possono specificare gli orari precisi per il recapito e la raccolta utilizzando le schermate Pianificazione della posta 393 . È inoltre possibile impostare delle condizioni che attivano l'elaborazione della posta a prescindere dagli orari pianificati, ad esempio al raggiungimento di un determinato numero di messaggi in attesa di essere consegnati oppure alla scadenza del tempo specificato. Inoltre, è possibile creare pianificazioni personalizzate che possono essere assegnate a code di posta remote personalizzate. Le pianificazioni personalizzate consentono di impostare pianificazioni differenti in base ai diversi tipi di messaggio. Ad esempio, è possibile creare pianificazioni per messaggi di grandi dimensioni, per messaggi di liste di distribuzione, per specifici domini e così via.

Utilizzare la sezione Aggiornamenti AntiVirus 385 della pianificazione eventi per programmare la frequenza con cui MDaemon controllerà la presenza di aggiornamenti di AntiVirus 658.

Impostazioni globali per la consegna e la raccolta della posta

Consegna subito posta in coda quando possibile
Se questa opzione è abilitata, quando un messaggio viene ricevuto e accodato per la consegna remota, anziché attivare l'elaborazione della posta dopo il successivo intervallo pianificato o a seguito di un altro evento, MDaemon elabora e consegna immediatamente tutta la posta remota inserita nella coda nel periodo di tempo indicato nell'opzione *Invia solo messaggi accodati negli ultimi XX minuti*.

...inclusa la posta memorizzata per i domini gateway
Selezionare questa casella di controllo se si desidera che i messaggi per i gateway di dominio vengano consegnati immediatamente. Questa opzione si applica, tuttavia, solo ai gateway per i quali sia stata abilitata l'opzione *Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota* nella schermata Gateway 262 di Gateway Editor.

Invia solo messaggi accodati negli ultimi XX minuti (0=invia tutti)
Questa opzione consente di specificare il tempo di attesa nella coda dei messaggi prima dell'esecuzione dell'opzione *Consegna subito posta in coda quando possibile*. Quando tale opzione attiva l'elaborazione della posta remota, MDaemon elabora solo i messaggi inseriti nella coda dal numero di minuti specificato anziché elaborare indiscriminatamente tutti i messaggi presenti nella coda. L'intera coda viene comunque elaborata quando si preme uno dei pulsanti *Elabora coda...* della barra degli strumenti o quando un normale evento di pianificazione attiva l'elaborazione della posta remota. L'impostazione predefinita di questa opzione è di un minuto. Se si desidera elaborare l'intera coda a ogni attivazione dell'elaborazione della posta remota è possibile impostare l'opzione su 0. Tuttavia, questa impostazione non è consigliabile in quanto molto meno efficiente.

Le opzioni descritte in precedenza vengono applicate solo alla pianificazione predefinita (Default) e non sono disponibili per le pianificazioni personalizzate. Vedere l'opzione *Nome* descritta successivamente.

Pianificazioni di consegna

Nome
Utilizzare questa casella di riepilogo a discesa per selezionare la pianificazione da modificare. La pianificazione Default viene utilizzata per le code di posta normali e remote, nonché per la posta raccolta mediante DomainPOP e MultiPOP. Nel caso di configurazioni che includano servizi di accesso remoto (RAS), la pianificazione Default viene utilizzata anche per i domini LAN, ossia per i domini remoti definiti come residenti nella rete locale in uso e che, di conseguenza, non prevedono l'uso di connessioni RAS. È possibile assegnare altre pianificazioni a code di posta remote personalizzate e instradare i messaggi verso tali code personalizzate 893 automaticamente utilizzando il Filtro contenuti 659. Dopo aver completato la modifica di una pianificazione, fare clic su OK oppure selezionare un'altra pianificazione da modificare. Se si apportano modifiche a una pianificazione e si seleziona un'altra pianificazione, viene visualizzata una casella di conferma che richiede di salvare o annullare le modifiche apportate prima di passare alla pianificazione desiderata.

Nuova
Fare clic su questa opzione per creare una nuova pianificazione. Viene aperta una casella per l'inserimento del nome. Dopo aver indicato il nome della pianificazione, nel menu di sinistra viene creata una schermata Pianificazione 393 apposita. Utilizzare la schermata per assegnare i tempi alla pianificazione.

Elimina
Per eliminare una pianificazione personalizzata, selezionarla nell'elenco a discesa *Nome*, quindi fare clic su *Elimina*. Viene visualizzata una finestra che richiede di confermare l'eliminazione. L'eliminazione di una pianificazione personalizzata non determina l'eliminazione delle code remote personalizzate o delle regole di Filtro contenuti associate alla pianificazione. Tuttavia, se si elimina una coda personalizzata, verranno eliminate anche le pianificazioni personalizzate e le regole di Filtro contenuti associate alla coda.

Intervallo di consegna posta in attesa (minuti):
Selezionare questa casella di controllo e spostare il cursore verso destra o sinistra per specificare l'intervallo di tempo tra ogni sessione di elaborazione della posta. Il conteggio alla rovescia può essere impostato su un valore compreso tra 1 e 60 minuti. Allo scadere del tempo stabilito, MDaemon elaborerà la posta remota e il conto alla rovescia verrà reimpostato sul valore originale. Se la casella di controllo è deselezionata, gli intervalli di elaborazione della *posta remota* saranno determinati dalle altre opzioni di pianificazione.

Consegna posta XX minuti dopo l'ultima consegna
Questa opzione consente di indicare l'esecuzione a intervalli di tempo regolari delle sessioni di elaborazione della posta remota successive all'ultima sessione, indipendentemente dall'evento che ha avviato quest'ultima. A differenza degli intervalli fissi stabiliti con l'impostazione di orari specifici o utilizzando la barra di scorrimento *Intervallo di consegna posta in attesa*, con questa opzione l'intervallo orario viene reimpostato ad ogni elaborazione della posta.

Consegna posta se XX o più messaggi sono in attesa
Se si abilita questa opzione, MDaemon avvia una sessione di posta quando il numero di messaggi in attesa nella coda remota è uguale o superiore al valore specificato in questo campo. Queste sessioni di posta sono aggiuntive rispetto a tutte le altre normalmente pianificate.

Consegna msg più vecchi di XX minuti
Se questa casella è abilitata, MDaemon avvia sempre una sessione di posta quando un messaggio è rimasto nella coda per il numero di minuti specificato. Queste sessioni sono aggiuntive rispetto a tutte le altre normalmente pianificate.

Code

Collega la pianificazione alla coda
Utilizzare questa opzione per associare la pianificazione selezionata a una specifica coda di posta remota personalizzata. Mediante Filtro contenuti sarà quindi possibile creare regole che consentano di inserire alcuni messaggi nella coda personalizzata. Se, ad esempio, si desidera pianificare la consegna in un determinato momento dei messaggi delle liste di distribuzioni indirizzati a destinatari remoti, è possibile creare

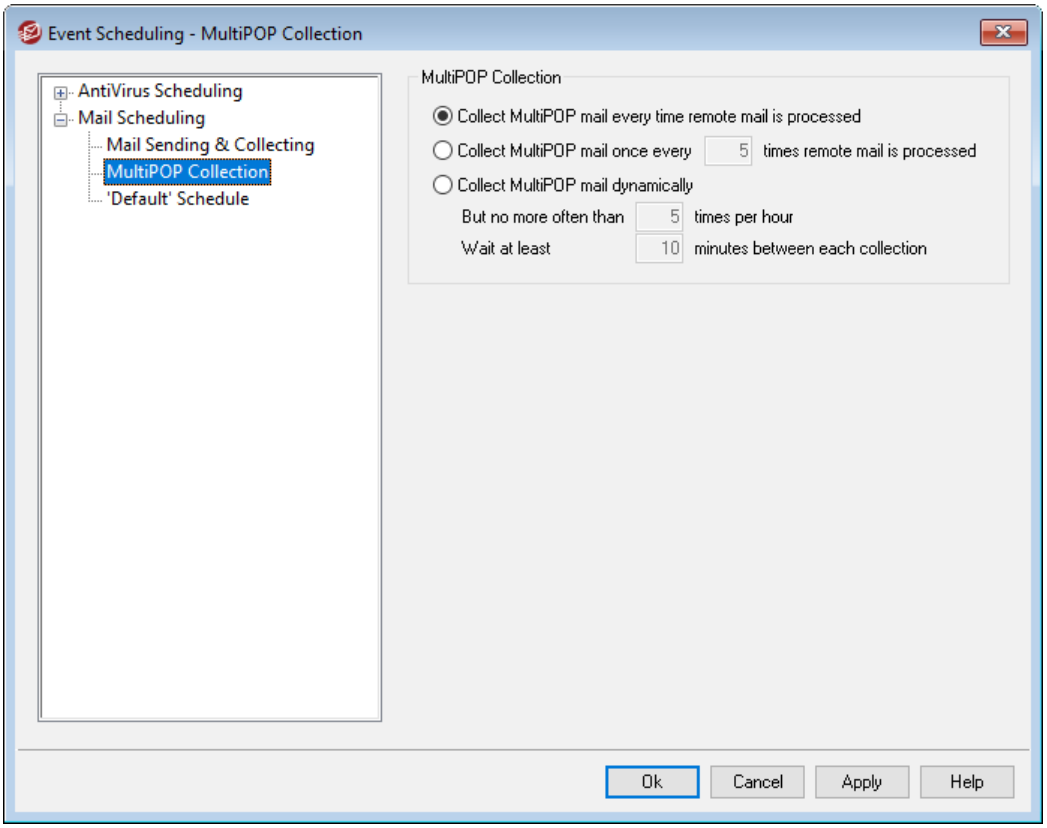
una coda personalizzata associata a tali messaggi, definire una regola che collochi tutti i messaggi di questo tipo nella coda personalizzata e creare una pianificazione personalizzata da assegnare alla coda in questione.

Code
Questo pulsante consente di aprire la schermata Code personalizzate 893, per la creazione di code remote personalizzate da utilizzare con Pianificazione eventi.

Vedere:

Pianificazione della posta 393
Aggiornamenti AntiVirus 385

3.7.2.2 Raccolta MultiPOP



Raccolta MultiPOP

Raccogli la posta MultiPOP a ogni elaborazione della posta remota
Scegliere questa opzione per consentire a MDaemon di raccogliere tutta la posta MultiPOP 754 a ogni elaborazione della posta remota.

Raccogli posta MultiPOP ogni XX elaborazioni della posta remota
Scegliere questa opzione e specificare un valore nel campo per raccogliere la posta MultiPOP con una frequenza inferiore a quella di elaborazione della posta remota. Il

valore indica per quante volte la posta remota viene elaborata prima della raccolta della posta MultiPOP.

Raccogli posta MultiPOP in modo dinamico
Scegliere questa opzione per raccogliere i messaggi MultiPOP in modo dinamico. Di norma, la posta MultiPOP viene raccolta per tutti gli utenti contemporaneamente a ogni intervallo di elaborazione remota della posta oppure ogni *x* intervalli. Quando raccolti dinamicamente, i messaggi MultiPOP vengono raccolti per ogni singolo utente che controlla la posta locale tramite POP, IMAP o Webmail, anziché per tutti gli utenti contemporaneamente. Tuttavia, poiché la raccolta MultiPOP viene attivata quando l'utente controlla la posta, gli eventuali nuovi messaggi MultiPOP raccolti non risulteranno visibili all'utente finché questi non controlla *nuovamente* la posta. Sarà quindi necessario controllare la posta due volte per visualizzare i nuovi messaggi MultiPOP, La prima volta per attivare MultiPOP e la seconda volta per visualizzare la posta raccolta.

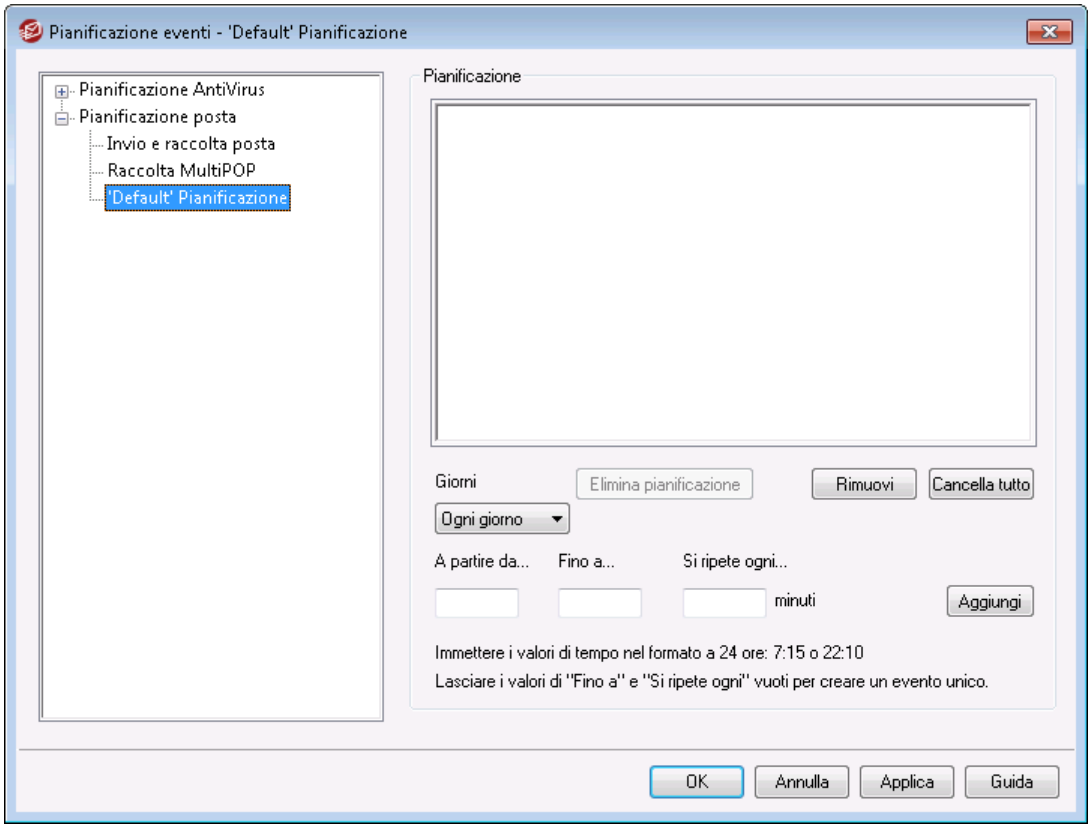
Ma non più di XX volte all'ora
Per ridurre ulteriormente il carico generato dall'uso frequente del metodo MultiPOP, è possibile avvalersi di questo comando e specificare quanto volte in un'ora deve essere raccolta la posta MultiPOP per ogni utente.

Attendi almeno XX minuti tra una raccolta e l'altra
Questa opzione è utile per ridurre il carico del server di posta, poiché limita la frequenza con cui i messaggi MultiPOP possono essere raccolti per ogni utente. L'opzione consente di impostare la raccolta della posta MultiPOP per utente in base a intervalli specifici, espressi in minuti. Specificare il numero di minuti che si desidera trascorrano prima che all'utente sia consentito di controllare di nuovo la posta MultiPOP.

Vedere:

MultiPOP 146
Account Editor | MultiPOP 754

3.7.2.3 Pianificazione della posta



Ciascuna Pianificazione della posta corrisponde alla pianificazione con il medesimo nome riportata nell'elenco a discesa *Nome* nella schermata Invio e raccolta posta 388. Le singole pianificazioni della posta consentono di indicare gli orari in cui, per quella pianificazione, si verificherà l'elaborazione remota della posta. Le pianificazioni della posta sono situate nel percorso: Impostazioni » Pianificazione eventi » Pianificazione della posta » Pianificazione "NomePianificazione".

Pianificazione

Elimina pianificazione
Questo pulsante consente di eliminare la pianificazione della posta personalizzata. La pianificazione verrà eliminata e la voce corrispondente sarà eliminata dall'elenco a discesa *Nome* nella schermata Invio e raccolta posta 388. Quando si seleziona questo pulsante, viene aperta una finestra con una richiesta di conferma. Questa opzione è disponibile solo per le pianificazioni personalizzate, mentre non è possibile eliminare la pianificazione Default.

Rimuovi

Per rimuovere una voce dall'elenco, selezionarla e fare clic su questo pulsante.

Cancella tutto
Con questo pulsante vengono rimosse tutte le voci della pianificazione.

Creazione di eventi pianificati

Giorni
Quando si crea un nuovo evento di pianificazione, è necessario selezionare innanzitutto in quali giorni si desidera che si verifichi. È possibile selezionare: tutti i giorni, giorni feriali (da lunedì a venerdì), fine settimana (sabato e domenica) oppure determinati giorni della settimana.

Ora inizio
Inserire l'ora in cui si desidera che l'evento abbia inizio. Il valore dell'ora deve essere in formato 24 ore e compreso tra le 00:00 e le 23:59. Se si desidera che l'evento sia isolato anziché ricorrente, inserire solo questo valore, lasciando vuote le opzioni *Ora fine* e *Ogni*.

Ora fine
Inserire l'ora in cui si desidera che l'evento si concluda. Il formato dell'orario deve essere di 24 ore, dalle 00:01 alle 23:59 e il valore deve essere successivo a quello di *Ora inizio*. Se, ad esempio, il valore di *Ora inizio* è "10:00", questo valore deve essere compreso tra le "10:01" e le "23:59". Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Ogni [xx] minuti
Indica l'intervallo orario in cui la posta verrà elaborata tra gli orari *Ora inizio* e *Ora fine* indicati. Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Aggiungi
Dopo aver indicato i *Giorni* e l'*Ora inizio*, l'*Ora fine* facoltativa e il valore *Ogni*, aggiungere l'evento alla pianificazione con questo pulsante.

A seconda delle esigenze, può essere sufficiente utilizzare le opzioni di pianificazione della schermata Invio e raccolta posta 388 per controllare gli intervalli di elaborazione della posta. Ad esempio, non è necessario stabilire una pianificazione specifica con eventi per ogni minuto di ogni giorno quando è sufficiente impostare la barra di scorrimento di Invio e raccolta della posta su intervalli di un minuto per ottenere lo stesso risultato. Per specificare intervalli di elaborazione superiori a 60 minuti, anche solo per alcuni giorni, è possibile avvalersi di una combinazione di opzioni di pianificazione e di orari specifici.

Vedere:

Invio e raccolta della posta 388
Aggiornamenti AntiVirus 385
Aggiornamenti Antispam 712

3.8 MDaemon Connector

Il supporto di MDaemon Private Cloud per MDaemon Connector (MC) consente a tutti gli utenti che lo desiderano di utilizzare Microsoft Outlook come client e-mail preferito, purché MC sia installato sul loro computer. MC offre funzionalità di groupware e collaborazione mettendo in connessione il client Outlook con il server MDaemon, per favorire l'impiego di e-mail, calendario con programmazione libero/occupato, rubrica, liste di distribuzione, attività e note di Outlook.

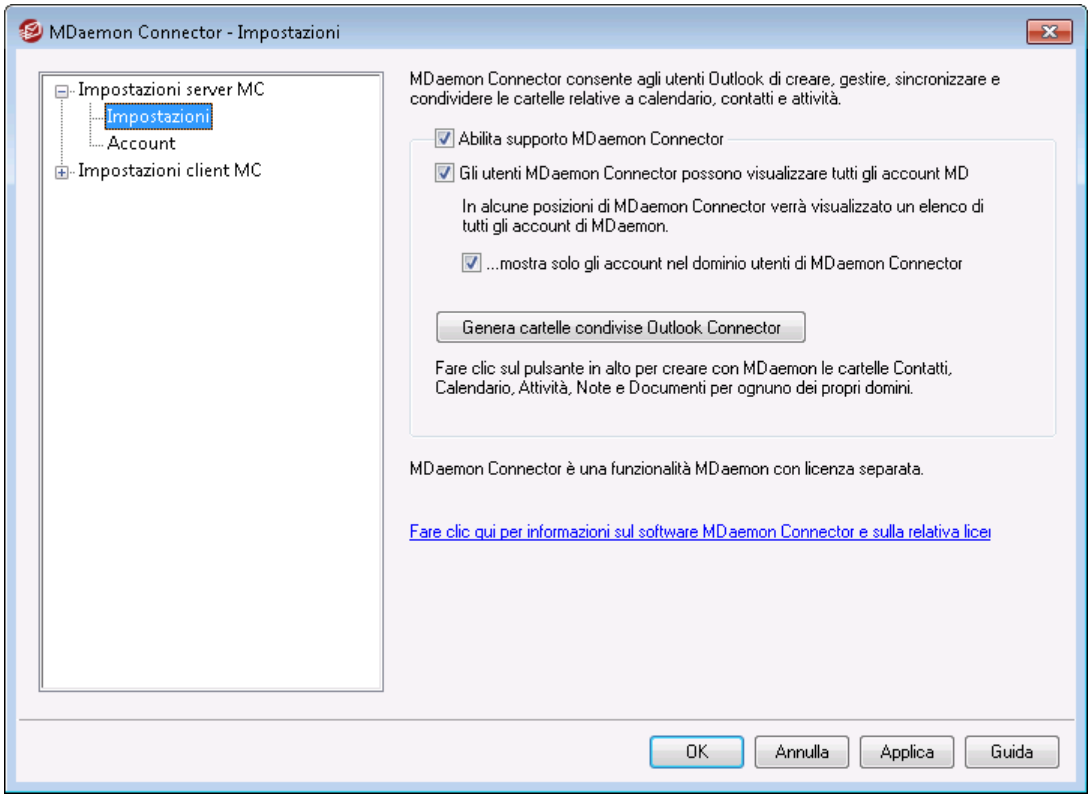
Disponibile in: Impostazioni » MDaemon Connector, la finestra di dialogo di MDaemon Connector può essere utilizzata per attivare e configurare il supporto di MC, nonché per autorizzarne l'uso a specifici account.

Vedere:

Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397
Impostazioni client MC 398

3.8.1 Impostazioni server MC

3.8.1.1 Impostazioni



MDaemon Connector

Abilita supporto MDaemon Connector
Fare clic su questa casella di controllo per abilitare il supporto per MDaemon Connector (MC). Se questa opzione è deselezionata, gli utenti non potranno utilizzare MC.

Gli utenti MDaemon Connector possono visualizzare tutti gli account MD
Selezionare questa opzione se si desidera che tutti gli account MDaemon autorizzati a connettersi tramite MC siano visibili nell'elenco *Autorizzazioni* che appare nel plug-in di MDaemon Connector nei client degli utenti. Da tale elenco gli utenti MC possono scegliere gli account a cui desiderano concedere l'autorizzazione per la condivisione dei propri elementi di Outlook. Se si disabilita questa opzione, l'elenco *Autorizzazioni* di MDaemon Connector risulterà vuoto e sarà necessario inserire gli indirizzi e-mail manualmente. In questo caso, potranno condividere gli elementi di Outlook solo gli indirizzi appartenenti agli account autorizzati per la connessione mediante MC. Se un utente immette un indirizzo non autorizzato, quest'ultimo non potrà condividere gli elementi, a meno che non venga autorizzato a connettersi mediante MC in un momento successivo.

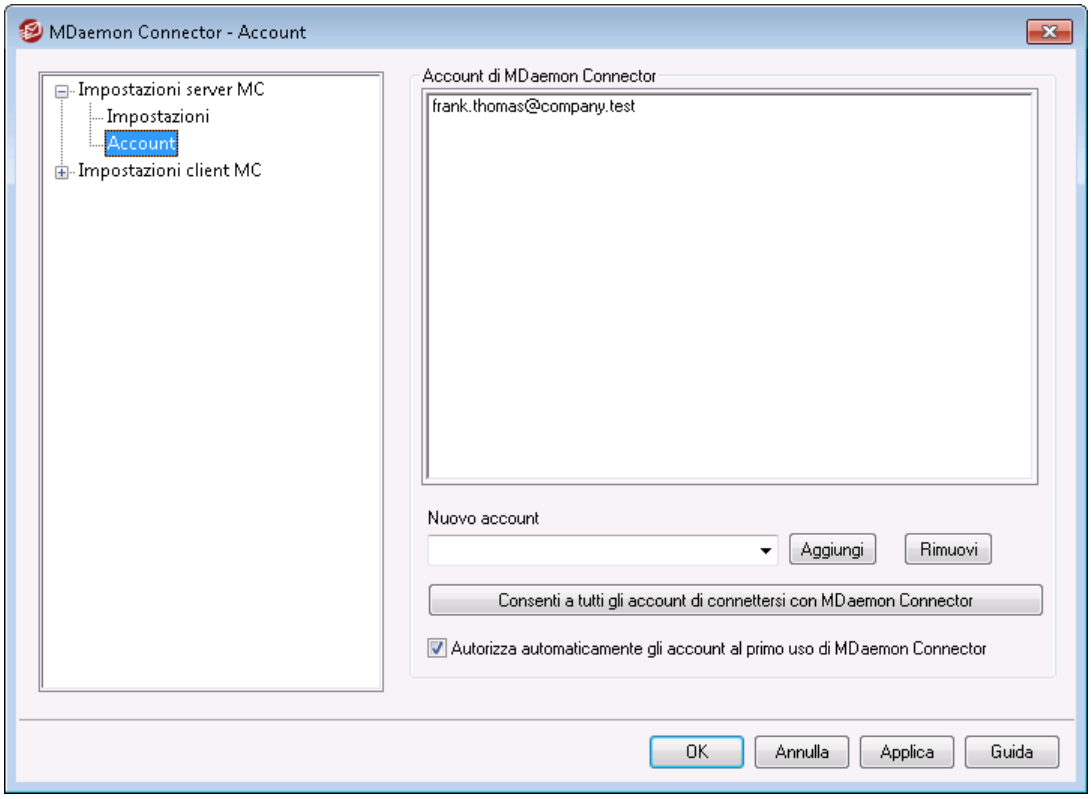
...mostra solo gli account nel dominio utenti di MDaemon Connector
Questa opzione è disponibile solo qualora sia stata abilitata l'opzione *Gli utenti MDaemon Connector possono visualizzare tutti gli account MD*. Selezionare questa casella di controllo se si desidera che gli utenti autorizzati a connettersi mediante MC, e che appartengono al medesimo dominio, siano riportati nell'elenco *Autorizzazioni* in MDaemon Connector. Gli account che appartengono ad altri domini non saranno inclusi nell'elenco anche se sono autorizzati a connettersi mediante MC.

Genera cartelle condivise MDaemon Connector
Fare clic su questo pulsante per generare un insieme di cartelle di MC per ogni dominio. Verranno create le cartelle dei contatti, degli appuntamenti, del diario, delle attività e delle note.

Vedere:

Impostazioni server MC » Account 397
Impostazioni client MC 398

3.8.1.2 Account



Account MDaemon Connector

In questo elenco vengono indicati gli account di MDaemon autorizzati a condividere le cartelle, il calendario, le note e le informazioni sui contatti di Outlook mediante MDaemon Connector. Per aggiungere account all'elenco, utilizzare le opzioni descritte di seguito.

Nuovo account
Per aggiungere un account di MDaemon all'elenco degli account autorizzati di MDaemon Connector, selezionare la voce desiderata nell'elenco a discesa e fare clic su *Aggiungi*. Per rimuovere un account, selezionarlo e fare clic su *Rimuovi*.

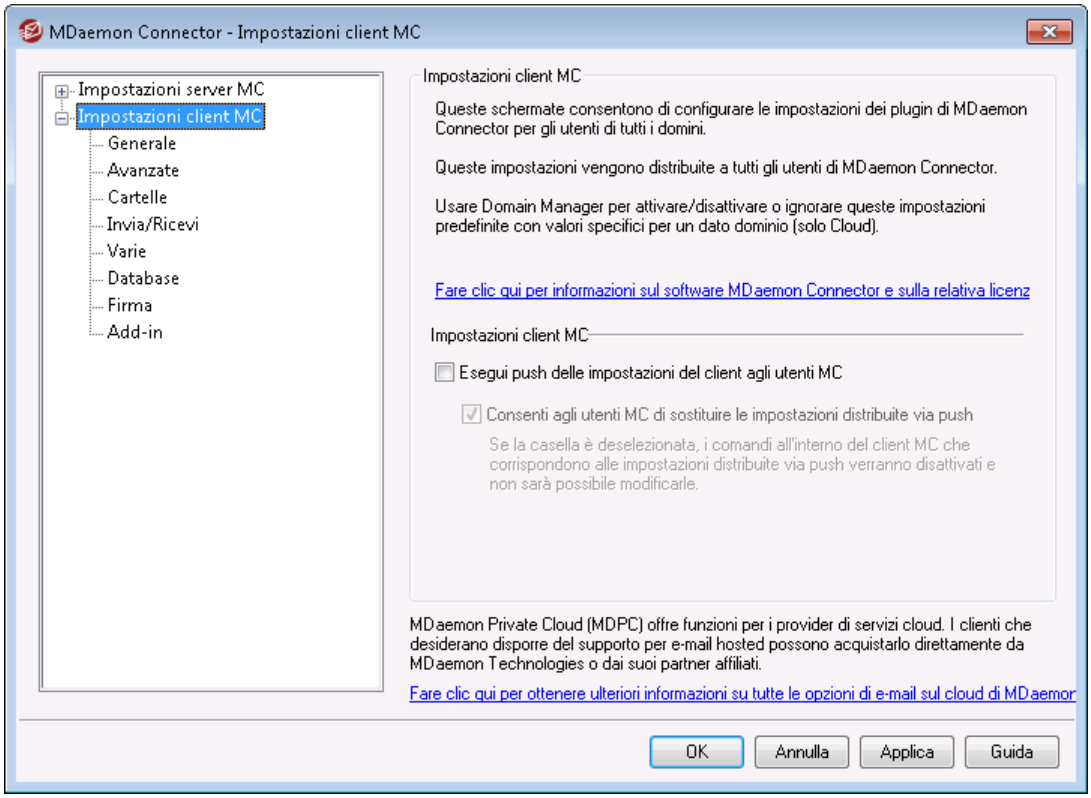
Consenti a tutti gli account di connettersi con MDaemon Connector
Per autorizzare immediatamente tutti gli account MDaemon a connettersi mediante MDaemon Connector, fare clic su questo pulsante. Tutti gli account verranno aggiunti all'elenco *Utenti MDaemon Connector*.

Autorizza automaticamente gli account al primo uso di MDaemon Connector
Selezionare questa casella di controllo se si desidera aggiungere automaticamente all'elenco *Account di MDaemon Connector* i singoli account al momento della prima connessione mediante MDaemon Connector. **Nota**: se si attiva questa opzione, si autorizzano implicitamente tutti gli account di MDaemon all'uso di MDaemon Connector. L'account non viene aggiunto all'elenco finché non viene utilizzato per la prima volta.

Vedere:

Impostazioni server MC » Impostazioni 395
Impostazioni client MC 398

3.8.2 Impostazioni client MC



Utilizzare la finestra di dialogo Impostazioni client MC per gestire centralmente le impostazioni client degli utenti di MDaemon Connector (MC). Configurare ogni schermata con le impostazioni client desiderate e MDaemon eseguirà il push di tali impostazioni nelle schermate del client corrispondenti come necessario, ogni volta che un utente MC si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client. Se l'opzione sottostante a "*Consenti agli utenti MC di sostituire le impostazioni distribuite via push*" è attivata, gli utenti possono ignorare le impostazioni inviate sui singoli client. Se l'opzione è disattivata, tutte le schermate del client sono bloccate e gli utenti MC non possono apportare modifiche.

Per consentire la configurazione di impostazioni che devono essere diverse per ciascun utente o dominio, Impostazioni client MC supporta macro come `$USERNAME$`, `$EMAIL$` e `$DOMAIN$`. Quando si esegue il push delle impostazioni a un client, le macro vengono convertite in dati specifici per il singolo utente o dominio. Accertarsi che non vengano inseriti valori statici nei campi che devono contenere macro, ad esempio nomi propri come "Franco Tommaso" nel campo Nome. In caso contrario per tutti gli utenti MC che

si connettono a MDaemon il nome sarebbe impostato su "Franco Tommaso". Per comodità dell'utente è disponibile un pulsante Riferimento macro nella schermata Generale 400 in cui viene riportato un semplice elenco delle macro supportate.

Per chi utilizza MDPC (MDaemon Private Cloud), è disponibile un'altra finestra di dialogo Impostazioni client MC in Domain Manager 185 per il controllo delle impostazioni client di MDaemon Connector a livello di singolo dominio.

Questa funzione è disattivata per impostazione predefinita ed è supportata solo nel client MDaemon Connector versione 4.0.0 o successiva.

Impostazioni client MC

Esegui push delle impostazioni del client agli utenti MC
Selezionare questa opzione se si desidera eseguire il push delle impostazioni preconfigurate nelle schermate Impostazioni client MC agli utenti MC ogni volta che si connettono. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client. L'opzione è disabilitata per impostazione predefinita.

Consenti agli utenti MC di sostituire le impostazioni distribuite via push
Se questa opzione è attivata, gli utenti possono ignorare le impostazioni inviate sui singolo client. Se invece è disattivata, tutte le schermate client sono bloccate e gli utenti di MDaemon Connector non possono apportare alcuna modifica.

Consentire agli utenti di ignorare le impostazioni ricevute non impedirà al server di inviare future modifiche ai client. Ad esempio, se un utente modifica una delle impostazioni MDaemon Connector e l'amministratore apporta modifiche a una delle schermate Impostazioni client MC sul server, tutte le impostazioni client MC verranno inviate al client di tale utente la volta successiva che si connette al server. Pertanto anche l'impostazione che in precedenza era stata ignorata dall'utente verrà modificata per creare corrispondenza tra le impostazioni del server.

Individuazione automatica delle impostazioni MC

Alla prima configurazione di MDaemon Connector sul client, gli utenti possono fare clic sul pulsante "*Prova e ricevi impostazioni account*" nella schermata Generale dopo aver inserito *Nome utente* e *Password*. Di conseguenza MDaemon Connector tenta di convalidare le credenziali e recupera automaticamente le informazioni server dell'account.

Per connettersi al server, il client proverà innanzitutto i valori FQDN comuni. Per IMAP, verrà tentata l'autenticazione con `mail.<domain>` (ovvero `mail.esempio.com`) tramite la porta SSL dedicata e quindi la porta non-SSL con TLS. Se l'operazione non riesce, il client ripeterà lo stesso processo per `imap.<dominio>`, poi per `<dominio>` e infine per

imap.mail.<dominio>. Se tutti i tentativi non vanno a buon fine, verrà tentato un accesso non crittografato per quelle stesse posizioni.

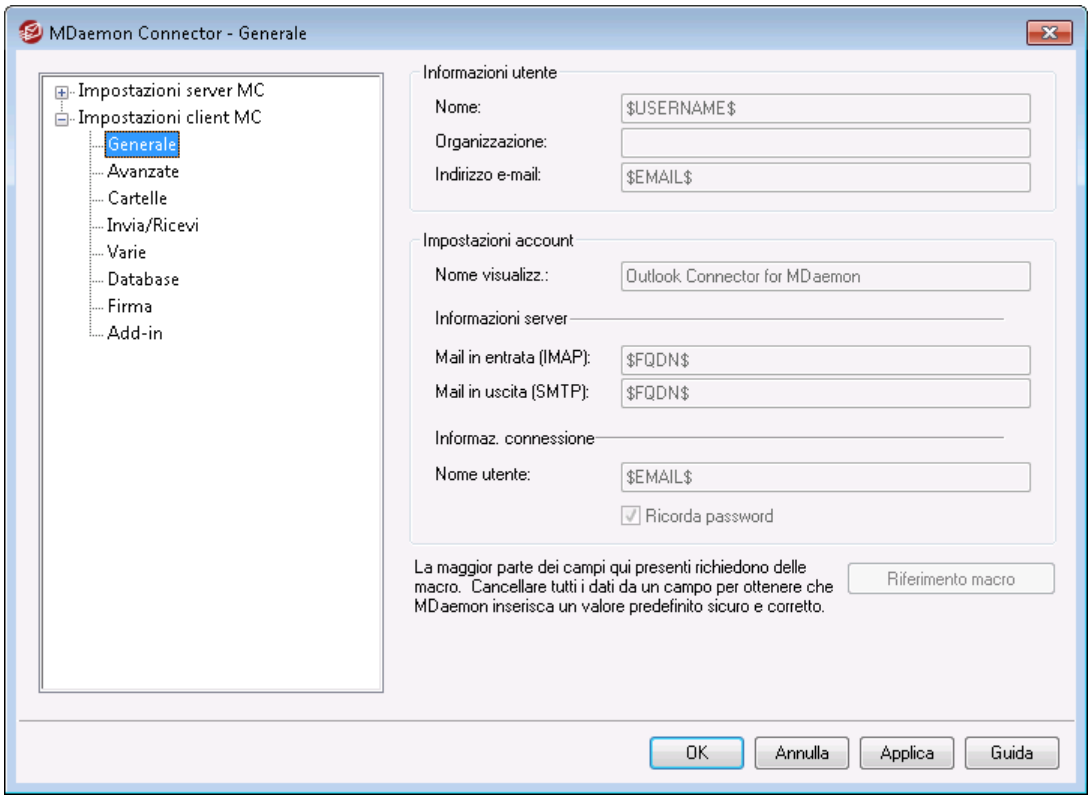
Per SMTP viene tentata l'autenticazione di mail.<dominio> tramite le porte 587, 25 e quindi 465, prima utilizzando SSL e poi TLS. L'operazione verrà ripetuta per smtp.<dominio>, <dominio> e smtp.mail.<dominio>. Se tutti i tentativi non vanno a buon fine, verrà tentato un accesso non crittografato per quelle stesse posizioni.

Se MDaemon Connector riesce a eseguire l'autenticazione, le informazioni del server in entrata e in uscita nonché le informazioni SSL/TLS vengono configurate automaticamente.

Vedere:

Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397
Impostazioni client MC » Generale 400

3.8.2.1 Generale



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata

rispetto all'ultima connessione e ricezione da parte del client. La maggior parte dei campi in questa schermata dovrebbe contenere macro piuttosto che valori statici. Vedere Riferimento macro 402 di seguito.

Informazioni utente

Nome
Per impostazione predefinita, per questa opzione si utilizza la macro $USERNAME$, che inserisce il nome e il cognome dell'utente. Il nome viene visualizzato nell'intestazione Da dei messaggi dell'utente.

Organizzazione
Questo è uno spazio opzionale per il nome dell'azienda o dell'organizzazione.

Indirizzo e-mail
Per impostazione predefinita, per questa opzione si utilizza la macro $EMAIL$, che inserisce l'indirizzo e-mail dell'utente. Il nome viene visualizzato nell'intestazione Da dei messaggi dell'utente.

Impostazioni account

Nome visualizz.
Questo nome viene visualizzato in Outlook per consentire all'utente di identificare l'account che sta utilizzando. La funzione è utile per gli utenti che hanno più account nel profilo. Queste informazioni vengono visualizzate solo dall'utente. Per impostazione predefinita, questa opzione è impostata su "MDaemon Connector".

Informazioni sul server

Mail in entrata (IMAP)
È il server a cui accederanno i client MC per raccogliere e gestire i messaggi e-mail di ciascun utente. L'impostazione predefinita è $FQDN$.

Mail in uscita (SMTP)
È il server a cui si connettono i client MC per inviare i messaggi in uscita degli utenti. Spesso corrisponde al server della posta in entrata (IMAP) sopra specificato. L'impostazione predefinita è $FQDN$.

Informaz. connessione

Nome Utente
È il nome utente richiesto per accedere e gestire l'account e-mail di MDaemon per ciascun utente. In genere corrisponde all'*indirizzo e-mail* riportato sopra. L'impostazione predefinita è $EMAIL$.

Ricorda password
Per impostazione predefinita i client MDaemon Connector sono configurati in modo da salvare la password dell'utente. Quando viene avviato, Outlook esegue quindi automaticamente l'accesso all'account e-mail senza chiedere le credenziali. Se si preferisce richiedere agli utenti di immettere la propria password all'avvio di Outlook, disattivare questa opzione.

Riferimento macro

Per consentire la configurazione di impostazioni che devono essere diverse per ciascun utente o dominio, Impostazioni client MC supporta macro come `$USERNAME$`, `$EMAIL$` e `$DOMAIN$`. Quando si esegue il push delle impostazioni a un client, le macro vengono convertite in dati specifici per il singolo utente o dominio. Accertarsi che non vengano inseriti valori statici nei campi che devono contenere macro, ad esempio nomi propri come "Franco Tommaso" nel campo *Nome*. In questo caso tutti gli utenti di MC che si connettono a MDaemon vedrebbero il proprio nome impostato su "Franco Tommaso". Fare clic sul pulsante Riferimento macro per visualizzare l'elenco delle macro disponibili:

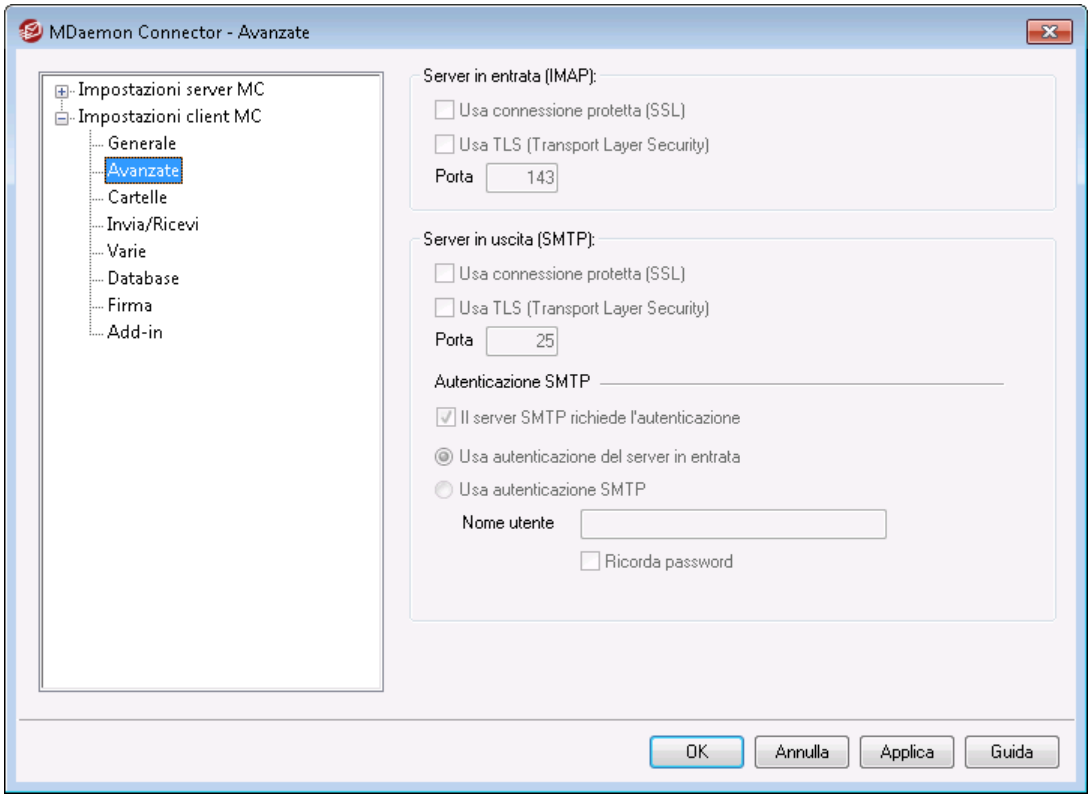
`$USERNAME$`	Questa macro inserisce il valore dell'opzione "*Nome e cognome*" nella schermata Dettagli account[729] dell'utente. Equivale a: "$USERFIRSTNAME$ $USERLASTNAME$"
`$EMAIL$`	Inserisce l'indirizzo e-mail dell'utente. Equivale a: $MAILBOX$@$DOMAIN$.
`$MAILBOX$`	Questa macro inserisce il nome della casella postale[729] dell'account.
`$USERFIRSTNAME$`	Mediante questa macro viene risolto il nome del titolare dell'account.
`$USERFIRSTNAMELC$`	Questa macro viene sostituita dal nome del titolare dell'account in lettere minuscole.
`$USERLASTNAME$`	Mediante questa macro viene risolto il cognome del titolare dell'account.
`$USERLASTNAMELC$`	Questa macro viene sostituita dal cognome del titolare dell'account in lettere minuscole.
`$USERFIRSTINITIAL$`	Mediante questa macro viene risolta la prima lettera del nome del titolare dell'account.
`$USERFIRSTINITIALLC$`	Questa macro viene sostituita dalla prima lettera del nome del titolare dell'account in lettere minuscole.
`$USERLASTINITIAL$`	Mediante questa macro viene risolta la prima lettera del cognome del titolare dell'account.
`$USERLASTINITIALLC$`	Questa macro viene sostituita dalla prima lettera del cognome del titolare dell'account in lettere minuscole.

$MAILBOXFIRSTCHARSn$	Dove "n" è un numero compreso tra 1 e 10. La macro viene sostituita con i primi "n" caratteri del nome della casella postale.
$DOMAIN$	Inserisce il dominio della casella postale 729 dell'account.
$DOMAINIP$	Questa macro risolve l'indirizzo IPv4 188 associato al dominio a cui appartiene l'account.
$DOMAINIP6$	Questa macro risolve l'indirizzo IPv6 188 associato al dominio a cui appartiene l'account.
$FQDN$	Inserisce il nome dominio completo o il nome host SMTP 188 del dominio a cui appartiene l'account.
$PRIMARYDOMAIN$	Questa macro risolve il nome del dominio predefinito 185 di MDaemon.
$PRIMARYIP$	Questa macro risolve l'indirizzo IPv4 188 associato al dominio predefinito 185 di MDaemon.
$PRIMARYIP6$	Questa macro risolve l'indirizzo IPv6 188 associato al dominio predefinito 185 di MDaemon.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.2 Avanzate



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client.

Server in entrata (IMAP):

Usa connessione protetta (SSL)
Selezionare questa casella di controllo se si desidera che i client utilizzino una connessione SSL sicura per la connessione al server della posta in entrata IMAP. Se si attiva questa opzione, l'impostazione della posta viene automaticamente modificata in "993", ovvero la porta SSL predefinita.

Usa TLS (Transport Layer Security)
Selezionare questa casella di controllo se si desidera che i client utilizzino una connessione TLS sicura per la connessione al server della posta in entrata IMAP.

Porta
È la porta utilizzata dai client MC per la connessione al server della posta in ingresso IMAP. L'impostazione predefinita è 143 per le connessioni IMAP o 993 per le connessioni IMAP con crittografia SSL.

Server in uscita (SMTP):

Usa connessione protetta (SSL)
Selezionare questa casella di controllo se si desidera che i client MC utilizzino una connessione SSL sicura per la connessione al server della posta in uscita SMTP. Se si attiva questa opzione, l'impostazione della posta viene automaticamente modificata in "465", ovvero la porta SSL predefinita.

Usa TLS (Transport Layer Security)
Selezionare questa casella di controllo se si desidera che i client MC utilizzino una connessione TLS sicura per la connessione al server della posta in uscita SMTP.

Porta
È la porta utilizzata dai client MC per la connessione al server della posta in uscita SMTP. L'impostazione predefinita è 25 per le connessioni SMTP o 465 per le connessioni SMTP con crittografia SSL.

Autenticazione SMTP

Il server SMTP richiede l'autenticazione
Per impostazione predefinita gli utenti devono utilizzare credenziali di accesso valide per autenticarsi alla connessione con il server della posta in uscita (SMTP) per l'invio di un messaggio e-mail.

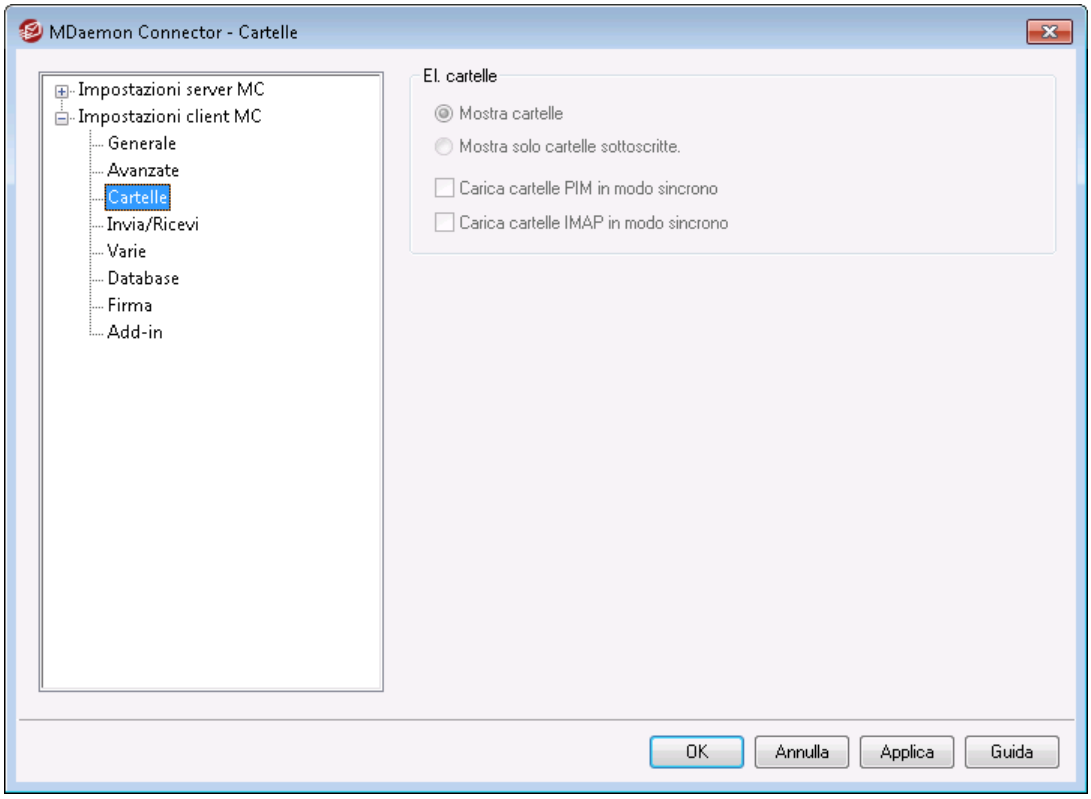
Usa autenticazione del server in entrata
Per impostazione predefinita i client MC eseguono l'autenticazione utilizzando le medesime credenziali di accesso per il server della posta in uscita (SMTP) e per il server della posta in entrata (IMAP).

Usa autenticazione SMTP
Questa opzione consente di richiedere agli utenti di MC di utilizzare credenziali di autenticazione diverse per l'invio dei messaggi, come può avvenire nel caso dell'utilizzo di un server e-mail per la posta in uscita.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.3 Cartelle



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client.

Elenco cartelle

Mostra cartelle
Per impostazione predefinita l'elenco delle cartelle in Outlook contiene tutte le cartelle del server della posta a cui l'utente di MDaemon Connector può accedere.

Mostra solo cartelle sottoscritte
Selezionare questa opzione per ottenere che nell'elenco delle cartelle di Outlook vengano visualizzate solo le cartelle sottoscritte dall'utente.

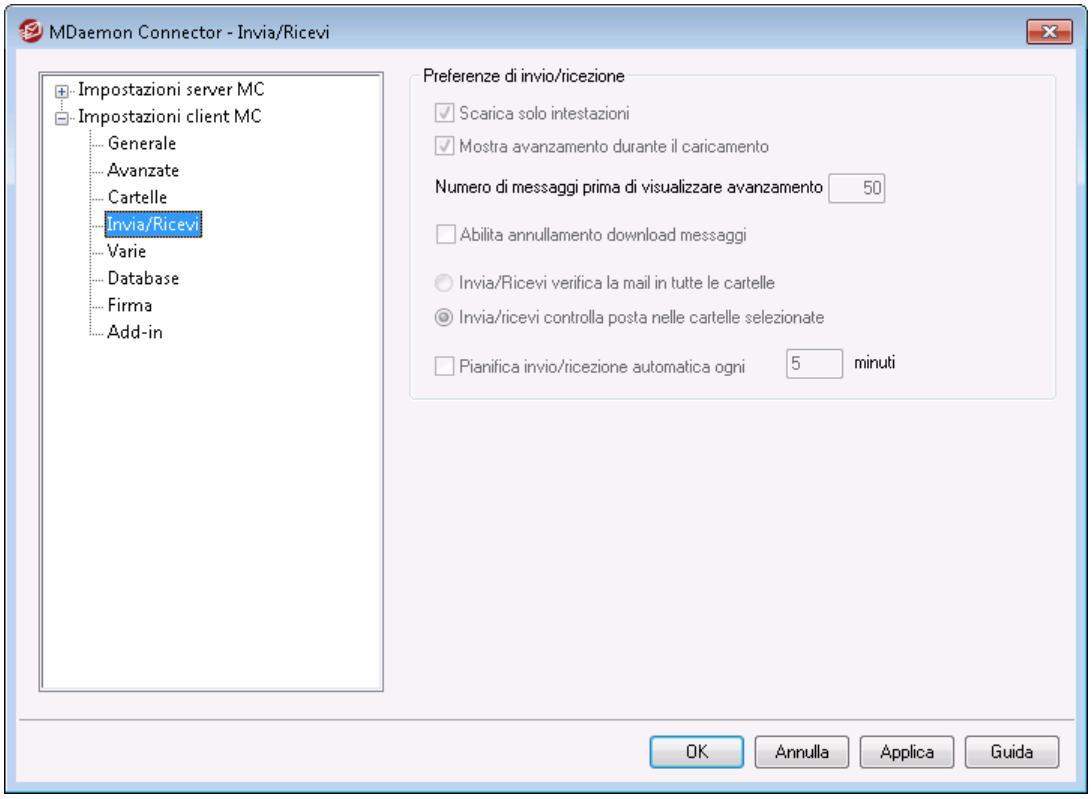
Carica cartelle PIM in modo sincrono
Nella maggior parte dei casi questa opzione deve essere lasciata deselezionata, in modo che l'utente di MDaemon Connector possa continuare a utilizzare Outlook mentre MDaemon Connector carica il contenuto delle cartelle PIM (vale a dire, le cartelle non di posta, come: Contatti, Calendari e Attività). Se si seleziona questa casella, l'uso di Outlook sarà impedito fino al completo caricamento dei dati. In genere questa opzione è necessaria quando gli utenti dispongono di applicazioni di terze parti che tentano di accedere al contenuto delle cartelle PIM.

Carica cartelle IMAP in modo sincrono
Nella maggior parte dei casi questa opzione deve essere lasciata deselezionata, in modo che l'utente di MDaemon Connector possa continuare a utilizzare Outlook mentre MDaemon Connector carica il contenuto delle cartelle di posta IMAP dell'utente. Se si seleziona questa casella, l'uso di Outlook sarà impedito fino al completo caricamento dei dati. In genere questa opzione è necessaria quando gli utenti dispongono di applicazioni di terze parti che tentano di accedere al contenuto delle cartelle di posta.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.4 Invia/ricevi



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client.

Preferenze per Invia/ricevi

Scarica solo intestazioni
Per impostazione predefinita, quando esegue un invio/ricezione e trova nuovi messaggi, MDaemon Connector scarica solo le intestazioni dei messaggi (ad esempio destinatario, mittente, oggetto e simili) da visualizzare nell'elenco dei messaggi. Il messaggio completo viene scaricato solo quando viene visualizzato.

Mostra indicatore caricamento messaggi
Durante il download di un numero elevato di messaggi MDaemon Connector visualizza un indicatore di avanzamento. Se non si desidera visualizzare l'indicatore, deselezionare questa casella di controllo.

Soglia indicatore (numero di messaggi)
Quando si attiva l'opzione *Mostra indicatore caricamento messaggi*, l'indicatore di avanzamento viene visualizzato solo durante il download di questo numero di messaggi o più.

Abilita annullamento download messaggi
Selezionare questa casella se si desidera che gli utenti di MDaemon Connector possano annullare il download quando MDaemon Connector ha già iniziato a scaricare un messaggio di grandi dimensioni.

Invia/ricevi controlla posta in tutte le cartelle
Selezionare questa opzione se si desidera che MDaemon Connector verifichi la presenza di nuovi messaggi per ciascuna cartella di posta durante l'azione di invio/ricezione per l'account dell'utente.

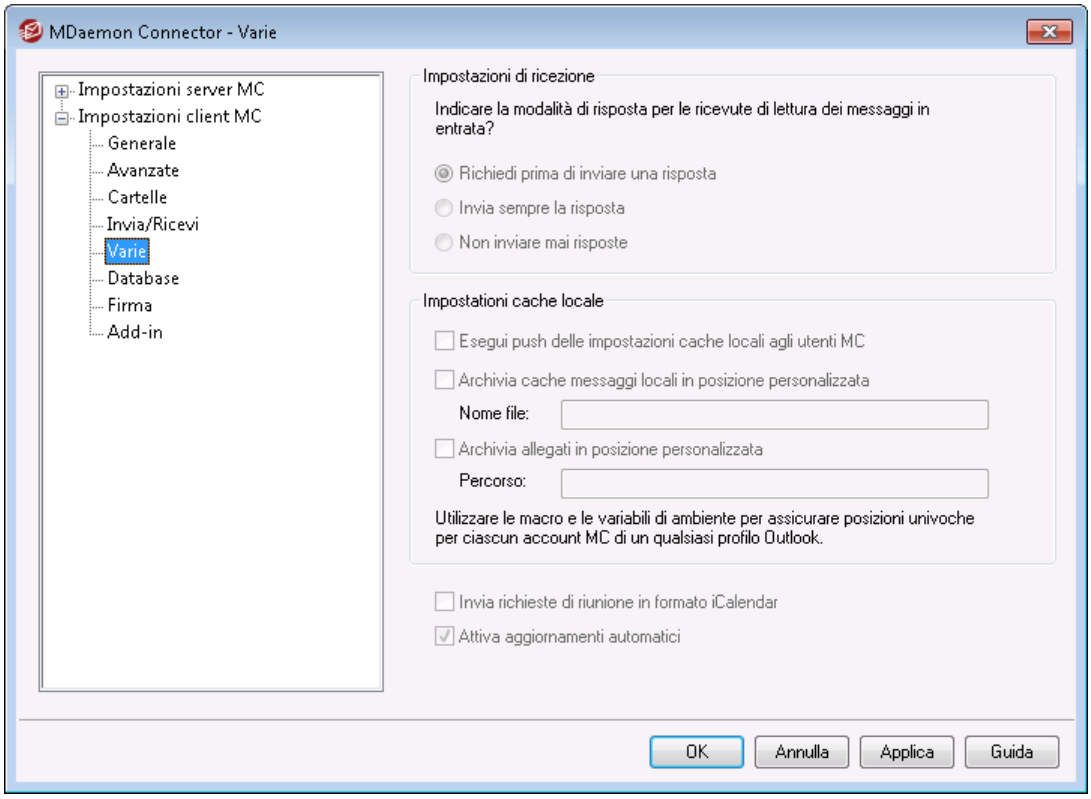
Invia/ricevi controlla la posta nelle cartelle selezionate
Selezionare questa opzione se si desidera che MDaemon Connector verifichi la presenza di nuovi messaggi per le cartelle specificate dall'utente durante l'azione di invio/ricezione per l'account.

Pianifica invio/ricezione automatica ogni [xx] minuti
Utilizzare questa opzione per inviare/ricevere in base all'intervallo specificato.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.5 Varie



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client.

Gestisci opzioni di ricezione

In alcuni casi i messaggi in arrivo contengono un'intestazione speciale con una richiesta di invio di un messaggio automatico al mittente, come conferma della lettura del messaggio. Impostare questa opzione per specificare il modo in cui si desidera che MDaemon Connector gestisca i messaggi che richiedono l'invio di conferme di lettura.

Richiedi prima di inviare una risposta
Scegliere questa opzione per chiedere agli utenti se desiderano che venga inviato un messaggio di conferma di lettura ogni volta che aprono un messaggio che ne richiede uno.

Invia sempre la risposta
Selezionare questa opzione per inviare automaticamente un messaggio di conferma di lettura ogni volta che un utente apre un messaggio che lo richiede.

Non inviare mai risposte
Selezionare questa opzione quando non si desidera che MDaemon Connector risponda alle richieste di conferma di lettura.

Opzioni cache locale

Le opzioni in questa sezione consentono di definire la posizione specifica della cache locale dei messaggi dell'utente di MDaemon Connector e la destinazione per il salvataggio degli allegati.

Le opzioni sono disponibili solo nelle versioni 4.5.0 e successive del plug-in di MDaemon Connector.

Esegui push delle impostazioni della cache locale agli utenti MC
Per impostazione predefinita, MDaemon non esegue il push di queste impostazioni ai client MDaemon Connector. Selezionare questa casella di controllo per eseguire invece il push. Il client MC sposta i file locali dalla posizione corrente alla posizione predefinita o in una posizione specificata dall'utente nelle opzioni di personalizzazione riportate di seguito.

Archivia cache messaggi locali in directory personalizzata | Nome file
Se si desidera che il client MC sposti i file locali in una posizione personalizzata, specificare un percorso locale e un nome file per la cache. Per specificare una posizione univoca per ciascun utente, è consigliabile utilizzare variabili d'ambiente e macro. Ad esempio:

```
%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE%\%
  OUTLOOKEMAIL%\LocalCache.db
```

Archivia allegati in una posizione personalizzata | Percorso
Per personalizzare la posizione della cartella in cui il client MC archivia i file allegati, specificare qui il percorso. Per specificare una posizione univoca per ciascun utente, è consigliabile utilizzare variabili d'ambiente e macro.

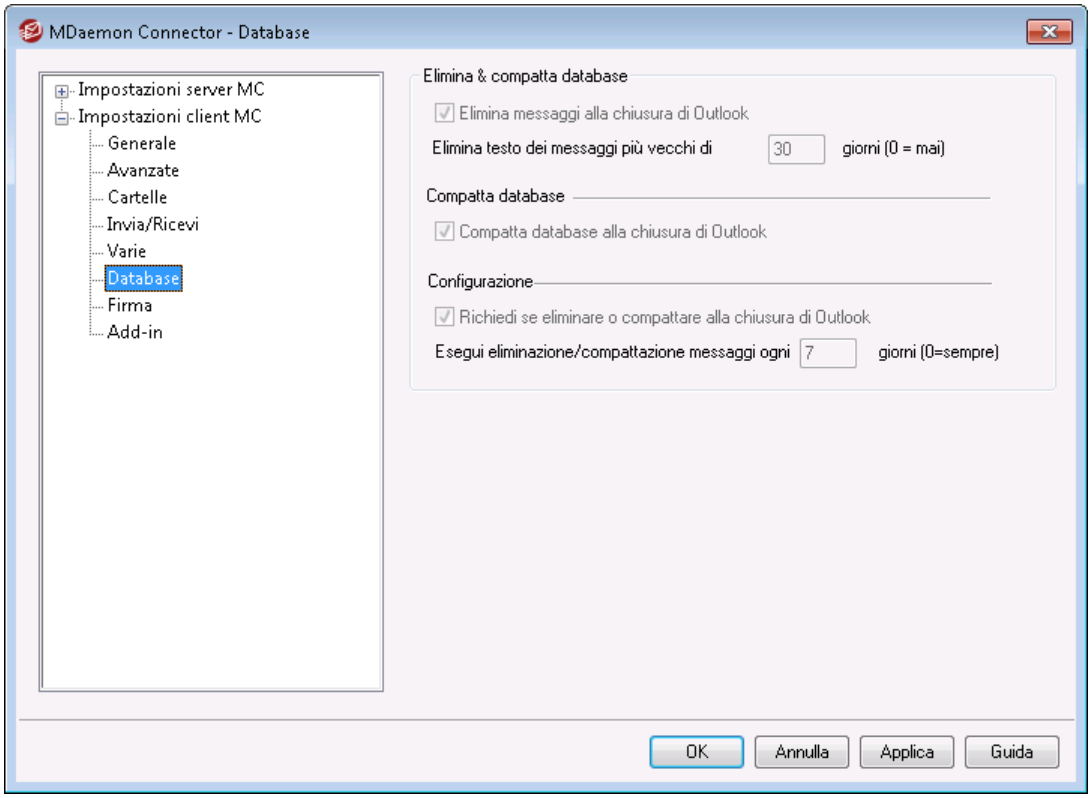
Invia richieste di riunione in formato iCalendar
Selezionare questa casella se si desidera che MC invii le richieste di riunione nel formato di iCalendar (iCal).

Attiva aggiornamenti automatici
Per impostazione predefinita, MC viene aggiornato automaticamente non appena si rende disponibile una nuova versione. Se non si desidera eseguire gli aggiornamenti in modo automatico, deselezionare questa casella di controllo.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.6 Database



Quando si attiva l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni configurate in questa schermata vengono estese alla schermata corrispondente del client MDaemon Connector ogni volta che un utente di MDaemon Connector si connette al server. Le impostazioni del client MC vengono inviate solo quando una delle impostazioni è nuova o è stata modificata rispetto all'ultima connessione e ricezione da parte del client.

Elimina & compatta database

Riduci database alla chiusura di Outlook
Per ridurre l'occupazione di spazio su disco e migliorare le prestazioni, MDaemon Connector è impostato in modo predefinito per l'eliminazione del corpo dei messaggi meno recenti quando si chiude Outlook. Le intestazioni dei messaggi non vengono rimosse e i messaggi originali archiviati sul server non vengono modificati; viene solo eliminato il corpo dei messaggi meno recenti presenti nella cache locale. Quando si apre uno di questi messaggi con il testo rimosso, il corpo del messaggio viene di nuovo scaricato sul computer locale. Inoltre, viene eliminato solo il corpo dei

messaggi e-mail; Contatti, Calendari, Attività, Diario e Note non sono interessati. Disattivare questa opzione se non si desidera ridurre il database alla chiusura di Outlook.

Elimina corpo dei messaggi più vecchi di XX giorni (0 = mai)
Utilizzare questa opzione per specificare il numero di giorni oltre il quale un messaggio viene considerato abbastanza datato da attivare la rimozione del corpo alla chiusura di Outlook. Per impostazione predefinita un messaggio deve risalire ad almeno 30 giorni prima per attivare la rimozione del testo. Il calcolo dell'età del messaggio si basa sulla data di ultima modifica. Per disabilitare la rimozione del corpo dei messaggi, inserire il valore "0".

Compatta database

Compatta database alla chiusura di Outlook
Per ridurre l'occupazione di spazio su disco e migliorare le prestazioni, MDaemon Connector è impostato in modo da compattare e deframmentare il file del database dei messaggi nella cache locale quando si chiude Outlook. Tuttavia, per attivare l'azione di compattamento, è necessario chiudere Outlook in modo corretto; se Outlook si chiude a causa di un errore del sistema o si utilizza "Termina attività" in Gestione attività, il database non verrà compattato. Si possono utilizzare le opzioni nella sezione Configurazione di seguito per specificare la frequenza con cui si desidera eseguire questa operazione e se si desidera ricevere un avviso prima dell'esecuzione.

Configurazione

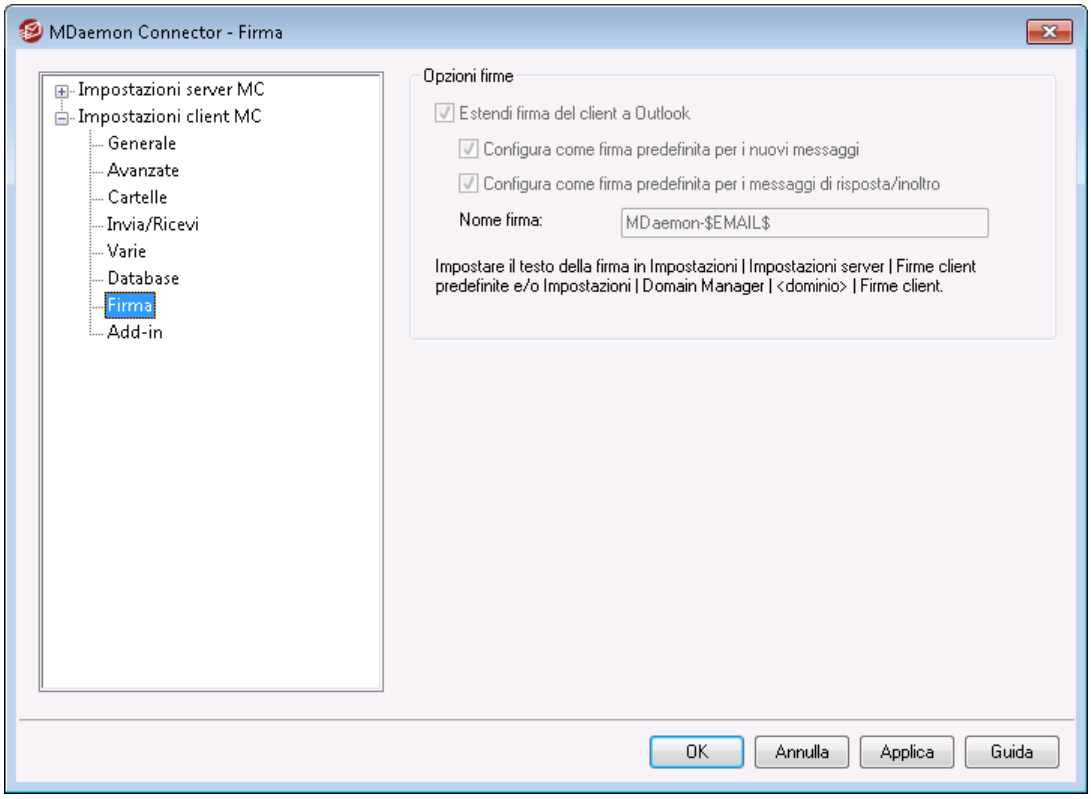
Chiedi prima di ridurre/compattare alla chiusura di Outlook
Utilizzare questa opzione se si desidera che gli utenti ricevano un avviso prima che MDaemon Connector compatti il file del database alla chiusura. Se l'utente fa clic su **Sì** viene avviata l'azione di compattamento, con la visualizzazione di un indicatore di avanzamento. Deselezionare la casella di controllo se non si desidera che gli utenti ricevano un avviso; alla chiusura di MDaemon Connector verrà automaticamente avviato il compattamento del database, con la visualizzazione di un indicatore di avanzamento.

Esegui riduzione/compattamento alla chiusura ogni XX giorni (0=sempre)
Questa opzione consente di specificare la frequenza con cui MDaemon Connector deve compattare il database alla chiusura. L'impostazione predefinita è 7 giorni, vale a dire che il processo di riduzione/compattamento viene eseguito ogni sette giorni alla chiusura del programma. Impostare questa opzione su "0" per ridurre/compattare il database ogni volta che un utente chiude Outlook.

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.8.2.7 Firma



Quando si è selezionata l'opzione "*Esegui push delle impostazioni del client agli utenti MC*" nella schermata Impostazioni client MC 398, le impostazioni selezionate in questa schermata saranno estese alla schermata Firme (disponibile in Outlook in **File » Opzioni » Posta » Firme**) ogni volta che un utente di MDaemon Connector si connette al server. Questa funzionalità richiede MDaemon 6.5.0 o versione successiva.

Opzioni firme

Estendi firma del client a Outlook
Attivare questa opzione se si desidera eseguire il push della firma client predefinita 141 (o della firma client 211 specifica del dominio, se ne è stata creata una) per gli utenti di MDaemon Connector. Specificare un nome per la firma nel campo *Nome firma* riportato sotto.

Configura come firma predefinita per i nuovi messaggi
Selezionare questa casella di controllo se si desidera rendere la firma client la firma predefinita per i nuovi messaggi.

Configura come firma predefinita per i messaggi di risposta/inoltro
Selezionare questa casella di controllo se si desidera rendere la firma client la firma predefinita utilizzata quando si risponde ai o si inoltrano i messaggi.

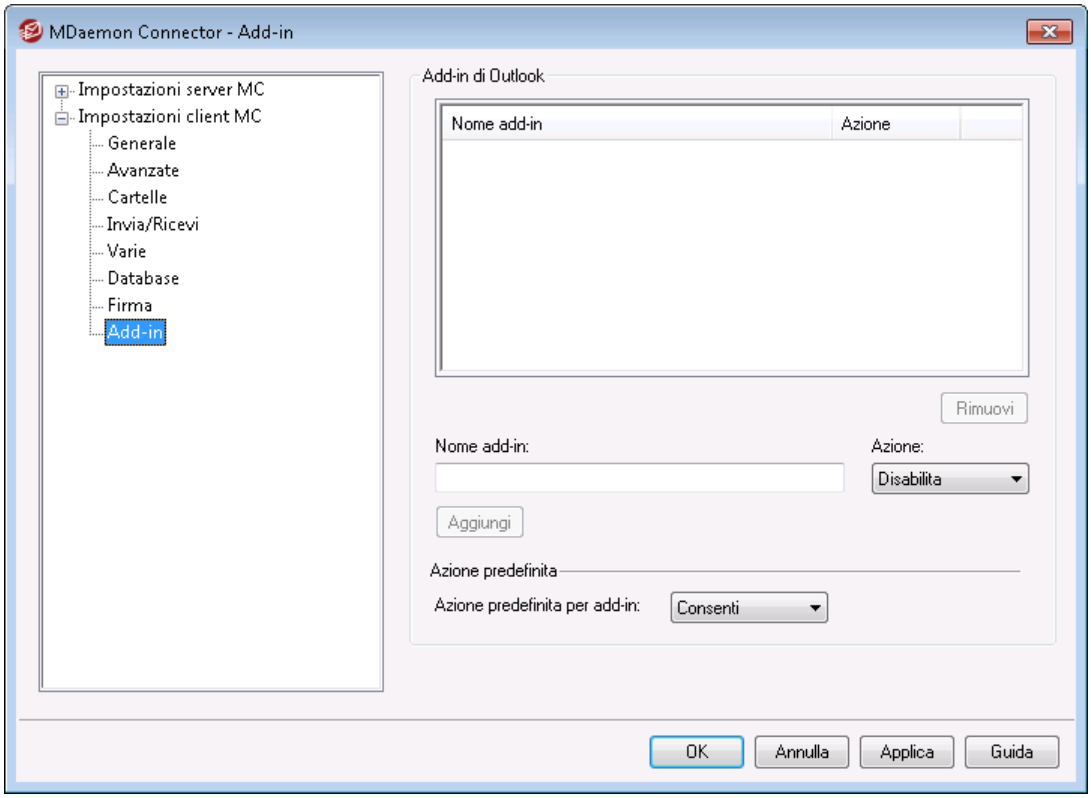
Nome firma:
È il nome assegnato alla firma di cui si è eseguito il push all'account e-mail dell'utente di MDaemon Connector in Outlook. Per impostazione predefinita, il

nome della firma è configurato come: "MDaemon-$EMAIL$". La macro $EMAIL$ sarà convertita nell'indirizzo e-mail dell'utente. Ad esempio, "MDaemon-Franco.Tommaso@company.test"

Vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397
Firme client predefinite 141
Domain Manager » Firme client 211

3.8.2.8 Componenti aggiuntivi



Nella schermata Componenti aggiuntivi è possibile gestire lo stato dei componenti aggiuntivi di Outlook installati dagli utenti di MDaemon Connector (MC). È possibile autorizzare il normale utilizzo di alcuni o tutti i componenti aggiuntivi oppure si possono disattivare quelli che non si desidera vengano utilizzati. Questa funzionalità si dimostra particolarmente utile quando si è a conoscenza di conflitti generati da un componente aggiuntivo specifico con MDaemon Connector e si desidera disattivarlo per evitare problemi. La funzionalità Componenti aggiuntivi richiede la presenza di MDaemon Connector 5.0 o versione successiva.

Componenti aggiuntivi di Outlook

In questa casella sono elencati i componenti aggiuntivi di Outlook degli utenti e l'azione associata a ciascun componente: *Disattiva*, *Consenti* o *Predefinito*. Quando un utente MC avvia Outlook, il client MC invia l'elenco dei componenti aggiuntivi dell'utente a MDaemon e quindi disattiva quelli impostati come*disattivati.* Quelli impostati come*consentiti* non vengono modificati. Quelli impostati come*predefiniti* utilizzeranno *l'azione predefinita per i componenti aggiuntivi* assegnati di seguito.

MDaemon Connector è in grado di gestire solo i componenti aggiuntivi di Outlook per gli utenti che hanno impostato il proprio account di MDaemon Connector come account predefinito in Microsoft Outlook.

Aggiunta, rimozione e modifica dei componenti aggiuntivi

Aggiunta di un componente aggiuntivo

Per aggiungere un componente aggiuntivo all'elenco, digitare il *Nome componente aggiuntivo* così come appare in Outlook, impostare l'*Azione* e fare clic su **Aggiungi**. Questa opzione si dimostra particolarmente utile quando si conosce un componente aggiuntivo e si desidera gestirlo ma non si è ancora connesso alcun utente con il componente aggiuntivo installato.

Rimozione di un componente aggiuntivo

Per rimuovere un componente aggiuntivo dall'elenco, selezionarlo e fare clic su *Rimuovi*.

Impostazione di un'azione per il componente aggiuntivo

Per modificare un componente aggiuntivo, selezionarlo, utilizzare l'elenco a discesa per impostare l'*Azione* e fare clic su **Aggiungi**.

Azione predefinita

Azione predefinita per i componenti aggiuntivi

Impostare *Consenti* o *Disattiva*. Quando impostato su *Consenti*, per impostazione predefinita MDaemon Connector disattiverà solo i componenti aggiuntivi specificamente impostati su "*Disattiva*". Tutti gli altri componenti aggiuntivi non vengono modificati. Quando impostato su *Disattiva*, MDaemon Connector disattiverà automaticamente tutti i componenti aggiuntivi eccetto quelli specificamente impostati su "*Consenti*". Per impostazione predefinita, questa opzione è impostata su *Consenti*.

Per ulteriori informazioni, vedere:

Impostazioni client MC 398
Impostazioni server MC » Impostazioni 395
Impostazioni server MC » Account 397

3.9 Servizio cluster

Il Servizio cluster di MDaemon consente di condividere la configurazione tra due o più server MDaemon sulla rete. Questo rende possibile utilizzare hardware o software di bilanciamento del carico per distribuire il carico dei messaggi di posta elettronica su più server MDaemon, aumentando in tal modo la velocità e l'efficienza e riducendo il sovraccarico e la congestione del traffico di rete per ottimizzare le risorse e-mail. Consente inoltre di garantire la ridondanza dei sistemi e-mail in caso di guasti dell'hardware o di errori del software.

Di seguito sono riportati una serie di elementi da tenere in considerazione quando si decide se configurare o meno un cluster MDaemon sulla rete:

Nodi

Un cluster MDaemon sarà composto da un nodo primario e da nodi secondari. Un server MDaemon sarà designato come server primario e tutti gli altri saranno secondari.

- La configurazione del server MDaemon che funge da nodo primario verrà replicata su tutti gli altri nodi. Per questo motivo il nodo primario è l'unico nodo che può essere utilizzato per apportare modifiche alla configurazione. Se si accede a un nodo secondario e si apportano modifiche alla configurazione, le modifiche saranno sovrascritte. Di conseguenza, la maggior parte delle opzioni di configurazione non è accessibile nell'interfaccia utente sui nodi secondari.
- Il Servizio cluster non replica le cartelle della casella postale o le cartelle pubbliche sui nodi. Tutti i nodi condividono la stessa serie di cartelle dei messaggi. Le cartelle di posta degli utenti e le cartelle pubbliche devono essere in una posizione sulla rete accessibile da parte di tutti i nodi.
- Eventuali modifiche alla posta effettuate su un nodo secondario vengono inviate al nodo primario e quindi viene inviata una notifica della modifica a tutti gli altri nodi.
- L'API XML sui nodi secondari è di sola lettura.
- Ogni nodo nel cluster deve essere sulla stessa rete. È sconsigliato l'uso del Servizio cluster sui server del cluster che si trovano in posizioni diverse.
- Ogni nodo del cluster deve eseguire la stessa versione di MDaemon.
- Ogni nodo del cluster deve avere la propria chiave MDaemon.

Instradamento

MDaemon non gestisce l'instradamento del traffico da e verso nodi specifici. È consigliabile utilizzare un programma di bilanciamento del carico di terze parti per gestire l'instradamento del traffico.

Le sessioni "sticky" nel programma di bilanciamento del carico sono richieste in modo che tutto il traffico dello stesso indirizzo IP venga instradato sullo stesso host. Le sessioni "sticky" sono particolarmente importanti per il traffico di MDRA, Webmail e XMPP in quanto non ancora compatibili con il cluster, il che significa che le informazioni delle sessioni non sono trasferite attraverso i nodi. Per risolvere questa limitazione:

- Tutte le connessioni MDRA devono essere instradate sul nodo primario.

- Quando qualcuno accede a Webmail su un server specifico, tutto il traffico per quella sessione deve essere instradato su quello stesso server.
- Il traffico Webmail e XMPP deve essere instradato sullo stesso server per consentire il funzionamento delle funzionalità integrate di chat di Webmail.
- Tutto il traffico XMPP deve essere instradato sullo stesso nodo. In caso contrario gli utenti che si connettono a server diversi non saranno in grado di utilizzare la chat per comunicare tra loro.
- Considerando i punti riportati sopra, è consigliabile instradare tutto il traffico HTTP e XMPP sul nodo primario, perché questa è la configurazione più semplice e che è meno probabile causi problemi. Se non si utilizzano alcune di queste funzionalità, tuttavia, è possibile modificare la configurazione (anche se le sessioni sticky sono comunque richieste).

Caselle postali e cartelle

Le caselle postali, le cartelle pubbliche e alcune altre cartelle devono essere memorizzate in un percorso condiviso accessibile da ciascun nodo del cluster. Si ricordi che se si utilizza un percorso UNC sarà necessario eseguire il servizio di the MDaemon come utente che ha accesso al percorso di rete.

- È necessario aggiornare manualmente i percorsi di caselle postali e cartelle e spostare i contenuti delle cartelle nella posizione accessibile del cluster. Questa non è una funzione automatizzata che MDaemon può eseguire per l'utente quando si configura il cluster. Il Servizio cluster aggiornerà il file MDaemon.ini con i percorsi di rete per le caselle postali e le cartelle pubbliche specificate nella configurazione del Servizio cluster.
- La directory Lockfiles deve essere spostata in una posizione condivisa. È possibile consentire al Servizio cluster di eseguire questa operazione automaticamente oppure eseguirla manualmente modificando la chiave `LockFiles` nella sezione `[Directories]` del file `MDaemon.ini`. Se si consente al Servizio cluster di eseguire questa operazione automaticamente, la directory LockFiles si troverà sotto il percorso della casella postale di rete.
- Anche la directory PEM deve essere spostata su una posizione condivisa. A tal fine, copiare la cartella `MDaemon\PEM\` sulla nuova posizione condivisa, modificare la chiave `PEM` nella sezione `[Directories]` del file `MDaemon.ini` e riavviare MDaemon.
- Il nuovo modello di account verrà aggiornato con il percorso della casella di posta specificato nella configurazione del Servizio cluster.

Vaglio dinamico

- Il vaglio dinamico 623 invia tutte le richieste al nodo del server primario e i dati del nodo primario sono replicati sui nodi secondari.
- Se il nodo primario è offline, i nodi secondari usano la propria configurazione di vaglio dinamico, che deve essere identica a quella del nodo primario nel momento in cui è diventato offline. Quando il nodo primario torna online, eventuali modifiche al vaglio dinamico apportate dai server secondari saranno sovrascritte.

Certificati

- I certificati SSL vengono automaticamente replicati dal nodo primario ai secondari.
- MDaemon inoltre replica le impostazioni dei certificati 587, in modo che ciascun nodo/server del cluster tenti di utilizzare lo stesso certificato. Se un nodo non dispone del certificato corretto, tutto il traffico SSL/TLS/HTTPS su tale nodo verrà interrotto.
- Le opzioni LetsEncrypt di MDaemon non supportano i nodi secondari per ora.

Altro

- Il Collegamento allegati 373 non può essere utilizzato in un cluster e pertanto è disattivato quando si abilita un cluster.
- L'installazione automatica degli aggiornamenti 509 deve essere disattivata.
- L'associazione Dominio-Indirizzo IP 188 deve essere disattivata.
- Tutti i nodi di un cluster devono essere impostati sullo stesso fuso orario ed esattamente sulla stessa ora. Se il fuso orario non è lo stesso, o se l'ora varia di più di 1 secondo, verrà registrata un'avvertenza nel registro del cluster.

Configurazione del Servizio cluster

Attenersi alla procedura seguente per configurare il Servizio cluster:

1. Assicurarsi di aver aggiornato tutti i percorsi delle caselle postali e modificato i percorsi delle cartelle pubbliche. Il server primario deve usare per i dati una posizione di archiviazione di rete e deve essere in grado di accedere ai dati senza problemi prima di procedere.
2. Tutti i certificati appropriati devono essere installati su ciascun nodo.
3. Installare MDaemon su un nodo secondario usando una chiave univoca.
4. Sul nodo primario, selezionare **Impostazioni » Servizio cluster**.
5. Fare clic con il pulsante destro sull'elenco Server registrati e scegliere **Aggiungi nuovo server MDaemon al cluster** (potrebbe essere necessario del tempo per la ricerca dei server disponibili sulla rete).
6. In *Nome server* immettere il nome NETBIOS, l'indirizzo IP o il nome DNS del nodo secondario su cui è installato MDaemon oppure selezionarlo dall'elenco a discesa. Potrebbe essere necessario del tempo per la ricerca dei server disponibili sulla rete.
7. Fare clic su **OK**.
8. Controllare il registro Plugins/Cluster per assicurarsi che i due server siano connessi e che sia in funzione la replica.
9. Selezionare **Impostazioni » Servizio cluster** sul nodo secondario per confermare che ora in Server registrati sono elencati sia il nodo primario che quelli secondari.

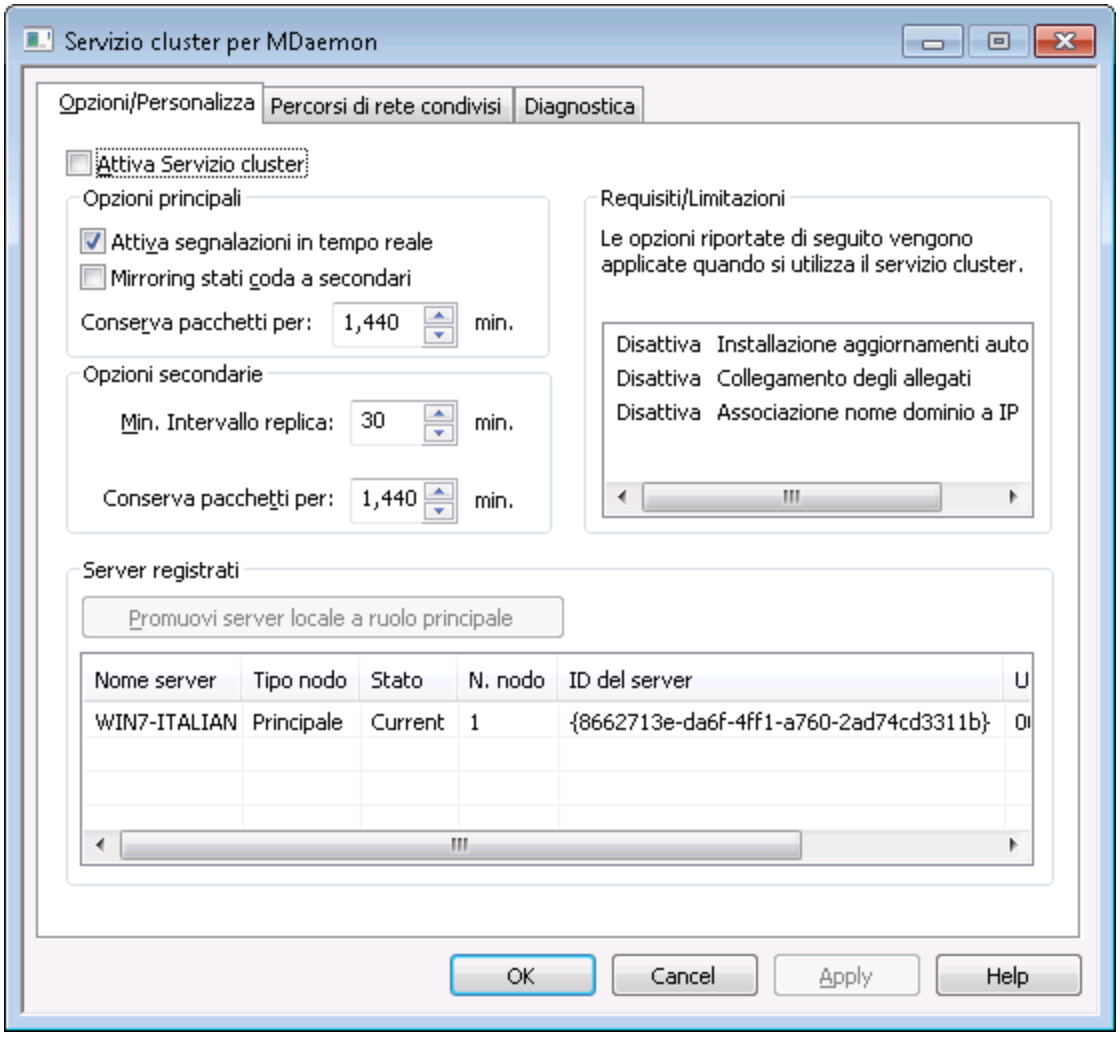
10. Configurare l'hardware o il software di bilanciamento del carico per instradare il traffico verso il cluster come discusso in precedenza.

Vedere:

Servizio cluster | Opzioni/Personalizza 419
Servizio cluster | Percorsi rete condivisi 420
Servizio cluster | Diagnostica 422

3.9.1 Opzioni/Personalizza

Opzioni/Personalizza



Attiva Servizio cluster

Selezionare Attiva Servizio cluster.

Opzioni primario

Attiva segnalazione in tempo reale
Per impostazione predefinita, ogni volta che viene effettuata una modifica sul nodo primario, viene inviato un segnale di replica ai nodi secondari, per notificare la necessità di effettuare una richiesta di replica per sincronizzare le impostazioni tra i nodi.

Mirroring stati coda a secondari
Selezionare questa casella di controllo se si desidera assicurarsi che se si modifica lo stato di una coda di posta (ad esempio in bloccata o sbloccata) sul nodo primario, lo stato verrà modificato anche sui nodi secondari.

Opzioni secondario

Intervallo replica [xx] minuti
Questa opzione determina la durata dell'attesa da parte di un nodo secondario del segnale di replica dal nodo primario prima di effettuare in ogni caso una richiesta di replica. Per impostazione predefinita, questa opzione è impostata su 30 minuti.

Server registrati

Visualizza tutti i nodi del cluster di server di MDaemon.

Promuovi server locale a ruolo primario
Per modificare un nodo secondario in nodo primario, sul nodo secondario che si desidera promuovere, selezionare il nodo nell'elenco e fare clic su **Promuovi**. Il nuovo nodo primario informerà il precedente nodo primario che deve unirsi di nuovo al cluster come nodo secondario. Per le configurazioni con più nodi secondari, gli altri nodi secondari dovranno essere rimossi e riaggiunti al cluster.

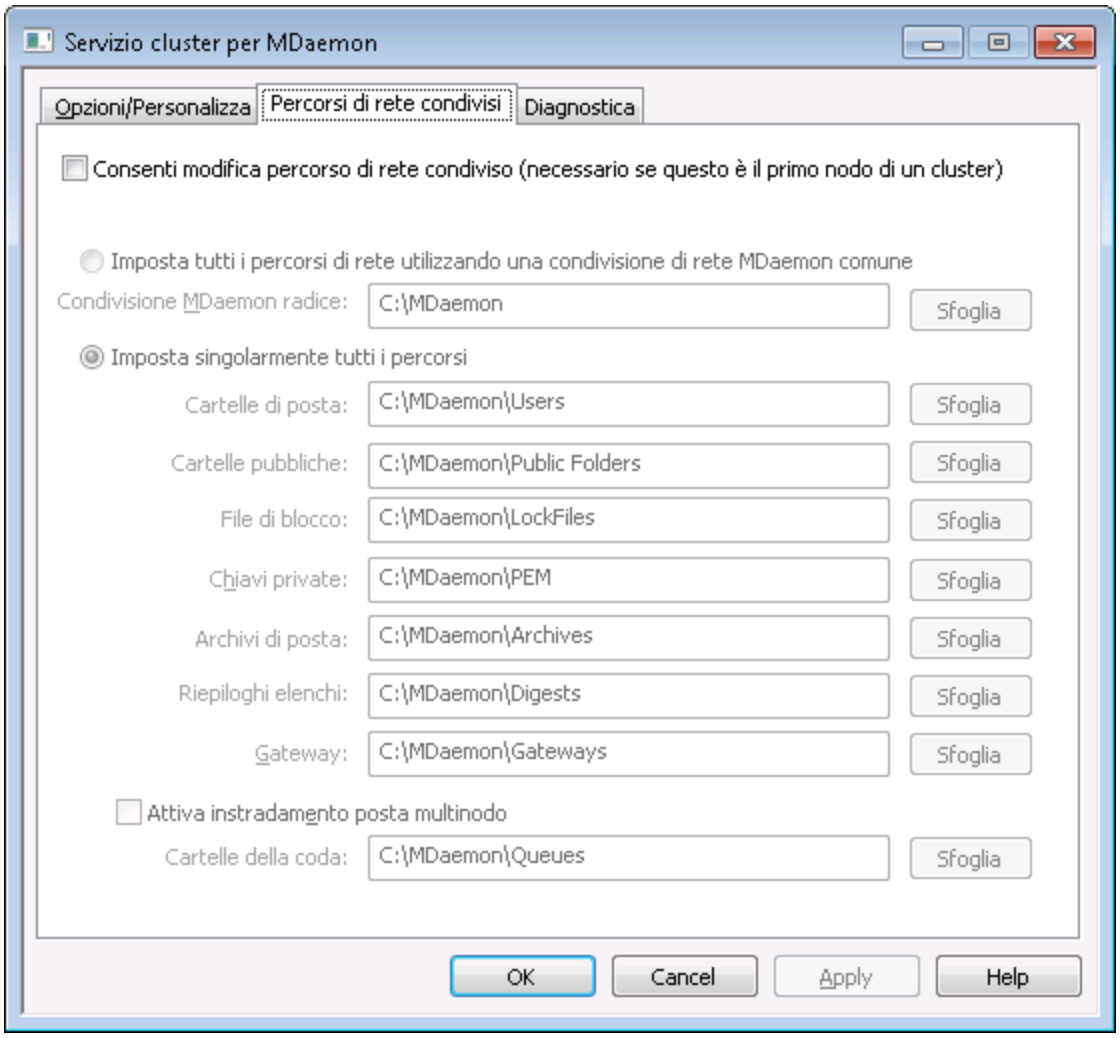
Aggiungi nuovo server MDaemon al cluster
Per aggiungere un nuovo server MDaemon al cluster, fare clic con il pulsante destro del mouse sull'elenco dei server, quindi fare clic su **Aggiungi nuovo server MDaemon al cluster**. Nella schermata visualizzata, immettere il nome NETBIOS, l'indirizzo IP o il nome DNS del server su cui è installato MDaemon oppure selezionarlo dall'elenco a discesa. Potrebbe essere necessario del tempo per la ricerca dei server disponibili sulla rete.

Vedere:

Servizio cluster 416
Servizio cluster | Percorsi rete condivisi 420
Servizio cluster | Diagnostica 422

3.9.2 Percorsi rete condivisi

Percorsi rete condivisi



Consenti modifica percorso di rete condiviso (obbligatorio se questo è il primo nodo di un cluster)

Utilizzare le opzioni riportate in questa schermata per impostare i percorsi di rete condivisi che il cluster MDaemon deve utilizzare. Questa impostazione è obbligatoria nel caso del primo nodo del cluster per fare in modo che i percorsi di rete condivisi vengano replicati sugli altri nodi.

Imposta tutti i percorsi di rete in modo che utilizzino una condivisione di rete MDaemon comune
Scegliere questa opzione se si desidera collocare tutti i percorsi di rete condivisi sotto un'unica condivisione di rete comune. Questa opzione provoca l'impostazione dei valori predefiniti per tutti i percorsi, con tutti i relativi controlli in sola lettura.

Imposta singolarmente tutti i percorsi di rete
Scegliere questa opzione se si desidera impostare singolarmente ciascun percorso di rete condiviso. Ad esempio, se si desidera conservare le cartelle di posta e gli archivi di posta in punti diversi della rete.

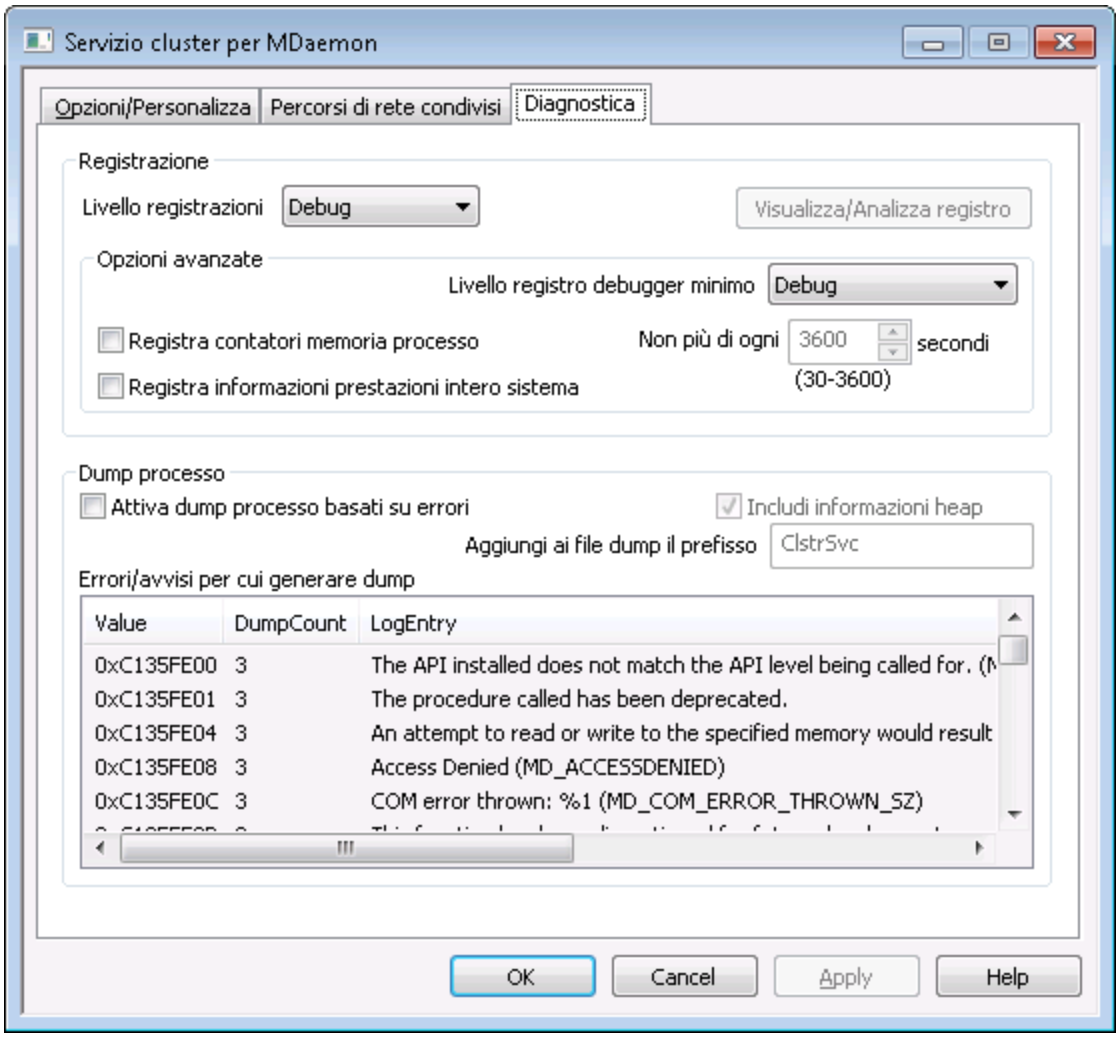
Consenti instradamento posta multinodo
Utilizzare l'instradamento della posta multinodo quando si desidera condividere le code della posta tra nodi del cluster diversi. L'elaborazione e il recapito dei messaggi da parte di più server consente di suddividere il lavoro in modo più equilibrato ed evita che i messaggi restino bloccati nelle code di eventuali server non attivi.

Vedere:

Servizio cluster 416
Servizio cluster | Opzioni/Personalizza 419
Servizio cluster | Diagnostica 422

3.9.3 Diagnostica

Diagnostica



Registrazione

Livello di registrazione
Sono supportati sei livelli di registrazione, dal più alto al più basso volume di dati registrati:

Debug	È il livello di registrazione più esteso. Registra tutte le voci disponibili ed è in genere usato per la diagnosi di un problema o quando l'amministratore necessita di informazioni dettagliate.
Info	Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.
Avviso	Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.
Errore	Vengono registrati errori, errori critici ed eventi di avvio e di arresto.
Critico	Vengono registrati errori critici ed eventi di avvio e di arresto.
Nessuno	Vengono registrati solo gli eventi di avvio e di arresto.

Visualizza/Analizza registro
Fare clic su questo pulsante per aprire il Visualizzatore del registro di sistema avanzato di MDaemon. Per impostazione predefinita i registri vengono archiviati in: "..\MDaemon\Logs\"

Opzioni avanzate

Livello minimo registro debugger
Livello minimo di registrazione da inviare al debugger. I livelli di registrazione disponibili sono identici a quelli descritti in precedenza.

Registra contatori di memoria del processo
Selezionare questa casella per registrare informazioni specifiche del processo su Memoria, Handle e Thread nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Registra dati delle prestazioni dell'intero sistema
Selezionare questa casella per registrare le informazioni sulle prestazioni dell'intero sistema nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Non più di ogni [xx] secondi
Utilizzare questa opzione per impostare il limite di frequenza della registrazione delle informazioni su processo e prestazioni.

Dump del processo

Attiva dump del processo in base agli errori
Attivare questa opzione per generare dump del processo ogni volta che si verifica un errore o un avviso specifico e indicata di seguito.

Includi informazioni heap nei dump
Per impostazione predefinita le informazioni heap sono incluse nei dump di processo. Se non si desidera includerli, deselezionare questa casella di controllo.

Prefisso file dump
I nomi dei file di dump del processo inizieranno con il prefisso indicato.

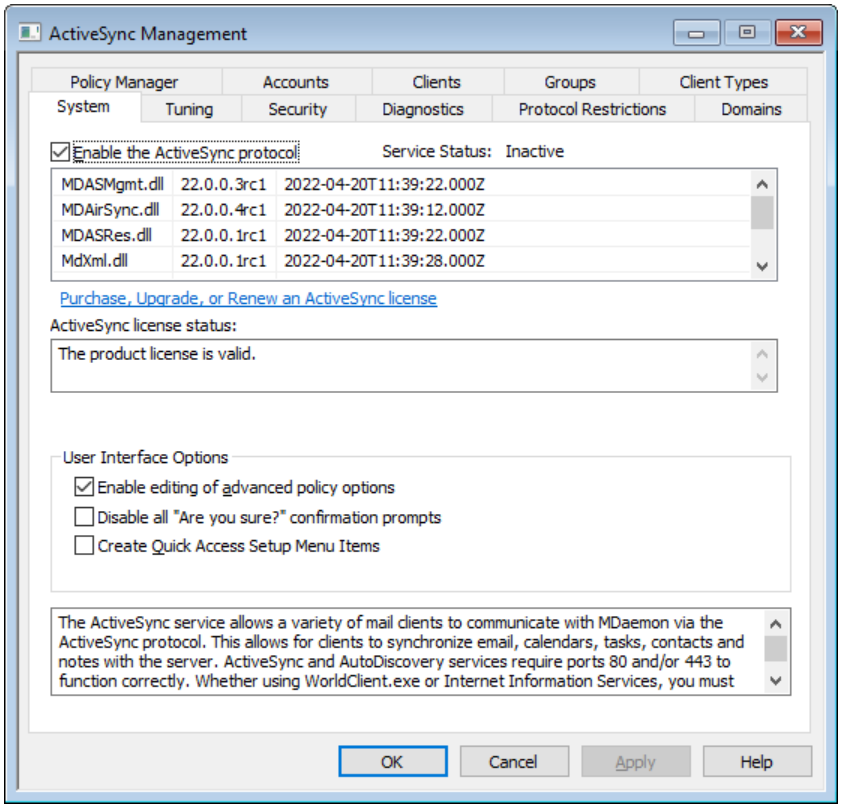
Errori/avvisi con generazione di dump
Fare clic con il pulsante destro del mouse in quest'area e utilizzare le opzioni *Aggiungi/Modifica/Elimina voce...* per gestire l'elenco degli errori o avvisi che avviano i dump del processo. Per ciascuna voce è possibile specificare il numero di dump di processo consentiti prima di essere disattivato.

Vedere:

Servizio cluster 416
Servizio cluster | Opzioni/Personalizza 419
Servizio cluster | Percorsi rete condivisi 420

3.10 ActiveSync

3.10.1 Sistema



MDaemon include il supporto per "ActiveSync for MDaemon", che è un server ActiveSync over-the-air (OTA) fornito come componente aggiuntivo facoltativo per MDaemon Private Cloud. Questo server è in grado di sincronizzare la Posta elettronica e i dati PIM (Contatti, Calendari e Attività) tra l'account MDaemon/Webmail e un dispositivo ActiveSync.

ActiveSync è l'estensione di un servizio Web che opera solo con le porte **80** (per http) e **443** (per https). Questo è un requisito di implementazione di ActiveSync. Se ActiveSync è attivato e si sta utilizzando il server Web integrato di Webmail, ma questo non utilizza la porta 80 o 443, il server inizierà automaticamente a utilizzare la porta 80, oltre a qualsiasi altra porta configurata sul Server Web 330 e nelle schermate SSL e HTTPS 336. Se si utilizza un altro server per Webmail come IIS, è necessario configurarlo manualmente per l'utilizzo della porta 80 o 443.

Per eseguire ActiveSync con IIS è necessario chiamare la libreria DLL ActiveSync (`MDAirSync.dll`) quando viene richiesto "`/Microsoft-Server-ActiveSync`". Questa richiesta è utilizzata da tutti i client ActiveSync. Alcune versioni di IIS non consentono questa funzione senza aver preventivamente scaricato, installato e configurato un software di terze parti.

Tutte le sincronizzazioni iniziali con ActiveSync sono unilaterali dal server al dispositivo. I dati correlati del dispositivo vengono persi durante la prima sincronizzazione con ActiveSync. Questo è un requisito di implementazione di ActiveSync. Pertanto si consiglia di effettuare il backup dei dati del dispositivo prima di utilizzare ActiveSync per la prima volta. La maggior parte dei dispositivi dotati del supporto ActiveSync avvisa l'utente che "**i dati del dispositivo andranno persi**", ma non tutti.

Attivazione/disattivazione di ActiveSync

Fare clic su *Attiva protocollo ActiveSync* per attivare ActiveSync per MDaemon. Le opzioni Domini 444 consentono di verificare la disponibilità in tutti i domini o soltanto in alcuni di essi.

Opzioni interfaccia utente

Abilita modifica opzioni criteri avanzati
Selezionare questa opzione per rendere visibile la scheda Impostazioni avanzate all'interno dell'editor criteri ActiveSync 453. Contiene diverse impostazioni di criteri avanzati che nella maggior parte non sarà necessario modificare. L'opzione è disabilitata per impostazione predefinita.

Disabilitare tutte le richieste di conferma
Per impostazione predefinita quando si modificano determinate impostazioni di ActiveSync viene visualizzata una finestra che chiede di confermare le modifiche da apportare. Fare clic su questa casella di controllo per disattivare le richieste.

Crea voci di menu configurazione accesso rapido
Se si attiva questa opzione, il menu Impostazioni » ActiveSync nell'interfaccia dell'applicazione MDaemon sarà modificato, con l'aggiunta di collegamenti al Monitoraggio connessione ActiveSync e al visualizzatore/analizzatore del registro. **Nota:** quando l'opzione è disattivata, questi strumenti si possono comunque raggiungere facendo clic con il pulsante destro su **ActiveSync** in Server nel riquadro Statistiche dell'interfaccia dell'applicazione.

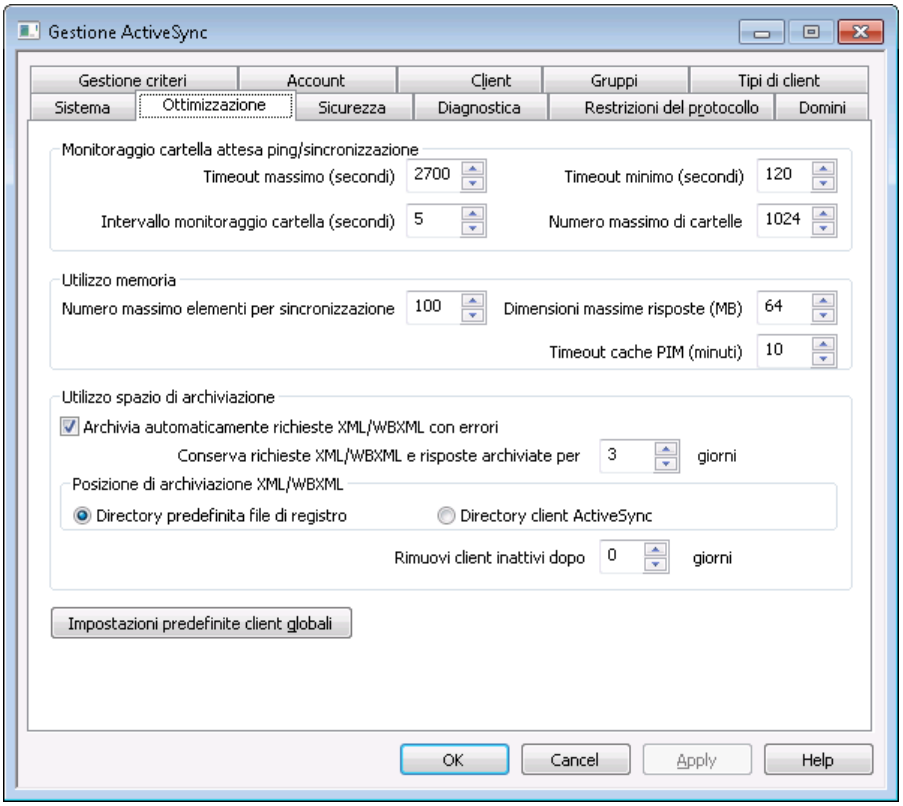
Servizio AutoDiscovery 79

MDaemon supporta il servizio AutoDiscovery 79, che consente agli utenti di configurare un account ActiveSync con il solo indirizzo e-mail e la password, senza che sia necessario conoscere il nome host del server ActiveSync. Per l'utilizzo di AutoDiscovery è necessario attivare HTTPS 336.

Vedere:

Account Editor » ActiveSync 779
ActiveSync » Domini 444
SSL/HTTPS 336
Server Web 330

3.10.2 Regolazione



Questa schermata contiene le opzioni avanzate, che nella maggior parte dei casi non dovranno essere modificate, e un pulsante che consente di aprire la finestra di dialogo Impostazioni predefinite client globali 430, che consente di regolare le impostazioni predefinite utilizzate per i client ActiveSync.

Attesa ping/sinc monitoraggio cartella

Timeout massimo (1200-7200 secondi)
Tempo massimo di attesa consentito in MDaemon ActiveSync Service (MDAS) per il monitoraggio di una cartella prima della risposta al client. Il valore predefinito è 2700 secondi (45 minuti).

Timeout minimo (120-480 secondi)
Tempo minimo di attesa consentito in MDAS per il monitoraggio di una cartella prima della risposta al client. Il valore predefinito è 120 secondi. Se necessario è possibile ridurre il numero di connessioni effettuate al server aumentando questo valore, perché in questo modo il client si connetterebbe meno spesso dato che il tempo di attesa sarebbe maggiore.

Intervallo monitoraggio cartella (3-50 secondi)
Numero di secondi di attesa del servizio ActiveSync tra le occorrenze di monitoraggio delle cartelle. Per impostazione predefinita, questa opzione è impostata su 5 secondi.

N. massimo di cartelle
Indica il numero massimo di cartelle che a ciascun client ActiveSync è consentito monitorare. Il valore predefinito è 2048.

Utilizzo memoria

N. massimo elementi per sinc.
Numero massimo di elementi che il servizio ActiveSync restituirà al client in risposta alla richiesta di sincronizzazione. L'impostazione di un valore basso in questa opzione consente di ridurre l'utilizzo della memoria su un server occupato, ma richiederà un numero maggiore di connessioni e una quantità più elevata di larghezza di banda. Può inoltre comportare una riduzione della durata della batteria poiché i dispositivi potrebbero avere la necessità di eseguire un maggior numero di richieste per recuperare tutte le modifiche durante una sincronizzazione. L'impostazione di valori più elevati in questa opzione comporta un maggiore utilizzo della memoria e aumenta la possibilità di errori di comunicazione. L'impostazione del valore predefinito 100 rappresenta in genere un buon compromesso. È bene notare comunque che i client specificheranno il valore che preferiscono, il che potrebbe effettivamente ridurre questo valore per alcuni client. Se un client richiede un valore maggiore del massimo valore consentito, verrà usato il valore massimo.

Dimensioni massime risposta (MB)
Dimensioni massime consentite di una risposta alla richiesta di sincronizzazione da parte di un client. Prima di elaborare un determinato elemento per la sincronizzazione da server a client, vengono controllate le dimensioni correnti della risposta e se queste sono maggiori o uguali a questo valore, la raccolta viene contrassegnata per la presenza di ulteriori modifiche e alla risposta non verranno aggiunti altri elementi. Questo è utile con i server le cui e-mail normalmente contengono molti allegati di grandi dimensioni.

Timeout cache PIM (5-60 minuti)
Poiché i dati di Contatti, Documenti, Eventi e altri dati PIM sono spesso statici e ricevono solo occasionali aggiornamenti dai client, MDAS memorizza questi dati nella cache per ridurre l'attività su disco. In caso di modifica dei dati su disco, questi vengono ricaricati automaticamente. Questo valore controlla la durata della permanenza nella cache dei dati dell'utente dopo l'ultimo accesso.

Utilizzo spazio di archiviazione

Archiviazione automatica di richieste XML/WBXML con errori
Nel caso in cui si siano disattivate le opzioni di *Archiviazione richieste e risposte [XML | WBXML]* nella schermata Impostazioni client 430, questa opzione consentirà di archiviare le richieste XML o WBXML con problemi. Saranno archiviate solo le richieste che causano errori. L'opzione è abilitata per impostazione predefinita.

Conserva richieste e risposte XML/WBXML archiviate per [xx] giorni
Questo è il numero di giorni per cui resteranno salvate le risposte archiviate automaticamente. Per impostazione predefinita, vengono conservate per 3 giorni.

Posizione di archiviazione XML/WBXML

Directory registri predefinita
Le richieste e i file di errori XML/WBXML archiviati automaticamente vengono conservati, per impostazione predefinita, nella directory dei registri di MDaemon.

Directory del client ActiveSync
Scegliere questa opzione se si preferisce archiviare i file nella directory di debug del client ActiveSync dell'utente.

Rimuovi client inattivi dopo [xx] giorni
Questo è il numero di giorni per cui un dispositivo ActiveSync 470 può restare senza connettersi a MDAS prima di essere rimosso. Quando il dispositivo viene rimosso, le relative impostazioni di configurazione e accesso vengono annullate. Se il dispositivo si connette di nuovo, MDaemon risponderà come se si trattasse di un nuovo dispositivo mai utilizzato sul server. Il sistema dovrà eseguire di nuovo il provisioning nel caso in cui sia impostato un criterio per il dominio 444 o l'account 461, effettuare una sincronizzazione iniziale delle cartelle e risincronizzare tutte le cartelle sottoscritte. Questa opzione consente di evitare la conservazione nel server di informazioni relative a dispositivi obsoleti e inutilizzati. Per impostazione predefinita, questa opzione è impostata su 31 giorni. Se si imposta "0", i dispositivi non saranno rimossi, indipendentemente dall'estensione del periodo di inattività.

Impostazioni predefinite client globali

Fare clic su questo pulsante per aprire la finestra di dialogo Impostazioni client ActiveSync globali 430 e configurare le impostazioni predefinite da utilizzare per ActiveSync » Client.

Notifiche di ActiveSync

Notifiche di rollback della sincronizzazione

Il servizio ActiveSync può inviare una notifica agli amministratori se un client invia ripetutamente o frequentemente chiavi di sincronizzazione scadute nelle operazioni di sincronizzazione.

Queste informano semplicemente l'amministratore che il server ha eseguito il rollback per una determinata raccolta perché un client ha fatto una richiesta di sincronizzazione con la chiave di sincronizzazione scaduta più di recente. L'oggetto riporta "Client ActiveSync che usa chiave di sincronizzazione scaduta". Questo può accadere a causa di errori di rete o del contenuto inviato in precedenza al client in quella raccolta. In alcuni casi, sarà presente l'ID dell'elemento, a seconda se la precedente sincronizzazione sulla specifica raccolta abbia inviato elementi o meno.

Gli avvisi di rollback non significano che il client non è sincronizzato, ma che è possibile che il client non sia sincronizzato in futuro e che il sistema lo ha rilevato. Gli avvisi di rollback sono emessi per una raccolta una sola volta ogni 24 ore. È possibile modificare le chiavi seguenti nell'intestazione [System] del file `\MDaemon\Data\AirSync.ini`:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (L'impostazione predefinita è disabilitato)
- [System] RollbackNotificationThreshhold=[1-254] : Il numero di rollback che deve essere eseguito su una specifica raccolta prima che venga inviata una notifica all'amministratore. Si consiglia di utilizzare un valore di almeno 5 in questo campo, dato che eventuali problemi della rete possono avere un ruolo in questo. (L'impostazione predefinita è 10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Se inviare o meno una notifica in CC all'utente il cui client ha inviato la chiave di sincronizzazione scaduta. (L'impostazione predefinita è disabilitato)

Notifiche dei messaggi corrotti di ActiveSync

Il servizio ActiveSync può inviare una notifica all'amministratore se non è possibile elaborare uno specifico messaggio. Le notifiche sono inviate in tempo reale per informare l'amministratore di elementi di posta che non è stato possibile analizzare e sui quali non è possibile eseguire altre operazioni. L'oggetto riporta "Notifica di messaggio corrotto". Questi elementi, nelle versioni precedenti, potevano portare a un errore del sistema. Nella maggior parte dei casi, il contenuto del file msg non sarà costituito da dati MIME. Se si tratta di dati MIME, è probabile che sia corrotto. È possibile scegliere di inviare in CC tali notifiche all'utente interessato con la chiave CMNCCUser in modo che sia a conoscenza del fatto che è arrivato un messaggio e-mail non leggibile nella casella postale. L'azione appropriata in questi casi consiste nello spostare il msg designato dalla casella postale dell'utente e analizzarlo, per determinare il motivo per cui non è possibile eseguire il parse e come è giunto ad assumere lo stato in cui si trova. È possibile modificare le seguenti chiavi sotto l'intestazione [System] del file `\MDaemon\Data\AirSync.ini`:

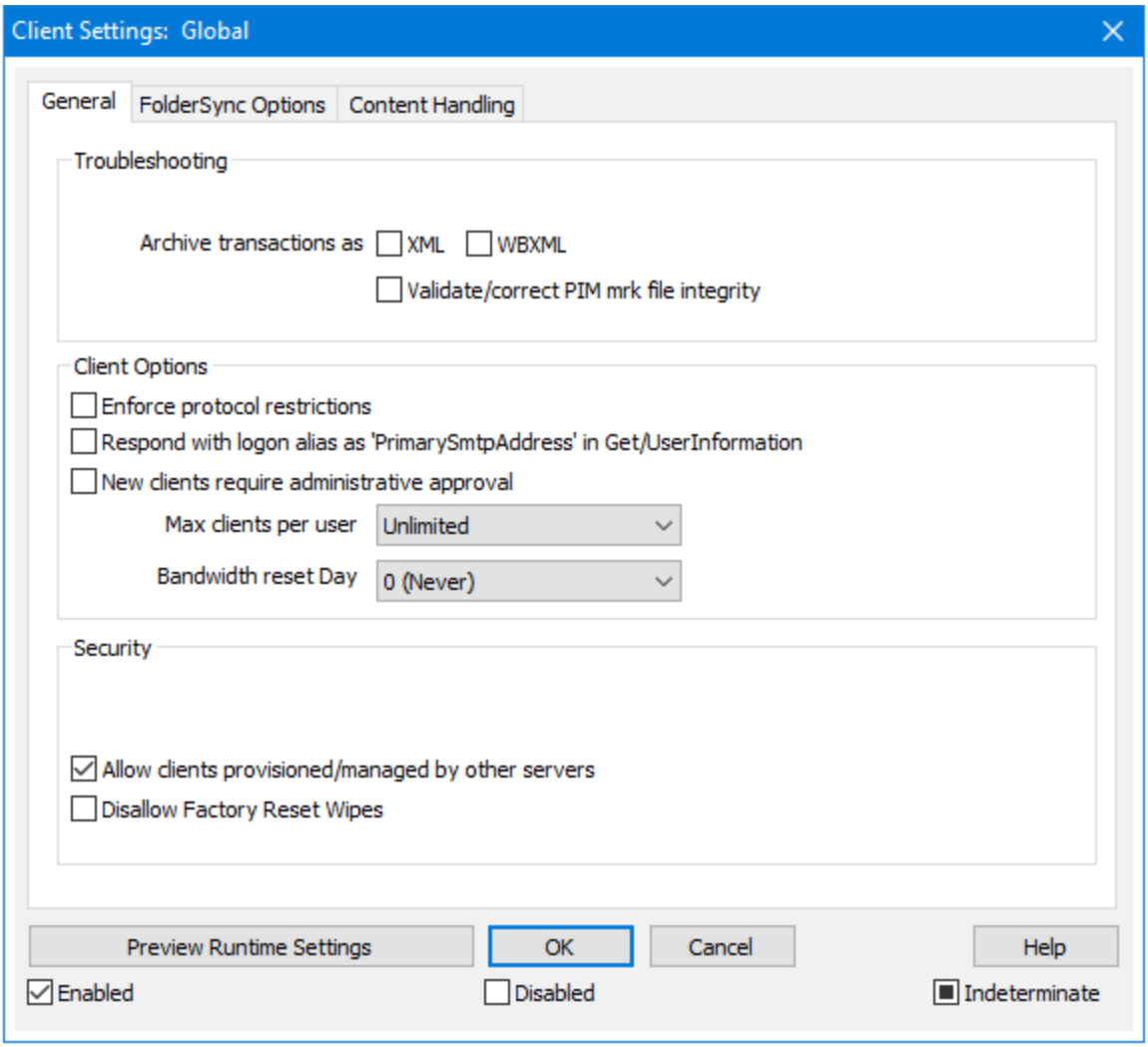
- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False] (L'impostazione predefinita è abilitato)
- [System] CMNCCUser==[0|1|Yes|No|True|False] (L'impostazione predefinita è abilitato)

Per ulteriori informazioni, vedere:

ActiveSync » Diagnostica 440

3.10.2.1 Impostazioni client

Nella pagina Impostazioni client sono riportati i profili delle impostazioni predefinite di ActiveSync configurati per ActiveSync. È possibile creare e modificare i profili delle impostazioni del client per: Globali, Domini 211, Gruppi 479, Account 461, Tipi client 486 e Client 470 (vale a dire, dispositivi) nelle rispettive finestre di dialogo.



Questa schermata contiene le impostazioni generali per la gestione dei client ActiveSync. Esistono impostazioni client corrispondenti nelle altre pagine di ActiveSync, ad esempio Domini 444, Account 461 e Client 470, che consentono di impostare queste opzioni rispettivamente per dominio, account e client. Le impostazioni globali sono impostate su valori specifici, ma il dominio, l'account, il client e altre opzioni sono impostate in modo predefinito per *Ereditare* le impostazioni dalle rispettive opzioni principali. Pertanto la modifica di un'impostazione in questa schermata comporterà la modifica della stessa impostazione in tutte le schermate secondarie, per consentire all'utente per impostazione predefinita di gestire tutti i client sul server modificando solo le impostazioni di quest'unica schermata. Tuttavia, la modifica di un'impostazione in una schermata secondaria annulla l'impostazione principale, per consentire di modificare le impostazioni a livello di dominio, account o altro quando necessario.

Analogamente ai Criteri 452, che sono assegnati al dispositivo e regolano in generale ciò che il dispositivo può fare, le Impostazioni client definiscono ciò che il server farà per quanto riguarda determinate opzioni relative ai client, ad esempio: definire il numero di client ActiveSync separati che un account può utilizzare, se le Cartelle pubbliche saranno sincronizzate o meno su un dispositivo insieme alle cartelle personali

dell'account, se si devono includere o meno le cartelle dei mittenti consentiti dell'utente e così via.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug	È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.
Info	Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.
Avviso	Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.
Errore	Vengono registrati errori, errori critici ed eventi di avvio e di arresto.
Critico	Vengono registrati errori critici ed eventi di avvio e di arresto.
Nessuno	Vengono registrati solo gli eventi di avvio e di arresto.
Ereditarietà	Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i

tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività[427] disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync**[470] nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

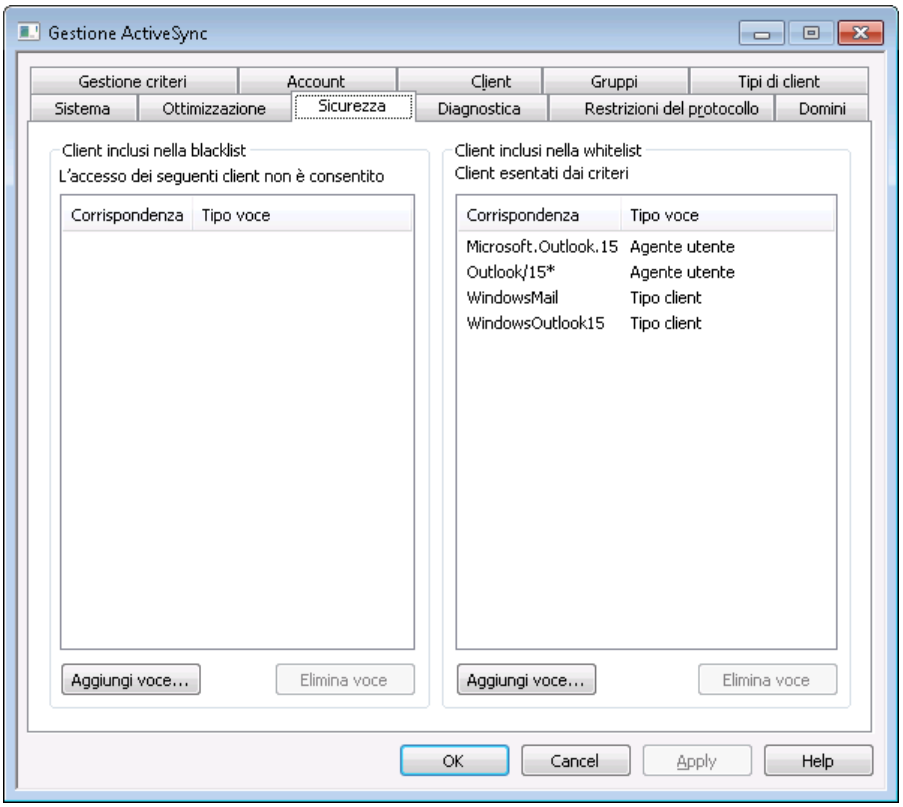
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

ActiveSync » Domini 444
ActiveSync » Account 461
ActiveSync » Client 470

3.10.3 Sicurezza

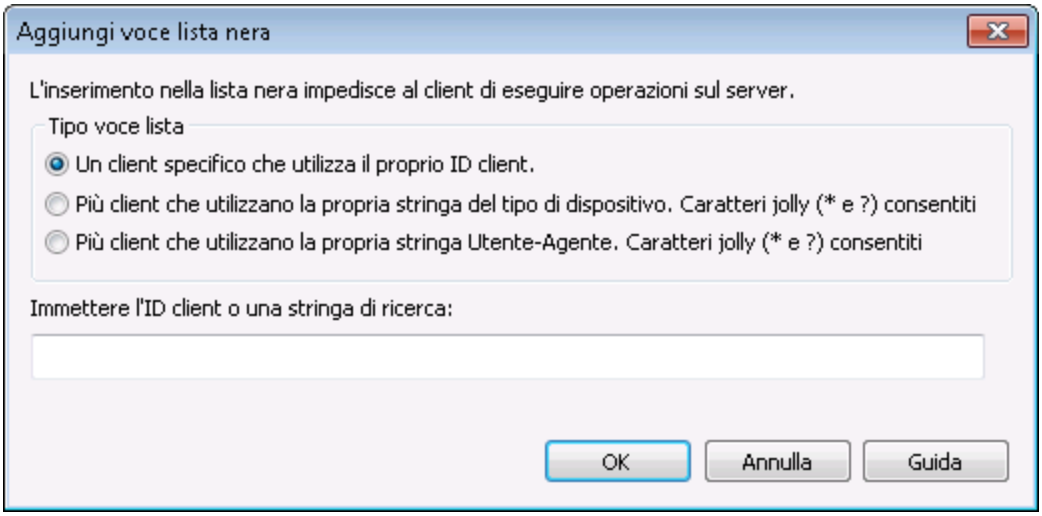


Client bloccati

Utilizzare questa opzione per impedire a un Type dispositivo, ID client o Agente utente di accedere al server ActiveSync di MDaemon.

Aggiunta di una voce bloccata

Per aggiungere una voce all'elenco, fare clic su **Aggiungi voce**, specificare le informazioni del dispositivo e fare clic su **Ok**. È possibile ottenere le informazioni sul dispositivo dal dispositivo stesso o dai file di registro di ActiveSync, se il dispositivo si è connesso al server ActiveSync di MDaemon.



È possibile bloccare facilmente un dispositivo dalla finestra di dialogo Client 470. Fare clic con il pulsante destro del mouse su un client dell'elenco e scegliere **Blocca questo client**.

Eliminazione di una voce bloccata

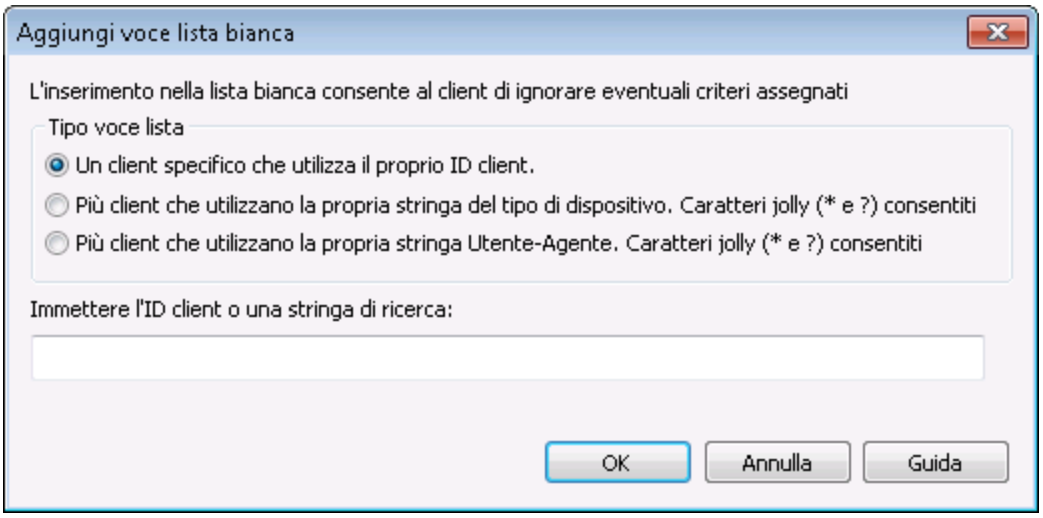
Per eliminare delle voci, selezionare una o più voci dall'elenco e fare clic su **Elimina voce**. Verrà chiesto di confermare l'operazione di eliminazione.

Client esentati

Utilizzare questa opzione per esentare un Type dispositivo, ID client o Agente utente specifico dalle limitazioni di provisioning o criteri 452.

Aggiunta di un client esentato

Per aggiungere una voce all'elenco, fare clic su **Aggiungi voce**, specificare le informazioni del dispositivo e fare clic su **Ok**. È possibile ottenere le informazioni sul dispositivo dal dispositivo stesso o dai file di registro di ActiveSync, se il dispositivo si è connesso al server ActiveSync di MDaemon.



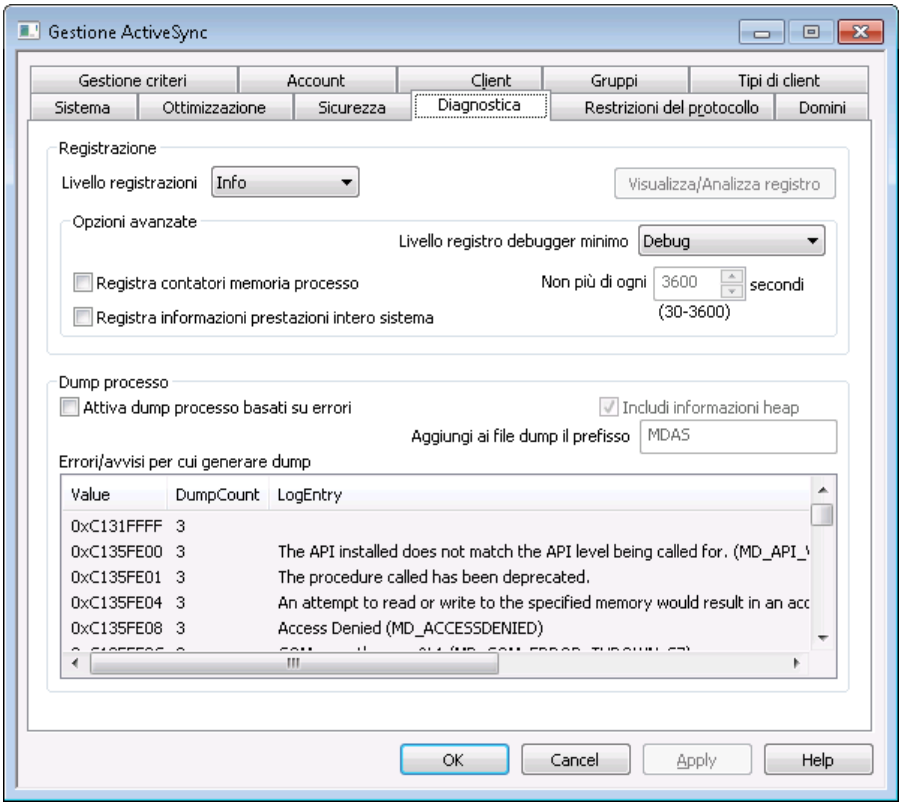
È possibile esentare facilmente un dispositivo dalla finestra di dialogo Client 470. Fare clic con il pulsante destro del mouse su un client dell'elenco e scegliere **Esenta questo client dai criteri**.

Eliminazione di un client esentato
Per eliminare delle voci, selezionare una o più voci dall'elenco e fare clic su **Elimina voce**. Verrà chiesto di confermare l'operazione di eliminazione.

Per ulteriori informazioni, vedere:

ActiveSync » Client 470

3.10.4 Diagnostica



In questa schermata sono disponibili le opzioni avanzate che nella maggior parte dei casi non sarà necessario utilizzare, se non per tentare di diagnosticare un problema o per una richiesta dell'assistenza tecnica.

Scrittura nel registro e archiviazione

In questa sezione sono riportate le impostazioni del livello di registrazione globale di ActiveSync. Impostazioni client dominio 220 con il livello di registrazione impostato su "Usa ereditate o predefinite" erediterà tale impostazione da qui.

Livello di registrazione

Sono supportati sei livelli di registrazione, dal più alto al più basso volume di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili ed è in genere usato per la diagnosi di un problema o quando l'amministratore necessita di informazioni dettagliate.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore	Vengono registrati errori, errori critici ed eventi di avvio e di arresto.
Critico	Vengono registrati errori critici ed eventi di avvio e di arresto.
Nessuno	Vengono registrati solo gli eventi di avvio e di arresto.

Visualizza/Analizza registro
Fare clic su questo pulsante per aprire il Visualizzatore del registro di sistema avanzato di MDaemon. Per impostazione predefinita i registri vengono archiviati in: "..\MDaemon\Logs\"

Opzioni avanzate

Livello minimo registro debugger
Livello minimo di registrazione da inviare al debugger. I livelli di registrazione disponibili sono identici a quelli descritti in precedenza.

Registra contatori di memoria del processo
Selezionare questa casella per registrare informazioni specifiche del processo su Memoria, Handle e Thread nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Registra dati delle prestazioni dell'intero sistema
Selezionare questa casella per registrare le informazioni sulle prestazioni dell'intero sistema nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Non più di ogni [xx] secondi
Utilizzare questa opzione per impostare il limite di frequenza della registrazione delle informazioni su processo e prestazioni.

Dump del processo

Attiva dump del processo in base agli errori
Attivare questa opzione per generare dump del processo ogni volta che si verifica un errore o un avviso specifico e indicata di seguito.

Includi informazioni heap nei dump
Per impostazione predefinita le informazioni heap sono incluse nei dump di processo. Se non si desidera includerli, deselezionare questa casella di controllo.

Prefisso file dump
I nomi dei file di dump del processo inizieranno con il prefisso indicato.

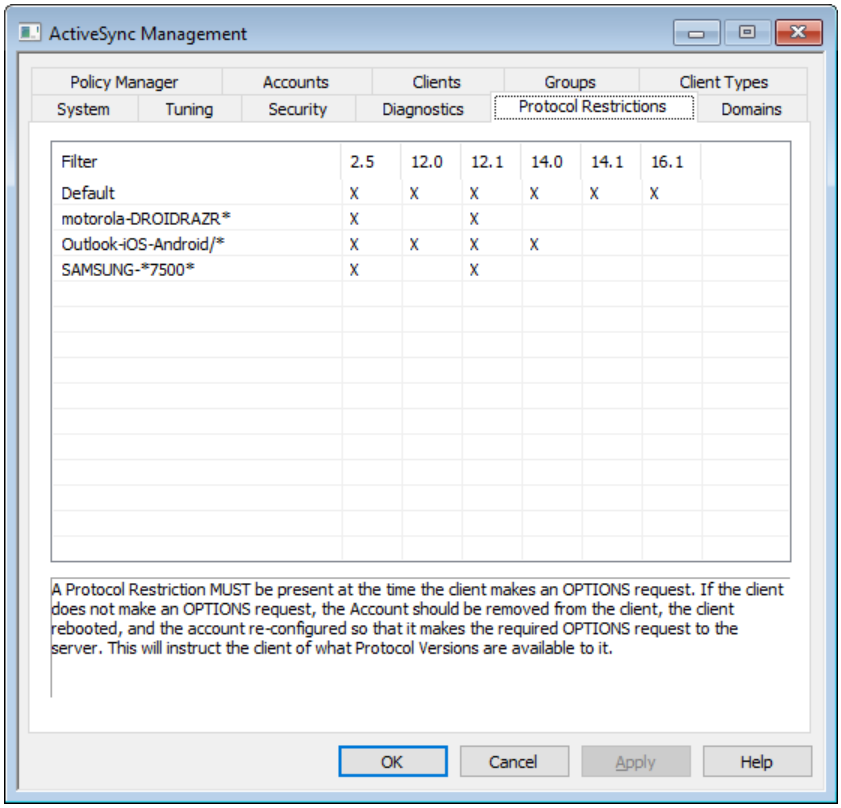
Errori/avvisi con generazione di dump
Fare clic con il pulsante destro del mouse in quest'area e utilizzare le opzioni *Aggiungi/Modifica/Elimina voce...* per gestire l'elenco degli errori o avvisi che

avviano i dump del processo. Per ciascuna voce è possibile specificare il numero di dump di processo consentiti prima di essere disattivato.

Per ulteriori informazioni, vedere:

ActiveSync » Regolazione 427

3.10.5 Restrizioni del protocollo



Restrizioni protocollo dispositivo

Utilizzare le opzioni presenti in "ActiveSync » Restrizioni protocollo" per limitare determinati client e dispositivi all'uso di protocolli ActiveSync specifici. Questa opzione risulta utile quando si rileva, ad esempio, che un determinato tipo di dispositivo offre un supporto affidabile solo per uno specifico protocollo. Utilizzando la finestra di dialogo Aggiungi/modifica restrizione protocollo 443 è possibile definire le restrizioni in base allo user agent o al tipo di dispositivo e limitare i dispositivi a una delle seguenti versioni dei protocolli ActiveSync: 2.5, 12.0, 12.1, 14.0, 14.1 e 16.1.

Per impostazione predefinita, le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Per

impedire connessioni che tentano di utilizzare i protocolli oggetto della restrizione, utilizzare l'opzione *Applica restrizioni protocollo* nelle finestre di dialogo Impostazioni client 430.

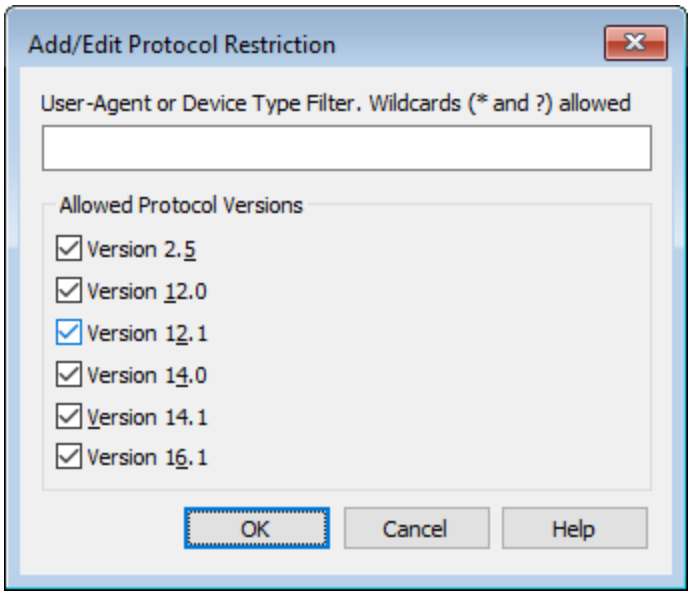
Fare clic con il pulsante destro del mouse sull'elenco per aprire un menu di scelta rapida con le seguenti opzioni:

Crea restrizione protocollo
Fare clic su questa opzione per aprire la finestra di dialogo Aggiungi/Modifica restrizione protocollo 443 (vedere di seguito), che si utilizza per aggiungere restrizioni relative ai protocolli.

Modifica restrizione protocollo
Per modificare una restrizione del protocollo, fare doppio clic su una voce riportata in questo elenco (oppure fare clic con il pulsante destro del mouse e scegliere **Modifica restrizione protocollo**). Una volta apportate le modifiche desiderate nell'editor delle restrizioni, fare clic su **OK**.

Elimina restrizione protocollo
Per eliminare una restrizione del protocollo, fare doppio clic su una voce riportata in questo elenco (oppure fare clic con il pulsante destro del mouse e scegliere **Elimina restrizione protocollo**). Fare clic su**Sì** per confermare l'eliminazione della restrizione.

Aggiungi/Modifica restrizione protocollo

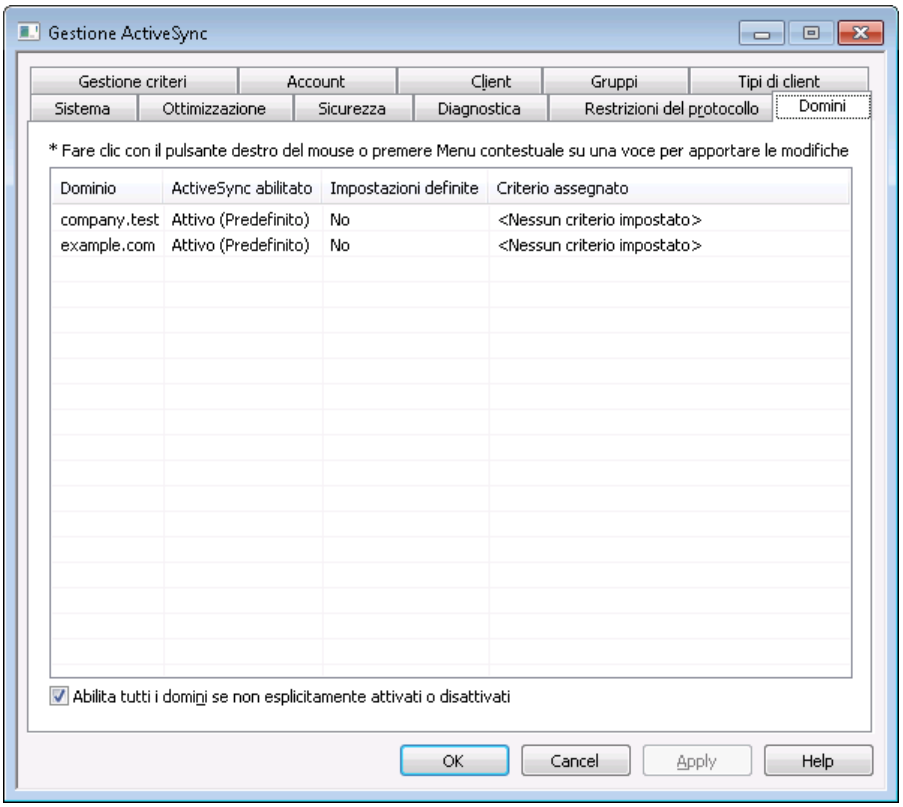


Filtro User Agent o tipo dispositivo
Immettere lo User Agent o il tipo di dispositivo al quale si applicherà la restrizione. Quando si identifica lo user agent, MDaemon utilizza tutti i caratteri che precedono e includono il primo carattere "/", se presente nella stringa. In caso contrario, viene utilizzata l'intera stringa. Se non si conosce il nome esatto dell'Agente utente o del

Tipo dispositivo, dopo che il client si è connesso a MDaemon ActiveSync (MDAS) è possibile passare alla schermata Client[470], selezionare il client dall'elenco e fare clic su Dettagli. È anche possibile trovare questa informazioni esaminando direttamente il file di registro di MDAS.

Versioni protocollo consentite
Fare clic su ciascun protocollo che si desidera supportare per il dispositivo o lo user agent. Quando si connette a MDaemon, al client specificato verrà indicato di utilizzare solo i protocolli selezionati.

3.10.6 Domini



Utilizzare questa schermata per gestire le impostazioni di ActiveSync per i domini[185]. È possibile abilitare o disabilitare ActiveSync per ciascun dominio, assegnare un criterio ActiveSync[452] predefinito, gestire le impostazioni client predefinite e gestire i dispositivi associati con il dominio.

Attivazione/disattivazione di ActiveSync per domini specifici
Per impostare lo stato ActiveSync di un dominio specifico:

1. Fare clic con il pulsante destro su un dominio nell'elenco.

2. Fare clic su **Attiva**, **Disattiva** o **Impostazione predefinita**. Se si sceglie "*Impostazione predefinita*" l'opzione riportata di seguito "*Abilita tutti i domini a meno che non siano esplicitamente abilitati o disabilitati*" determinerà se ActiveSync potrà essere utilizzato o meno per il dominio.

Per utilizzare ActiveSync è necessario configurare nel dispositivo dell'utente un client ActiveSync. Per istruzioni, seguire il collegamento *Acquistare, aggiornare o esaminare ActiveSync per MDaemon* disponibile nella schermata ActiveSync per MDaemon 425 e scorrere fino a visualizzare le istruzioni per la configurazione del dispositivo.

Impostazioni dello stato predefinito ActiveSync

I domini con la colonna *ActiveSync abilitato* impostata su **Abilitato/Disabilitato (predefinito)** derivano la propria impostazione di ActiveSync dallo stato dell'opzione: **Abilita tutti i domini a meno che non esplicitamente abilitati o disabilitati**. Quando l'opzione è attivata, per impostazione predefinita in tutti i domini ActiveSync risulterà attivato. Quando è disattivata, ActiveSync verrà disattivato per impostazione predefinita. Se si imposta un dominio su **Abilitato** o **Disabilitato** in modo specifico, si sostituisce l'impostazione predefinita.

Se si modifica l'impostazione *ActiveSync abilitato* di un dominio su **Disabilitato**, viene visualizzata una finestra di conferma con cui si chiede all'utente di confermare la revoca dell'accesso ad ActiveSync per tutti gli utenti del dominio specificato. Scegliere **No** se si desidera che gli utenti del dominio specificato possano continuare a utilizzare ActiveSync. Se si sceglie **Sì**, ActiveSync verrà disabilitato per tutti gli utenti del dominio specificato.

Modifica delle impostazioni di un client del dominio

Fare clic con il pulsante destro su un dominio per gestire le impostazioni del client per il dominio. Per impostazione predefinita queste impostazioni sono ereditate dalla schermata Impostazioni generali client 430. Vedere Gestione delle impostazioni del client di un dominio 446 di seguito.

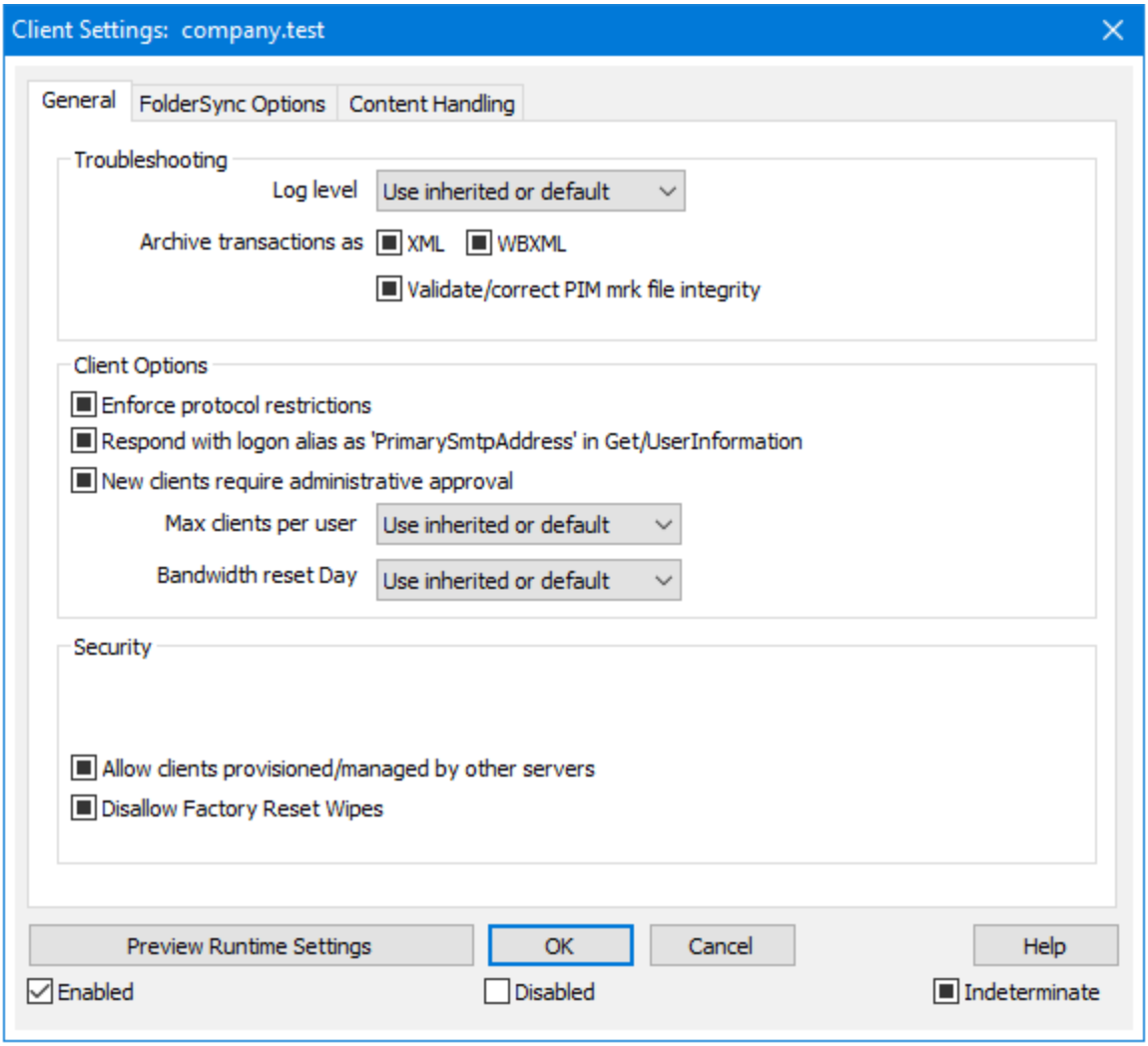
Assegnazione di un criterio ActiveSync predefinito

Per assegnare un criterio ActiveSync predefinito a un dominio:

1. Fare clic con il pulsante destro su un dominio nell'elenco.
2. Fare clic su **Applica criterio**.
3. In "Criterio da assegnare" selezionare il criterio desiderato dall'elenco a discesa (per la gestione dei criteri disponibili, vedere Gestione criteri 452).
4. Fare clic su **OK**.

Gestione delle impostazioni del client di un dominio

La schermata Impostazioni client del dominio consente di gestire le impostazioni predefinite di account e client associati al dominio.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Impostazioni client globali 430. Allo stesso modo, le impostazioni client per gli Account 461 del dominio erediteranno le impostazioni da questa schermata, perché la schermata Impostazioni client del dominio è la schermata principale. Le modifiche apportate alle opzioni in questa schermata verranno riportate anche nelle altre. A seguire, per i Tipi client sono disponibili schermate di impostazioni che ereditano i valori dalle impostazioni a livello di account e, infine, anche i singoli client 470 hanno impostazioni proprie. Questa configurazione rende possibile all'utente apportare modifiche a tutti i client e gli account del dominio semplicemente apportando le modifiche in quest'unica schermata, consentendo inoltre all'utente di sovrascrivere tali impostazioni per qualsiasi account o client quando necessario.

Generale

Risoluzione dei problemi

Livello di registrazione

ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]

Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM

Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo

Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per

il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata

per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se

richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

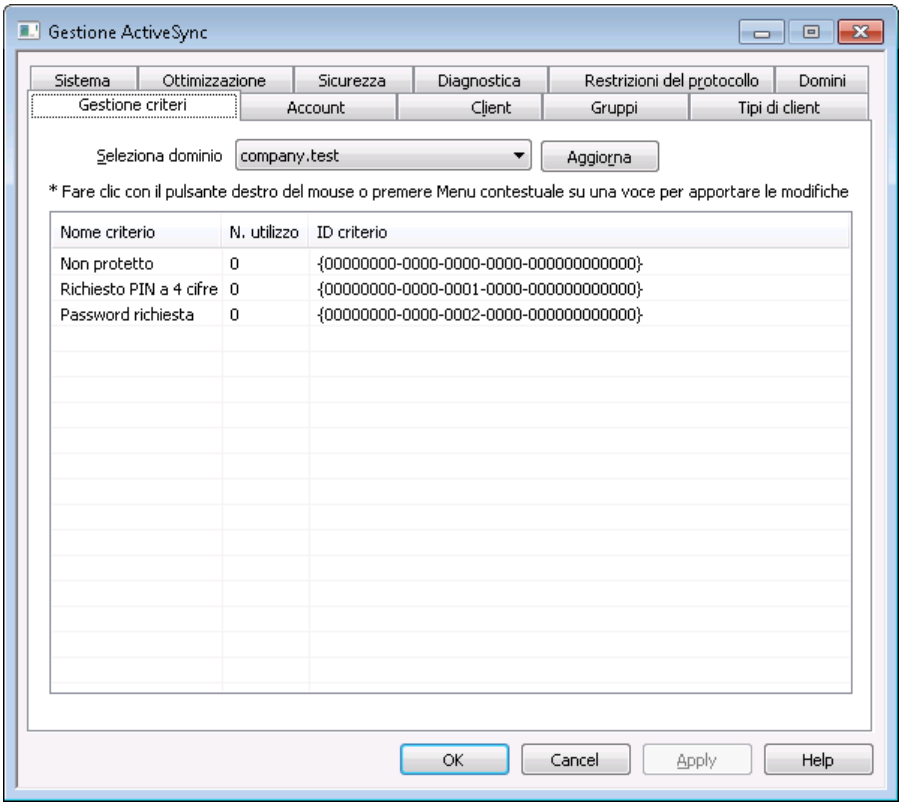
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Vedere:

Domain Manager » Impostazioni client ActiveSync 220
Domain Manager » Client ActiveSync 246
ActiveSync » Policy Manager 452

3.10.7 Policy Manager



Utilizzare questa schermata per gestire i criteri ActiveSync che è possibile assegnare ai dispositivi degli utenti per regolare diverse opzioni. Sono disponibili criteri predefiniti ed è possibile creare, modificare ed eliminare criteri personalizzati. È possibile assegnare criteri predefiniti per dominio 444 e per account 461. È inoltre possibile assegnare i criteri a client specifici 246.

Non tutti i dispositivi ActiveSync riconoscono o applicano i criteri in modo coerente. Alcuni potrebbero ignorare del tutto i

> criteri o alcuni elementi dei criteri, mentre altri potrebbero richiedere un riavvio del dispositivo per rendere effettive le modifiche. Inoltre, quando si tenta di assegnare un nuovo criterio a un dispositivo, il criterio viene applicato solo alla successiva connessione del dispositivo al server ActiveSync; non è possibile inviare i criteri ai dispositivi fino a quando questi ultimi non eseguono la connessione.

Criteri ActiveSync

Fare clic con il pulsante destro del mouse sull'elenco per aprire un menu di scelta rapida con le seguenti opzioni:

Crea criterio
Fare clic su questa opzione per aprire l'editor dei criteri di ActiveSync, che consente di creare e modificare i criteri.

Elimina
Per eliminare un criterio, selezionare un criterio personalizzato dall'elenco, quindi fare clic su **Elimina**. Fare clic su **Sì** per confermare l'azione. Non è possibile eliminare i criteri predefiniti.

Modifica criterio
Per modificare un criterio, fare clic con il pulsante destro su un criterio personalizzato dell'elenco e scegliere **Modifica criterio**. Una volta apportate le modifiche desiderate nell'editor dei criteri, fare clic su**OK**. Non è possibile modificare i criteri predefiniti.

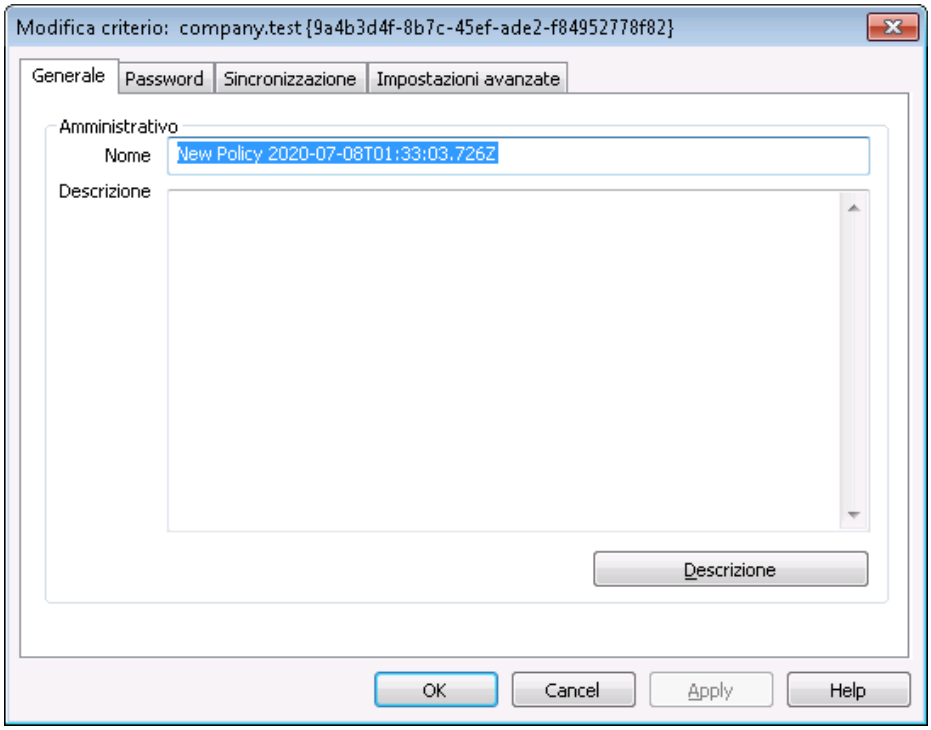
Visualizza utilizzo criterio
Fare clic con il pulsante destro su un criterio, quindi scegliere questa opzione per visualizzare un elenco di tutti i domini, gli account e i client configurati per l'utilizzo di questo criterio.

Editor criteri ActiveSync

Editor criteri ActiveSync contiene quattro schede: Generale, Password, Sincronizzazione e Impostazioni avanzate. La scheda Impostazioni avanzate resta nascosta fino a che non si attiva *Consenti modifica impostazioni avanzate criteri* 425, disponibile nella schermata Sistema ActiveSync.

Generale

Utilizzare questa schermata per specificare un nome e una descrizione per il criterio. È possibile anche visualizzare l'anteprima del documento XML del criterio.



Amministrativo

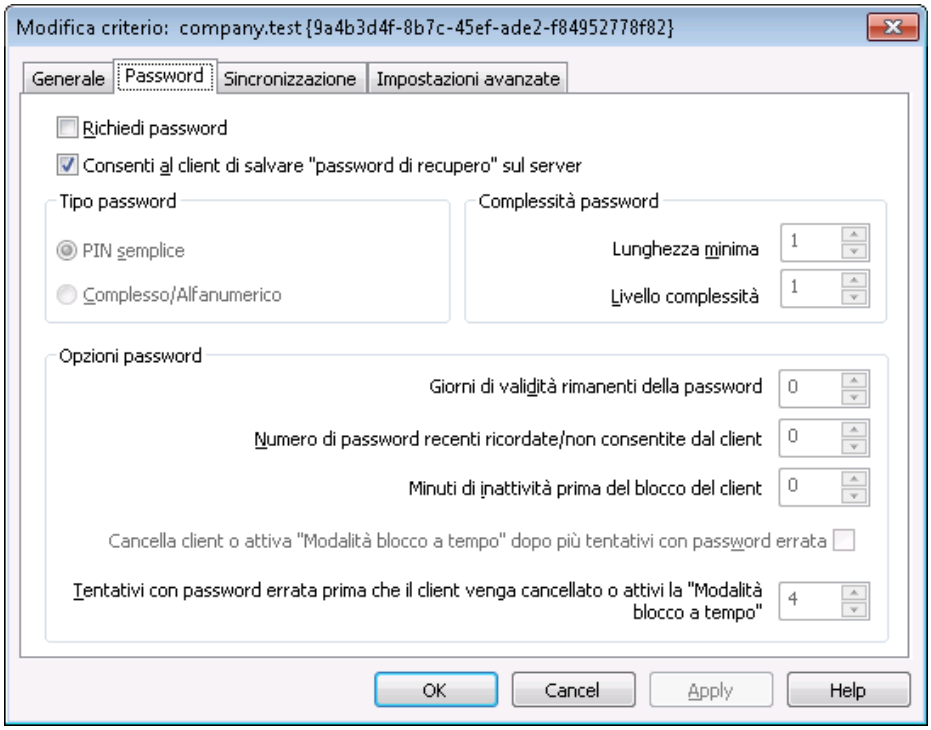
Nome
Consente di specificare il nome del criterio personalizzato.

Descrizione
Quest'area consente di descrivere il criterio personalizzato. La descrizione viene visualizzata nella finestra di dialogo Applica criterio quando si seleziona un criterio da applicare a un dominio, account o client.

Anteprima documento criterio
Fare clic su questo pulsante per visualizzare l'anteprima del documento XML per questo criterio.

Password

Opzioni e requisiti della password per il criterio si possono specificare in questa scheda.



Richiedi password
Selezionare questa casella per richiedere una password per il dispositivo. Questa opzione è disabilitata per impostazione predefinita.

Consenti al dispositivo di salvare "password di recupero" sul server
Attivare questa opzione per consentire ai client di utilizzare l'opzione di recupero della password di ActiveSync, che permette a un dispositivo di salvare una password di recupero temporanea sul server per sbloccare il dispositivo in caso di password dimenticata. L'amministratore può trovare la password di recupero nei Dettagli 470 del client. La maggior parte dei dispositivi non supporta questa funzionalità.

Tipo password

PIN semplice
Il modo in cui viene implementata questa opzione dipende in larga parte dal dispositivo, ma se si seleziona *PIN semplice* come tipo di password, in genere significa che non vengono imposte limitazioni o requisiti di complessità particolari per la password del dispositivo, a parte l'opzione *Lunghezza minima password* riportata di seguito. In questo modo si consentono password semplici come: "111", "aaa", "1234", "ABCD" e simili.

Complessa/Alfanumerica
Utilizzare questa opzione del criterio per richiedere password del dispositivo più complesse e sicure rispetto all'opzione *PIN semplice*. Utilizzare l'opzione *Livello*

complessità riportata di seguito per definire esattamente il livello di complessità della password. Questa è l'opzione predefinita quando il criterio richiede una password.

Sicurezza password

Lunghezza minima
Utilizzare questa opzione per impostare il numero minimo di caratteri, compreso tra 1 e 16, che la password del dispositivo deve contenere. Per impostazione predefinita, questa opzione è impostata su "1".

Livello complessità
Utilizzare questa opzione per impostare il requisito del livello di complessità per la password del dispositivo di tipo *Complessa/Alfanumerica*. Il livello equivale al numero dei diversi tipi di caratteri che la password deve contenere: lettere maiuscole, lettere minuscole, numeri e caratteri non alfanumerici (come punteggiatura o caratteri speciali). È possibile richiedere da 1 a 4 tipi di caratteri. Se, ad esempio, si imposta questa opzione su "2", allora la password deve contenere almeno due dei quattro tipi di carattere: maiuscole e numeri, maiuscole e minuscole, numeri e simboli e così via. Per impostazione predefinita, questa opzione è impostata su "1".

Opzioni password

Giorni fino alla scadenza della password (0 = mai)
Indica il numero di giorni che devono trascorrere prima che diventi obbligatorio modificare la password del dispositivo. Questa opzione è disabilitata per impostazione predefinita (impostata su "0").

Numero di password recenti ricordate/non consentite dal dispositivo (0 = nessuno)
Utilizzare questa opzione se si desidera impedire al dispositivo di riutilizzare un numero specificato di password precedenti. Se, ad esempio, questa opzione è impostata su "2" e si modifica la password del dispositivo, non sarà possibile reimpostare una delle ultime due password utilizzate. L'opzione è disabilitata per impostazione predefinita (impostata su "0").

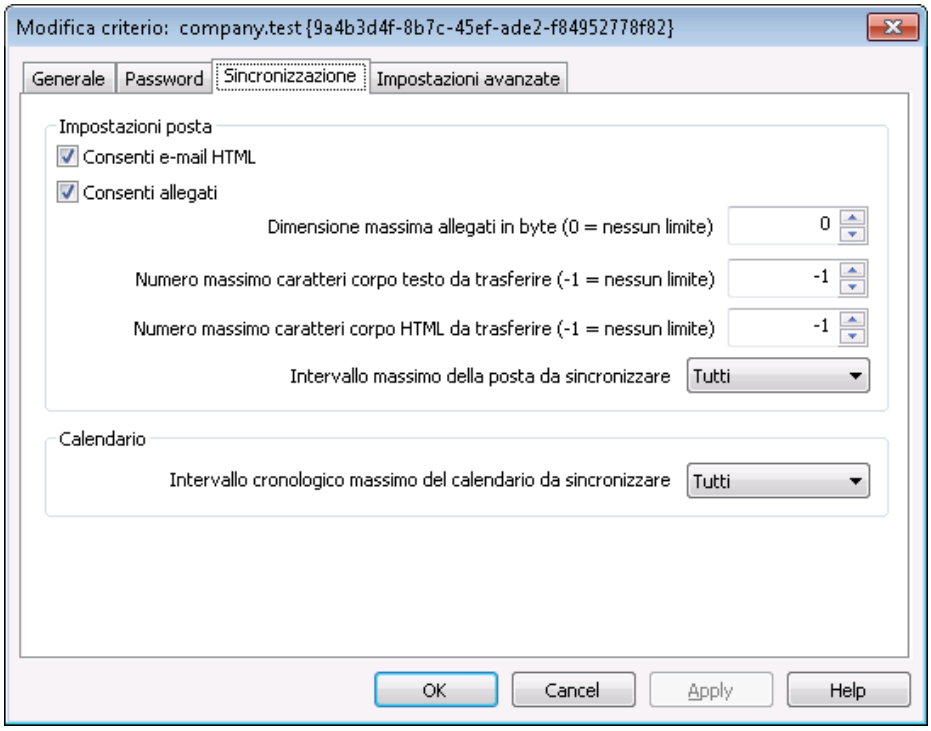
Minuti di inattività prima del blocco del dispositivo (0 = mai)
Indica il numero di minuti in cui un dispositivo può essere utilizzato senza alcun input dell'utente prima che si blocchi automaticamente. Questa opzione è disabilitata per impostazione predefinita (impostata su "0").

Pulisci dispositivo o attiva "Modalità blocco a tempo" dopo più tentativi con password errata
Quando si attiva questa opzione e un utente immette una password errata nel dispositivo per il numero di tentativi specificato, il dispositivo si blocca automaticamente per un determinato periodo di tempo oppure esegue la cancellazione di tutti i dati, a seconda del dispositivo. L'opzione è disabilitata per impostazione predefinita.

Tentativi con password errata prima che il dispositivo cancelli i dati o attivi la "Modalità blocco a tempo"
Quando si attiva l'opzione di *cancellazione dei dati* sopra specificata e un utente immette una password errata per il numero di tentativi indicato, il dispositivo cancella i dati o si attiva la "Modalità blocco a tempo", a seconda del dispositivo.

Sincronizzazione

In questa schermata sono disponibili le impostazioni per i messaggi e-mail in HTML, gli allegati, la limitazione del numero di caratteri da trasferire e il numero massimo di messaggi e il periodo di calendario da sincronizzare.



Impostazioni e-mail

Consenti e-mail in HTML
Per impostazione predefinita è possibile sincronizzare i messaggi e-mail in HTML con i client ActiveSync. Deselezionare questa casella di controllo per inviare solo messaggi in testo normale.

Consenti allegati
Consente il download dei file allegati sul dispositivo. L'opzione è abilitata per impostazione predefinita.

Dimensioni massime allegati in byte (0 = nessun limite)
Rappresenta la dimensione massima dell'allegato che può essere scaricato automaticamente sul dispositivo. L'impostazione predefinita non prevede alcun limite di dimensione ("0").

Numero massimo di caratteri di testo da trasferire (-1 = nessun limite)
Questo è il numero massimo di caratteri del corpo dei messaggi e-mail in testo normale che verranno inviati al client. Se il corpo del messaggio contiene più caratteri di quelli consentiti, il corpo del messaggio viene troncato al limite specificato. L'impostazione predefinita non prevede alcun limite (opzione impostata su "-1"). Se si imposta l'opzione su "0", viene inviata solo l'intestazione del messaggio.

Numero massimo di caratteri HTML da trasferire (-1 = nessun limite)
Questo è il numero massimo di caratteri del corpo dei messaggi e-mail in HTML che verranno inviati al client. Se il corpo del messaggio contiene più caratteri di quelli consentiti, il corpo del messaggio viene troncato al limite specificato. L'impostazione predefinita non prevede alcun limite (opzione impostata su "-1"). Se si imposta l'opzione su "0", viene inviata solo l'intestazione del messaggio.

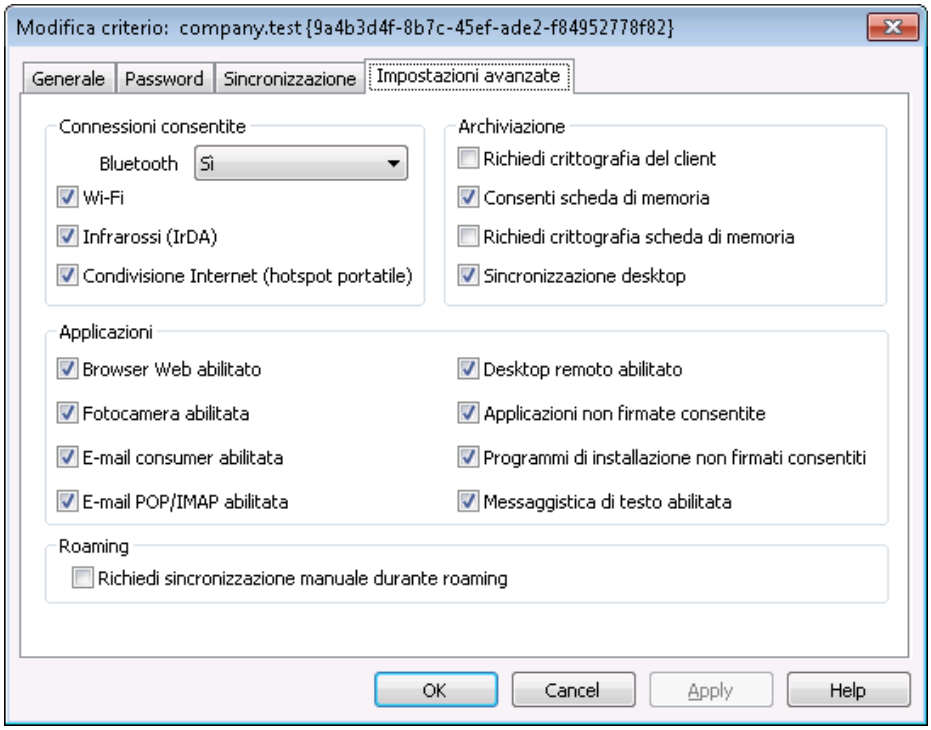
Periodo di tempo massimo per i messaggi e-mail da sincronizzare
Indica la quantità di messaggi e-mail precedenti, per intervallo di date a partire dalla data odierna, che può essere sincronizzata dal dispositivo. Per impostazione predefinita, questa opzione è configurata su "Tutto", ovvero è possibile sincronizzare tutta la posta elettronica, indipendentemente dalla data.

Calendario

Periodo cronologia calendario massimo da sincronizzare
La lunghezza del periodo precedente per cui possono essere sincronizzate le voci di calendario del dispositivo. Per impostazione predefinita, questa opzione è configurata su "Tutto", ovvero è possibile sincronizzare tutte le voci passate, indipendentemente dalla data.

Impostazioni avanzate

Nella scheda Impostazioni avanzate sono disponibili le opzioni per definire i tipi di connessione consentiti, la possibilità di abilitare determinate applicazioni, l'archiviazione, la crittografia e il roaming.



La scheda resta nascosta, a meno che non si attivi l'opzione *Abilita modifica opzioni avanzate criteri*[425], disponibile nella schermata ActiveSync per MDaemon.

Connessioni consentite

Bluetooth

Utilizzare questa opzione per specificare se le connessioni Bluetooth sono consentite o meno per il dispositivo. È possibile scegliere **Sì** per consentire le connessioni Bluetooth, **No** per impedirle o **Viva voce** per limitare la connessione Bluetooth alla sola funzione Viva voce. Per impostazione predefinita, questa opzione è impostata su **Sì**.

WIFI

Consente le connessioni WIFI. L'opzione è abilitata per impostazione predefinita.

Infrarossi (IrDA)

Consente le connessioni a infrarossi (IrDA). L'opzione è abilitata per impostazione predefinita.

Condivisione Internet (hotspot portatile)

L'opzione consente al dispositivo di utilizzare la condivisione Internet (hotspot portatile). L'opzione è abilitata per impostazione predefinita.

Archiviazione

Richiedi crittografia dispositivo
Selezionare questa opzione per richiedere la crittografia sul dispositivo. Non tutti i dispositivi applicano la crittografia. È disabilitata per impostazione predefinita.

Consenti scheda di memoria
Consente di utilizzare una scheda di memoria nel dispositivo. Per impostazione predefinita, questa opzione è abilitata.

Richiedi crittografia scheda di memoria
Selezionare questa opzione per richiedere la crittografia della scheda di memoria. È disabilitata per impostazione predefinita.

Sincronizzazione desktop
Consente di utilizzare ActiveSync per il desktop sul dispositivo. L'opzione è abilitata per impostazione predefinita.

Applicazioni

Browser Web abilitato
Consente l'utilizzo di un browser sul dispositivo. Questa opzione non è supportata su alcuni dispositivi e potrebbe non essere applicabile a browser di terze parti. L'opzione è abilitata per impostazione predefinita.

Videocamera abilitata
Consente l'utilizzo di una videocamera sul dispositivo. L'opzione è abilitata per impostazione predefinita.

E-mail consumer abilitate
Il dispositivo consente all'utente di configurare un account di posta elettronica personale. Se si disattiva questa opzione, i tipi di account di posta elettronica o servizi non consentiti dipendono completamente dal client ActiveSync specifico. L'opzione è abilitata per impostazione predefinita.

Posta POP/IMAP abilitata
Consente l'accesso alla posta elettronica mediante POP e IMAP. L'opzione è abilitata per impostazione predefinita.

Desktop remoto abilitato
Consente al client di utilizzare Desktop remoto. L'opzione è abilitata per impostazione predefinita.

Applicazioni senza firma consentite
Questa opzione consente l'uso di applicazioni senza firma sul dispositivo. Per impostazione predefinita, questa opzione è abilitata.

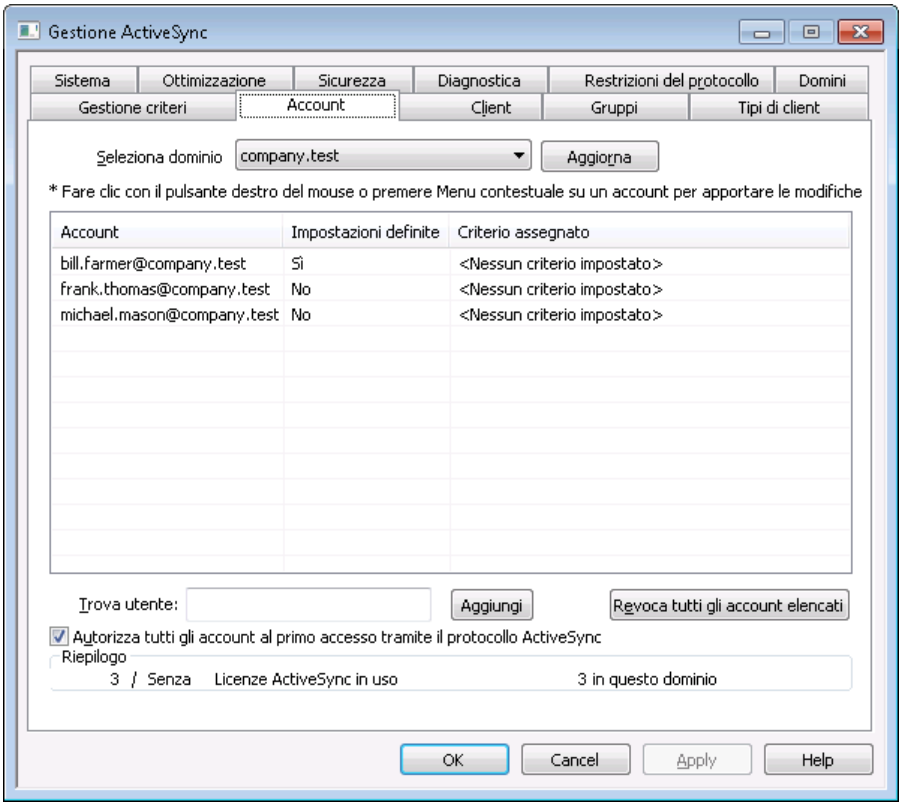
Programmi di installazione senza firma consentiti
Questa opzione consente l'esecuzione di programmi di installazione senza firma sul dispositivo. Per impostazione predefinita, questa opzione è abilitata.

Messaggi di testo consentiti
Questa opzione consente di utilizzare i messaggi di testo sul dispositivo. I messaggi di testo sono abilitati per impostazione predefinita.

Roaming

Richiedi sincronizzazione manuale in roaming
Utilizzare questa opzione per richiedere la sincronizzazione manuale del dispositivo durante il roaming. La sincronizzazione automatica durante il roaming potrebbe aumentare i costi dei dati per il dispositivo, a seconda del gestore e del piano dati. L'opzione è disabilitata per impostazione predefinita.

3.10.8 Account

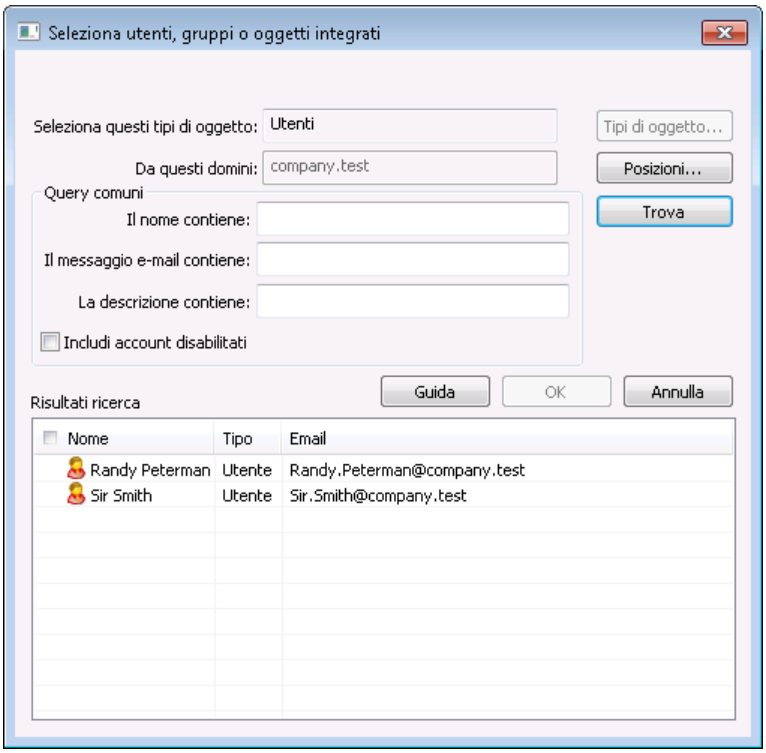


Utilizzare questa schermata per specificare gli account autorizzati a utilizzare ActiveSync. È possibile autorizzare o revocare manualmente le autorizzazioni agli

account o impostare MDaemon in modo da autorizzare automaticamente ciascun account quando si connette mediante ActiveSync.

Account con autorizzazione manuale

Nella schermata Account, selezionare un dominio dall'elenco a discesa *Seleziona dominio*, quindi fare clic su **Aggiungi** per autorizzare manualmente uno o più degli account all'utilizzo di ActiveSync. Viene visualizzata la finestra di dialogo Utenti per la ricerca e la selezione degli account.



Da questi domini
Qui sono elencati i domini selezionati nell'opzione *Seleziona dominio* della schermata Account. È possibile cercare gli utenti di questo dominio.

Interrogazioni comuni
Utilizzare le opzioni presenti in questa sezione per restringere la ricerca specificando in tutto o in parte nome dell'utente, indirizzo e-mail o i contenuti della Descrizione[729] dell'account. Lasciare questi campi vuoti se si desidera che i risultati contengano tutti gli utenti del dominio selezionato.

Includi account disabilitati
Selezionare questa casella di controllo se si desidera includere gli account disabilitati[729] nella ricerca.

Trova
Dopo aver specificato tutti i criteri di ricerca, fare clic su **Trova** per eseguire la ricerca.

Risultati ricerca
Dopo aver eseguito la ricerca, selezionare gli utenti desiderati nei Risultati della ricerca e fare clic su **OK** per aggiungerli all'elenco degli account autorizzati.

Revoca degli account

Per revocare l'autorizzazione di un account all'uso di ActiveSync, fare clic con il pulsante destro del mouse su un account dell'elenco e selezionare **Revoca autorizzazione ActiveSync**. Per revocare l'autorizzazione di tutti gli account, fare clic sul pulsante **Revoca tutti gli account in elenco**.

Se si è abilitata l'opzione per *autorizzare tutti gli account al primo accesso tramite il protocollo ActiveSync*, la revoca dell'autorizzazione di accesso di un utente lo rimuoverà dall'elenco, ma quando un dispositivo si connetterà nuovamente per l'account, l'autorizzazione verrà concessa nuovamente.

Autorizza tutti gli account al primo accesso mediante protocollo ActiveSync

Selezionare questa casella se si desidera autorizzare automaticamente ciascun account a connettersi a MDaemon mediante ActiveSync.

Assegnazione di un criterio ActiveSync

Per assegnare un Criterio 452 all'account:

1. Fare clic con il pulsante destro del mouse su un account dell'elenco.
2. Fare clic su **Applica criterio**.
3. In "Criterio da assegnare" selezionare il criterio desiderato dall'elenco a discesa (per la gestione dei criteri disponibili, vedere Gestione criteri 452).
4. Fare clic su **OK**.

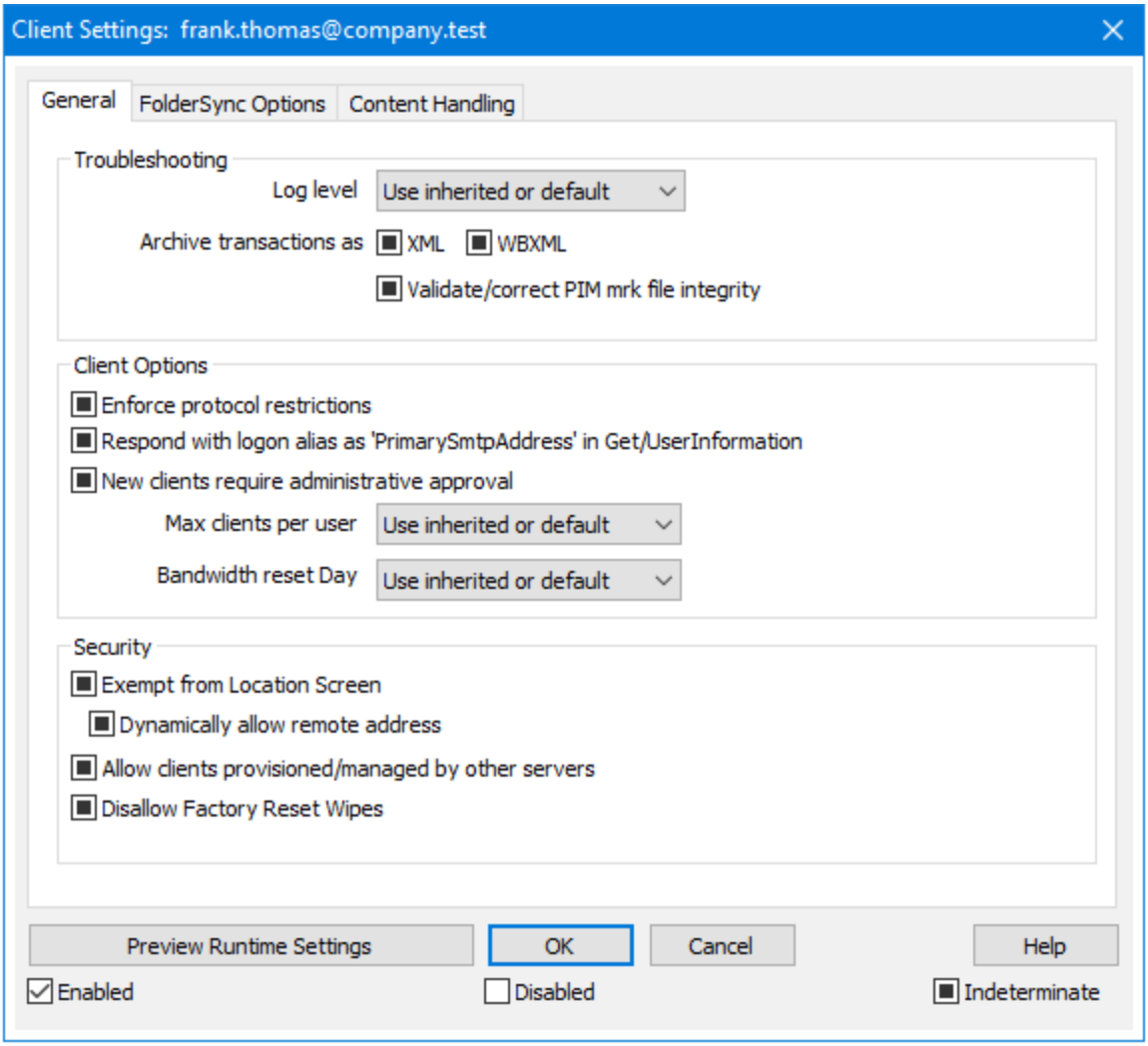
Questo criterio sarà assegnato ai nuovi dispositivi che si connettono per l'account.

Ricerca dell'elenco degli account autorizzati

Se si dispone di un numero elevato di account autorizzati all'uso di ActiveSync, è possibile utilizzare la casella **Trova utente** per cercare l'elenco di un account specifico. Per selezionare l'utente, è sufficiente digitare le prime lettere dell'indirizzo e-mail dell'account.

Impostazioni client account

Fare clic con il pulsante destro su un account e scegliere **Personalizza impostazioni client** per gestire le impostazioni del client per l'account. Queste impostazioni saranno applicate ai client ActiveSync che si connettono per l'account.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che se l'account è membro di un Gruppo[479], le impostazioni di tutte le opzioni saranno ereditate dalle impostazioni del clienti di tale gruppo. Se l'account non fa parte di un gruppo, oppure se per il gruppo non sono state configurate impostazioni del client, ciascuna opzione verrà impostata come l'opzione corrispondente disponibile nella schermata Impostazioni client del dominio[220]. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra. Al contrario, le modifiche apportate in questa schermata sovrascriveranno le impostazioni a livello di gruppo o dominio per l'account.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per

il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata

per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se

richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

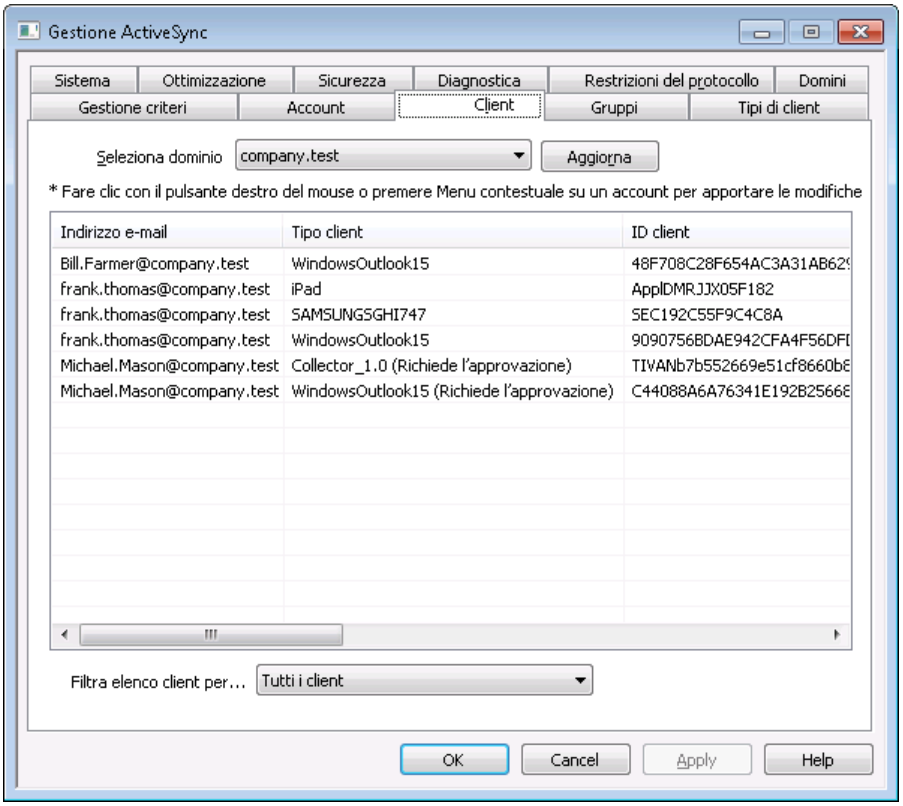
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

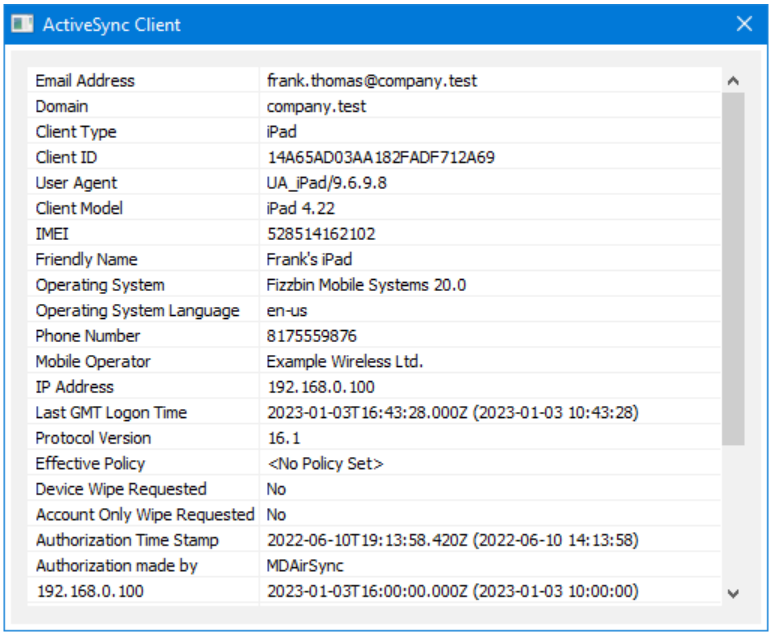
ActiveSync » Impostazioni client 430
ActiveSync » Domini 444
ActiveSync » Client 470
Account » Impostazioni client ActiveSync 780
Account » Client ActiveSync 787

3.10.9 Client



In questa schermata viene riportata una voce per ogni client ActiveSync associato al dominio selezionato. Fare doppio clic su una voce per visualizzare ulteriori dettagli sul client. Fare clic con il pulsante destro per aprire il menu di scelta rapida, che si può utilizzare per personalizzare le impostazioni del client, visualizzare le statistiche ed eseguire diverse altre funzioni.

Dettagli client ActiveSync



Fare doppio clic su una voce oppure fare clic con il pulsante destro sulla voce e scegliere **Visualizza dettagli client** per visualizzare la finestra di dialogo Dettagli client. In questa schermata sono riportate informazioni relative al client, come Tipo client, ID client, ora di ultimo accesso e simili.

Impostazioni client

Fare clic con il pulsante destro su un client e scegliere **Personalizza impostazioni client** per gestire le impostazioni del client. Per impostazione predefinita queste impostazioni vengono ereditate da Tipo client, ma si possono modificare secondo necessità. Vedere Gestione delle impostazioni del client di un dispositivo 472 di seguito.

Assegnazione di un criterio ActiveSync

Per assegnare un Criterio 452 al dispositivo:

1. Fare clic con il pulsante destro su un dispositivo nell'elenco.
2. Fare clic su **Applica criterio**. Verrà aperta la finestra di dialogo Applicazione criterio.
3. Fare clic sull'elenco a discesa **Criterio da assegnare** e scegliere il criterio desiderato.
4. Fare clic su **OK**.

Statistiche

Fare clic con il pulsante destro su una voce, quindi su **Visualizza statistiche** per visualizzare la finestra di dialogo Statistiche client, che contiene alcune statistiche sull'uso del client.

Ripristina statistiche

Per azzerare le statistiche di un client, fare clic con il pulsante destro sul client, quindi su **Azzera statistiche**, infine su **OK** per confermare l'azione.

Rimozione di un client ActiveSync

Per rimuovere un client ActiveSync, fare clic con il pulsante destro sul client e scegliere **Elimina**, quindi selezionare **Sì**. In questo modo si rimuove il client dall'elenco e si eliminano tutte le informazioni di sincronizzazione a esso correlate in MDaemon. Ne consegue che, se in futuro l'account utilizzerà ActiveSync per la sincronizzazione dello stesso client, MDaemon tratterà tale client come se non fosse mai stato utilizzato prima sul server; sarà dunque necessario risincronizzare tutti i dati del client con MDaemon.

Cancellazione completa di un client ActiveSync

Quando un criterio 452 è stato applicato a un client ActiveSync selezionato e il client l'ha applicato e ha risposto, per tale client sarà disponibile un'opzione Cancellazione completa. Per effettuare una cancellazione completa, fare clic con il tasto destro del mouse sul client (o selezionarlo se si utilizza MDRA) e fare clic su **Cancellazione completa**. Al successivo collegamento del client, MDaemon imposterà il dispositivo in modo da eliminare tutti i dati o da ripristinare le impostazioni di fabbrica. In base al client, ciò potrebbe comportare la totale rimozione di tutti i dati, app scaricate incluse. Inoltre, finché esisterà la voce ActiveSync del client, MDaemon continuerà a inviare la richiesta di cancellazione ogni volta che il dispositivo si connetterà. Se a un certo punto si desidera eliminare il client, accertarsi di aggiungerlo prima alla Lista bloccati 437, in modo che non possa connettersi di nuovo in futuro. Infine, se un dispositivo eliminato viene recuperato e si desidera consentirgli di connettersi nuovamente, selezionare il dispositivo e fare clic su **Annulla azioni di cancellazione**. Sarà anche necessario rimuoverlo dalla Lista bloccati.

Cancellazione account di un client ActiveSync

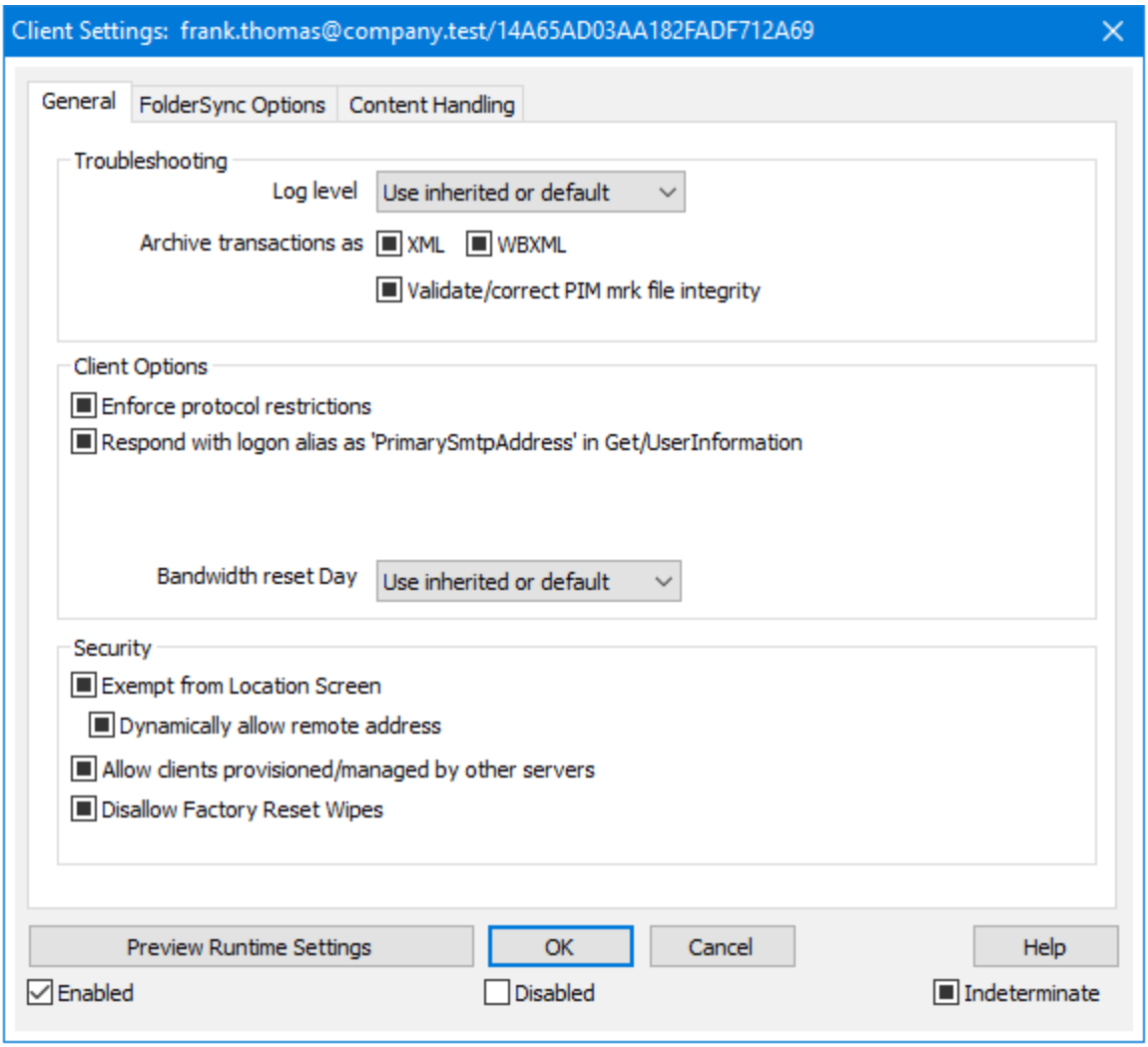
Per cancellare la posta dell'account e i dati PIM dal client o dal dispositivo, fare clic con il pulsante destro e scegliere **Cancella posta e PIM dell'account dal client**. L'opzione *Cancellazione account* è simile all'opzione *Cancellazione completa* descritta sopra, ma invece di eliminare tutti i dati, elimina solo i dati dell'account, come i messaggi di posta elettronica, le voci di calendario, i contatti e così via. Tutto il resto, come applicazioni, foto e musica, viene lasciato dove si trova.

Autorizzazione del client

Se l'opzione "*I nuovi client richiedono l'approvazione dell'amministratore*" nella schermata Impostazioni client ActiveSync 430 è attivata, selezionare un client e fare clic su Approva sincronizzazione client per autorizzarlo alla sincronizzazione con il server.

Gestione delle impostazioni del client di un dispositivo

La schermata Impostazioni client a livello di dispositivo consente di gestire le impostazioni per un dispositivo specifico.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Tipi client Impostazioni client 486. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra. Al contrario, le modifiche apportate in questa schermata sovrascriveranno le impostazioni a livello di tipi di client per il dispositivo.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei

problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo

modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a

MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

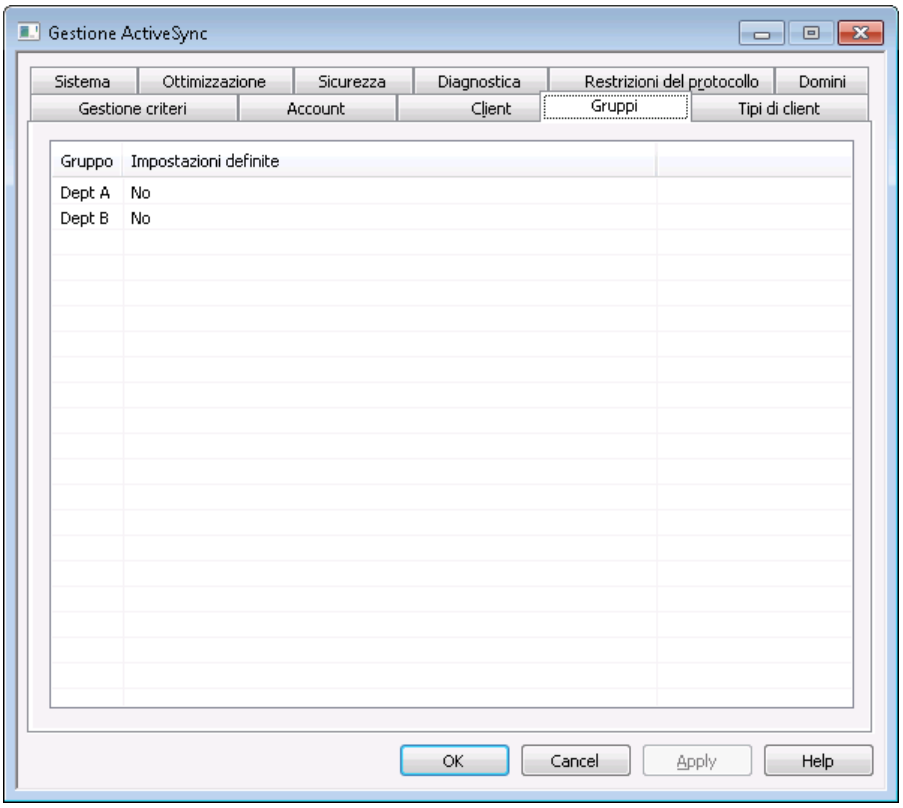
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

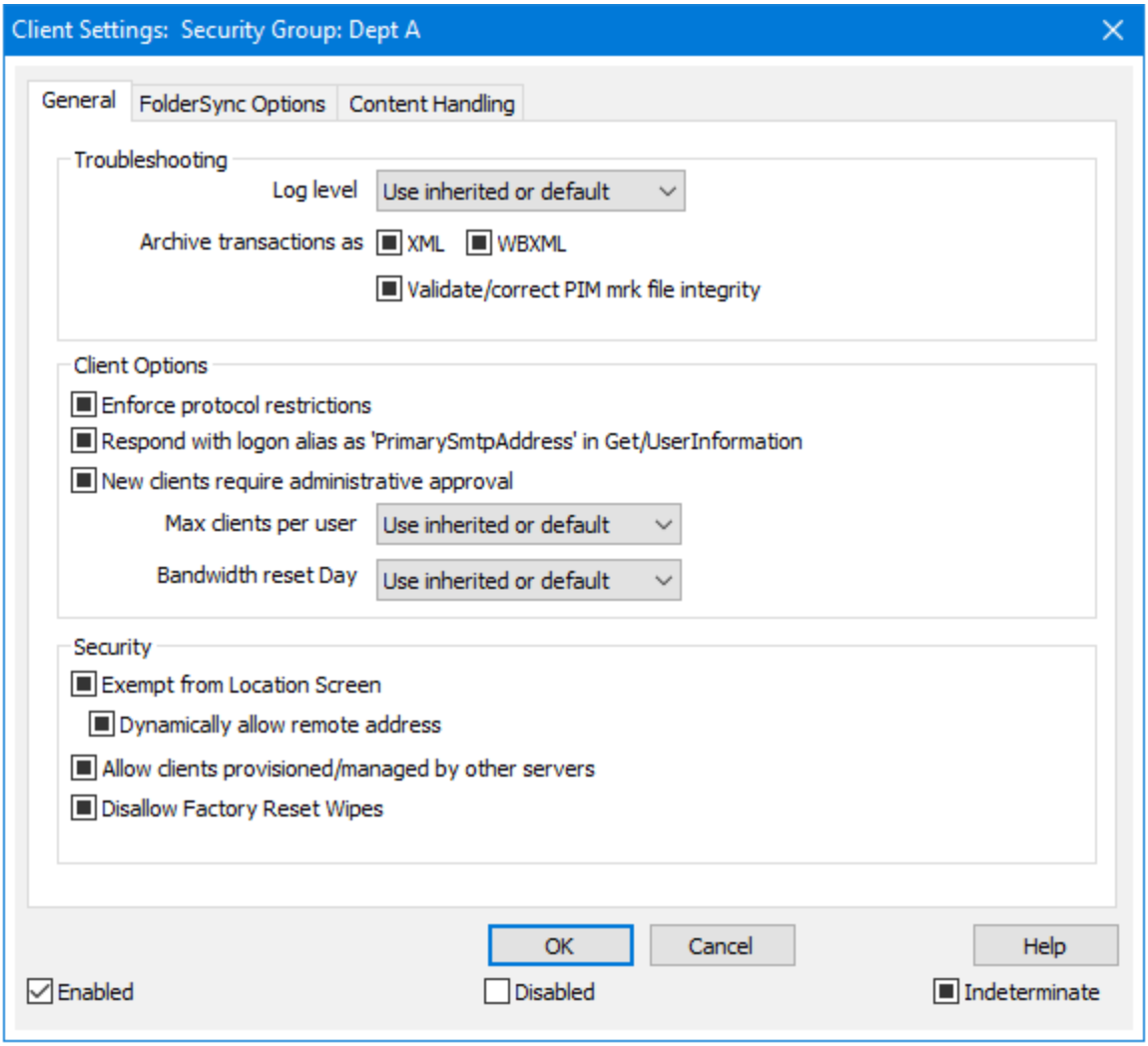
ActiveSync » Impostazioni client 430
ActiveSync » Domini 444
ActiveSync » Account 461

3.10.10 Gruppi



Per definire le impostazioni del client ActiveSync personalizzate per un account Gruppo 796, utilizzare questa schermata per gestire le impostazioni. Tutti i gruppi sono riportati qui e ciascuna voce di gruppo indica se le relative impostazioni sono state o meno personalizzate. Per modificare le impostazioni del client di un Gruppo, fare doppio clic sul Gruppo oppure fare clic con il pulsante destro del mouse sul Gruppo e scegliere **Personalizza impostazioni client**.

Impostazioni client gruppo



Per impostazione predefinita, ogni impostazione del client del Gruppo eredita lo stato da Impostazioni client dominio 220 dell'utente. Se si modificano le impostazioni del gruppo, si sostituiscono le impostazioni del dominio per tutti gli account membri di tale gruppo. Se non si desidera che le impostazioni dei client del gruppo vengano applicate a un membro o dispositivo specifico, è possibile sostituire le impostazioni del gruppo modificando le Impostazioni del client per l'Account 461, il Tipo client 486 o il Client 470.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci

disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo

principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un

altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche[317] a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca[319] sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche[317] padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise[122] a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise[757] a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client[470] e tipi di client[486] che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

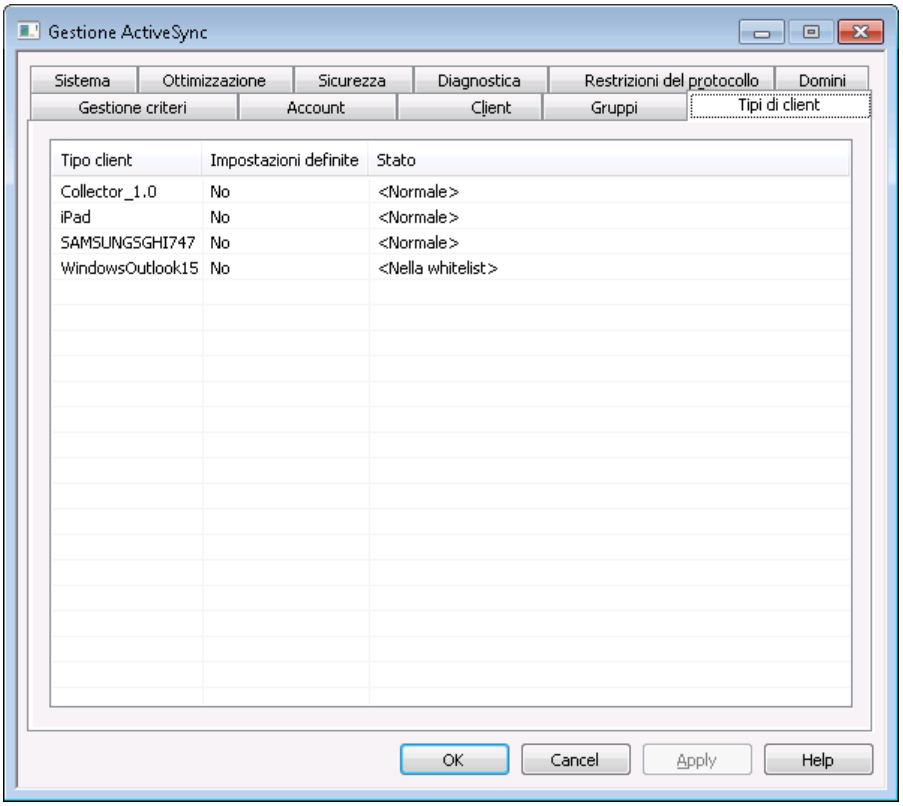
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Vedere:

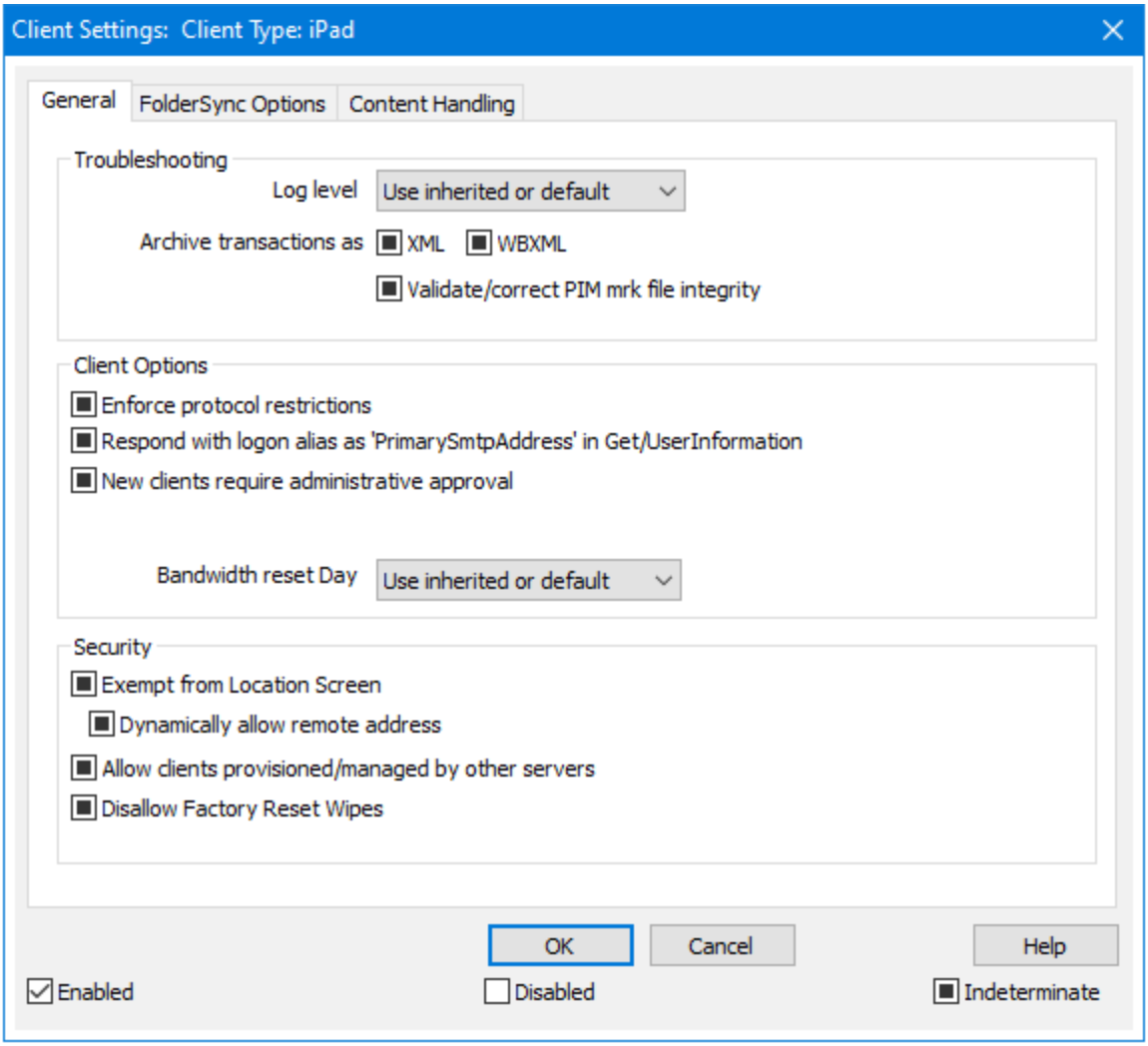
ActiveSync » Domini 444
ActiveSync » Account 461
ActiveSync » Client 470

3.10.11 Tipi client



Per definire impostazioni del client ActiveSync personalizzate per un tipo specifico di client di ActiveSync, utilizzare questa schermata per gestire le impostazioni. Il Tipo client di tutti i client al momento autorizzati 470 all'uso di ActiveSync è riportato qui e ciascuna voce di Tipo client indica se le relative impostazioni sono state definite. Per modificare le impostazioni del client di un Tipo client, fare doppio clic sulla voce desiderata oppure fare clic con il pulsante destro del mouse e scegliere **Personalizza impostazioni client**. È inoltre possibile fare clic con il pulsante destro del mouse su una voce per rimuovere le impostazioni personalizzate oppure per aggiungere o rimuovere il Tipo client dalla lista consentiti o esentati di ActiveSync 437.

Impostazioni client tipo client



Per impostazione predefinita, ogni impostazione del client del Tipo client eredita lo stato dalle impostazioni del client dell'account 780. Le impostazioni di Tipo client modificate sostituiscono le impostazioni dell'account di tutti gli account che utilizzano un client dello stesso tipo. Se non si desidera che le impostazioni del client del Tipo client vengano applicate a un client specifico, è possibile sostituire le impostazioni del Tipo client modificando le Impostazioni client 470 di tale client.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci

disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo

principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un

altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

Anteprima impostazioni applicate

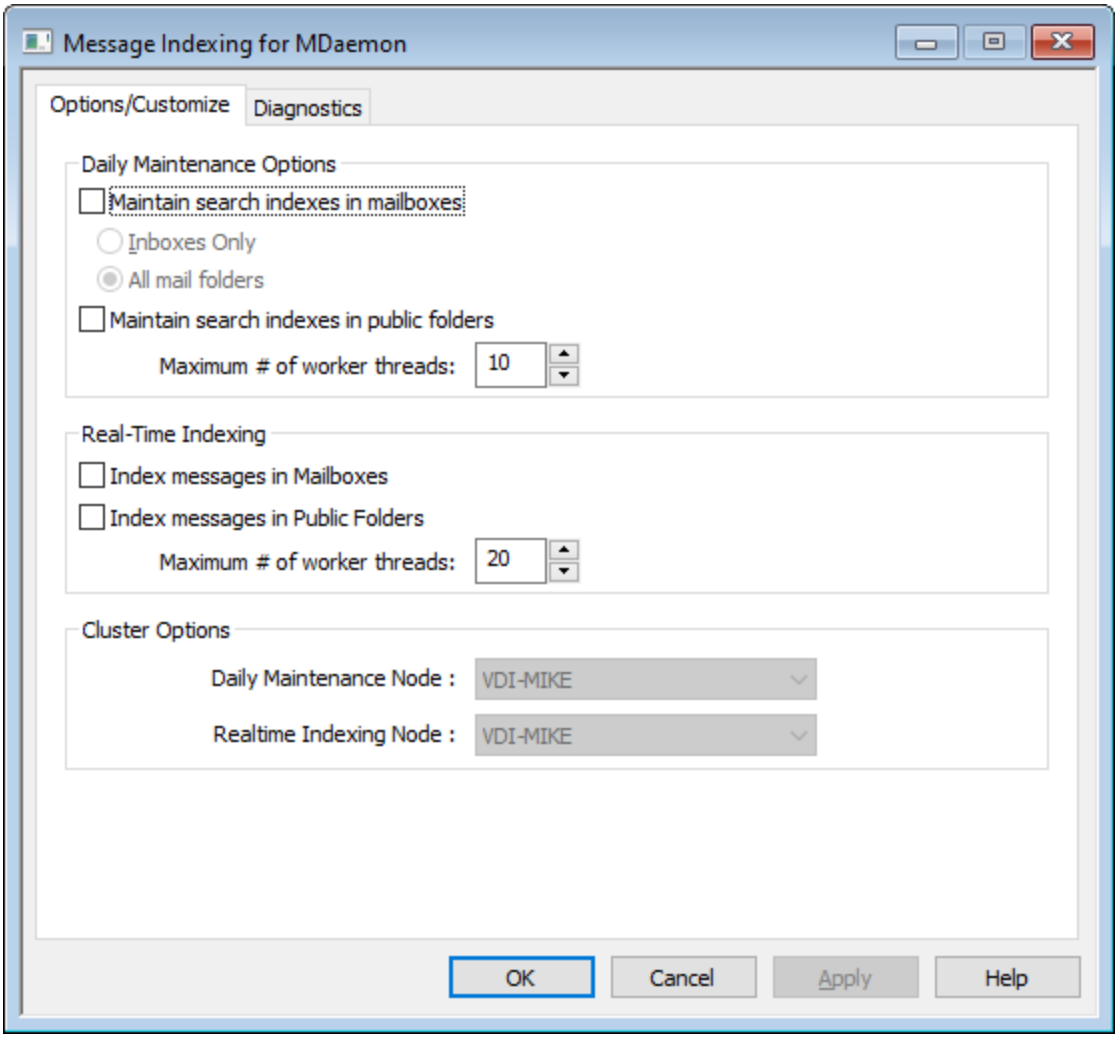
Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Vedere:

ActiveSync » Account 461
ActiveSync » Client 470
ActiveSync » Sicurezza 437

3.11 Indicizzazione dei messaggi

3.11.1 Opzioni/Personalizza



La finestra di dialogo Indicizzazione dei messaggi consente di configurare la manutenzione in tempo reale e notturna degli indici di ricerca utilizzati da Webmail, ActiveSync e Remote Administration.

Opzioni della manutenzione giornaliera

Le opzioni in questa sezione consentono di impostare l'indicizzazione notturna per la ricerca.

Gestisci indici di ricerca nelle cassette postali
Selezionare questa casella di controllo se si desidera gestire gli indici di ricerca nelle cartelle della propria cassetta postale. È possibile eseguire questa operazione solo per le cartelle Posta in arrivo o per tutte le cartelle di posta.

Gestisci indici di ricerca nelle cartelle pubbliche
Selezionare questa casella di controllo se si desidera gestire gli indici di ricerca nelle cartelle pubbliche 317. È inoltre possibile specificare un numero massimo di thread contemporanei consentiti per questa attività.

Indicizzazione in tempo reale

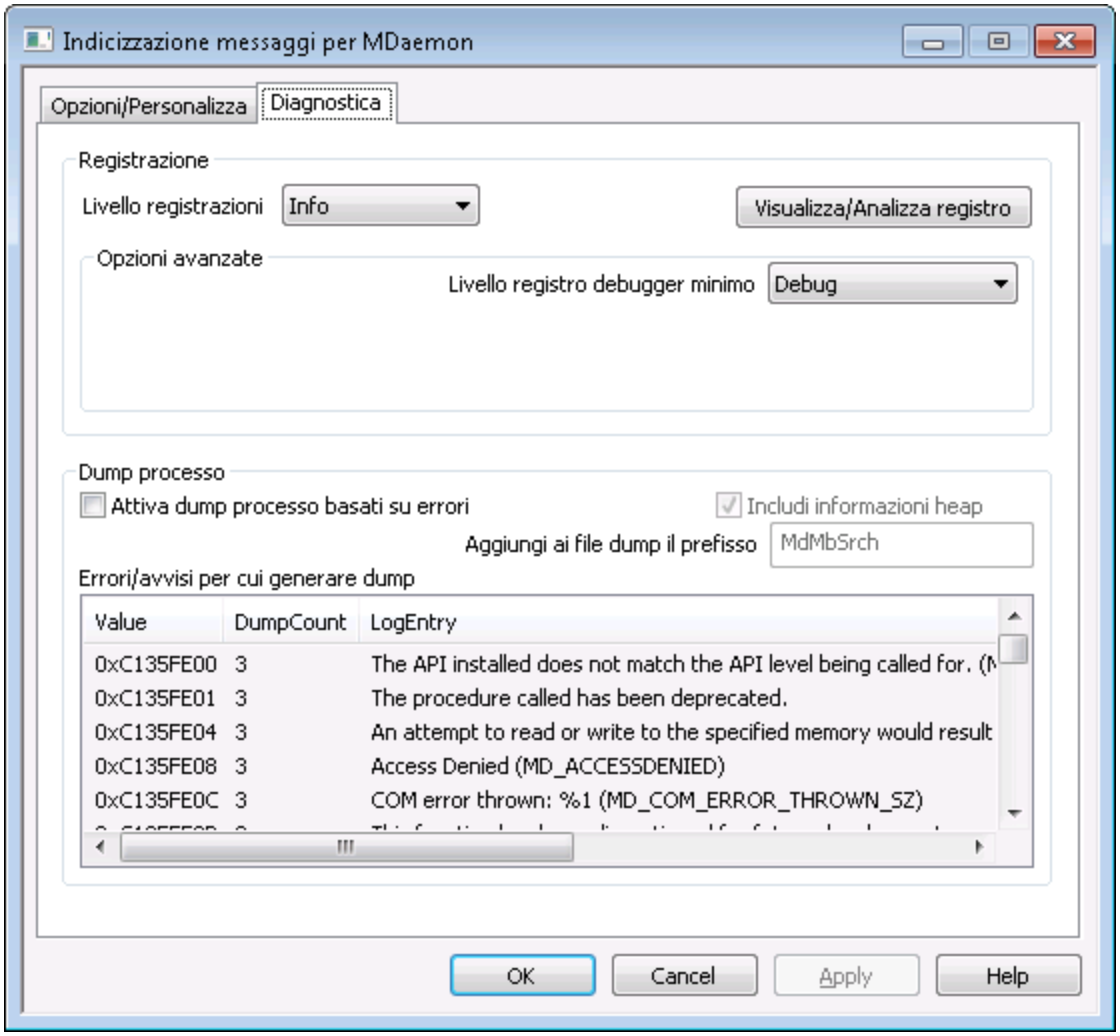
Indicizza messaggi nelle cassette postali
Attivare questa opzione se si desidera eseguire l'indicizzazione della ricerca in tempo reale nelle cassette postali, in modo che gli indici di ricerca siano sempre aggiornati.

Indicizza messaggi nelle cartelle pubbliche
Selezionare questa casella di controllo se si desidera eseguire l'indicizzazione di ricerca in tempo reale per le cartelle pubbliche 317.

Opzioni cluster

Se si utilizza il clustering, con le opzioni riportate in questa sezione è possibile designare i nodi del cluster che saranno dedicati alla manutenzione dell'indicizzazione giornaliera e in tempo reale.

3.11.2 Diagnostica



In questa schermata sono disponibili le opzioni avanzate che nella maggior parte dei casi non sarà necessario utilizzare, se non per tentare di diagnosticare un problema di Indicizzazione dei messaggi o per una richiesta dell'assistenza tecnica.

Registrazione

Livello di registrazione
Sono supportati sei livelli di registrazione, dal più alto al più basso volume di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili ed è in genere usato per la diagnosi di un problema o quando l'amministratore necessita di informazioni dettagliate.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso	Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.
Errore	Vengono registrati errori, errori critici ed eventi di avvio e di arresto.
Critico	Vengono registrati errori critici ed eventi di avvio e di arresto.
Nessuno	Vengono registrati solo gli eventi di avvio e di arresto.

Visualizza/Analizza registro
Fare clic su questo pulsante per aprire il Visualizzatore del registro di sistema avanzato di MDaemon. Per impostazione predefinita i registri vengono archiviati in: "..\MDaemon\Logs\"

Opzioni avanzate

Livello minimo registro debugger
Livello minimo di registrazione da inviare al debugger. I livelli di registrazione disponibili sono identici a quelli descritti in precedenza.

Dump del processo

Attiva dump del processo in base agli errori
Attivare questa opzione per generare dump del processo ogni volta che si verifica un errore o un avviso specifico e indicata di seguito.

Includi informazioni heap nei dump
Per impostazione predefinita le informazioni heap sono incluse nei dump di processo. Se non si desidera includerli, deselezionare questa casella di controllo.

Prefisso file dump
I nomi dei file di dump del processo inizieranno con il prefisso indicato.

Errori/avvisi con generazione di dump
Fare clic con il pulsante destro del mouse in quest'area e utilizzare le opzioni *Aggiungi/Modifica/Elimina voce...* per gestire l'elenco degli errori o avvisi che avviano i dump del processo. Per ciascuna voce è possibile specificare il numero di dump di processo consentiti prima di essere disattivato.

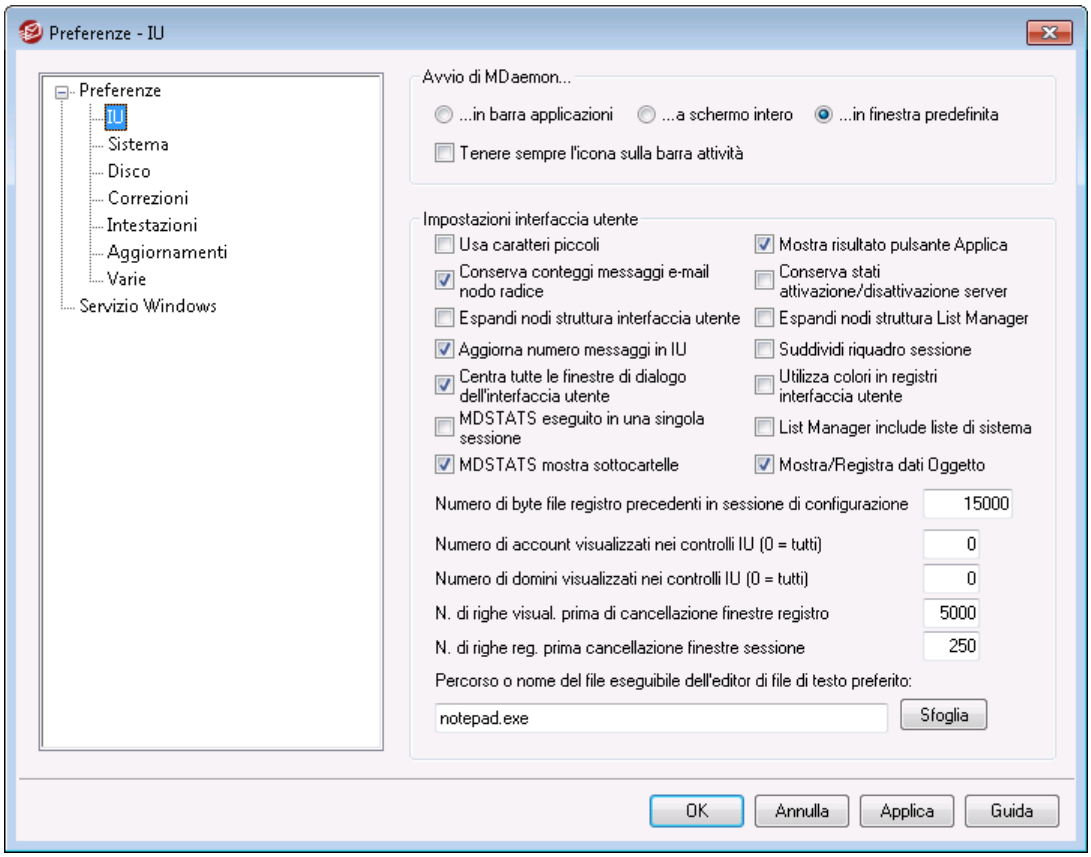
Vedere:

Vaglio dinamico » Opzioni/Personalizza 623

3.12 Preferenze

3.12.1 Preferenze

3.12.1.1 IU



Avvio di MDaemon

...in barra applicazioni
Questa opzione consente di non visualizzare l'interfaccia di MDaemon all'avvio. L'icona di MDaemon, tuttavia, verrà comunque visualizzata nella barra delle applicazioni.

...a schermo intero
Questa opzione consente di ingrandire l'interfaccia di MDaemon all'avvio.

...in finestra predefinita
Questa opzione consente di visualizzare l'interfaccia di MDaemon in una finestra predefinita all'avvio.

Mantieni sempre icona sulla barra delle applicazioni
Se questa opzione è selezionata, MDaemon verrà avviato ridotto a icona e verrà visualizzato sia nella barra delle applicazioni sia nell'area di notifica. Deselezionare questa casella di controllo se non si desidera che, una volta ridotto a icona,

MDaemon venga visualizzato nella barra delle applicazioni di Windows ma solo nell'area di notifica.

Impostazioni IU

Usa caratteri piccoli
Scegliere questa opzione se si desidera che le informazioni esposte nelle finestre Monitoraggio eventi e Sessioni vengano visualizzate in caratteri piccoli.

Mostra risultato pulsante Applica
Per impostazione predefinita, quando si fa clic sul pulsante Applica di una finestra di dialogo, viene aperta una finestra di messaggio che conferma il salvataggio delle modifiche apportate alle impostazioni. Per applicare le modifiche senza visualizzare il messaggio, deselezionare questa casella.

Mantieni contatori posta nodo principale
Abilitare questa opzione se si desidera salvare i valori dei contatori del nodo principale tra i riavvii del server. I contatori del nodo principale sono elencati nella sezione "Statistiche" del riquadro Statistiche di MDaemon.

Conserva gli stati attivo/inattivo del server
Selezionare questa casella di controllo per garantire che lo stato (abilitato/disabilitato) dei server di MDaemon non subisca variazioni dopo il riavvio.

Espandi i nodi della IU
Fare clic su questa casella se si desidera che i nodi presenti nel riquadro a sinistra delle diverse finestre di dialogo vengano espansi automaticamente. L'opzione non si applica al Mailing List Manager 275. Per espandere automaticamente i nodi della lista di distribuzione, utilizzare l'opzione *Espandi nodi Mailing List Manager* riportata di seguito.

Espandi nodi Mailing List Manager
Fare clic su questa casella di controllo se si desidera che i nodi di Mailing List Manager 275 presenti nel riquadro a sinistra vengano espansi automaticamente.

Aggiorna numero messaggi in IU
Questa opzione consente di controllare il disco per contare i messaggi in attesa nelle code di posta.

Separa riquadro sessione
Attivare questa opzione se si desidera che la scheda Sessioni dell'interfaccia utente principale di MDaemon venga separata dalle altre schede in un riquadro a parte. Per applicare questa impostazione, è necessario riavviare l'interfaccia utente di MDaemon. L'opzione di menu di Windows per passare da un riquadro all'altro non sarà più disponibile.

Centra tutte le finestre di dialogo della IU
Per impostazione predefinita tutte le finestre di dialogo sono centrate sulla schermata quando vengono aperte, invece di sovrapporsi l'un l'altra. Deselezionare questa casella di controllo se si desidera che le finestre di dialogo si sovrappongano,

ma questo può far sì che occasionalmente siano parzialmente fuori dalla schermata o dall'inquadratura.

Usa colori nei registri della IU
Questa opzione consente di applicare colori al testo visualizzato nelle diverse schede Monitoraggio e registrazione eventi[75] nell'interfaccia utente di MDaemon. L'opzione è attivata per impostazione predefinita e per modificarla è necessario un riavvio di MDaemon prima che la modifica diventi effettiva. Vedere: Registri di sessioni contraddistinti da colori[183] per ulteriori informazioni.

Mailing List Manager include liste di sistema
Attivare questa opzione se si desidera visualizzare le liste di distribuzione generate dal sistema di MDaemon (ad esempio, Everyone@ e MasterEveryone@) nel Mailing List Manager[275]. Nelle liste generate dal sistema esistono elementi limitati configurabili dall'utente. Quando l'opzione è disattivata, le liste di sistema sono nascoste ma comunque disponibili. L'opzione è disabilitata per impostazione predefinita.

MDSTATS eseguito in istanza singola
Selezionare questa casella di controllo per eseguire una singola copia di Gestione code e statistiche[899] alla volta. Se si tenta di avviare il programma di gestione quando ne è già in esecuzione un'istanza, viene attivata la finestra relativa a quest'ultima.

MDSTATS mostra le sottocartelle
Selezionare questa casella di controllo per visualizzare le sottocartelle contenute nelle varie code e cartelle della posta degli utenti di Gestione code e statistiche[899].

Mostra/Registra dati relativi all'oggetto
Per impostazione predefinito i dati della riga dell'oggetto sono visualizzati nelle schede dell'interfaccia utente di MDaemon e scritti nei file di registro. Si noti, tuttavia, che la riga dell'oggetto può contenere informazioni che il mittente di un messaggio non desidera siano visualizzate e tracciate nei file di registro e le liste di distribuzione possono avere una password che gli utenti inseriscono nella riga Oggetto. Per questo motivo è consigliabile disattivare questa opzione.

La sessione di configurazione indica il numero di byte dei vecchi registri
Quando si esegue una sessione di configurazione, questa è la quantità massima di dati di registrazione visualizzata in una scheda Monitoraggio e registrazione eventi[75]. L'impostazione predefinita è 15000 byte.

Numero di account visualizzati nei controlli IU (0 = tutti)
Rappresenta il numero massimo di account visualizzati negli elenchi a discesa delle varie finestre di dialogo. Se, inoltre, il valore di questa opzione è inferiore al numero degli account esistenti, non è più possibile visualizzare le opzioni "Modifica account" ed "Elimina account" del menu Account. Per modificare o eliminare gli account sarà necessario utilizzare Account Manager[726]. Per rendere effettive le modifiche apportate a questa opzione, riavviare MDaemon. Il valore predefinito è "0" e fa in modo che vengano visualizzati tutti gli account.

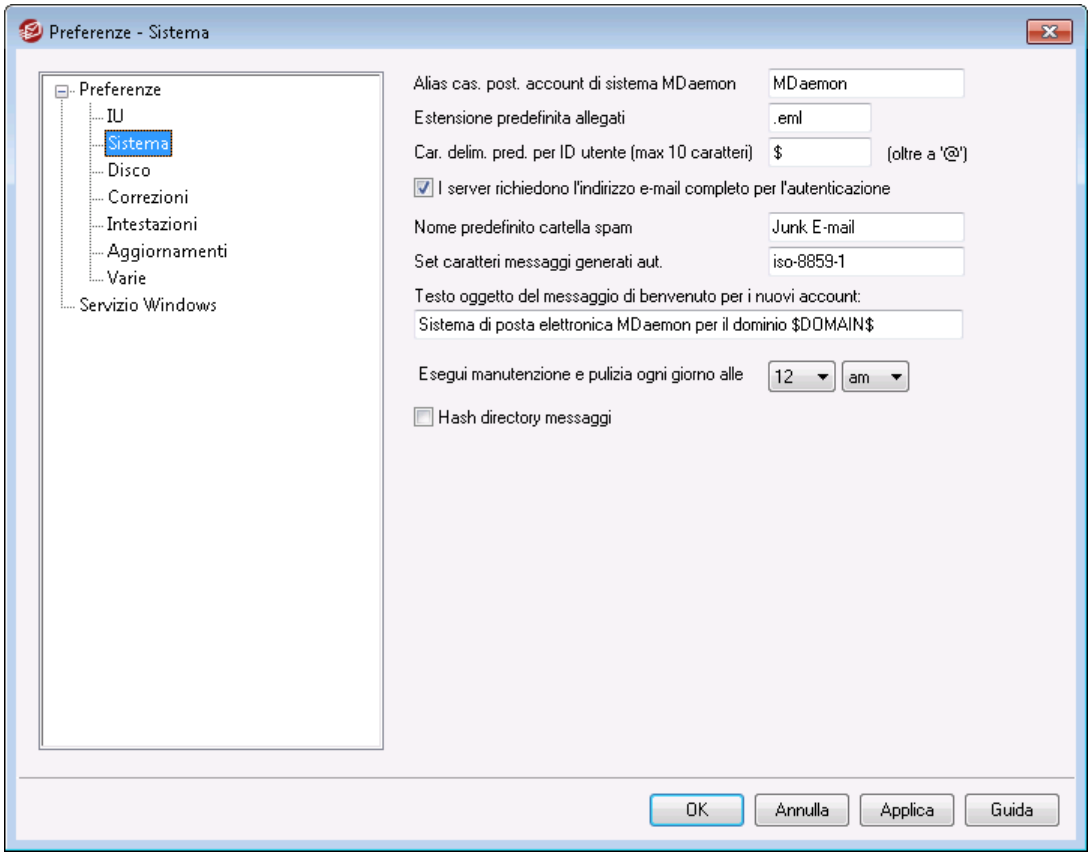
Numero di domini visualizzati nei controlli IU (0 = tutti)
Indica il numero massimo di domini visualizzati nella interfaccia grafica utente principale, indipendentemente dalla quantità dei domini esistenti. Per rendere effettive le modifiche apportate a questo valore, riavviare MDaemon. Il valore predefinito è "0" e fa in modo che vengano visualizzati tutti i domini.

N. di righe visual. prima di cancellazione finestre registro
Indica il numero massimo di righe visualizzate nelle finestre di registro della visualizzazione principale. Il contenuto della finestra viene cancellato ogni volta che viene raggiunto questo numero di righe, senza influire sul file di registro, in quanto viene cancellata solo la visualizzazione.

N. di righe reg. prima cancellazione finestre sessione
Indica il numero massimo di righe visualizzate nella finestra Sessione 89 prima della cancellazione. La cancellazione non influisce sul file di registro.

Percorso o nome del file eseguibile dell'editor di file di testo preferito
Notepad.exe è l'editor di testo generico che, quando necessario, viene avviato dall'interfaccia utente di MDaemon per impostazione predefinita. Se si preferisce utilizzare un altro editor di testo, immettere qui il percorso o il nome del file eseguile corrispondente.

3.12.1.2 Sistema



Alias cas. post. account di sistema MDaemon [indirizzo]
In questo campo è riportato l'indirizzo e-mail da cui provengono i messaggi generati dal sistema. I messaggi di sistema includono le conferme di iscrizione, i messaggi DSN (Delivery Status Notification, notifica dello stato della consegna), altri tipi di messaggi di notifica e così via.

Estensione predefinita allegati
In questo campo è indicata l'estensione dei messaggi generati dal sistema. Tale estensione viene utilizzata anche per gli allegati inclusi nei messaggi generati dal sistema. Ad esempio, se MDaemon genera un avviso per il postmaster relativo a un messaggio specifico, all'avviso verrà allegato il messaggio con l'estensione specificata in questo campo.

Car. delim. pred. per ID utente (max 10 caratteri)
Se l'ID utente dell'account corrisponde all'indirizzo e-mail, è possibile utilizzare questo carattere o stringa di caratteri in alternativa al simbolo "@". L'opzione può rivelarsi necessaria se i client e-mail degli utenti non supportano il carattere "@" nel campo ID utente. Ad esempio, se il carattere immesso in questo campo è "$", gli utenti possono connettersi sia con "utente1@esempio.com" sia con "utente1$esempio.com".

È necessario indicare l'indirizzo e-mail completo per l'autenticazione del server
Per accedere a MDaemon, i server POP e IMAP richiedono, per impostazione predefinita, l'indirizzo di posta elettronica completo. Per consentire l'accesso con la sola casella postale, ad esempio "utente1" invece di "utente1@esempio.com", disabilitare questa opzione, sebbene questo non sia consigliabile poiché l'accesso con la sola casella postale è ambiguo se MDaemon serve più domini.

Nome predefinito cartella spam
Inserire in questa casella di testo il nome predefinito della cartella spam che MDaemon creerà automaticamente per gli utenti. Il nome predefinito è "Junk E-mail" che corrisponde al valore predefinito di numerosi altri prodotti molto diffusi.

Set caratteri messaggi generati aut.
Specificare in questo campo il set caratteri da utilizzare per i messaggi generati automaticamente. L'impostazione predefinita è iso-8859-1.

Testo oggetto del messaggio di benvenuto per i nuovi account
MDaemon invia automaticamente un messaggio di benvenuto ai nuovi account. Il testo verrà visualizzato come intestazione "Subject" del messaggio. Il messaggio di benvenuto viene creato in base al file `NEWUSERHELP.DAT` presente nella directory `...\MDaemon\app\`. In questa intestazione possono essere incluse tutte le macro consentite negli script di risposta automatica 857.

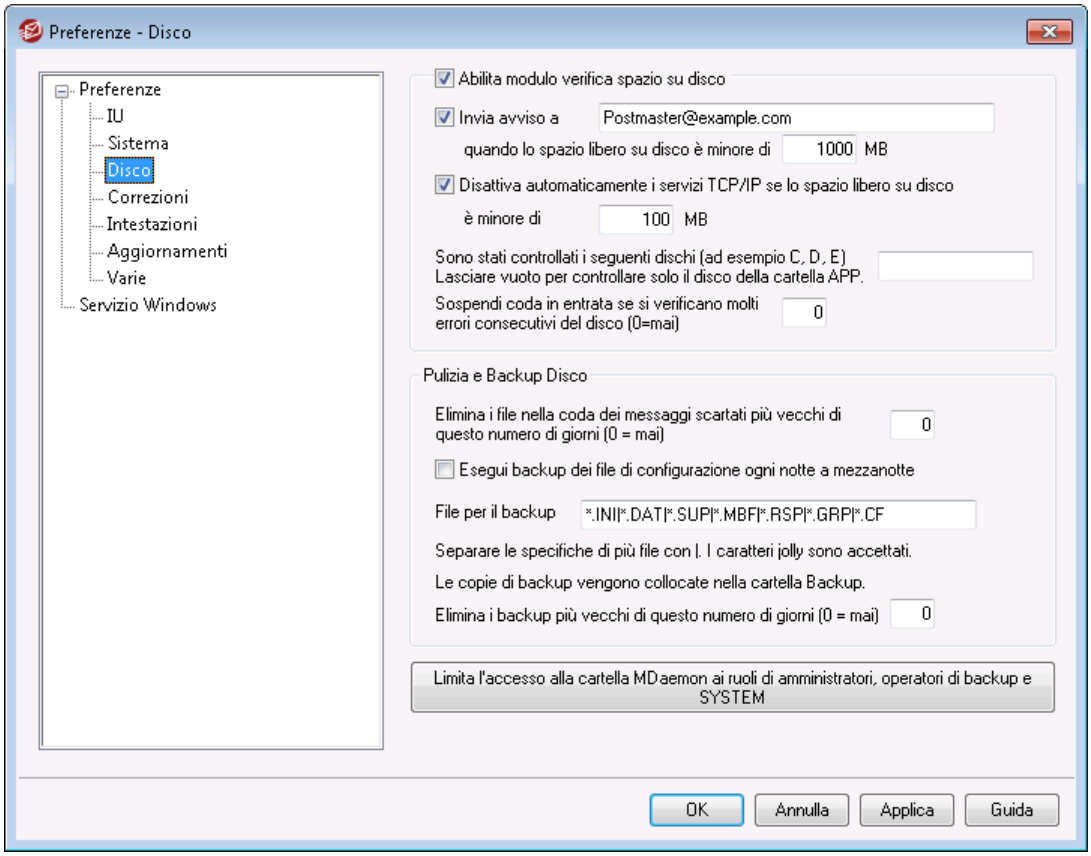
Esegui manutenzione e pulizia ogni giorno alle [1-12] [am/pm]
Utilizzare questa opzione per impostare l'ora in cui deve essere eseguito l'evento giornaliero di manutenzione e pulizia. L'impostazione predefinita e consigliata è 12 am.

Indipendentemente dall'ora impostata per questa opzione, esistono eventi giornalieri che si verificano sempre a mezzanotte, come l'esecuzione e la manutenzione del file di registro `midnight.bat`.

Sposta le cartelle di posta dell'account dopo la modifica dei valori di dominio o casella postale
Se questa opzione è selezionata, quando si modifica un nome dominio o una casella postale, le cartelle di posta degli account interessati vengono spostate nella nuova posizione. In caso contrario, MDaemon continua a utilizzare i nomi delle cartelle di posta precedenti.

Hash directory messaggi
Selezionare questa casella di controllo per abilitare l'hashing della directory. MDaemon eseguirà l'hashing di alcune directory creando fino a 65 sottocartelle. La procedura di hashing consente di migliorare le prestazioni di siti particolarmente voluminosi, ma può ridurre quelle dei siti MDaemon tradizionali. L'opzione è disabilitata per impostazione predefinita.

3.12.1.3 Disco



Abilita modulo verifica spazio su disco
Selezionare questa casella di controllo per attivare il monitoraggio dello spazio disponibile su disco per l'unità su cui è in esecuzione `MDaemon.exe`.

Invia avviso a [utente o indirizzo] se lo spazio libero è minore di [xx] MB
Selezionare questa opzione per inviare a un utente o indirizzo un messaggio di notifica in cui si segnala che lo spazio su disco disponibile è inferiore a una determinata soglia. Il valore predefinito è 1000 MB.

Disattiva automaticamente i servizi TCP/IP se lo spazio libero su disco è minore di [xx] MB
Selezionare questa casella per disabilitare i servizi TCP/IP quando lo spazio disponibile su disco è inferiore a una determinata soglia. Il valore predefinito è 100 MB.

Sono stati controllati i seguenti dischi (ad esempio C, D, E)
Questa opzione consente di monitorare lo spazio disponibile in più dischi, specificando la lettera di ciascuna unità. Se lasciata vuota, viene controllato solo il disco contenente la cartella `\app\` di MDaemon.

Sospendi coda in entrata se si verificano molti errori consecutivi del disco (0=mai)
Se durante l'elaborazione della coda in entrata si verifica il numero di errori del disco indicato, MDaemon interrompe l'elaborazione della coda fino a quando la condizione non viene risolta. L'interruzione viene notificata con un messaggio e-mail alla casella postale del postmaster.

Pulizia e backup disco

Elimina i file nella coda dei messaggi scartati più vecchi di questo numero di giorni (0 = mai)
Utilizzare questa opzione per fare in modo che MDaemon elimini i file vecchi dalla coda dei messaggi scartati ogni volta che viene superato il numero di giorni specificato. Per non eliminare i messaggi in modo automatico, impostare il valore "0" per l'opzione.

Esegui backup dei file di configurazione ogni notte a mezzanotte
Selezionare questa casella di controllo per archiviare tutti i file di configurazione di MDaemon ogni notte a mezzanotte nella directory Backups.

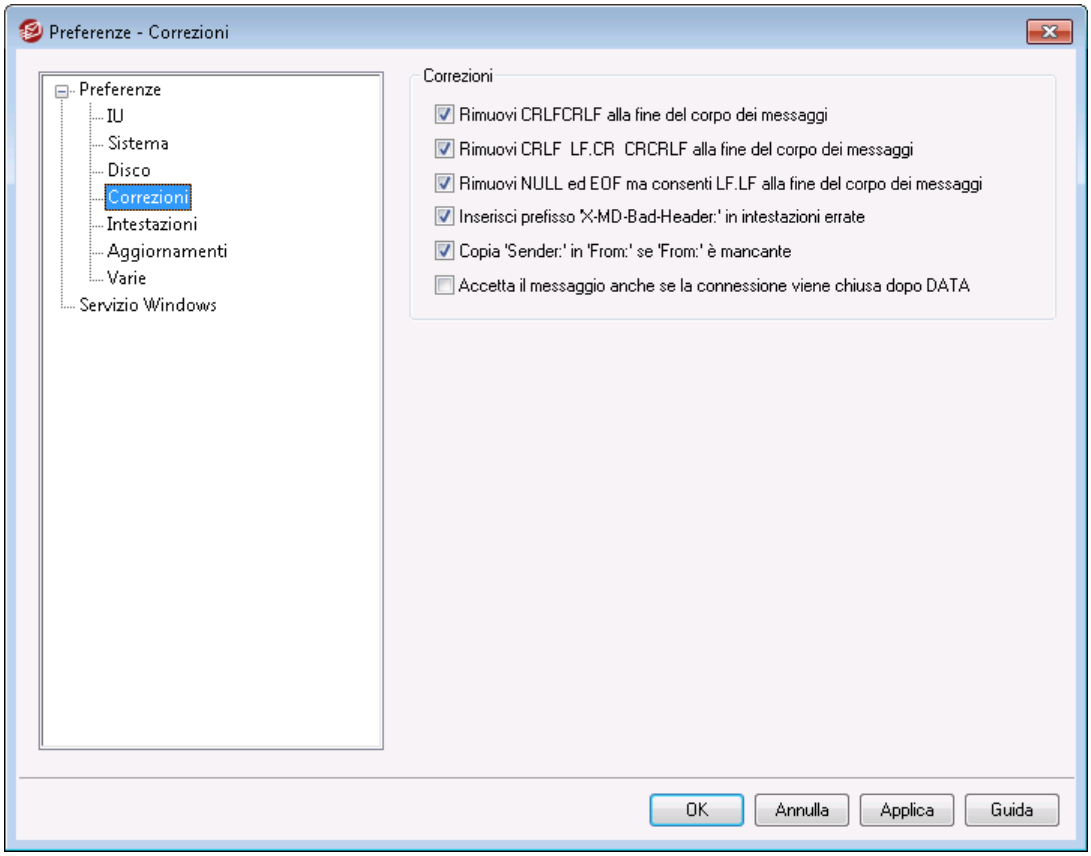
File per il backup
Specificare nella casella di testo i file e le estensioni dei file di cui si desidera effettuare il backup. I caratteri jolly sono consentiti. È necessario separare ogni nome di file o estensione con il carattere "|".

Elimina i backup più vecchi di questo numero di giorni (0 = mai)
Con questa opzione è possibile eliminare automaticamente i file di backup precedenti. I file più vecchi del numero di giorni specificato saranno eliminati durante la pulizia giornaliera di mezzanotte. L'impostazione predefinita è "0", che significa che i file di backup precedenti non saranno eliminati.

Limitare l'accesso alla cartella MDaemon ad amministratori, operatori di backup e SYSTEM

Questo pulsante consente di limitare l'accesso alla cartella principale di `\MDaemon\` e alle relative sottocartelle ai seguenti account/gruppi di Windows: Administrators, Backup Operators e SYSTEM.

3.12.1.4 Correzioni



Rimuovi CRLFCRLF alla fine del corpo dei messaggi
Determinati client di posta possono presentare problemi nella visualizzazione dei messaggi che si concludono con più caratteri CRLF consecutivi. Quando si abilita questa casella, MDaemon elimina le sequenze `CRLFCRLF` consecutive al termine del corpo del messaggio. L'opzione è abilitata per impostazione predefinita.

Rimuovi CRLF LF.CR CRCRLF alla fine del corpo dei messaggi
Per impostazione predefinita, MDaemon rimuove questa sequenza alla fine dei messaggi, in quanto potrebbe determinare problemi con alcuni client di posta. Per non eliminare questa sequenza dai messaggi, disabilitare questa casella.

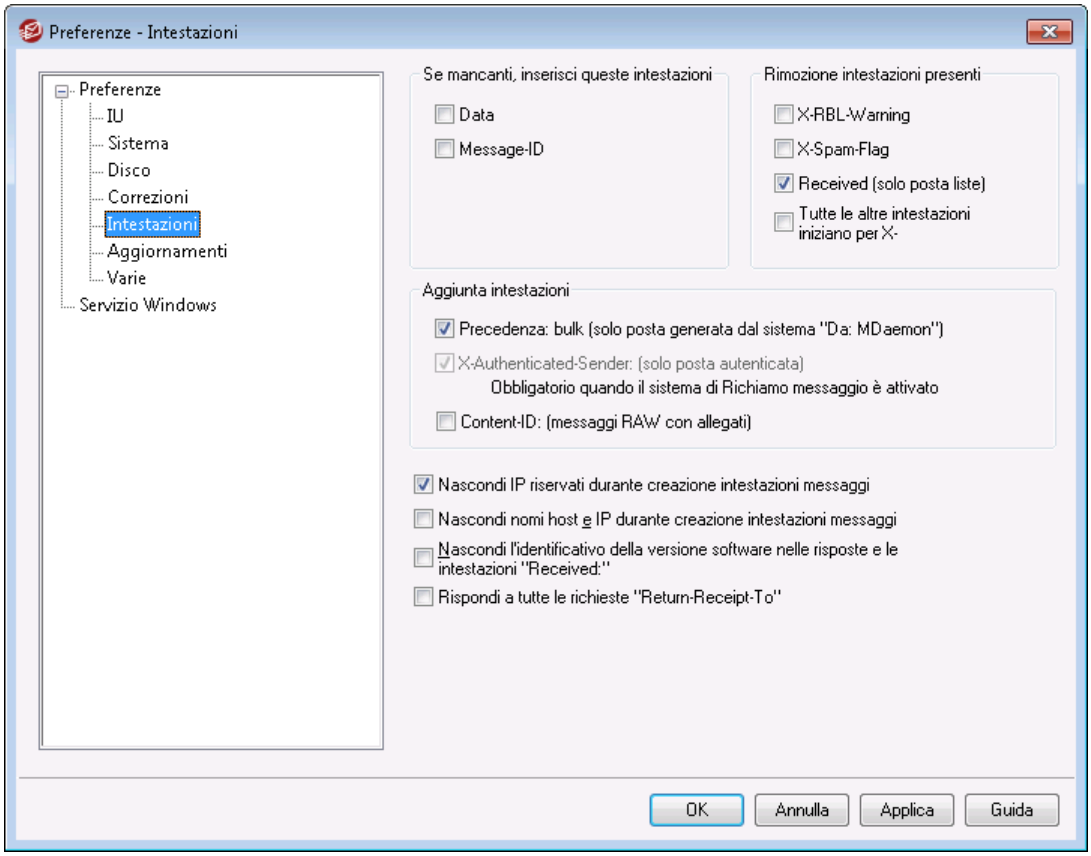
Rimuovi NULL ed EOF ma consenti LF.LF alla fine del corpo dei messaggi
Quando si abilita questa casella di controllo, MDaemon rimuove i caratteri `Null` ed EOF dalla fine del corpo dei messaggi, ma accetta i messaggi che terminano con `LF.LF`, nonché quelli che terminano con una normale sequenza `CRLF.CRLF` che indica la fine del messaggio. L'opzione è abilitata per impostazione predefinita.

Inserisci prefisso "X-MD-Bad-Header:" in intestazioni errate
Quando si abilita questa opzione e MDaemon incontra un'intestazione errata, le antepone il prefisso "`X-MD-Bad-Header:`" L'opzione è abilitata per impostazione predefinita.

Copia 'Sender:' in 'From:' se 'From:' è mancante
Con alcuni client di posta non è possibile creare l'intestazione `FROM:` durante la composizione del messaggio. Le informazioni dell'intestazione `FROM:` vengono collocate, invece, nell'intestazione `Sender:` . Questo problema costituisce una fonte di confusione per alcuni server di posta e per il destinatario del messaggio. Per prevenire questi problemi, se si abilita questa casella, MDaemon crea l'intestazione `FROM:` mancante a partire dal contenuto dell'intestazione `Sender:`. L'opzione è abilitata per impostazione predefinita.

Accetta il messaggio anche se la connessione viene chiusa dopo DATA
Se si abilita questa opzione, MDaemon accetta e consegna i messaggi anche se la connessione si interrompe durante o subito dopo il comando `DATA` nel corso dell'elaborazione SMTP. Questa opzione non dovrebbe essere utilizzata normalmente, poiché può condurre alla duplicazione di messaggi.

3.12.1.5 Intestazioni



Se mancanti, inserisci queste intestazioni

Date
Se si abilita questa opzione, in presenza di un messaggio privo dell'intestazione "`Date:`", MDaemon ne crea una e la aggiunge al file del messaggio. Il valore

dell'intestazione corrisponde alla data di ricezione del messaggio, non a quella di creazione. Questa funzione consente di consegnare i messaggi inviati da client di posta che non creano le intestazioni relative alla data e che di norma non vengono accettati da alcuni server di posta.

Message-ID
In presenza di un messaggio privo dell'intestazione "`Message-ID`", MDaemon ne crea una e la inserisce nel messaggio.

Rimozione intestazioni presenti

Received (solo posta liste)
Abilitare questa casella di controllo per eliminare tutte le intestazioni "`Received:`" esistenti dai messaggi della lista di distribuzione.

X-RBL-Warning
Abilitare questa casella di controllo per rimuovere tutte le intestazioni "`X-RBL-Warning:`" dai messaggi. L'opzione è disabilitata per impostazione predefinita.

X-Spam-Flag
Abilitare questa opzione se si desidera eliminare le intestazioni "`X-Spam-Flag:`" obsolete dai messaggi.

Tutte le altre intestazioni iniziano per X-
Per inoltrare la posta ed eseguire alcune altre funzioni, MDaemon e altri server di posta utilizzano numerose intestazioni specifiche dette di `tipo X`. Se questa opzione è attivata, MDaemon elimina le intestazioni dai messaggi. **Nota:** con questa opzione non vengono rimosse le intestazioni `X-RBL-Warning`. Per rimuovere le intestazioni, utilizzare l'opzione "*X-RBL-Warning*".

Aggiunta intestazioni

Precedence: bulk (solo alla posta generata dal sistema 'From: MDaemon')
Se si abilita questa casella, viene inserita un'intestazione "Precedence: bulk" in tutti i messaggi generati dal sistema MDaemon, ad esempio messaggi di benvenuto, avvisi, messaggi che segnalano difficoltà di consegna e così via.

X-Authenticated-Sender: (solo posta autenticata)
Per impostazione predefinita, MDaemon aggiunge l'intestazione "X-Authenticated-Sender:" ai messaggi pervenuti mediante una sessione autenticata con il comando `AUTH`. Per evitare che venga aggiunta questa intestazione, disabilitare questa casella.

Content-ID: (messaggi RAW con allegati)
Selezionare questa casella di controllo per aggiungere intestazioni `Content-ID` MIME univoche ai messaggi creati da un file RAW contenente allegati.

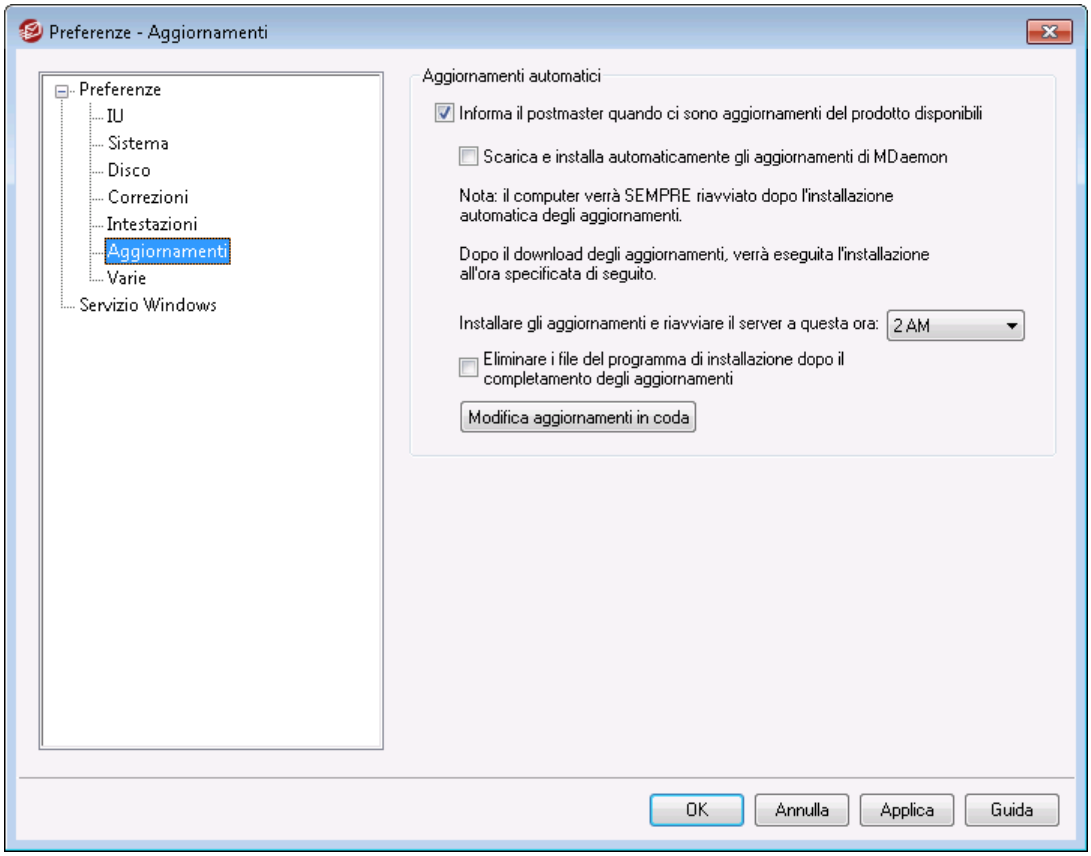
Nascondi IP riservati durante creazione intestazioni messaggi
L'opzione è abilitata per impostazione predefinita e impedisce la visualizzazione degli indirizzi IP riservati in alcune intestazioni di messaggi creati da MDaemon. Alcuni indirizzi IP riservati sono: `127.0.0.*`, `192.168.*.*`, `10.*.*.*` e `172.16.0.0/12`. Se inoltre si desidera nascondere gli IP dei propri domini (compresi i domini della LAN) dall'elenco delle intestazioni, impostare manualmente il seguente switch nel file `app\MDaemon.ini` di MDaemon: `[Special] HideMyIPs=Yes` (l'impostazione predefinita è `No`).

Nascondi nomi host e IP durante creazione intestazioni messaggi
Fare clic su questa opzione per omettere i nomi host e gli indirizzi IP dalle intestazioni "Received:" quando questa vengono costruite. L'opzione è disabilitata per impostazione predefinita.

Nascondi l'identificativo della versione software nelle risposte e le intestazioni "Received:"
Utilizzare questa opzione per evitare che MDaemon dichiari la propria versione software e altre informazioni di identificazione quando si creano intestazioni `Received` o si risponde a varie richieste del protocollo. L'opzione è disabilitata per impostazione predefinita.

Rispondi a tutte le richieste 'Return-Receipt-To:'
Selezionare questa casella di controllo per soddisfare le richieste di conferma dell'avvenuta consegna dai messaggi in entrata e inviare automaticamente un messaggio di conferma al mittente. L'opzione è disabilitata per impostazione predefinita.

3.12.1.6 Aggiornamenti



Aggiornamenti automatici

Grazie alle funzionalità di aggiornamento automatico, è possibile configurare MDaemon in modo da informare il postmaster ogni volta che si rende disponibile un aggiornamento per MDaemon e da scaricare e installare gli aggiornamenti automaticamente. Ogni volta che viene installato automaticamente un aggiornamento, il server viene riavviato. I file vengono scaricati non appena viene rilevato l'aggiornamento, ma installazione e riavvio si possono eseguire nel momento che l'utente ritiene più opportuno. L'intera attività di installazione viene registrata nel registro di sistema di MDaemon, mentre il postmaster riceve una notifica dopo ogni aggiornamento.

Informa il postmaster quando ci sono aggiornamenti del prodotto disponibili
Con questa opzione MDaemon invia una notifica al postmaster per ogni nuovo aggiornamento MDaemon disponibile. Per impostazione predefinita, questa opzione è abilitata.

Quandosi imposta l'aggiornamento automatico per MDaemon, il messaggio non viene inviato. Il postmaster viene invece informato dell'avvenuta installazione dell'aggiornamento e delle eventuali Considerazioni speciali relative all'aggiornamento.

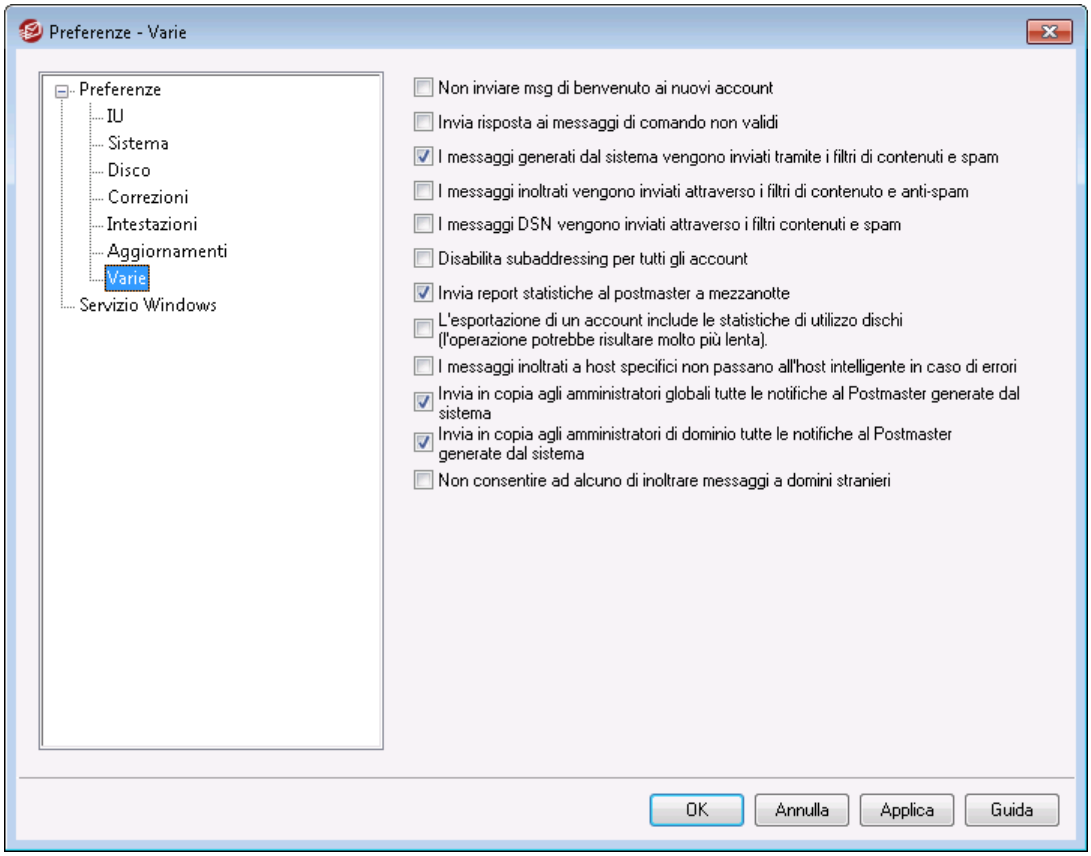
Scarica e installa automaticamente gli aggiornamenti di MDaemon
Selezionare questa casella per scaricare e installare automaticamente gli aggiornamenti di MDaemon. Gli aggiornamenti vengono scaricati non appena rilevati e installati nell'orario specificato in basso. L'opzione è disabilitata per impostazione predefinita.

Installare gli aggiornamenti e riavviare il server a questa ora:
Gli aggiornamenti automatici vengono scaricati non appena vengono rilevati e archiviati quindi nella cartella `\MDaemon\Updates`. L'installazione, tuttavia, viene eseguita solo all'ora specificata in questo campo. Il server su cui è installato MDaemon verrà riavviato automaticamente dopo ogni aggiornamento. Per impostazione predefinita, questa opzione è impostata sulle 02.00.

Eliminare i file del programma di installazione dopo il completamento degli aggiornamenti
Selezionare questa casella per eliminare i file di installazione archiviati al termine dell'installazione.

Modifica aggiornamenti in coda
Dopo essere stato rilevato e scaricato, l'aggiornamento viene inserito nella coda di installazione per l'orario specificato. L'elenco degli aggiornamenti in attesa è memorizzato nel file `QueuedUpdates.dat`. Fare clic su questo pulsante per esaminare l'elenco o rimuovere un aggiornamento in attesa.

3.12.1.7 Varie



Non inviare msg di benvenuto ai nuovi account
Per impostazione predefinita, MDaemon genera un messaggio di benvenuto in base al file `NEWUSERHELP.DAT` e lo distribuisce ai nuovi utenti quando viene creato il relativo account. Selezionare questa casella di controllo per impedire la generazione di tale messaggio.

Invia risposta ai messaggi di comando non validi
Per impostazione predefinita quando qualcuno invia una e-mail all'account di sistema che non contiene un comando valido, MDaemon non risponde con una e-mail "Impossibile trovare un comando valido". Attivare questa opzione per inviare una risposta a questi messaggi e-mail.

I messaggi generati dal sistema vengono inviati attraverso i filtri di contenuto e anti-spam
Per impostazione predefinita, i messaggi generati dal sistema vengono elaborati mediante Filtro contenuti e Spam Filter. Per escluderli da Filtro contenuti e dal filtro anti-spam, disabilitare la casella di controllo.

I messaggi inoltrati vengono inviati attraverso i filtri di contenuto e anti-spam
Selezionare questa casella se si desidera elaborare i messaggi inoltrati attraverso il filtro contenuti e il filtro anti-spam. È disabilitata per impostazione predefinita.

I messaggi DSN vengono inviati attraverso i filtri di contenuto e anti-spam
Attivare questa opzione per inviare messaggi DSN[896] attraverso i filtri di contenuto e anti-spam. L'opzione è disabilitata per impostazione predefinita.

Disabilita subaddressing per tutti gli account
Selezionare questa opzione se si desidera disabilitare a livello globale la funzionalità subaddressing. Tale funzionalità verrà quindi disattivata per tutti gli account, indipendentemente dalle impostazioni dei singoli account. Per ulteriori informazioni sulla funzionalità subaddressing, vedere la schermata Filtri IMAP[751] di Account Editor.

Invia report statistiche al postmaster a mezzanotte
Per impostazione predefinita, il report statistiche viene inviato al postmaster ogni notte a mezzanotte. Deselezionare questa casella se non si desidera che il report venga inviato. Questa opzione corrisponde alla scheda Statistiche[75] situata nella visualizzazione principale di MDaemon.

L'esportazione account comprende le statistiche di utilizzo dischi (ciò potrebbe rallentare molto l'esportazione)
Per impostazione predefinita, l'esportazione account non comprende conteggi di file su disco e spazio utilizzato. Per inserire queste informazioni nell'esportazione, abilitare questa casella di controllo. L'operazione tuttavia potrebbe rallentare molto l'esportazione.

I messaggi inoltrati a host specifici non passano agli host intelligenti in caso di errori
Utilizzando le impostazioni di inoltro avanzate nella schermata Inoltro[742] di Account Editor, è possibile impostare gli account in modo da inoltrare i messaggi a uno specifico host intelligente anziché utilizzare il processo di consegna standard di MDaemon. Per impostazione predefinita, quando MDaemon rileva un errore di consegna durante il tentativo di inoltro di uno di questi messaggi, il messaggio verrà inserito nella coda dei messaggi scartati. Attivare questa opzione se si desidera che MDaemon inserisca il messaggio nella Coda tentativi[888] per eseguire ulteriori tentativi di consegna utilizzando il normale processo di consegna di MDaemon.

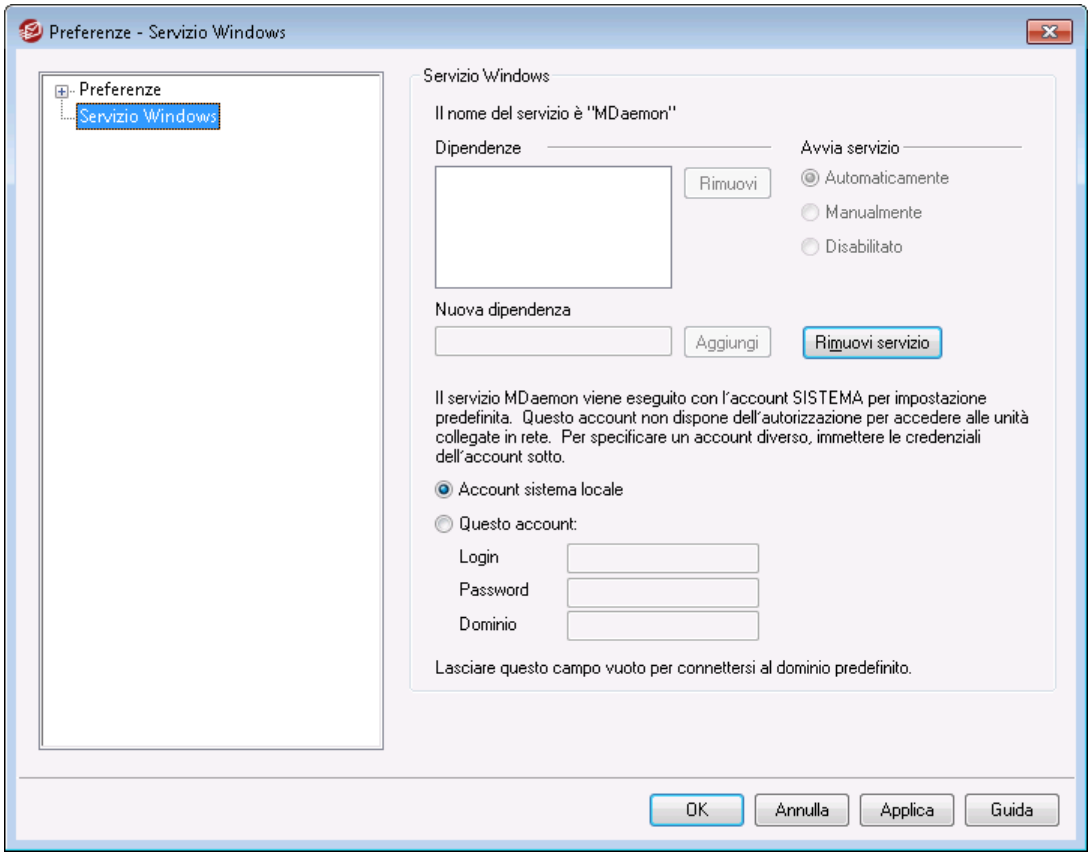
Invia in copia agli amministratori globali tutte le notifiche al Postmaster generate dal sistema
Per impostazione predefinita, le notifiche generate dal sistema inviate al Postmaster verranno inviate anche agli Amministratori globali[773]. Gli amministratori di livello Globale ricevono tutto, inclusi i rapporti di riepilogo code e quelli statistici, le Note di rilascio, le notifiche di "Utente inesistente" (per tutti i domini), di errori del disco, di blocco e disattivazione degli account per tutti i domini (che, come tutti gli amministratori del dominio, possono sbloccare e riattivare), avvertenze relative a licenze e versioni beta-test che stanno per scadere, rapporti di riepilogo su Spam e così via. Se non si desidera che gli amministratori globali ricevano queste notifiche, disattivare questa impostazione.

Invia in copia agli amministratori di dominio tutte le notifiche al Postmaster generate dal sistema
Per impostazione predefinita, le notifiche generate dal sistema inviate al Postmaster verranno inviate anche agli Amministratori di dominio[773]. Tuttavia, gli amministratori di livello Dominio possono ricevere solo le e-mail relative al proprio dominio. Se non si

desidera che gli amministratori di dominio ricevano queste notifiche, disattivare questa impostazione.

Non consentire ad alcuno di inoltrare messaggi a domini stranieri
Selezionare questa casella di controllo se non si desidera consentire che l'inoltro della posta dell'account invii messaggi e-mail all'esterno del dominio. Se un utente configura l'inoltro della posta per il proprio account in modo da inviare messaggi a un dominio esterno, gli indirizzi di inoltro remoti saranno ignorati. Questa impostazione si applica solo ai messaggi che sono inoltrati usando le opzioni di inoltro della posta dell'account. Questa impostazione si applica solo ai messaggi che sono inoltrati usando le opzioni di inoltro della posta[742] dell'account.

3.12.2 Servizio Windows



Servizio Windows
Se MDaemon viene eseguito come servizio, il nome del servizio è "MDaemon".

Dipendenze
Questa opzione consente di indicare i servizi che devono essere in esecuzione **prima** dell'avvio del servizio MDaemon.

Avvia servizio
Questo è lo stato iniziale del servizio: avvio automatico, avvio manuale o disabilitato.

Installa/Rimuovi servizio
Per installare o rimuovere il servizio MDaemon, fare clic su questo pulsante.

Accesso alle risorse di rete

Per impostazione predefinita, MDaemon viene eseguito come servizio di sistema nell'ambito dell'account SYSTEM. Poiché tale account non ha accesso alle periferiche di rete, MDaemon non è in grado di accedere alla posta se questa si trova su altri computer della rete LAN. Per risolvere questo problema, è sufficiente fornire le credenziali di connessione di un account che consenta al servizio MDaemon di accedere alle condivisioni di rete. In questo caso è possibile creare un account utente Windows specifico per l'esecuzione di MDaemon, contenente tutte le restrizioni necessarie e l'accesso alle condivisioni di rete che devono essere disponibili per MDaemon. Tutte le applicazioni avviate da MDaemon utilizzeranno le stesse credenziali.

Login
Indica il nome dell'ID utente dell'account Windows nel cui ambito viene eseguito il servizio MDaemon.

Password
È la password dell'accountdi Windows.

Dominio
Indica il dominio Windows al quale appartiene l'account. Per connettersi al dominio predefinito, lasciare questo campo vuoto.

Sezione

4 Menu Sicurezza

MDaemon dispone di una suite completa di funzioni e di comandi di sicurezza. Fare clic su Sicurezza nella barra dei menu di MDaemon per accedere alle funzioni di sicurezza illustrate di seguito:

- **AntiVirus** 658 - Le funzionalità AntiVirus di MDaemon Private Cloud consentono di impedire la ricezione di virus via e-mail fornendo il maggior livello possibile di protezione integrata per i clienti di MDaemon. Questo sistema cattura, mette in quarantena, pulisce e/o elimina tutti i messaggi e-mail infetti. Il componente Protezione attacchi 653 offre ulteriori funzioni di protezione da spam, da virus e da attacchi di tipo phishing talvolta non individuati dalle misure di protezione tradizionali, basate sul contenuto dei messaggi e sulle definizioni dei virus.
- **Filtro contenuti** 659 - Un sistema di filtro dei contenuti molto versatile e totalmente multi-thread consente di personalizzare il comportamento del server in base al contenuto dei messaggi e-mail in entrata e in uscita. È possibile inserire e aggiungere intestazioni di messaggio, aggiungere piè di pagina ai messaggi, rimuovere gli allegati, inoltrare copie ad altri utenti, attivare l'invio automatico di un messaggio istantaneo, eseguire programmi e altro ancora.
- **Spam Filter** 691 - Una nuova tecnologia di filtro dei messaggi spam per esaminare, tramite un procedimento euristico, i messaggi e-mail calcolando un "punteggio". Questo viene usato per determinare la probabilità che un messaggio sia di tipo spam. In base al punteggio, il server può intraprendere determinate azioni, ad esempio respingendo il messaggio o contrassegnandolo. Vedere anche: Spam Trap 723
- **Liste bloccati DNS** 717: consente di specificare diversi servizi di liste bloccati DNS che verranno controllati ogni volta che qualcuno tenta di inviare un messaggio al proprio server. Se l'IP di connessione è stato incluso da uno di questi host, il messaggio sarà rifiutato.
- **Controllo inoltro** 519 - Questa funzione consente di controllare il comportamento di MDaemon quando al server viene recapitato un messaggio in cui né il mittente né il destinatario sono indirizzi locali.
- **Scudo IP** 528 - Questa funzione consente la connessione al server solo se l'indirizzo IP del nome di dominio che richiede la connessione è presente in questo elenco.
- **Ricerca inversa** 521 - Questa funzione consente di interrogare i server DNS per verificare la validità dei nomi di dominio e degli indirizzi riportati nei messaggi in entrata. I comandi di questa schermata consentono di respingere i messaggi dubbi o di inserirvi un'intestazione speciale. I dati di Ricerca inversa vengono inoltre riportati nei registri di MDaemon.
- **Verifica POP prima di SMTP** 525 - I comandi di questa schermata consentono di obbligare ogni utente ad accedere alla propria casella postale prima di poter inviare un messaggio mediante MDaemon. In questo modo, l'utente viene autenticato come titolare di un account valido e viene autorizzato a utilizzare il sistema di posta.

- **Host accreditati** 526 - Questa funzione elenca i nomi di dominio e gli indirizzi IP associati a eccezioni delle regole di inoltro specificate nella scheda Impostazioni di inoltro.
- **Autenticazione SMTP** 531 - Questa funzione consente di impostare diverse opzioni che controllano il comportamento di MDaemon nel caso in cui un utente che invia un messaggio è già stato precedentemente autenticato o nel caso inverso.
- **SPF** 533 - La maggior parte dei domini pubblicano i record MX per identificare i sistemi che possono ricevere posta per essi, ma questa funzione non è in grado di identificare le posizioni consentite per l'invio. SPF (Sender Policy Framework) è un mezzo attraverso il quale i domini possono anche pubblicare i record "MX inversi" per identificare le posizioni che sono autorizzate a inviare messaggi.
- **DomainKeys Identified Mail** 536 - DKIM (DomainKeys Identified Mail) è un sistema di verifica della posta elettronica che può essere utilizzato per prevenire lo "spoofing". Questo sistema si può usare anche per garantire l'integrità dei messaggi in arrivo o per assicurarsi che il messaggio non sia stato alterato nell'intervallo di tempo trascorso dal momento in cui ha lasciato il server di posta del mittente al momento in cui è arrivato a destinazione. Ciò è possibile grazie all'uso di un sistema di coppie di chiavi pubbliche o private crittografate. I messaggi in uscita vengono firmati usando una chiave privata mentre i messaggi in arrivo dispongono di proprie firme verificate controllandole con una chiave pubblica pubblicata sul server DNS del mittente.
- **Certificazione** 560 - Nel processo di certificazione dei messaggi, un'entità garantisce o "certifica" la correttezza del comportamento relativo alla posta elettronica tenuto da un'altra entità. La certificazione rappresenta un vantaggio perché consente di evitare l'applicazione delle funzionalità di analisi antispam a messaggi per i quali non è necessaria, nonché di ridurre le risorse necessarie per l'elaborazione di ciascun messaggio.
- **Lista mittenti bloccati** 568 contiene gli indirizzi che non sono autorizzati a inviare traffico di posta attraverso il server.
- **Vaglio IP** 571 - Questa funzione è utilizzata per specificare gli indirizzi IP ai quali accordare o rifiutare le connessioni al server.
- **Vaglio host** 573 - Questa funzione è utilizzata per specificare gli host (nomi di dominio) ai quali consentire o rifiutare le connessioni al server.
- **Vaglio dinamico** 623 - Utilizzando Vaglio dinamico, MDaemon è in grado di tenere traccia del comportamento delle connessioni in ingresso per identificare attività sospette e rispondere di conseguenza. È possibile bloccare un indirizzo IP 627 (o un intervallo di indirizzi) dalla connessione quando non supera l'autenticazione per il numero di volte specificato entro il periodo di tempo indicato. È anche possibile bloccare gli account 627 che tentano di autenticarsi quando non superano l'autenticazione troppe volte e troppo rapidamente.
- **SSL e TLS** 585: MDaemon supporta il protocollo Secure Sockets Layer (SSL) per SMTP, POP e IMAP e per il server Web di Webmail. SSL è il metodo standard per la protezione delle comunicazioni Web tra server e client.
- **Protezione backscatter** 607 - Il termine "Backscatter" si riferisce ai messaggi di risposta ricevuti dagli utenti relativi a messaggi mai spediti. Ciò si verifica quando i messaggi spam o i messaggi inviati da virus includono un indirizzo di

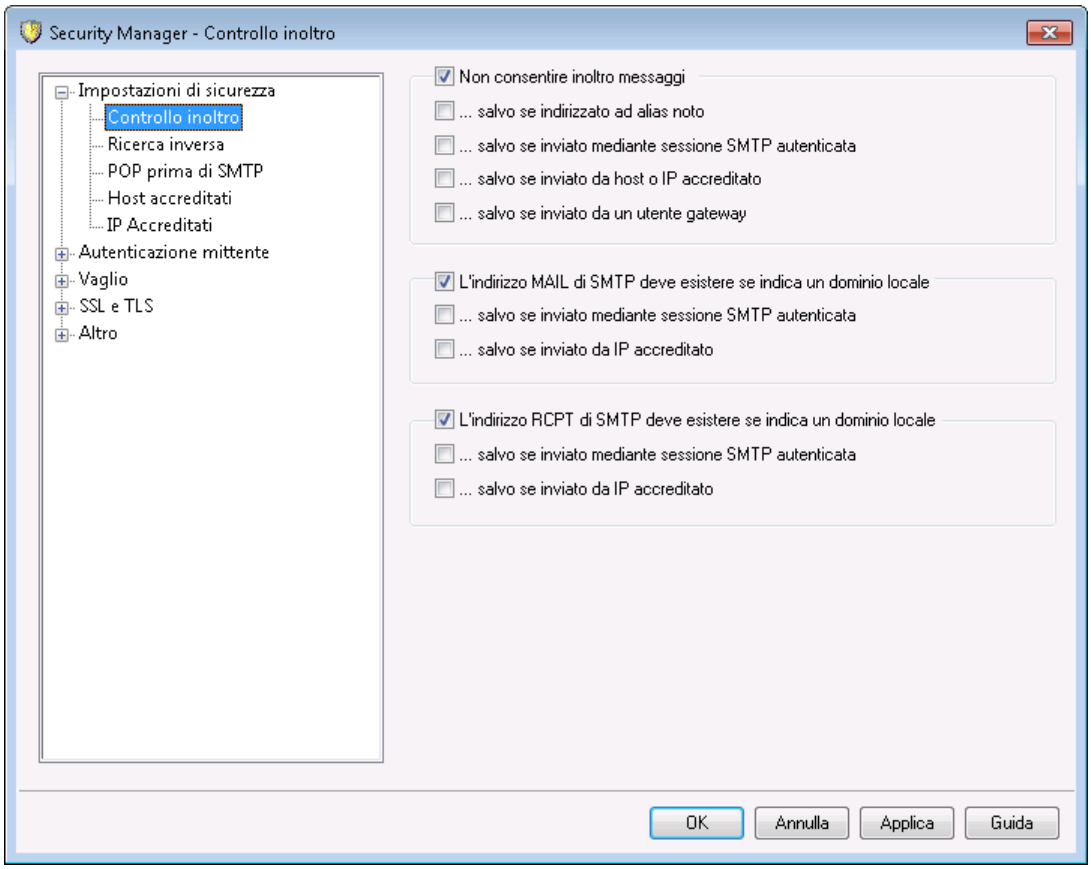
ritorno contraffatto. Questa funzionalità utilizza un metodo di codifica hash di una chiave privata per generare e inserire nell'indirizzo del percorso di ritorno dei messaggi in uscita uno speciale codice con validità temporale limitata, in modo da consentire la ricezione dei soli messaggi di risposta automatica e di notifica di recapito legittimi.

- **Regolazione larghezza di banda** 610 - La funzionalità di regolazione della larghezza di banda è una nuova funzione che consente di controllare la larghezza di banda utilizzata da MDaemon. È possibile controllare la velocità di avanzamento delle sessioni o dei servizi, impostando velocità diverse per ogni servizio principale di MDaemon in base al dominio, compresi i domini aggiuntivi e i gateway di dominio.
- **Tarpitting** 614 - Questa funzione consente di rallentare deliberatamente una connessione a seguito della ricezione di un determinato numero di comandi RCPT dal mittente. Ciò consente di scoraggiare l'invio di messaggi e-mail non desiderati. L'assunto che sottende a questa tecnica consiste nell'imporre ai mittenti di messaggi indesiderati un periodo di attesa lungo e variabile per l'invio di ogni messaggio, scoraggiandoli così nel ritentare l'operazione.
- **Greylisting** 616 - È una tecnica antispam che sfrutta il fatto che i server SMTP ritentano la consegna di qualsiasi messaggio riceva un codice di errore temporaneo del tipo "riprovare più tardi". Con questa tecnica, quando arriva un messaggio da un mittente non presente nella lista consentiti o comunque sconosciuto, il mittente, il destinatario e l'indirizzo IP del server mittente verranno registrati e il messaggio verrà rifiutato come previsto dal processo di Greylisting con un codice di errore temporaneo durante la sessione SMTP. Quando i server legittimi tentano di recapitare nuovamente i messaggi alcuni minuti più tardi, questi vengono accettati. Dal momento che gli "spammer" in genere non eseguono ulteriori tentativi di consegna, questa funzione consente di ridurre considerevolmente il numero di messaggi spam ricevuti.
- **IP LAN** 620 - In questa schermata vengono elencati gli indirizzi IP presenti sulla rete LAN in uso. Per quanto attiene alla regolazione della larghezza di banda, tali indirizzi IP vengono considerati come locali e possono essere esclusi da varie altre limitazioni di sicurezza e antispam.
- **Criteri sito** 621 - Questa funzione consente di creare i criteri di utilizzo del sito da trasmettere ai server di invio all'inizio di ogni sessione di posta SMTP. Un esempio comune di criterio di utilizzo del sito potrebbe essere il seguente: "Questo server non provvede all'inoltro."

4.1 Security Manager

4.1.1 Impostazioni di sicurezza

4.1.1.1 Controllo dell'inoltro



La schermata Controllo inoltro, disponibile in Sicurezza » Impostazioni sicurezza » Controllo inoltro consente di definire il funzionamento del server per l'inoltro della posta. Quando riceve un messaggio non proveniente né destinato a un indirizzo locale, il server di posta in uso provvede a inoltrare (ossia consegnare) tale messaggio per conto di un altro server: se si preferisce non inoltrare la posta degli utenti sconosciuti, impostare i comandi descritti di seguito.

L'inoltro indiscriminato di e-mail per altri server può provocare l'inserimento del proprio dominio nella lista bloccati da parte di uno o più servizi DNS-BL 717. Questo tipo di inoltro aperto è caldamente sconsigliato poiché gli spammer sfruttano i server aperti per nascondere le proprie tracce.

Inoltro posta

Non consentire inoltro messaggi
Se questa opzione è selezionata, MDaemon respinge i messaggi da inoltrare in cui i mittenti (FROM) e i destinatari (TO) includano utenti non locali.

...salvo se indirizzato ad alias noto
Selezionare questa casella di controllo se si desidera che a questi alias[847] vengano inoltrati messaggi, a prescindere dalle impostazioni di Controllo inoltro.

...salvo se inviato mediante sessione SMTP autenticata
Se questa opzione è abilitata, MDaemon inoltra sempre la posta, se inviata mediante una sessione SMTP autenticata.

...salvo se inviato da host o IP accreditato
Abilitare questa opzione qualora si desideri consentire l'inoltro se la posta proviene da un host o da un indirizzo IP accreditato.

...salvo se inviato da un utente gateway
Selezionare questa casella di controllo per consentire l'inoltro della posta mediante i gateway di dominio, indipendentemente dalle impostazioni di inoltro. Per impostazione predefinita, questa funzione è disabilitata (opzione consigliata).

Verifica account

L'indirizzo MAIL di SMTP deve esistere se indica un dominio locale
Selezionare questa opzione se si desidera verificare che il valore MAIL trasmesso durante il processo SMTP, se fa riferimento a un dominio o a un gateway locale, indichi un account effettivamente esistente.

...salvo se inviato mediante sessione SMTP autenticata
Selezionare questa opzione se si desidera escludere i messaggi inviati mediante sessioni di posta SMTP autenticate dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

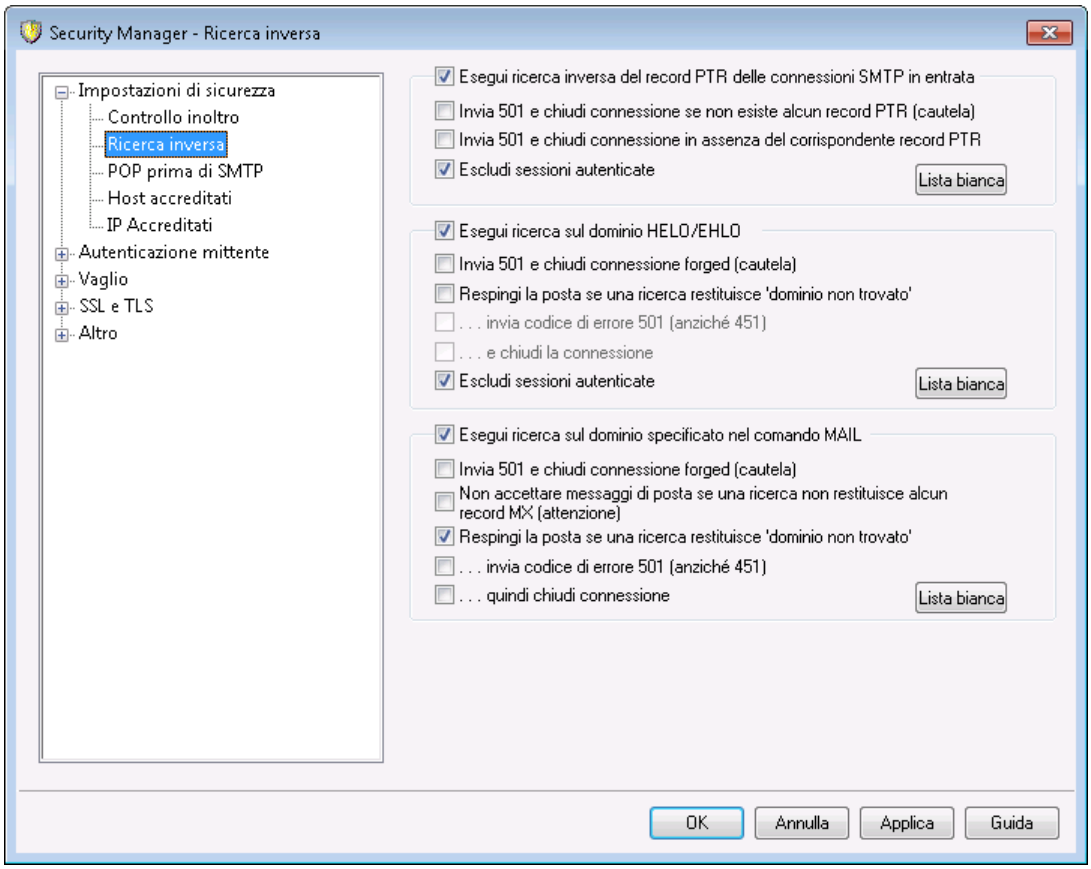
...salvo se inviato da host o IP accreditato
Selezionare questa opzione se si desidera escludere i messaggi inviati da un indirizzo IP accreditato dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

L'indirizzo RCPT di SMTP deve esistere se indica un dominio locale
Selezionare questa opzione se si desidera verificare che il valore RCPT trasmesso durante il processo SMTP, se fa riferimento a un dominio o a un gateway locale, indichi un account effettivamente esistente.

...salvo se inviato mediante sessione SMTP autenticata
Selezionare questa opzione se si desidera escludere i messaggi inviati mediante sessioni di posta SMTP autenticate dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

...salvo se inviato da host o IP accreditato
Selezionare questa opzione se si desidera escludere i messaggi inviati da un indirizzo IP accreditato dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

4.1.1.2 Ricerca inversa



Le opzioni di questa schermata consentono di configurare MDaemon in modo da eseguire una ricerca inversa sul dominio trasmesso nei comandi `HELO/EHLO` e `MAIL`. Durante le ricerche, MDaemon tenta di acquisire tutti gli indirizzi IP dei record MX e A per il dominio specifico; successivamente, l'indirizzo IP del computer che richiede la connessione viene confrontato con l'elenco allo scopo di determinare l'esatta identità del mittente.

La ricerca inversa può inoltre essere eseguita sui record PTR (puntatore) degli indirizzi IP in entrata: mediante questa opzione, se l'indirizzo IP in entrata non corrisponde ad alcun record PTR, è possibile interrompere la connessione o inserire un'intestazione di avviso nel messaggio.

È opinione comune che l'accettazione di posta proveniente da utenti che si identificano mediante un dominio inesistente debba essere facoltativa: a tale scopo, è disponibile un comando per rifiutare i messaggi per i quali la ricerca inversa restituisce un messaggio "dominio non trovato", proveniente dal server DNS. In questi casi, MDaemon restituisce

il codice di errore `451`, respinge il messaggio e consente il proseguimento della sessione SMTP. Tuttavia, è possibile inviare il codice di errore `501`, chiudere la connessione socket oppure eseguire entrambe le operazioni. A tale scopo sono disponibili ulteriori comandi.

Gli indirizzi IP e l'host locale (127.0.0.1) accreditati sono sempre esclusi dalle ricerche inverse.

Esegui ricerca inversa del record PTR delle connessioni SMTP in entrata
Selezionare questa opzione per effettuare la ricerca del record PTR in tutte le connessioni SMTP in entrata.

Invia 501 e chiudi connessione se non esiste alcun record PTR (cautela)
Se questa casella di controllo è selezionata, MDaemon invia il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, e chiude la connessione qualora non venga trovato alcun record PTR relativo al dominio.

Invia 501 e chiudi connessione in assenza del corrispondente record PTR
Se questa casella di controllo è selezionata, MDaemon invia il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, e chiude la connessione qualora la ricerca del record PTR non restituisca alcuna corrispondenza.

Escludi sessioni autenticate
Selezionare questa opzione se si desidera differire la ricerca PTR per le connessioni SMTP in entrata fino all'invio del comando MAIL del protocollo SMTP, utilizzato per verificare se la connessione è autenticata o meno.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni per le ricerche PTR in cui è possibile specificare gli indirizzi IP che si desidera esentare dalle ricerche inverse PTR.

Esegui ricerca sul dominio HELO/EHLO
Selezionare questa casella di controllo per eseguire una ricerca sul nome di dominio riportato durante la parte `HELO/EHLO` della sessione. Il comando `HELO/EHLO` viene utilizzato dal client (computer mittente) per identificarsi presso il server. Il nome di dominio trasmesso dal client in questo comando viene inserito dal server nella sezione `da` dell'intestazione `Received`.

Invia 501 e chiudi connessione forged (cautela)
Fare clic su questa casella di controllo per provocare l'invio di un codice di errore 501 e la chiusura della connessione quando il risultato della ricerca visualizzato sembra un'identificazione falsificata.

Spesso il risultato della ricerca inversa che rileva un'identificazione contraffatta non è corretto; è molto

> frequente, infatti, che i server di posta identifichino se stessi con valori che non corrispondono ai relativi indirizzi IP. Ciò può dipendere da restrizioni e limiti ISP oltre ad altre possibili cause. Per questo motivo è opportuno prestare la massima attenzione prima di attivare questa opzione in quanto il server potrebbe respingere posta accettabile.

Respingi la posta se una ricerca restituisce 'dominio non trovato'
Se questa opzione è abilitata e la ricerca non trova il dominio (restituisce, cioè, l'errore "`domain not found`"), il messaggio viene respinto e abbinato al codice di errore `451` (Azione richiesta interrotta: errore locale di elaborazione), quindi la sessione prosegue e si conclude normalmente.

...invia codice di errore 501 (anziché 451)
Selezionare questa casella di controllo per inviare in risposta al risultato "dominio non trovato" il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, anziché il codice di errore `451`.

...quindi chiudi connessione
Selezionare questa casella di controllo per chiudere immediatamente la connessione, anziché consentirne il proseguimento, se la ricerca inversa restituisce il risultato "`dominio non trovato`".

Escludi sessioni autenticate
Selezionare questa opzione se si desidera differire la ricerca fino all'invio del comando MAIL del protocollo SMTP al fine di verificare se la connessione utilizzerà l'autenticazione o meno.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni per la ricerca HELO/EHLO in cui è possibile designare indirizzi IP e i nomi di dominio/host dei siti che si desidera escludere dalle ricerche inverse HELO/EHLO.

Esegui ricerca sul valore trasferito nel comando MAIL
Se questa opzione è abilitata, la ricerca viene effettuata sul nome di dominio trasmesso durante la parte relativa al comando `MAIL` della transazione di posta. L'indirizzo trasmesso nel comando `MAIL` coincide generalmente con l'indirizzo del mittente, cioè con la casella postale da cui è partito il messaggio; tuttavia, a volte può trattarsi dell'indirizzo a cui devono essere inviati i messaggi di errore.

Invia 501 e chiudi connessione forged (cautela)
Selezionare questa casella di controllo se si desidera inviare il codice di errore 501 e chiudere la connessione quando dalla ricerca risulta un'identificazione contraffatta.

Spesso il risultato della ricerca inversa che rileva un'identificazione contraffatta non è corretto; è molto frequente, infatti, che i server di posta identifichino se stessi con valori che non corrispondono ai relativi indirizzi IP. Ciò può dipendere da restrizioni e limiti ISP oltre ad altre possibili cause. Per questo motivo è opportuno prestare la massima attenzione prima di attivare questa opzione in quanto il server potrebbe respingere posta accettabile.

Respingi la posta se una ricerca restituisce nessun record MX (attenzione)
Selezionare questa casella se si desidera rifiutare posta dai domini che non contengono record MX. L'opzione è disattivata per impostazione predefinita e deve essere utilizzata con cautela, poiché i domini non devono contenere record MX per poter esistere, essere validi o inviare e ricevere posta.

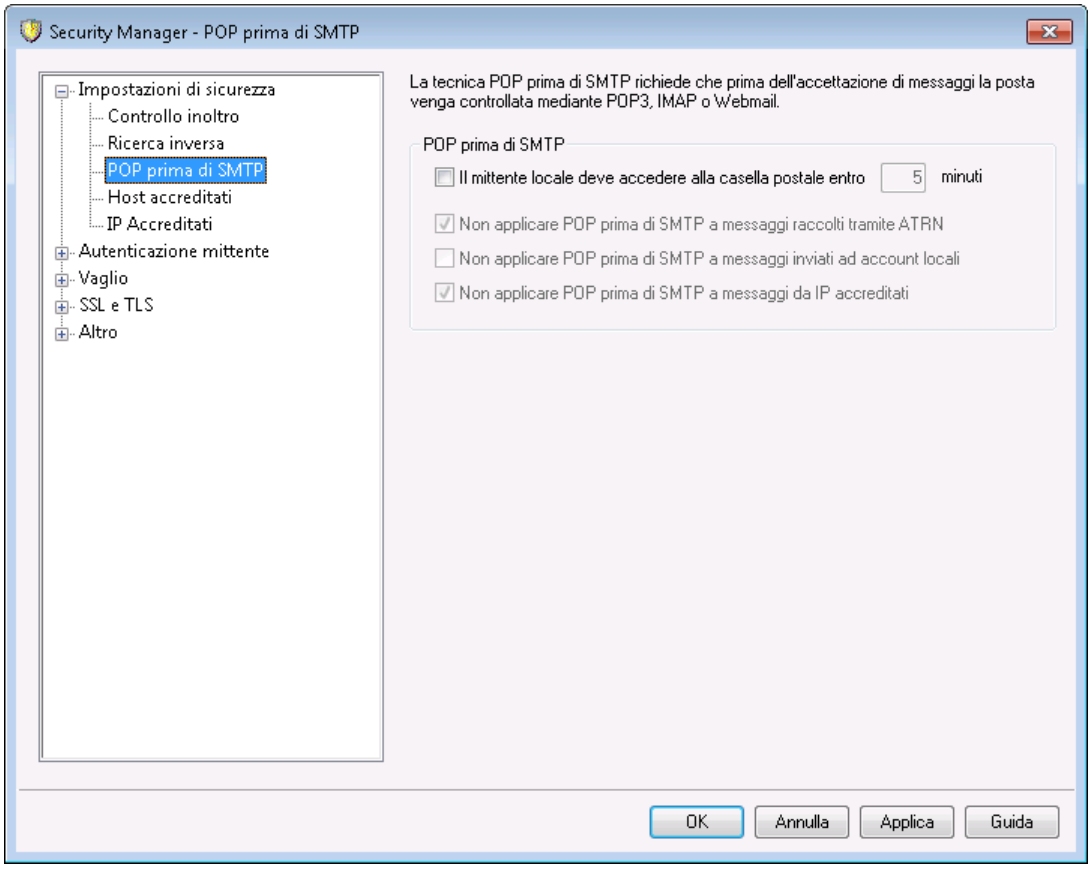
Respingi la posta se una ricerca restituisce 'dominio non trovato'
Se questa opzione è abilitata e la ricerca non trova il dominio (restituisce, cioè, l'errore "`domain not found`"), il messaggio viene respinto e abbinato al codice di errore `451` (Azione richiesta interrotta: errore locale di elaborazione), quindi la sessione prosegue e si conclude normalmente.

...invia codice di errore 501 (anziché 451)
Selezionare questa casella di controllo per inviare in risposta al risultato "dominio non trovato" il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, anziché il codice di errore `451`.

...quindi chiudi connessione
Selezionare questa casella di controllo per chiudere immediatamente la connessione, anziché consentirne il proseguimento, se la ricerca inversa restituisce il risultato "`dominio non trovato`".

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni per le ricerche MAIL. In questa finestra è possibile designare indirizzi IP e i nomi di dominio/host dei siti che si desidera escludere dalle ricerche inverse MAIL.

4.1.1.3 POP prima di SMTP



POP prima di SMTP

Il mittente locale deve accedere alla casella postale entro [XX] minuti
Se questa funzionalità è abilitata, per inviare messaggi di posta provenienti da mittenti locali è necessario che l'utente locale si connetta e controlli la propria casella postale entro l'intervallo di tempo, espresso in minuti, specificato in questo campo.

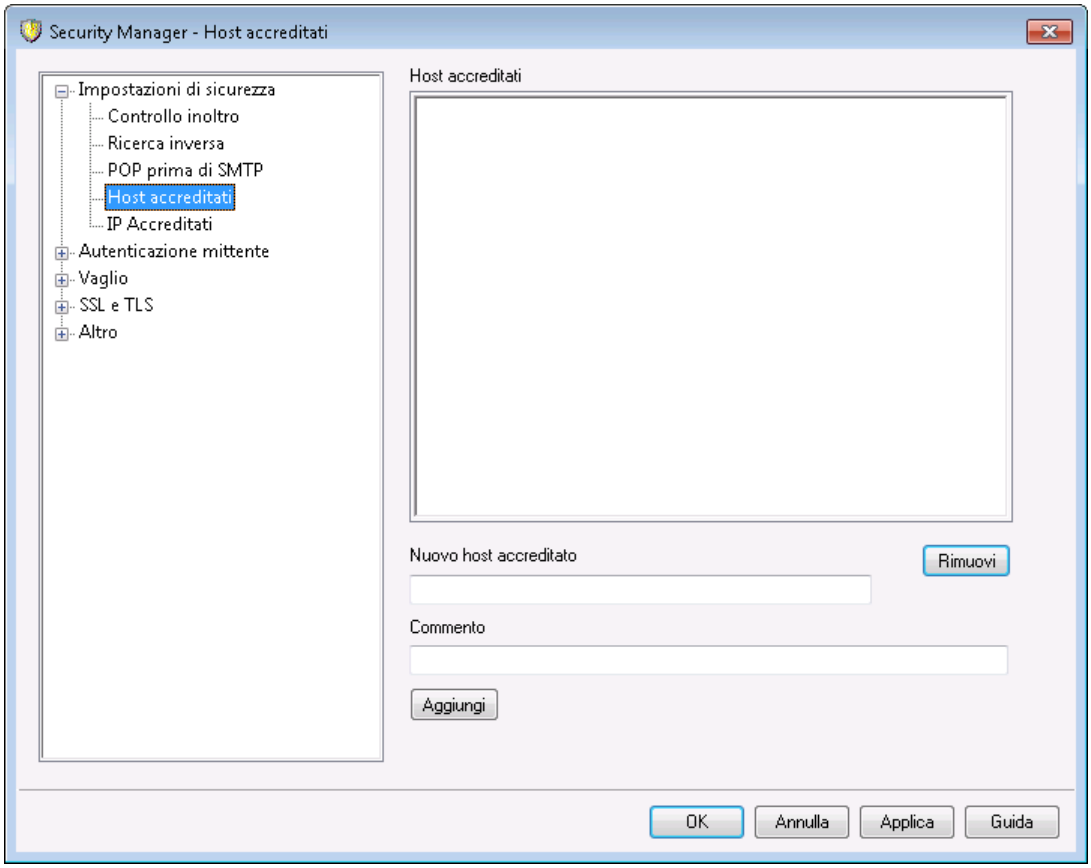
Non applicare POP prima di SMTP ai messaggi raccolti mediante ATRN
Selezionare questa casella di controllo per non applicare ai messaggi raccolti mediante ATRN 269 la funzionalità POP prima di SMTP.

Non applicare POP prima di SMTP ai messaggi inviati ad account locali
Fare clic su questa casella di controllo per non applicare la funzionalità POP prima di SMTP ai messaggi inviati da un utente locale a un altro. In genere, MDaemon applica la funzione POP prima di SMTP non appena riconosce il mittente ma, se questa opzione è abilitata, MDaemon procede al riconoscimento del destinatario del messaggio prima di determinare se tale funzionalità debba essere applicata o meno.

Non applicare POP prima di SMTP ai messaggi raccolti da IP affidabili
Se questa casella di controllo è abilitata, i messaggi provenienti da un indirizzo IP elencato nella schermata Host accreditati 526 vengono esclusi dalla funzionalità POP prima di SMTP.

Per non applicare la funzionalità POP prima di SMTP alle sessioni autenticate è possibile utilizzare un'opzione della schermata Autenticazione SMTP 531.

4.1.1.4 Host accreditati



Numerose finestre di dialogo e funzioni di sicurezza di MDaemon includono opzioni che consentono di scegliere se escludere o meno dall'elaborazione gli "host accreditati" o i "domini accreditati". Tali opzioni fanno riferimento agli host visualizzati in questa schermata.

Host accreditati
Viene visualizzato un elenco degli host esclusi da specifiche opzioni di sicurezza.

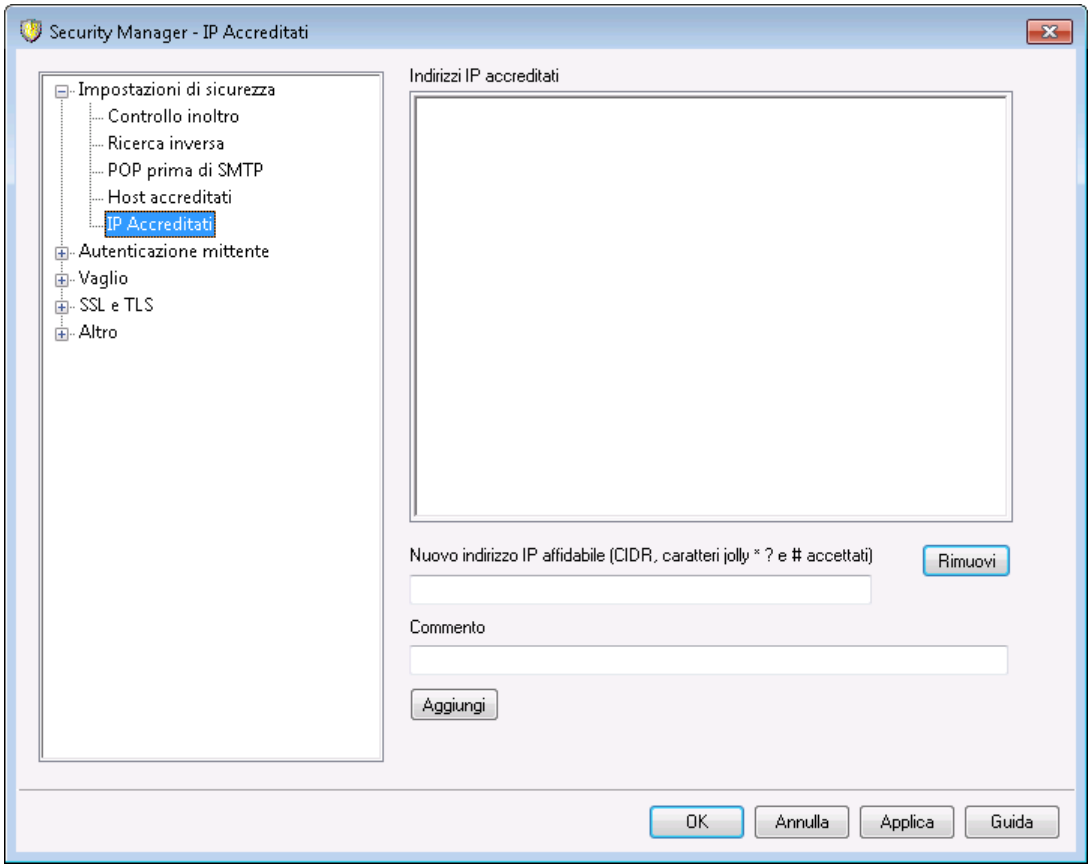
Nuovo host accreditato
Inserire un nuovo host da aggiungere all'elenco degli *host accreditati*.

Commento
Da utilizzare per aggiungere eventuali commenti a una voce.

Aggiungi
Fare clic su questo pulsante per aggiungere il nuovo dominio all'elenco degli *host accreditati*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco degli *host accreditati*.

4.1.1.5 IP accreditati



Numerose finestre di dialogo di MDaemon includono opzioni che consentono di scegliere se escludere o meno dall'elaborazione gli "indirizzi IP accreditati". Tali opzioni fanno riferimento agli indirizzi IP accreditati visualizzati in questa schermata.

Indirizzi IP accreditati
Viene visualizzato un elenco degli indirizzi IP esclusi da specifiche opzioni di sicurezza.

Nuovo indirizzo IP accreditato
Inserire l'indirizzo IP da aggiungere all'elenco degli *Indirizzi IP accreditati*.

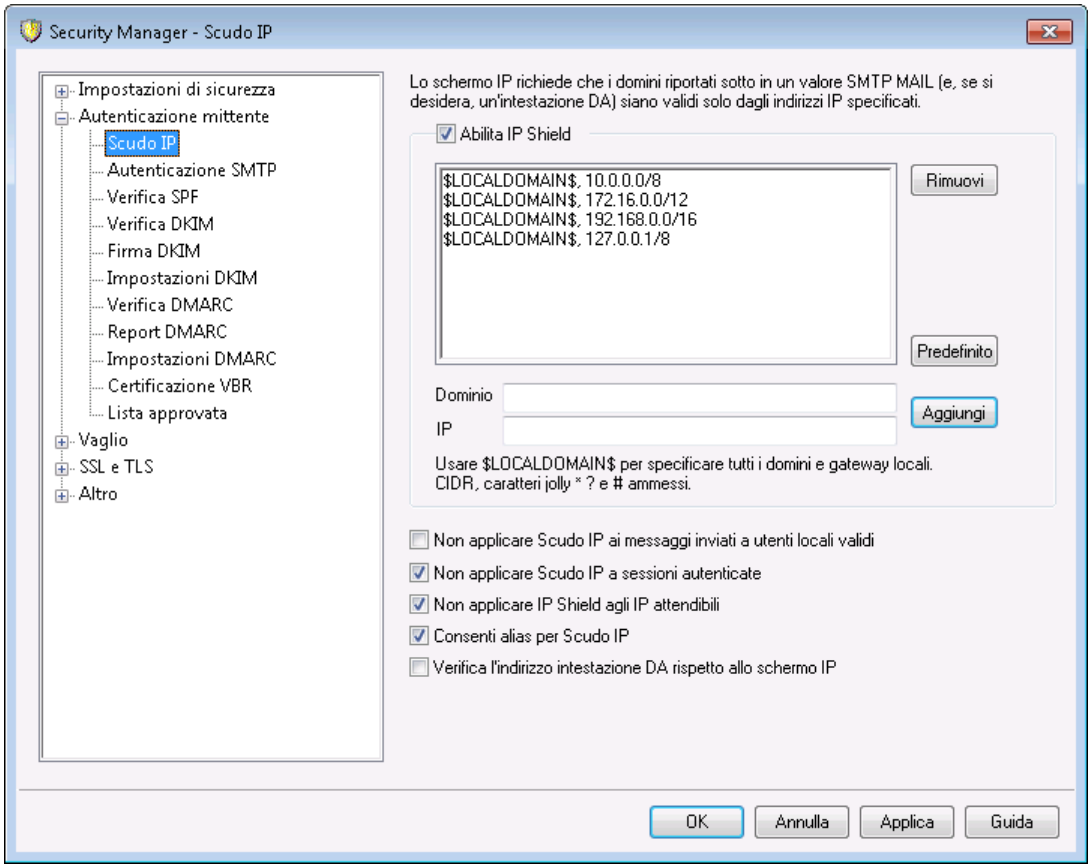
Commento
Da utilizzare per aggiungere eventuali commenti a una voce.

Aggiungi
Fare clic su questo pulsante per aggiungere il nuovo indirizzo IP all'elenco degli *Indirizzi IP accreditati*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco degli *Indirizzi IP accreditati*.

4.1.2 Autenticazione mittente

4.1.2.1 Scudo IP



Lo Scudo IP, disponibile nel menu Sicurezza » Impostazioni sicurezza » Autenticazione mittente è un elenco di nomi di dominio e dei corrispondenti indirizzi IP che vengono verificati durante il comando `MAIL From` impartito nella sessione SMTP. Una sessione SMTP proveniente da un utente appartenente a uno dei domini elencati viene accettata solo se proviene da uno dei relativi indirizzi IP. Ad esempio, si supponga che il nome di dominio sia esempio.com e che i computer della rete locale LAN usino gli indirizzi IP compresi tra 192.168.0.0 e 192.168.0.255. Con queste informazioni, lo scudo IP può essere configurato per associare il nome dominio esempio.com alla serie di indirizzi IP 192.168.0.* (i caratteri jolly sono consentiti). Pertanto, se un computer richiede una connessione SMTP al server, inviando l'istruzione "`MAIL FROM <nome@esempio.com>`", la sessione SMTP viene accettata solo se il computer che si connette presenta un indirizzo IP compreso tra 192.168.0.0 e 192.168.0.255.

Abilita scudo IP

Deselezionare questa casella di controllo se si desidera disabilitare lo scudo IP. Lo scudo IP è abilitato per impostazione predefinita.

Nome dominio
Immettere il nome del dominio da associare a un intervallo di indirizzi IP specifico. È possibile utilizzare anche la macro `$LOCALDOMAIN$` da estendere a tutti i domini locali (compresi i gateway). Se si utilizza questa macro non sarà necessario tenere aggiornato lo scudo IP in caso di modifica di domini locali o gateway. Per impostazione predefinita, vengono aggiunte a Scudo IP le voci che associano a `$LOCALDOMAIN$` tutti gli intervalli di indirizzi IP riservati.

Indirizzo IP
Inserire l'indirizzo IP da associare con il nome di dominio. L'indirizzo prevede il formato con punti decimali.

Aggiungi
Per aggiungere all'elenco l'intervallo di domini e di indirizzi IP, fare clic sul pulsante *Aggiungi*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco.

Non applicare IP Shield ai messaggi inviati a utenti locali validi
Selezionare questa opzione per verificare la corrispondenza dominio/IP solo per i messaggi destinati a utenti non locali o a utenti locali non validi. In questo modo si impedisce che terzi si fingano utenti locali allo scopo di inoltrare la propria posta mediante il server e, al contempo, si risparmiano risorse in quanto non viene effettuata la verifica dei messaggi indirizzati agli utenti del server in uso. Se si seleziona sia questa opzione che l'opzione *Consenti alias per Scudo IP* descritta di seguito, verranno accettati anche i messaggi inviati ad alias validi.

Non applicare IP Shield alle sessioni autenticate
Con l'attivazione di questo controllo, gli utenti autenticati vengono esclusi dalle restrizioni dello scudo IP. La posta proveniente da questi utenti viene accettata a prescindere dall'indirizzo IP di connessione. Inoltre, quando un utente non è autenticato e l'accesso viene negato, il messaggio restituito al client SMTP è

"Autenticazione necessaria", che suggerisce all'utente che il problema può essere risolto configurando il client di posta per l'utilizzo dell'autenticazione prima dell'invio di un messaggio. L'opzione è abilitata per impostazione predefinita.

Non applicare IP Shield agli IP affidabili
Con l'attivazione di questo controllo, lo Scudo IP non viene applicato con connessioni provenienti da un Indirizzo IP accreditato 526. L'opzione è abilitata per impostazione predefinita.

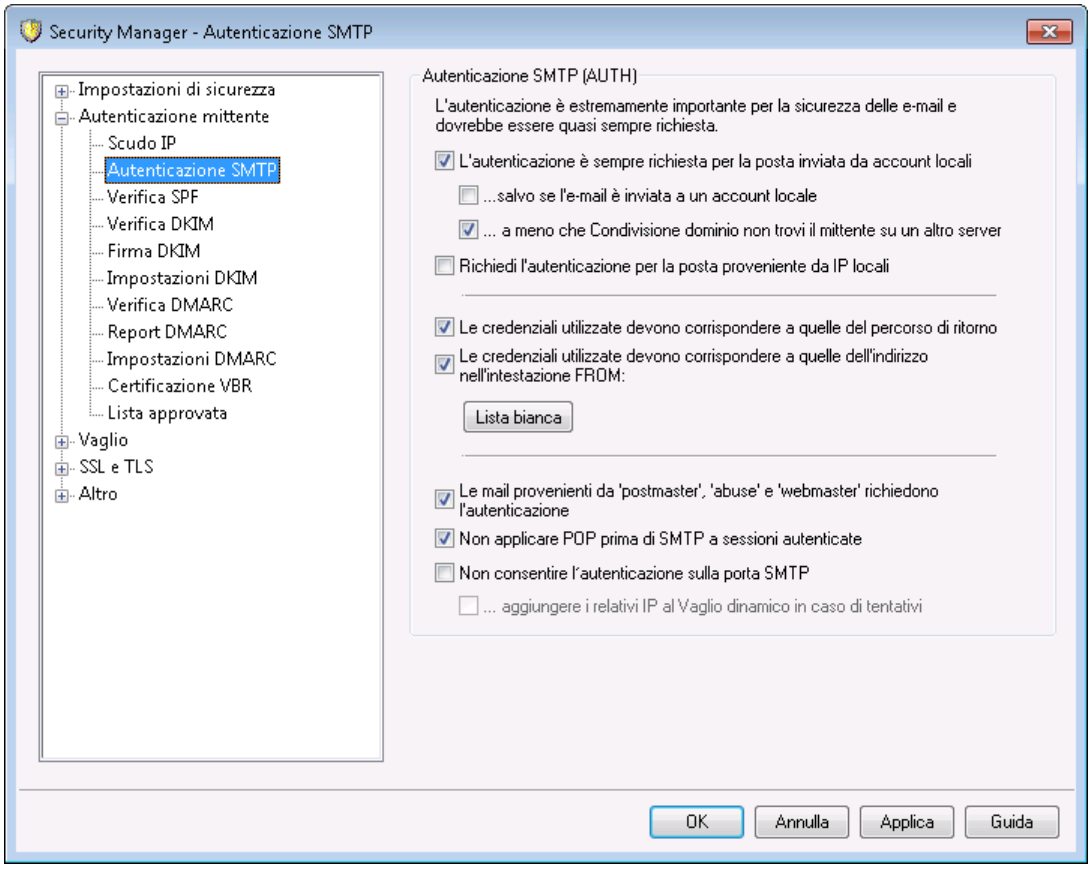
Consenti alias per Scudo IP
Abilitare questa opzione se si desidera che Scudo IP accetti gli alias degli indirizzi durante la verifica dell'associazione tra domini e indirizzi IP. Con Scudo IP, l'alias viene convertito nell'account reale cui fa riferimento e, di conseguenza, viene accettato se il controllo ha esito positivo. Se questa opzione è disattivata, ogni alias viene considerato come indirizzo indipendente dall'account che rappresenta. Di conseguenza, se l'indirizzo IP di un alias viola il controllo, il messaggio viene rifiutato. Questa opzioni è disponibile anche nella schermata Impostazioni 849 di Alias: se si modifica l'impostazione qui, la modifica sarà riportata anche nell'altra schermata.

Se si desidera che i messaggi in entrata indirizzati ad alias validi siano esclusi dalle verifiche di Scudo IP, abilitare sia questa opzione che l'opzione *Non applicare Scudo IP ai messaggi inviati a utenti locali validi*.

Verifica indirizzo intestazione FROM con Scudo IP
Selezionare questa casella se si desidera che lo scudo IP confronti l'indirizzo contenuto nell'intestazione FROM del messaggio insieme a quello contenuto nel valore SMTP MAIL. L'opzione è disabilitata per impostazione predefinita.

Questa opzione potrebbe causare problemi con alcuni tipi di messaggi, ad esempio quelli provenienti da liste di distribuzione, pertanto deve essere abilitata solo se strettamente necessario.

4.1.2.2 Autenticazione SMTP



Autenticazione SMTP (AUTH)

Richiedi autenticazione per la posta proveniente da account locali
Se questa opzione è abilitata e il messaggio in arrivo sembra provenire da uno dei domini di MDaemon, per evitare che MDaemon rifiuti la consegna del messaggio l'account deve essere preventivamente autenticato. L'opzione è abilitata per impostazione predefinita.

...salvo se il messaggio è per un account locale
Se l'autenticazione dei messaggi provenienti da un mittente locale è obbligatoria, selezionare questa opzione per evitare la restrizione relativa all'autenticazione quando anche il destinatario è locale. Nota: in alcuni casi questa funzione risulta necessaria, ad esempio quando si richiede agli utenti l'uso di server di posta differenti per i messaggi in entrata e quelli in uscita.

...a meno che Condivisione dominio non trovi il mittente su un altro server
Per impostazione predefinita, quando Condivisione dominio 117 trova il mittente su un altro server, tale mittente viene esentato dall'opzione *Richiedi l'autenticazione per la posta proveniente da account locali...* riportata sopra. Deselezionare la casella di controllo per richiedere l'autenticazione anche da tali utenti.

Richiedi l'autenticazione per la posta proveniente da IP locali
Selezionare questa opzione per richiedere l'autenticazione quando un messaggio in entrata viene inviato da un indirizzo IP locale. Se non è autenticato, il messaggio verrà respinto. Gli indirizzi IP affidabili 527 sono esclusi e questa opzione viene attivata per impostazione predefinita per le nuove installazioni.

Le credenziali utilizzate devono corrispondere a quelle del percorso di ritorno
Per impostazione predefinita, le credenziali utilizzate durante l'autenticazione SMTP devono corrispondere a quelle dell'indirizzo rilevato nel percorso di ritorno del messaggio. Disattivare questa opzione se non si desidera richiedere la corrispondenza con il percorso di ritorno. Per supportare l'archiviazione e l'inoltro della posta del gateway, è disponibile un'opzione corrispondente disponibile nella schermata Impostazioni gateway globali 258 che presenta l'opzione "*Esenta posta gateway dai requisiti di corrispondenza credenziali autenticazione*" attivata per impostazione predefinita.

Le credenziali utilizzate devono corrispondere a quelle dell'indirizzo nell'intestazione FROM:
Per impostazione predefinita, le credenziali utilizzate durante l'autenticazione SMTP devono corrispondere a quelle dell'indirizzo rilevato nell'intestazione "From:" del messaggio. Disattivare questa opzione se non si desidera richiedere la corrispondenza con l'intestazione "From:". Per supportare l'archiviazione e l'inoltro della posta del gateway, è disponibile un'opzione corrispondente disponibile nella schermata Impostazioni gateway globali 258 che presenta l'opzione "*Esenta posta gateway dai requisiti di corrispondenza credenziali autenticazione*" attivata per impostazione predefinita.

Elenco esenzioni
Utilizzare l'elenco esenzioni da corrispondenza credenziali per esentare un indirizzo dalle opzioni "*Le credenziali utilizzate devono corrispondere...*" sopra descritte. Per l'esenzione dall'opzione "*...devono corrispondere a quelle dell'indirizzo di return-path*", l'indirizzo esentato deve corrispondere all'indirizzo di **Return-Path** del messaggio. Per l'esenzione dall'opzione "*...devono corrispondere a quelle dell'indirizzo nell'intestazione "From:"*", l'indirizzo esentato deve corrispondere all'indirizzo riportato nell'intestazione **From:** del messaggio.

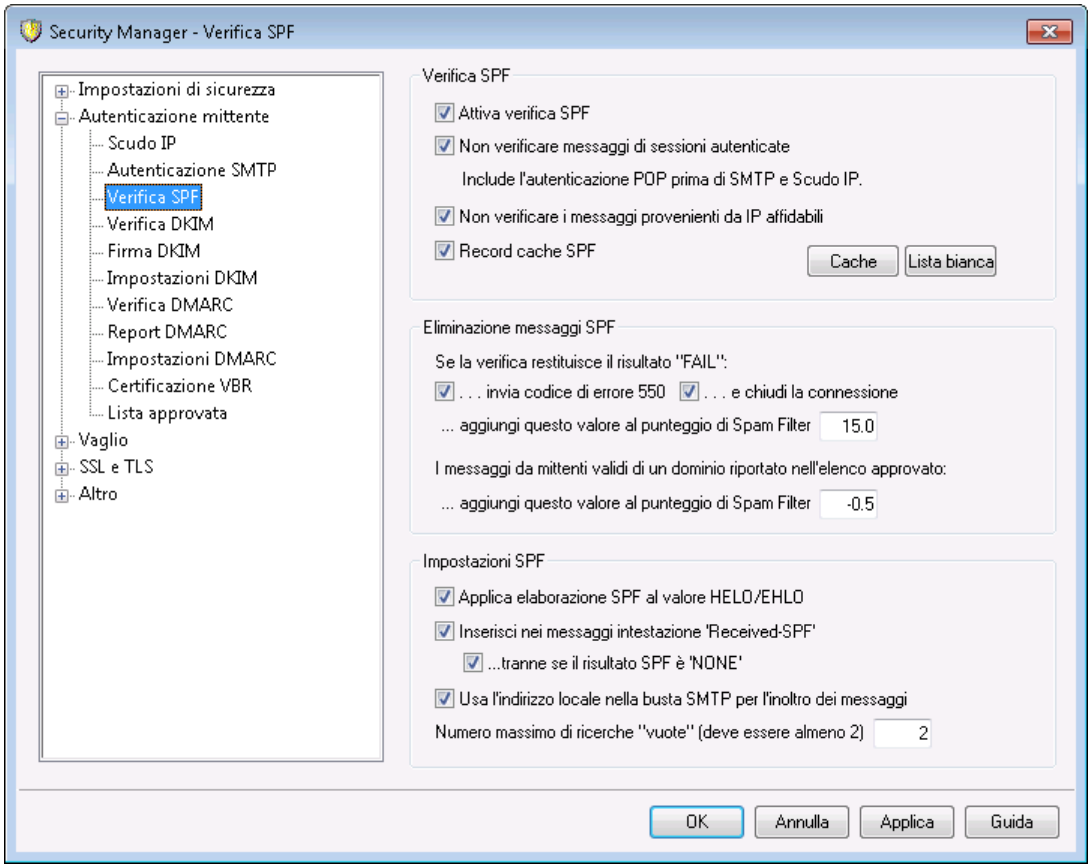
Le mail provenienti da 'postmaster', 'abuse' e 'webmaster' richiedono l'autenticazione
Selezionare questa casella di controllo per richiedere l'autenticazione dei messaggi che dichiarano di provenire dagli alias o dagli account "postmaster@...", "abuse@..." o "webmaster@..." prima dell'accettazione da parte di MDaemon. Spammer e hacker sono a conoscenza della potenziale esistenza di tali indirizzi e possono, quindi, tentare di utilizzarli per inviare posta attraverso il sistema. Questa opzione consente di evitare questa eventualità. Questa opzione è duplicata nella schermata Impostazioni 849 di Alias. Qualsiasi modifica apportata in questa sede viene riportata anche nell'altra posizione.

Non applicare POP prima di SMTP alle sessioni autenticate
Se si è abilitata la funzione di sicurezza POP prima di SMTP 525, è sufficiente fare clic su questa opzione per escludere gli utenti autenticati da questa restrizione. In questo modo, non è necessario che un utente autenticato esegua una verifica della posta prima dell'invio.

Non consentire l'autenticazione sulla porta SMTP
Questa opzione disattiverà il supporto di AUTH sulla porta SMTP. AUTH non verrà offerto nella risposta EHLO e verrà considerato un comando sconosciuto se fornito dal client SMTP. Questa impostazione e l'opzione "*...aggiungere i relativi IP al Vaglio dinamico*" successiva sono utili in configurazioni in cui tutti gli account legittimi utilizzano MSA o un'altra porta per inviare la posta autenticata. In queste configurazioni si presume che qualsiasi tentativo di autenticazione sulla porta SMTP avvenga da parte di malintenzionati.

...aggiungere i relativi IP al Vaglio dinamico in caso di tentativi
Quando si utilizza l'opzione *Non consentire l'autenticazione sulla porta SMTP* precedente, questa opzione aggiungerà al Vaglio dinamico l'indirizzo IP di qualsiasi client che tenta di eseguire l'autenticazione. La connessione verrà interrotta immediatamente.

4.1.2.3 Verifica SPF



MDaemon supporta SPF (Sender Policy Framework) per consentire la verifica dei server di invio e proteggere dallo spoofing e dal phishing, che rappresentano due tipi di contraffazione della posta elettronica con cui il mittente tenta di far passare i messaggi come inviati da qualcun altro.

Molti domini pubblicano i record MX nel DNS (Domain Name System) per identificare le postazioni a cui è consentito ricevere la posta elettronica, ma ciò non consente di identificare in alcun modo le postazioni a cui è consentito *inviare* la posta. SPF è un mezzo attraverso il quale i domini possono pubblicare anche i record relativi ai mittenti per identificare le postazioni autorizzate all'invio dei messaggi. Eseguendo una ricerca SPF sui messaggi in entrata, MDaemon può tentare di determinare se al server di invio è consentito consegnare la posta per il dominio di invio responsabile e, di conseguenza, se l'indirizzo del mittente può essere stato contraffatto o "mascherato".

Per configurare le impostazioni SPF del server, usare le opzioni contenute in questa schermata.

Per ulteriori informazioni su SPF, vedere:

http://www.open-spf.org

Verifica SPF

Attiva verifica SPF
Quando questa opzione è abilitata, MDaemon esegue una query DNS per i dati relativi al record SPF su ciascun server responsabile per i messaggi in entrata, per assicurare che il server di invio sia autorizzato all'invio di messaggi per suo conto. L'host di cui MDaemon esegue la verifica viene ricavato dal valore `MAIL` trasferito durante l'elaborazione SMTP. La verifica SPF è abilitata per impostazione predefinita.

Non verificare i messaggi da sessioni autenticate
Per impostazione predefinita le connessioni autenticate sono escluse dalle interrogazioni SPF. Le sessioni autenticate includono quelle verificate mediante l'autenticazione SMTP 531, POP prima di SMTP 525 o Scudo IP 528. Se non si desidera escludere le sessioni autenticate da SPF, disabilitare questa opzione.

Non verificare i messaggi provenienti da IP affidabili
Per impostazione predefinita tutti i messaggi provenienti da un indirizzo IP accreditato 527 sono esclusi dalla verifica SPF.

Memorizza risultati delle verifiche
Per impostazione predefinita MDaemon memorizza temporaneamente nella cache ciascun record di criteri SPF di un dominio, ottenuto durante una query DNS. Se non si desidera memorizzare nella cache i criteri SPF, deselezionare questa casella di controllo.

Cache
Con questo pulsante si apre la cache SPF, che riporta tutti i record SPF memorizzati attualmente nella cache.

Elenco esenzioni
Fare clic su questo pulsante per aprire la Lista eccezioni SPF in cui è possibile designare indirizzi IP, indirizzi e-mail e domini che si desidera esentare dalle ricerche di SPF. Gli indirizzi e-mail vengono confrontati ai valori dell'envelope SMTP, non con l'intestazione From del messaggio. I domini sono esentati dall'anteposizione di "spf" al nome del dominio. MDaemon inserirà il record SPF di tale dominio in ogni valutazione di SPF utilizzando il tag specifico di MDaemon "wlinclude:<dominio>". In questo modo è possibile ottenere che il proprio provider MX di backup venga trattato come un'origine SPF valida per tutti i mittenti.

Eliminazione messaggi SPF

Se la verifica restituisce il risultato ERRORE:

...invia codice di errore 550
Selezionare questa casella di controllo per inviare il codice di errore 550 quando il risultato dell'interrogazione SPF è "Fail".

...quindi chiudi connessione
Attivare questa opzione per chiudere la connessione subito dopo l'invio del codice di errore 550.

...aggiungi questo valore al punteggio di Spam Filter
Indicare il valore da aggiungere al punteggio di spam del messaggio quando esso non supera la verifica SPF.

I messaggi da mittenti validi di un dominio riportato nell'elenco approvato

...aggiungi questo valore al punteggio di Spam Filter
Indicare il valore che si desidera aggiungere al punteggio di spam del messaggio quando SPF conferma che esso proviene da un dominio situato nell'elenco approvato 566.

In genere, il valore specificato in questo campo deve essere un numero negativo in modo da diminuire il punteggio di spam per i messaggi approvati.

Impostazioni SPF

Applica elaborazione SPF a valore HELO/EHLO
L'opzione consente di applicare la verifica SPF al valore passato nel comando HELO o EHLO all'inizio del processo SMTP. L'opzione è abilitata per impostazione predefinita.

Inserisci nei messaggi intestazione 'Received-SPF'
Selezionare questa opzione per inserire in ciascun messaggio un'intestazione "Received-SPF".

...tranne se il risultato SPF è 'NESSUNO'
Attivare questa opzione per non inserire nel messaggio l'intestazione "Received-SPF" quando il risultato dell'interrogazione SPF è "nessuno".

Usa l'indirizzo locale nella busta SMTP per l'inoltro dei messaggi
Attivare questa opzione se si desidera che tutta la posta inoltrata da MDaemon utilizzi un indirizzo locale nella busta SMTP. Ciò consente di ridurre i problemi associati all'inoltro della posta. In genere, i messaggi inoltrati vengono inviati utilizzando l'indirizzo di posta del mittente originale e non quello di chi esegue l'inoltro. In alcuni casi, l'uso di un indirizzo locale si rivela necessario per impedire al server ricevente di interpretare erroneamente il messaggio inoltrato come contraffatto tramite "spoofing". L'opzione è abilitata per impostazione predefinita.

Numero massimo di ricerche "vuote" (deve essere almeno 2)
Questo è il numero massimo di risultati di ricerche vuote consentito in una query SPF prima che MDaemon generi un errore permanente. Una ricerca vuota genera come risultati "il dominio non esiste" o "non esistono risposte". Questo valore deve essere almeno 2.

4.1.2.4 DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) è un sistema crittografico di verifica della posta elettronica che si può utilizzare per impedire lo "spoofing", ovvero la pratica del contraffare l'indirizzo e-mail di un altro utente fingendosi un mittente diverso. Inoltre, poiché numerosi messaggi spam contengono indirizzi contraffatti, la tecnologia DKIM consente di ridurne significativamente il numero, pur non essendo nata come strumento antispam. La tecnologia DKIM si può utilizzare per garantire l'integrità dei messaggi in arrivo o per assicurarsi che il messaggio non sia stato alterato nell'intervallo di tempo trascorso dal momento in cui ha lasciato il server di posta del firmatario al momento in cui è arrivato a destinazione. In altre parole, grazie alla verifica crittografica DKIM, il server ha la certezza di ricevere il messaggio dal server che lo ha firmato e la garanzia che nessun altro lo abbia in alcun modo alterato.

Per garantire la validità e l'integrità dei messaggi, la tecnologia DKIM si avvale di un sistema di coppie di chiavi pubbliche e private. Sui record DNS del server di invio viene pubblicata una chiave pubblica crittografata, quindi ciascun messaggio in uscita viene firmato dal server usando la corrispondente chiave privata crittografata. Per i messaggi in arrivo, quando il server ricevente rileva la firma del messaggio, recupera la chiave pubblica dai record DNS del server di invio, quindi confronta la chiave con la firma crittografata del messaggio per determinarne la validità. Se il server ricevente non riesce a verificare il messaggio in arrivo, ciò vuol dire che contiene un indirizzo contraffatto oppure che è stato alterato o modificato. Il messaggio bloccato viene quindi respinto oppure accettato ma associato a un punteggio di spam.

Per configurare MDaemon al fine di verificare la firma crittografica dei messaggi in arrivo, utilizzare le opzioni incluse nella schermata Verifica DKIM 537. Per configurare MDaemon al fine di firmare i messaggi in uscita, utilizzare le opzioni incluse nella schermata Firma DKIM 539. Entrambe le schermate si trovano nella sezione Autenticazione mittente della finestra di dialogo Impostazioni sicurezza, disponibile in: Sicurezza » Impostazioni sicurezza » Autenticazione mittente. L'interfaccia

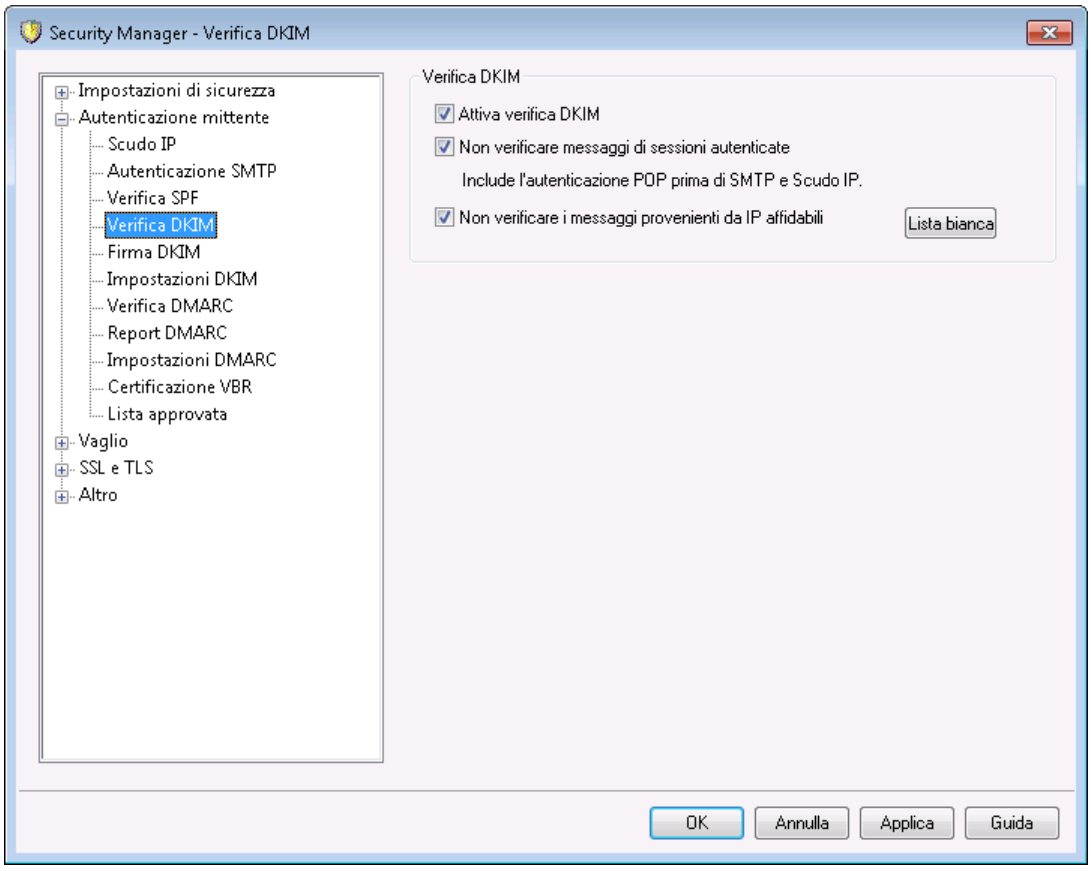
principale[74] di MDaemon contiene la scheda DKIM, all'interno della scheda Sicurezza, che consente di monitorare l'attività in tempo reale di DKIM. Per registrare tale attività, utilizzare le opzioni disponibili in: Impostazioni » Impostazioni server » Registrazione » Impostazioni.

Vedere:

Verifica DKIM[537]
Firma DKIM[539]
Impostazioni DKIM[542]

Per ulteriori informazioni su DomainKeys Identified Mail, visitare il sito http://www.dkim.org/.

4.1.2.4.1 Verifica DKIM



In questa schermata è possibile configurare MDaemon affinché verifichi le firme DomainKeys Identified Mail (DKIM) nei messaggi remoti in arrivo. Se si attiva questa funzionalità e un messaggio in arrivo contiene una firma crittografata, MDaemon recupera la chiave pubblica dal record DNS del dominio individuato mediante la firma e utilizza la chiave per determinare la validità della firma DKIM del messaggio.

Se la verifica della firma ha esito positivo, l'elaborazione del messaggio passa alla fase successiva del normale processo di consegna. Se il dominio individuato mediante la firma è presente anche nell'elenco approvato 566, inoltre, il punteggio spam del messaggio viene corretto in senso positivo.

Per ulteriori informazioni su DKIM, vedere: http://www.dkim.org/

Verifica DKIM

Attiva verifica DKIM
Per attivare la verifica DomainKeys Identified Mail sui messaggi remoti in arrivo, selezionare questa opzione.

Non verificare i messaggi da sessioni autenticate
Questa opzione consente di escludere i messaggi dalla verifica crittografica quando la sessione è autenticata. Le sessioni autenticate includono quelle verificate mediante l'autenticazione SMTP 531, POP prima di SMTP 525 o Scudo IP 528.

Non verificare i messaggi provenienti da IP affidabili
Questa opzione consente di escludere dalla verifica DKIM le connessioni provenienti da indirizzi IP accreditati 526.

Elenco esenzioni
Questo pulsante consente di aprire l'elenco delle eccezioni. I messaggi provenienti da un qualsiasi indirizzo IP presente in questo elenco non sono soggetti a verifica crittografica.

Intestazione "Authentication-Results"

Ogni volta che un messaggio viene autenticato tramite verifica SMTP AUTH, SPF, DomainKeys Identified Mail o DMARC, MDaemon inserisce nel messaggio l'intestazione "Authentication-Results" elencando i risultati del processo di autenticazione. Se MDaemon è configurato in modo da accettare anche i messaggi che non superano l'autenticazione, l'intestazione "Authentication-Results" contiene un codice indicante la causa dell'errore.

L'IETF (Internet Engineering Task Force) è attualmente impegnata a modificare alcuni standard relativi a questa intestazione e ai protocolli citati in questa sezione. Per ulteriori informazioni consultare il sito Web IETF all'indirizzo: http://www.ietf.org/.

Intestazioni DKIM nei messaggi delle liste di distribuzione

Per impostazione predefinita, MDaemon rimuove le firme DKIM dai messaggi delle liste in arrivo poiché le firme potrebbero essere danneggiate a causa delle modifiche apportate alle intestazioni o ai contenuti dei messaggi durante l'elaborazione delle liste. Se si desidera che MDaemon lasci le firme nei messaggi di una lista, è possibile configurarlo manualmente impostando la seguente opzione nel file `MDaemon.ini`:

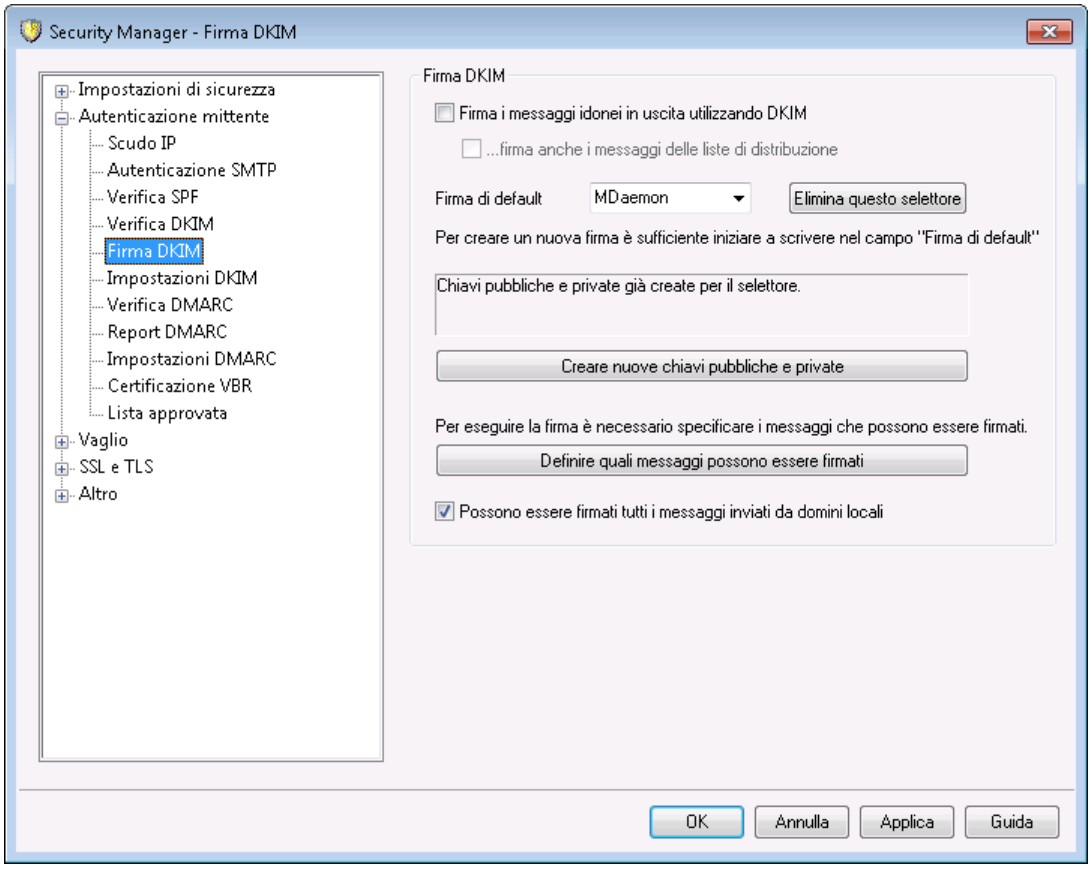
```
[DomainKeys]
```

```
StripSigsFromListMail=No (il valore predefinito è "Yes")
```

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 536
Firma DKIM 539
Impostazioni DKIM 542

4.1.2.4.2 Firma DKIM



Utilizzare le opzioni contenute nella schermata Firma DKIM per configurare MDaemon in modo da firmare i messaggi in uscita idonei utilizzando DKIM e definire i criteri che renderanno idoneo un messaggio. È possibile, inoltre, utilizzare questa finestra per indicare i selettori e generare le chiavi pubbliche e private corrispondenti, compatibili con la specifica DKIM. All'avvio vengono creati automaticamente i valori predefiniti relativi al selettore ("MDaemon"), alla chiave pubblica e alla chiave privata. Tutte le chiavi sono univoche e diverse da un sito all'altro, indipendentemente dal selettore specificato. Per impostazione predefinita, le chiavi sono generate con una profondità in bit sicura di 2048 bit.

Firma DKIM

Firma i messaggi idonei in uscita utilizzando DKIM
Selezionare questa opzione se si desidera applicare ad alcuni messaggi in uscita una firma crittografica utilizzando DomainKeys Identified Mail. Perché venga firmato, un messaggio deve soddisfare i criteri specificati in *Definire quali messaggi possono essere firmati* e deve essere ricevuto da MDaemon per la consegna in una sessione autenticata. Questa azione corrisponde all'opzione "*Firma con il selettore DKIM*" di Filtro contenuti usata per firmare i messaggi.

...firma i messaggi delle liste di distribuzione
Selezionare questa casella di controllo se si desidera applicare una firma crittografica a tutti i messaggi in uscita delle liste di distribuzione. Poiché tutta la posta inviata alle liste di distribuzione viene firmata da MDaemon, per consentire la firma crittografica non è necessario utilizzare l'opzione "*Definire quali messaggi possono essere firmati*".

Per firmare la posta di una lista è necessario applicare il filtro contenuti a ciascun messaggio dopo la ripartizione della lista. Se le liste di distribuzione hanno grandi dimensioni e sono molto attive, ciò può determinare una diminuzione delle prestazioni del server.

Firma di default
Dall'elenco a discesa, scegliere il selettore di cui si desidera utilizzare la chiave pubblica/privata corrispondente quando si firmano i messaggi. Se si desidera creare una nuova coppia di chiavi con un selettore differente, digitare in questo campo il nome del selettore desiderato e selezionare l'opzione "*Creare nuove chiavi pubbliche e private*". Se si desidera firmare alcuni messaggi utilizzando un selettore alternativo, indicare un selettore specifico nell'opzione "*Definire quali messaggi possono essere firmati*" oppure creare una regola di Filtro contenuti utilizzando l'azione "*Firma con il selettore DKIM*".

Elimina questo selettore
Per eliminare un selettore, fare clic su questo pulsante. Seguire le istruzioni visualizzate sullo schermo.

Creare nuove chiavi pubbliche e private
Fare clic su questo pulsante per generare una coppia di chiavi pubbliche o private per il selettore indicato precedentemente. Oltre alla coppia di chiavi viene generato il file `dns_readme.txt` che viene automaticamente aperto. Questo file contiene esempi di dati DKIM che è necessario pubblicare nei record DNS del dominio, elencando i criteri DKIM e la chiave pubblica per il selettore specificato. Il file riporta esempi relativi sia allo stato di verifica che non, indicando se vengono firmati tutti i messaggi o solo alcuni fra quelli provenienti dal proprio dominio. Se si esegue una verifica DKIM o del selettore, sarà necessario utilizzare le informazioni contenute nelle voci di Verifica relative ai criteri o al selettore, a seconda della verifica che si sta eseguendo. In caso contrario, sarà necessario utilizzare le voci di Non verificare.

Tutte le chiavi sono memorizzate in formato PEM. Tutti i selettori e le chiavi vengono salvati nella cartella \MDaemon\Pem con le modalità seguenti:

```
\MDaemon\Pem\<Selettore>\rsa.public - chiave pubblica per il
selettore
\MDaemon\Pem\<Selettore>\rsa.private - chiave privata per il
selettore.
```

I file contenuti in queste cartelle non sono né nascosti né crittografati. Tuttavia, è necessario impedire l'accesso non autorizzato a questi file, contenenti le chiavi crittografiche private RSA. È quindi necessario proteggere queste cartelle e le relative sottocartelle utilizzando gli strumenti disponibili nel sistema operativo in uso.

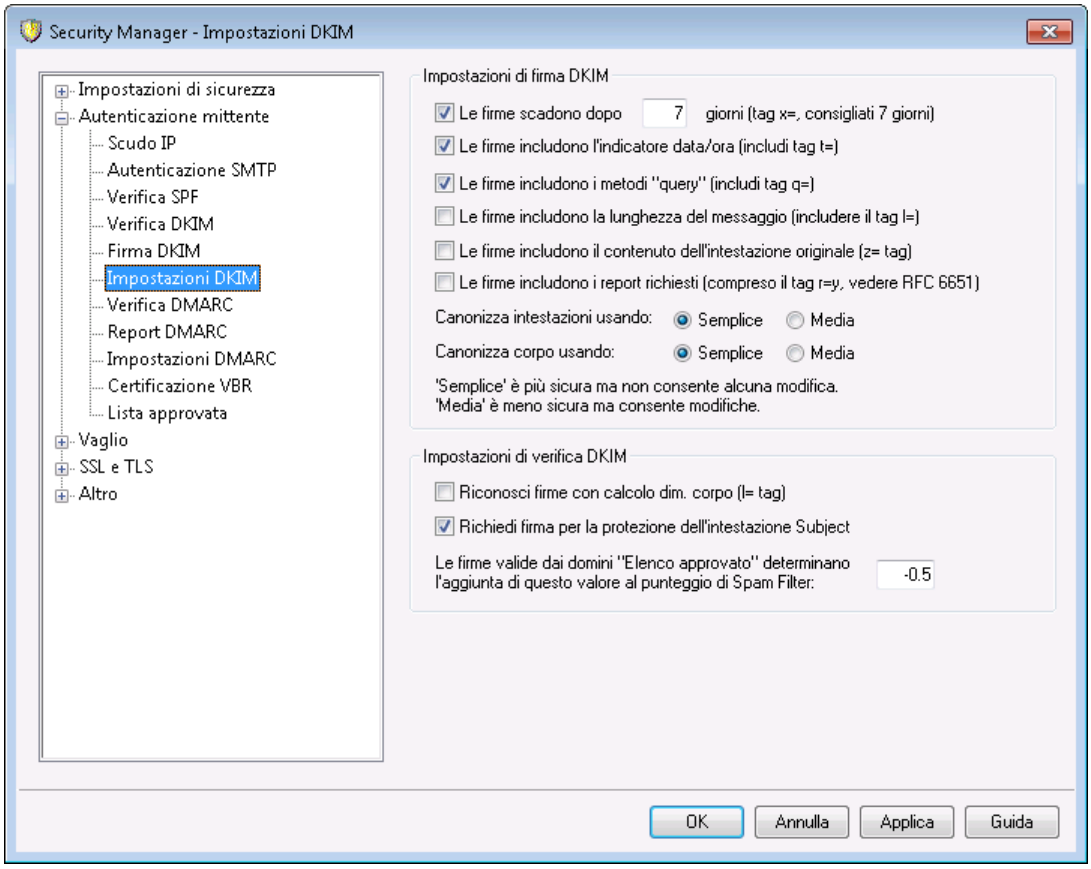
Definire quali messaggi possono essere firmati
Se si è deciso di firmare i messaggi in uscita idonei, fare clic su questo pulsante per modificare il file DKSign.dat che contiene l'elenco dei domini e degli indirizzi che MDaemon usa per stabilire se un messaggio debba essere firmato o meno. È necessario definire i messaggi da firmare in base agli indirizzi presenti in To o From oppure in base ad altre intestazioni del messaggio, ad esempio "Reply-To" o "Sender". È possibile, se si desidera, definire per ciascuna voce il selettore che verrà utilizzato quando si firma un messaggio corrispondente alla voce. Infine, è possibile specificare un dominio facoltativo per la firma da utilizzare nel tag "d=" dell'intestazione della firma. Questa caratteristica risulta utile, ad esempio, quando i messaggi vengono firmati da più sottodomini. In questi casi, è possibile utilizzare il tag "d=" per far sì che i server riceventi ricerchino le chiavi DomainKeys Identified Mail nel record DNS di un solo dominio in modo da gestire tutte le chiavi in un solo record anziché gestire i record separatamente per ciascun sottodominio. Nei domini e negli indirizzi sono accettati i caratteri jolly.

Possono essere firmati tutti i messaggi inviati da domini locali
Utilizzare questa opzione se si desidera che tutti i messaggi provenienti dai domini locali possano essere firmati. Se si utilizza questa opzione non è necessario aggiungere alcun altro dominio alla lista dei messaggi che è possibile firmare, ossia al file DKSign.dat, a meno che non si desideri indicare un selettore o un tag "d=" specifico da utilizzare per firmare i messaggi di un determinato dominio. L'opzione è abilitata per impostazione predefinita.

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 536
Impostazioni DKIM 542
Verifica DKIM 537

4.1.2.4.3 Impostazioni DKIM



Impostazioni firma DKIM

Le firme scadono dopo XX giorni (tag x=, consigliati 7 giorni)
Se si desidera limitare la validità di una firma ad un numero di giorni, attivare questa opzione e indicare il numero di giorni desiderato. I messaggi con le firme scadute non superano mai la verifica. Questa opzione corrisponde al tag "x=" della firma. Per impostazione predefinita, questa opzione è abilitata con il valore preimpostato di 7 giorni.

Le firme includono l'indicatore data/ora (compreso il tag t=)
Se si abilita questa opzione, nella firma viene incluso l'indicatore orario data-ora (tag "t=") di creazione della firma. Per impostazione predefinita, questa opzione è abilitata.

Le firme includono i metodi interrogazione (compreso il tag q=)
Per impostazione predefinita, questa funzione è abilitata. Con questa impostazione la firma include il tag relativo al metodo di interrogazione (ad esempio, "q=dns").

Le firme includono il calcolo della lunghezza del corpo (compreso il tag l=)
Attivare questa opzione se si desidera includere nelle firme DKIM il tag relativo al calcolo della lunghezza del corpo del messaggio.

Le firme includono il contenuto dell'intestazione originale (includi z= tag)
Selezionare questa opzione se si desidera includere nelle firme DKIM il tag "z=". Il tag contiene una copia delle intestazioni originali dei messaggi. Questo potrebbe far aumentare notevolmente la dimensione della firma.

Le firme includono i report richiesti (compreso il tag r=y)
Selezionare questa opzione se si desidera includere il tag r=y nei messaggi firmati. La presenza di questo tag indica che si desidera ricevere report sugli errori AFRF dai server riceventi che riconoscono il tag quando tali server rilevano messaggi che dichiarano di provenire dal proprio dominio ma non superano la verifica DKIM. Per ricevere questi report, tuttavia, è necessario anche configurare un record TXT per i report DKIM nel server DNS del proprio dominio. Vedere l'RFC-6651: *Estensioni di DomainKeys Identified Mail (DKIM) per la segnalazione degli errori* per la sintassi e le istruzioni su come ottenere questo risultato. Poiché richiede modifiche DNS, questa opzione è disattivata per impostazione predefinita.

Canonizzazione

La canonizzazione è un processo tramite il quale le intestazioni e il corpo dei messaggi vengono convertiti in uno standard regolamentato e "normalizzati" prima della creazione di una firma DKIM. Questa operazione è necessaria poiché alcuni server di posta e sistemi di inoltro apportano durante l'elaborazione diverse modifiche al messaggio che possono causare malfunzionamenti se per la preparazione del messaggio non viene utilizzato uno standard "canonico". Al momento, sono disponibili due metodi di regolamentazione per la firma e la verifica DKIM: Semplice e Media. Il metodo semplice è quello più rigido e consente di apportare lievi modifiche al messaggio. Il metodo medio è meno rigido di quello semplice e consente di apportare al messaggio più modifiche, anche non consequenziali.

Canonizza intestazioni utilizzando: Semplice, Media
Si tratta del metodo di canonizzazione utilizzato per le intestazioni dei messaggi al momento della firma. Il metodo Semplice non consente mai alcuna modifica ai campi di intestazione. Il metodo Media consente di convertire i nomi dell'intestazione (non i valori dell'intestazione) in lettere minuscole e uno o più spazi consecutivi in un unico spazio, nonché di apportare altre modifiche non di lieve entità. L'impostazione predefinita è "Semplice".

Canonizza corpo usando: Semplice, Media
Si tratta del metodo di canonizzazione utilizzato per il corpo del messaggio al momento della firma. Quello semplice ignora le righe vuote alla fine del corpo del messaggio e non consente alcuna altra modifica al corpo. Con il metodo Media, le righe vuote alla fine del messaggio sono consentite, gli spazi alla fine delle righe vengono ignorati, tutti gli spazi consecutivi di una riga vengono convertiti in un unico spazio ed è possibile apportare altre piccole modifiche. L'impostazione predefinita è "Semplice".

Impostazioni verifica DKIM

Riconosci firme con calcolo dim. corpo (l= tag)
Quando viene attivata questa opzione, MDaemon riconoscerà il tag per il calcolo della dimensione del corpo trovato in una firma DKIM di un messaggio in entrata. Quando il calcolo della dimensione del corpo supera il valore contenuto nel tag,

MDaemon eseguirà la verifica solo in base al valore indicato nel tag e il resto del messaggio non verrà verificato. Ciò indica che al messaggio sono stati aggiunti altri dati e che, di conseguenza, la porzione non verificata può essere considerata sospetta. Se il calcolo della lunghezza effettiva del messaggio è inferiore al valore contenuto nel tag, la firma non supera la verifica, ossia darà come risultato "`Fail`". Ciò indica che una parte del messaggio è stata eliminata per cui il calcolo della lunghezza del messaggio risulta inferiore al valore indicato nel tag.

Richiedi firma per la protezione dell'intestazione Subject
Abilitare questa opzione se si desidera che la firma DKIM dei messaggi in entrata applichi la protezione all'intestazione Subject.

Le firme valide da domini "Elenco approvato" aggiungono questo al punteggio Spam Filter:
Se il dominio individuato tramite la firma si trova nell'elenco approvato 566, il valore indicato in questo campo viene aggiunto al punteggio spam di ogni messaggio firmato mediante DKIM che supera la verifica. Quando la firma di un messaggio viene verificata, ma il dominio non si trova nell'elenco approvato, il punteggio spam non viene modificato e il superamento della verifica non incide sul punteggio. Tuttavia, al messaggio continuano ad essere applicati l'elaborazione e il punteggio normali di Spam Filter.

In genere, il valore specificato in questo campo deve essere un numero negativo in modo da diminuire il punteggio di spam per i messaggi contenenti firme crittografiche valide quando il dominio individuato mediante la firma si trova nell'elenco approvato 566. Il valore predefinito per questa opzione è `-0,5`.

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 536
Verifica DKIM 537
Firma DKIM 539

4.1.2.5 DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) è una specifica progettata per ridurre gli abusi tramite i messaggi e-mail, come messaggi di phishing e spam in arrivo che dissimulano le proprie origini mediante la contraffazione dell'intestazione `From:` del messaggio. DMARC consente ai proprietari di dominio di utilizzare il sistema DNS (Domain Name System) per informare i server riceventi dei criteri DMARC, che specificano in che modo tali server devono gestire i messaggi che dichiarano di provenire dal proprio dominio ma non possono essere autenticati come messaggi effettivamente inviati da tale dominio. Questi criteri, che vengono recuperati dal server ricevente tramite un'interrogazione DNS durante l'elaborazione del messaggio in arrivo, possono indicare al server di porre in quarantena o rifiutare i messaggi non in linea con i criteri o di non intraprendere alcuna azione (lasciando ad esempio che il messaggio venga elaborato normalmente). Oltre ai criteri, il record DNS DMARC del

dominio può anche contenere richieste the indicano al server di inviare i report DMARC a un utente, definendo il numero di messaggi in arrivo che dichiarano di provenire da tale dominio, specificando se hanno superato o meno le procedure di autenticazione e fornendo informazioni dettagliate su eventuali errori. Le funzioni di generazione di report di DMARC possono essere utili per determinare l'efficacia delle procedure di autenticazione dei messaggi e-mail e la frequenza con cui il nome del dominio viene utilizzato nei messaggi contraffatti.

Nella sezione Autenticazione mittente della finestra di dialogo Impostazioni di sicurezza sono disponibili schermate per la configurazione delle funzioni di generazione di report e verifica DMARC di MDaemon: Verifica DMARC, Report DMARC e Impostazioni DMARC.

Verifica DMARC 552

MDaemon, come parte del processo di verifica DMARC, esegue un'interrogazione DNS DMARC sul dominio presente nell'intestazione `From:` di ciascun messaggio in arrivo. Questa operazione viene eseguita per determinare se il dominio utilizza DMARC e, in tal caso, per recuperare il relativo record DNS DMARC 546, che contiene i criteri e altre informazioni correlate alla specifica DMARC. Inoltre, DMARC utilizza SPF 533 e DKIM 537 per convalidare ciascun messaggio e richiede che il messaggio superi almeno uno di questi controlli per superare la verifica DMARC. Se supera la verifica, il messaggio procederà normalmente con le fasi successive dei processi di filtraggio e recapito di MDaemon. Se non supera la verifica, il messaggio verrà gestito in base a una combinazione dei criteri DMARC del dominio e della modalità di configurazione di MDaemon per la gestione di tali messaggi.

Se un messaggio non supera la verifica DMARC e il dominio DMARC contiene il criterio "`p=none`", non verranno intraprese contromisure e si proseguirà con la normale elaborazione del messaggio. Al contrario, quando il dominio DMARC contiene i criteri restrittivi "`p=quarantine`" o "`p=reject`", MDaemon può filtrare automaticamente il messaggio nella cartella Spam (posta indesiderata) del destinatario. È inoltre possibile scegliere di configurare MDaemon in modo da rifiutare completamente il messaggio che non ha superato la verifica quando il dominio utilizza il criterio "`p=reject`". Oltre ai messaggi che non hanno superato la verifica con criteri restrittivi, MDaemon inserirà l'intestazione "`X-MDDMARC-Fail-policy: quarantine`" o "`X-MDDMARC-Fail-policy: reject`", a seconda dei criteri definiti. Questo consente di utilizzare la funzione Filtro contenuti per eseguire alcune azioni in base alla presenza di tali intestazioni, come l'invio del messaggio a una specifica cartella per un ulteriore controllo.

L'opzione Verifica DMARC è attivata per impostazione predefinita ed è consigliata per la maggior parte delle configurazioni MDaemon.

Report DMARC 555

Quando MDaemon esegue interrogazioni sul server DNS relative a un record DMARC, il record potrebbe contenere diversi tag che indicano che il proprietario del dominio desidera ricevere report aggregati o sugli errori DMARC relativi ai messaggi che dichiarano di provenire da tale dominio. Le opzioni nella schermata Report DMARC consentono di indicare se si desidera inviare o meno i tipi di report richiesti e per specificare i metadati che tali report devono contenere. I report aggregati vengono inviati quotidianamente in corrispondenza della mezzanotte UTC, mentre i report sugli errori vengono inviati per ciascun messaggio, quando si verificano gli incidenti che determinano tali report. I report vengono sempre inviati come allegati di file XML

compressi. Sono disponibili diversi strumenti di analisi online che possono facilitarne la visualizzazione da parte dei destinatari.

Per impostazione predefinita, MDaemon non invia report aggregati o sugli errori. Se si desidera inviare uno di questi tipi di report, attivare le opzioni corrispondenti nella schermata Report DMARC.

Impostazioni DMARC 559

La schermata Impostazioni DMARC contiene diverse opzioni per l'inclusione di informazioni specifiche nei report DKIM, la registrazione di record DNS DMARC e l'aggiornamento del file dei suffissi pubblici utilizzato da MDaemon per DMARC.

Verifica DMARC e liste di distribuzione

Poiché lo scopo della specifica DMARC è assicurare che il dominio presente nell'intestazione `From:` di un messaggio non sia stato contraffatto, è necessario che al server di invio sia consentito inviare messaggi per conto di tale dominio. Questo può rappresentare un problema per le liste di distribuzione, in quanto le liste di distribuzione in genere distribuiscono i messaggi per contro dei membri delle liste da domini esterni, lasciando invariata l'intestazione `From:`. Ne consegue che, quando un server ricevente tenta di utilizzare la verifica DMARC in uno di questi messaggi, è possibile che il messaggio sia stato inviato da un server che ufficialmente non appartiene al dominio dell'intestazione `From:`. Se il dominio DMARC utilizza un criterio DMARC restrittivo, il messaggio potrebbe essere posto in quarantena o persino rifiutato dal server ricevente. In alcuni casi, questo potrebbe anche causare la rimozione del destinatario dalla lista dei membri. Per aggirare questo problema, quando MDaemon rileva che un messaggio per una lista proviene da un dominio con un criterio DMARC restrittivo, MDaemon sostituirà l'intestazione `From:` del messaggio con l'indirizzo della lista di distribuzione. In alternativa, è possibile configurare MDaemon in modo da rifiutare qualsiasi messaggio per una lista quando proviene da un dominio con criteri restrittivi. Questa seconda opzione renderebbe impossibile l'invio di un messaggio alla lista da parte di un utente appartenente a un dominio con criteri restrittivi. L'opzione per sostituire l'intestazione `From:` è disponibile nella schermata Intestazioni 288 dell'editor delle liste di distribuzione. L'opzione per rifiutare i messaggi è disponibile nella schermata Impostazioni 284.

Utilizzo di DMARC per i domini MDaemon

Se si desidera utilizzare DMARC per uno dei domini di appartenenza, ad esempio nel caso in cui si desideri che i server di posta riceventi che supportano DMARC utilizzino questa specifica per verificare i messaggi che dichiarano di provenire dal proprio dominio, è necessario innanzitutto assicurarsi di creare record DNS SPF e DKIM formattati correttamente per il dominio. Per utilizzare DMARC, è necessario che almeno una di queste opzioni funzioni in modo appropriato. Se si utilizza DKIM, è necessario configurare le opzioni di Firma DKIM 539 di MDaemon per firmare i messaggi del dominio. È necessario inoltre creare un record DNS DMARC per il dominio. Eseguendo un'interrogazione sul server DNS relativa a questo record `TXT` in formato speciale, il server ricevente può determinare i criteri DMARC e diversi parametri opzionali, ad esempio è possibile specificare il metodo di autenticazione utilizzato, se si desidera o meno ricevere report aggregati, l'indirizzo e-mail a cui i report devono essere inviati e altre opzioni.

Dopo aver configurato correttamente DMARC e aver iniziato a ricevere i report XML DMARC, è possibile leggere questi report e diagnosticare potenziali problemi mediante l'uso di un'ampia gamma di strumenti online. Per comodità, è possibile anche utilizzare lo strumento DMARC Reporter, disponibile nella cartella \MDaemon\App\. Consultare il file DMARCReporterReadMe.txt per le istruzioni relative all'uso del file.

Definizione di un record di risorse TXT DMARC

Di seguito viene riportata una panoramica dei componenti di base più comunemente utilizzati di un record DMARC. Per ulteriori informazioni o per informazioni su configurazioni più avanzate, visitare il seguente sito: www.dmarc.org.

Campo Proprietario

Il campo Proprietario (denominato anche "Nome" o "di sinistra") del record di risorse DMARC deve essere sempre nel formato **_dmarc** o può essere espresso nel formato **_dmarc.domain.name** se si desidera specificare il dominio o il sottodominio a cui il record si applica.

Esempio:

Record DMARC per il dominio **esempio.com**

```
_dmarc IN TXT "v=DMARC1;p=none"
```
Questo record è applicabile ai messaggi e-mail provenienti da utente@esempio.com o qualsiasi sottodominio di esempio.com, come utente@supporto.esempio.com, utente@posta.supporto.esempio.com e così via.

```
_dmarc.support.esempio.com IN TXT "v=DMARC1;p=none"
```
Questo record è applicabile solo ai messaggi e-mail inviati da utente@supporto.esempio.com, non ai messaggi e-mail provenienti, ad esempio, da utente@esempio.com.

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
Questo record è applicabile ai messaggi e-mail inviati da: utente@supporto.esempio.com, utente@a.supporto.esempio.com, utente@a.b.supporto.esempio.com e così via.

Tag e valori dei record DMARC

Tag obbligatori

Tag	Valore	Note
v=	**DMARC1**	Tag relativo alla versione, il primo tag nella porzione di testo del record specifica di DMARC. Anche se i valori degli altri tag DMARC non rilevano la distinzione tra lettere maiuscole e minuscole, il valore del tag **v=** deve essere scritto in caratteri maiuscoli: **DMARC1**. Esempio:

		`_dmarc IN TXT "v=DMARC1;p=none"`
p=	**nessuno** **quarantine** **reject**	Tag relativo ai criteri, il secondo tag nel record DMARC, successivo al tag **v=**. **p=none** indica che il server ricevente non deve intraprendere alcuna azione in base ai risultati dell'interrogazione DMARC. I messaggi che non superano il controllo DMARC non devono essere posti in quarantena né rifiutati per questo motivo. I messaggi possono essere posti in quarantena o rifiutati per altri motivi, ad esempio nel caso in cui non superino i test di filtro spam o altri controlli di sicurezza non correlati a DMARC. L'utilizzo di **p=none**è talvolta definito "monitoraggio" o "modalità di monitoraggio" in quanto è possibile utilizzare questo criterio con il tag **rua=** per ricevere report aggregati dai domini dei destinatari relativi ai propri messaggi, ma tali messaggi non verranno penalizzati dai domini qualora non superino il controllo DMARC. Questo criterio deve essere utilizzato fino a quando l'implementazione DMARC non è stata completamente testata e non si è pronti per passare a un criterio più restrittivo, come **p=quarantine**. **p=quarantine** è il criterio da utilizzare quando si desidera che altri server di posta gestiscano un messaggio come sospetto quando la relativa intestazione **From:** indica la provenienza del messaggio ma il messaggio non supera il controllo DMARC. In base ai criteri locali del server, l'utilizzo di questo criterio può determinare la necessità di sottoporre il messaggio a un ulteriore controllo, spostandolo nella cartella spam del destinatario, instradandolo a un server differente o intraprendendo un altro tipo di azione. **p=reject** indica che si desidera che il server ricevente rifiuti tutti i messaggi che non superano la verifica DMARC. Alcuni server, tuttavia, possono comunque accettare questi messaggi, ma i messaggi potrebbero essere posti in quarantena o sottoposti a ulteriore controllo. Questo è il criterio più restrittivo e, è in generale, è consigliabile non utilizzarlo, a meno che non si conoscano con certezza assoluta i criteri dei messaggi e-mail e i tipi di messaggi o servizi che si desidera vengano utilizzati dagli account. Se, ad esempio, si desidera consentire agli utenti di unirsi a liste di distribuzione di terze parti, usufruire dei servizi di inoltro posta, utilizzare funzioni di condivisione sui siti Web o altre funzionalità simili, l'utilizzo di **p=reject** potrebbe determinare quasi certamente il rifiuto di alcuni messaggi legittimi. L'uso di questo criterio potrebbe inoltre causare la rimozione o

		l'esclusione automatica di alcuni utenti da specifiche liste di distribuzione. Esempio: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@esempio.net"`

Tag opzionali
Tutti i tag elencati di seguito sono opzionali. Se uno di questi tag non viene utilizzato in un record, verrà utilizzato il relativo valore predefinito.

Tag	Valore	Note
sp=	**nessuno** **quarantine** **reject** — **Valore predefinito:** Se **sp=** non viene utilizzato, il tag **p=** si applica al dominio e ai sottodomini.	Questo tag viene utilizzato per specificare un criterio da utilizzare per i sottodomini del dominio a cui il record DMARC si applica. Se, ad esempio, questo tag viene utilizzato in un record che copre il dominio esempio.com, il criterio designato nel tag **p=** sarà applicabile ai messaggi provenienti da esempio.com, mentre il criterio designato nel tag **sp=** sarà applicabile ai messaggi provenienti dai sottodomini di esempio.com, come posta.esempio.com. Se questo tag viene escluso dal record, il tag **p=** verrà applicato al dominio e ai relativi sottodomini. Esempio: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	Elenco separato da virgola di indirizzi e-mail a cui i report aggregati DMARC devono essere inviati. Gli indirizzi devono essere immessi come URI nel seguente formato: **mailto:utente@esempio.com**
	—
	Valore predefinito: none
	Se questo tag non viene utilizzato, non verranno inviati report aggregati.
		Questo tag indica che si desidera ricevere i report aggregati DMARC dai server che ricevono messaggi che dichiarano nell'intestazione **From:** di provenire da un mittente nel proprio dominio. Specificare uno o più indirizzi e-mail come URI nel seguente formato: **mailto:utente@esempio.com**, separando più URI con virgole.
		Esempio:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:utente01@esempio.com, mailto:utente02@esempio.com"`
		In genere, questi indirizzi appartengono al dominio coperto da questo record. Se si desidera inviare i report a un indirizzo appartenente a un altro dominio, il file di zona DNS di tale dominio deve anche contenere un record DMARC speciale che indica che accetterà i report DMARC per il dominio.
		Record di esempio in esempio.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:utente-non-locale@esempio.net"`
		Record obbligatorio in esempio.net:
		`esempio.com._report._dmarc TXT "v=DMARC1"`

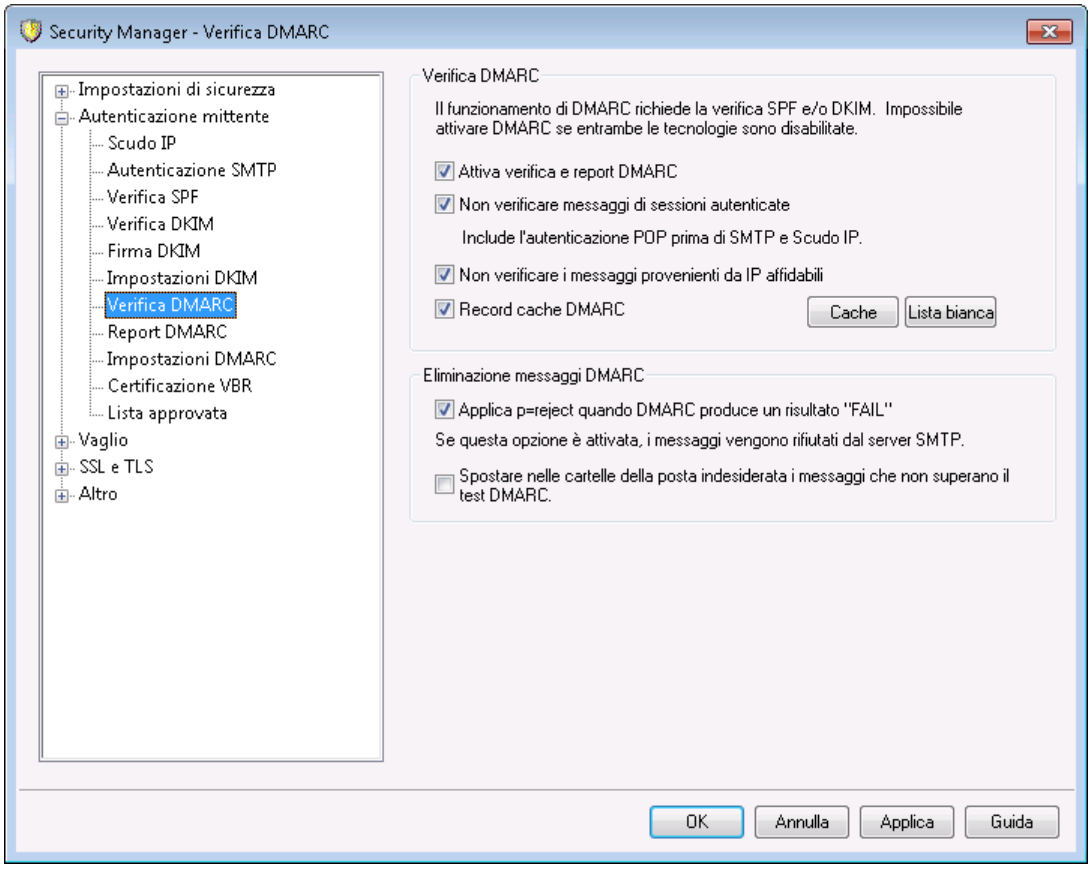
ruf=	Elenco separato da virgola di indirizzi e-mail a cui i report sugli errori DMARC devono essere inviati. Gli indirizzi devono essere immessi come URI nel seguente formato: **mailto:utente@esempio.com**
	—
	Valore predefinito: none
	Se questo tag non viene utilizzato, non verranno inviati report sugli errori.
		Questo tag indica che si desidera ricevere i report sugli errori DMARC dai server che ricevono messaggi che dichiarano nell'intestazione **From:** di provenire da un mittente nel proprio dominio, una volta soddisfatte le condizioni specificate nel tag **fo=**. Per impostazione predefinita, se non viene specificato alcun tag **fo=**, i report sugli errori vengono inviati qualora il messaggio non superi tutti i controlli di verifica DMARC (ad esempio non supera le verifiche SPF e DKIM). Specificare uno o più indirizzi e-mail come URI nel seguente formato: **mailto:utente@esempio.com**, separando più URI con virgole.
		Esempio:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-errori@esempio.com"`
		In genere, questi indirizzi appartengono al dominio coperto da questo record. Se si desidera inviare i report a un indirizzo appartenente a un altro dominio, il file di zona DNS di tale dominio deve anche contenere un record DMARC speciale che indica che accetterà i report DMARC per il dominio.
		Record di esempio in esempio.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:utente-non-locale@esempio.net"`
		Record obbligatorio in esempio.net:
		`esempio.com._report._dmarc TXT "v=DMARC1"`

Per ulteriori informazioni sulla specifica DMARC, visitare il seguente sito: www.dmarc.org.

Vedere:

Verifica DMARC 552
Report DMARC 555
Impostazioni DMARC 559
Lista di distribuzione » Impostazioni 284
Lista di distribuzione » Intestazioni 288

4.1.2.5.1 Verifica DMARC



Verifica DMARC

Attiva verifica e report DMARC
Quando questa opzione è selezionata, MDaemon eseguirà query DMARC DNS sul dominio indicato nell'intestazione `From:` dei messaggi in arrivo e invierà report di aggregazione e resoconti di errori se così configurato nella schermata Report DMARC 555. DMARC utilizza le verifiche SPF 533 e DKIM 537 per convalidare i messaggi. Pertanto, per utilizzare DMARC, è necessario attivare almeno una di queste funzioni. L'opzione Attiva verifica e report DMARC è attivata per impostazione predefinita ed è consigliabile utilizzarla nella maggior parte delle configurazioni MDaemon.

La disattivazione del supporto per DMARC potrebbe consentire un aumento del numero di messaggi spam, di phishing o altri tipi di messaggi contraffatti inviati agli utenti. Potrebbe inoltre causare il rifiuto di alcuni messaggi delle liste di distribuzione da parte di altri server nonché la rimozione di alcuni membri dalle liste. È consigliabile disattivare la specifica DMARC solo se si è assolutamente certi che non sia necessario utilizzarla.

Non verificare i messaggi da sessioni autenticate
Per impostazione predefinita, MDaemon non eseguirà interrogazioni DMARC sui messaggi ricevuti tramite una sessione autenticata. Le sessioni autenticate includono quelle verificate mediante l'autenticazione SMTP 531, POP prima di SMTP 525 o Scudo IP 528.

Non verificare i messaggi provenienti da IP affidabili
Per impostazione predefinita, MDaemon non eseguirà interrogazioni DMARC sui messaggi provenienti da un indirizzo IP affidabile 527.

Record cache DMARC
Per impostazione predefinita, MDaemon memorizzerà nella cache i dati dei record DMARC rilevati durante la ricerca DNS. Memorizzando momentaneamente nella cache queste informazioni, è possibile aumentare l'efficienza di elaborazione dei successivi messaggi simili provenienti dallo stesso dominio.

Cache
Questo pulsante consente di aprire il file della cache di DMARC, in cui sono elencati tutti i record DMARC correntemente memorizzati nella cache.

Elenco esenzioni
Fare clic su questo pulsante per aprire la finestra l'elenco esenzioni di DMARC. I messaggi provenienti da un qualsiasi indirizzo IP presente in questo elenco non sono soggetti a verifica DMARC.

La verifica DMARC applica anche Certificazione VBR 563 ed Elenco approvato 566, che possono disporre delle esenzioni in base a identificatori DKIM e percorsi SPF verificati da fonti ritenute affidabili. Se, ad esempio, arriva un messaggio che non supera la verifica DMARC ma ha una firma DKIM valida da un dominio sull'elenco approvato, il messaggio non è soggetto ai criteri di DMARC (ovvero, il messaggio viene trattato come se il criterio fosse "p=none"). Lo stesso accade se la verifica del percorso SPF corrisponde a un dominio presente nell'elenco approvato.

Eliminazione messaggi DMARC

Applica p=reject quando DMARC produce un risultato "FAIL"
Per impostazione predefinita questa opzione è attiva, quindi MDaemon applica il criterio DMARC `p=reject` qualora il dominio `From:` di un messaggio applichi tale criterio nel relativo record DMARC e il messaggio non superi la verifica DMARC. I messaggi che non superano la verifica DMARC vengono rifiutati durante la sessione SMTP.

Quando l'opzione è disattivata e il messaggio non supera la verifica DMARC, MDaemon inserirà l'intestazione "`X-MDDMARC-Fail-policy: reject`" nel messaggio anziché rifiutare di accettarlo. In tal caso, è possibile utilizzare la funzione Filtro contenuti per eseguire alcune azioni in base alla presenza di tale intestazione, come l'invio del messaggio a una specifica cartella per un ulteriore controllo. Inoltre, è

possibile utilizzare l'opzione "*Filtra messaggi che non superano il test DMARC nelle cartelle spam*" per far sì che il messaggio venga inserito nella cartella spam del destinatario.

Anche se si lascia disattivata questa opzione, il messaggio potrebbe essere rifiutato per altri motivi non correlati a DMARC, ad esempio nel caso in cui si sia impostato un punteggio di Spam Filter 692 al di sopra della soglia consentita.

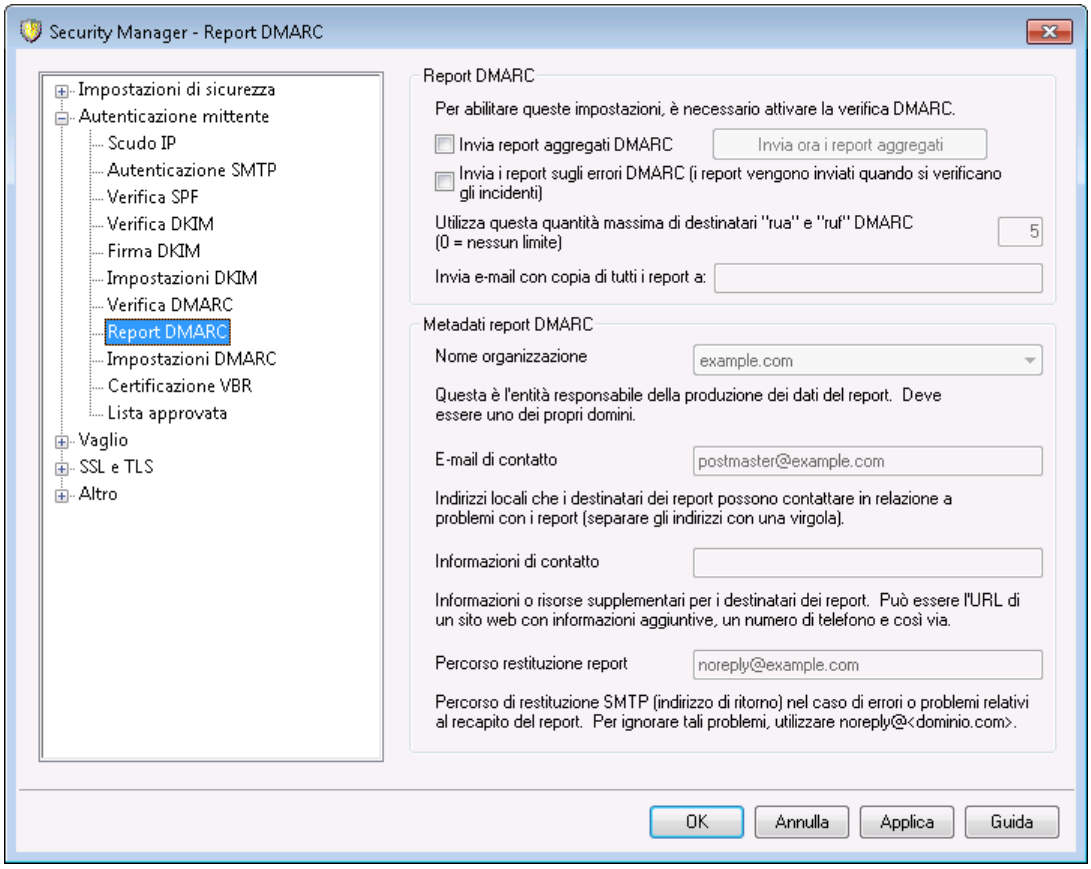
Filtra messaggi che non superano il test DMARC nelle cartelle spam
Attivare questa opzione se si desidera filtrare automaticamente i messaggi nella cartella spam (posta indesiderata) dell'account del destinatario ogni volta che un messaggio non supera il test DMARC. Se questa cartella non esiste ancora per l'utente, MDaemon ne creerà una quando necessario.

Quando attivata, questa opzione viene applicata solo quando il dominio From: applica criteri DMARC restrittivi (ad esempio p=quarantine o p=reject). Quando il dominio applica un criterio p=none, questo significa che il dominio sta solo monitorando DMARC e non occorre intraprendere contromisure.

Vedere:

DMARC 544
Report DMARC 555
Impostazioni DMARC 559
Lista di distribuzione » Impostazioni 284
Lista di distribuzione » Intestazioni 288
Lista approvata 566

4.1.2.5.2 Report DMARC



Quando MDaemon esegue interrogazioni sul server DNS relative a un record DMARC, il record potrebbe contenere diversi tag che indicano che il proprietario del dominio desidera ricevere report DMARC relativi ai messaggi che dichiarano di provenire da tale dominio. Le opzioni nella schermata Report DMARC consentono di indicare se si desidera inviare o meno report sugli errori o aggregati DMARC ai domini i cui record DMARC richiedono tali report e per specificare i metadati che i report devono contenere. Le opzioni in questa schermata sono disponibili solo quando l'opzione "*Attiva verifica e report DMARC*" è attivata nella schermata Verifica DMARC 552. Inoltre, la specifica DMARC richiede l'uso di STARTTLS 587 ogni volta che viene offerta dai destinatari dei report. È opportuno quindi attivare STARTTLS, se possibile.

Report DMARC

Invia report aggregati DMARC
Attivare questa opzione se si desidera inviare report aggregati DMARC ai domini che li richiedono. Quando un'interrogazione DNS DMARC sul dominio `From:` di un messaggio in arrivo indica che il relativo record DMARC contiene il tag "`rua=`" (ad esempio `rua=mailto:dmarc-reports@esempio.com`), questo significa che il proprietario del dominio desidera ricevere report aggregati DMARC. MDaemon pertanto memorizzerà le informazioni DMARC sul dominio e sui messaggi in arrivo che dichiarano di provenire da tale dominio. Registrerà gli indirizzi e-mail a cui il report aggregato deve essere inviato, i metodi di verifica utilizzati per ciascun messaggio (SPF, DKIM o entrambi), l'esito ottenuto, ad esempio se il messaggio ha superato o meno i controlli, il server

di invio, il relativo indirizzo IP, i criteri DMARC applicati e così via. Successivamente, ogni giorno in corrispondenza della mezzanotte UTC, MDaemon utilizzerà i dati memorizzati per generare il report di ciascun dominio e lo invierà agli indirizzi specificati. Una volta inviati i report, i dati DMARC memorizzati vengono cancellati e MDaemon avvia nuovamente l'intero processo.

MDaemon non supporta il tag di intervallo tra i report DMARC ("`ri=`") per i report aggregati. MDaemon invierà i report aggregati ogni giorno, in corrispondenza della mezzanotte UTC, a qualsiasi dominio per il quale sono stati compilati i dati DMARC a partire dall'ultima generazione e dall'ultimo invio dei report DMARC.

Invia ora i report aggregati
Fare clic su questo pulsante se si desidera generare e inviare un batch di report aggregati dai dati DMARC correntemente memorizzati anziché attendere che queste operazioni vengano eseguite automaticamente da MDaemon al successivo evento che si verifica in corrispondenza della mezzanotte UTC. I report vengono inviati immediatamente e i dati DMARC memorizzati vengono cancellati, come accade ogni giorno in corrispondenza della mezzanotte UTC. MDaemon inizia quindi a memorizzare nuovamente i dati DMARC fino al successivo evento che si verifica in corrispondenza della mezzanotte UTC o fino a quando non si fa di nuovo clic sul pulsante.

Poiché, per poter inviare i report aggregati e cancellare automaticamente i dati DMARC memorizzati, è necessario che MDaemon sia in esecuzione in corrispondenza della mezzanotte UTC, se a tale ora MDaemon è inattivo, non verrà generato alcun report e i dati DMARC non verranno cancellati. La raccolta dei dati DMARC viene ripresa a ogni nuova esecuzione del sistema MDaemon, ma i report non verranno generati e i dati non verranno cancellati fino al successivo evento in corrispondenza della mezzanotte UTC o fino a quando non si fa clic sul pulsante "*Invia ora i report aggregati*".

Invia i report sugli errori DMARC (i report vengono inviati quando si verificano gli incidenti)
Attivare questa opzione se si desidera inviare report sugli errori DMARC ai domini che li richiedono. Quando un'interrogazione DNS DMARC sul dominio `From:` di un messaggio in arrivo indica che il relativo record DMARC contiene il tag "`ruf=`" (ad esempio `ruf=mailto:dmarc-failure@esempio.com`), questo significa che il proprietario del dominio desidera ricevere report sugli errori DMARC. A differenza dei report aggregati, questi report vengono creati in tempo reale, quando si verificano gli incidenti che li determinano, e contengono dettagli particolareggiati su tutti gli incidenti e i problemi che hanno causato l'errore. Questi report possono essere utilizzati per l'analisi forense dagli amministratori del dominio per correggere eventuali problemi relativi alla configurazione del sistema e-mail o identificare altri tipi di problemi, come attacchi di phishing in corso.

Il tipo di errore che determinerà la generazione di un report sugli errori dipende dal valore del tag "fo=" nel record DMARC del dominio. Per impostazione predefinita, un report sugli errori viene generato solo se tutti i controlli DMARC sottostanti hanno esito negativo (ad esempio le verifiche SPF e DKIM hanno entrambe esito negativo), ma i domini possono utilizzare diversi valori del tag "fo=" per indicare che desiderano ricevere i report solo in determinate condizioni, ad esempio solo se la verifica SPF ha esito negativo, solo se la verifica DKIM ha esito negativo, se entrambe le verifiche hanno esito negativo o in presenza di qualche altra combinazione. Di conseguenza, si possono generare più report sugli errori da un singolo messaggio, in base al numero dei destinatari nel tag "ruf=" del record DMARC, al valore del tag "fo=" e al numero di errori di autenticazione indipendenti rilevati durante l'elaborazione del messaggio. Se si desidera limitare il numero di destinatari a cui MDaemon deve inviare uno specifico report, utilizzare l'opzione "*Utilizza questa quantità massima di destinatari "rua" e "ruf" DMARC*" riportata di seguito.

Per il formato dei report, MDaemon utilizzerà solo il tag rf=afrf (Report sugli errori di autenticazione mediante l'uso del formato di segnalazione degli abusi), ovvero l'impostazione predefinita di DMARC. Tutti i report vengono inviati in questo formato, anche se il record DMARC di un dominio contiene il tag rf=iodef.

Per supportare i report sugli errori DMARC, MDaemon fornisce il supporto completo per: RFC 5965: Un formato estensibile per i report di feedback sulla posta elettronica, RFC 6591: Report sugli errori di autenticazione mediante l'uso del formato di segnalazione degli abusi, RFC 6652: Report sugli errori di autenticazione del Sender Policy Framework (SPF) mediante l'uso del formato di segnalazione degli abusi, RFC 6651: Estensioni di DomainKeys Identified Mail (DKIM) per la segnalazione degli errori e RFC 6692: Porte di origine nei report in formato ARF (formato di segnalazione degli abusi).

Quando il tag "fo=" di DMARC richiede la generazione di report per gli errori SPF, MDaemon invia i report sugli errori SPF in base a RFC 6522. Ne consegue che le estensioni della specifica devono essere presenti nel record SPF del dominio. I report sugli errori SPF non vengono inviati indipendentemente dall'elaborazione DMARC o in assenza delle estensioni RFC 6522.

Quando il tag "fo=" di DMARC richiede la generazione di report per gli errori DKIM, MDaemon invia i report sugli errori DKIM in base a RFC 6651. Pertanto, le estensioni della specifica devono essere presenti nel campo di intestazione DKIM-Signature e il dominio deve pubblicare un record TXT dei report DKIM valido nel DNS. I report sugli errori DKIM non vengono inviati indipendentemente dall'elaborazione DMARC o in assenza delle estensioni RFC 6651.

Utilizza questa quantità massima di destinatari "rua" e "ruf" DMARC (0 = nessun limite)
Se si desidera limitare il numero di destinatari a cui MDaemon deve inviare uno specifico report aggregato DMARC o un report sugli errori DMARC, specificare il numero massimo in questa opzione. Se un tag "`rua=`" o "`ruf=`" di un record DMARC contiene un numero di indirizzi maggiore rispetto al limite specificato, MDaemon invierà uno specifico report agli indirizzi elencati, in ordine, fino a quando non viene raggiunto il numero massimo di indirizzi. L'impostazione predefinita non prevede alcun limite.

Invia una copia di tutti i report via e-mail a:
Immettere uno o più indirizzi e-mail separati da virgole in questo campo per inviare una copia di tutti i report aggregati DMARC e dei report sugli errori DMARC (fo=0 oppure fo=1 solo).

Metadati report DMARC

Utilizzare queste opzioni per specificare i metadati della propria azienda o organizzazione, che verranno inclusi nei report DMARC inviati.

Nome organizzazione
Questa è l'entità responsabile della produzione dei report DMARC. Deve essere uno dei propri domini MDaemon. Scegliere il dominio nell'elenco a discesa.

E-mail di contatto
Utilizzare questa opzione per specificare gli indirizzi e-mail locali che i destinatari dei report possono contattare in relazione a problemi con i report. Separare indirizzi multipli con una virgola.

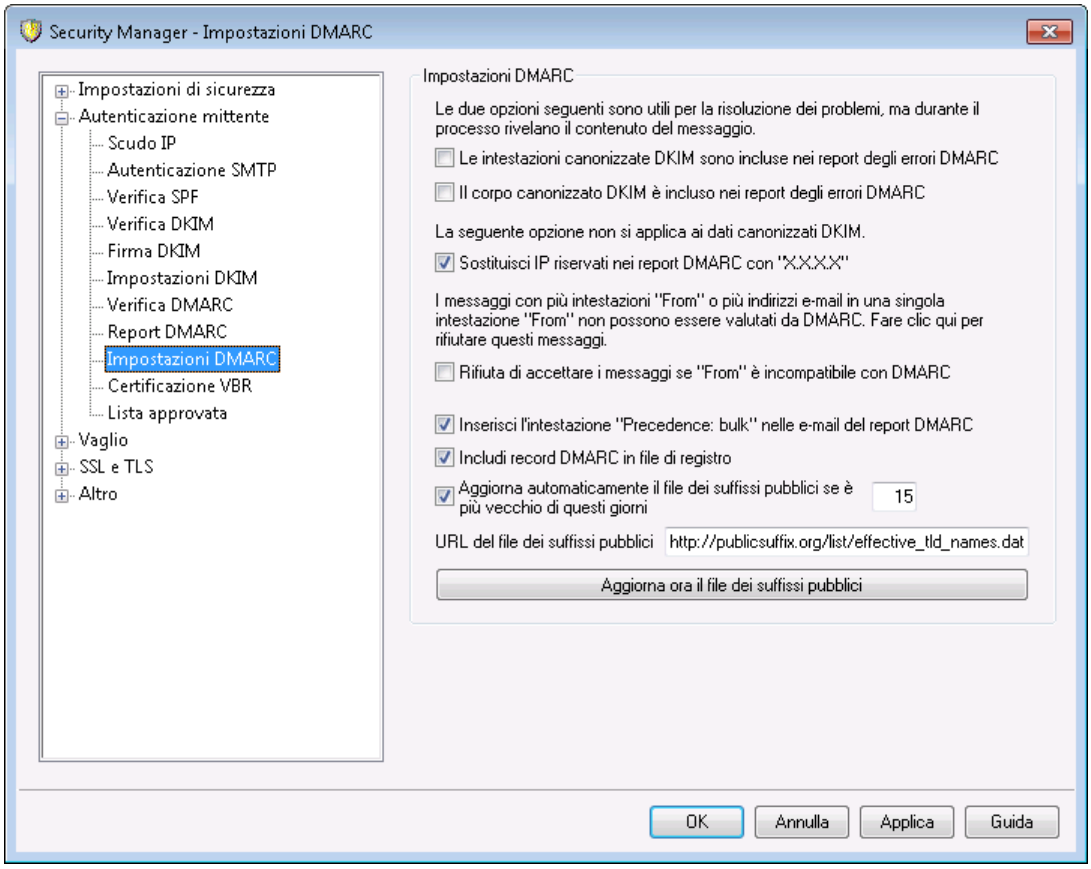
Informazioni di contatto
Utilizzare questa opzione per includere informazioni di contatto supplementari per i destinatari dei report, quali sito Web, numero di telefono e così via.

Percorso restituzione report
Si tratta del percorso di restituzione SMTP (indirizzo di ritorno) utilizzato per i messaggi relativi ai report inviati da MDaemon, nel caso in cui si verifichino problemi di recapito. Per ignorare tali problemi, utilizzare `noreply@<dominio.com>`.

Vedere:

DMARC 544
Verifica DMARC 552
Impostazioni DMARC 559

4.1.2.5.3 Impostazioni DMARC



Impostazioni DMARC

Le intestazioni canonizzate DKIM sono incluse nei report degli errori DMARC
Attivare questa opzione se si desidera includere le intestazioni canonizzate 542 DKIM nei report sugli errori 555 DMARC. È disabilitata per impostazione predefinita.

Il corpo canonizzato DKIM è incluso nei report degli errori DMARC
Attivare questa opzione se si desidera includere il corpo canonizzato 542 DKIM nei report sugli errori 555 DMARC. È disabilitata per impostazione predefinita.

Sostituisci IP riservati nei report DMARC con "X.X.X.X"
Per impostazione predefinita, MDaemon sostituisce gli indirizzi IP riservati nei report DMARC con "X.X.X.X". Disattivare questa opzione se si desidera rendere visibili gli indirizzi IP riservati nei report DMARC. Questa opzione non si applica ai dati canonizzati DKIM.

Rifiutare i messaggi se l'intestazione "From" è incompatibile con DMARC
Attivare questa opzione se si desidera rifiutare i messaggi che non sono compatibili con i requisiti DMARC relativi alla costruzione dell'intestazione "From". Si tratta dei messaggi con intestazioni "From" multiple o indirizzi e-mail multipli in una singola intestazione "From". Tali messaggi sono correntemente esclusi dall'elaborazione DMARC. Questa opzione è disattivata per impostazione predefinita perché la

presenza di più indirizzi in una singola intestazione "From" non è tecnicamente una violazione del protocollo, ma l'attivazione dell'impostazione può aiutare a massimizzare la protezione mediante DMARC. L'impostazione viene applicata solo quando è abilitata la verifica DMARC 552.

Inserisci intestazione "Preference:bulk" nei messaggi e-mail dei report DMARC
Per impostazione predefinita MDaemon inserisce un intestazione di posta bulk nei messaggi e-mail dei report DMARC. Se non si desidera inserire l'intestazione, deselezionare questa casella di controllo.

Includi record DMARC in file di registro
Per impostazione predefinita, MDaemon registra il record DNS DMARC completo ottenuto durante le interrogazioni DNS DMARC. Disattivare questa opzione se non si desidera includere il record DMARC completo nel file di registro.

Aggiorna automaticamente il file dei suffissi pubblici se è più vecchio di questi giorni
DMARC richiede un file dei suffissi pubblici per determinare in modo affidabile i domini corretti su cui eseguire interrogazioni relative ai record DNS DMARC. Per impostazione predefinita, MDaemon aggiorna automaticamente il relativo file dei suffissi pubblici memorizzato quando supera i 15 giorni. Modificare il valore di questa opzione a seconda della frequenza con cui si desidera aggiornare il file dei suffissi pubblici. Disattivare questa opzione se non si desidera aggiornarlo automaticamente.

URL del file dei suffissi pubblici
Si tratta dell'URL da cui MDaemon scaricherà il file dei suffissi pubblici da utilizzare per DMARC. Per impostazione predefinita, MDaemon utilizza il file disponibile al seguente indirizzo: http://publicsuffix.org/list/effective_tld_names.dat.

Aggiorna ora il file dei suffissi pubblici
Fare clic su questa opzione per aggiornare manualmente il file dei suffissi pubblici dall'*URL del file dei suffissi pubblici* sopra specificato.

Vedere:

DMARC 544
Verifica DMARC 552
Report DMARC 555
Impostazioni DKIM 542

4.1.2.6 Certificazione dei messaggi

Nel processo di certificazione dei messaggi, un'entità garantisce o "certifica" la correttezza del comportamento relativo alla posta elettronica tenuto da un'altra entità. Di conseguenza, se l'entità certificante è accreditata presso un server di posta ricevente, i messaggi inviati da un dominio certificato da tale entità possono essere considerati più affidabili. Il server ricevente può ritenere, con un sufficiente grado di certezza, che il dominio mittente utilizza procedure ottimali relative alla posta e che non invia messaggi spam o altri messaggi contenenti rischi per la sicurezza. La certificazione

rappresenta un vantaggio perché consente di evitare l'applicazione delle funzionalità di analisi antispam a messaggi per i quali non è necessaria, nonché di ridurre le risorse necessarie per l'elaborazione di ciascun messaggio.

MDaemon supporta la certificazione dei messaggi con la prima implementazione commerciale del mondo di un nuovo protocollo di posta Internet denominato "Vouch-By-Reference" (VBR), che MDaemon Technologies sta collaborando a creare ed espandere mediante la partecipazione al Domain Assurance Council (DAC). Il protocollo VBR offre il meccanismo che consente ai CSP (Certification Service Provider, provider di servizi di certificazione) o alle entità "certificanti" di garantire la conformità a procedure ottimali relative alla posta elettronica utilizzate da specifici domini.

Certificazione dei messaggi in entrata

Per configurare la funzionalità di certificazione dei messaggi in entrata di MDaemon È sufficiente selezionare l'opzione *Abilita certificazione messaggi in entrata* della finestra di dialogo Certificazione VBR (Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR) e indicare uno o più provider di servizi di certificazione accreditati per la posta in entrata (ad esempio `vbr.emailcertification.org`). È inoltre possibile scegliere se escludere i messaggi certificati dall'elaborazione di Spam Filter o se correggerne il punteggio spam in senso positivo.

Certificazione dei messaggi in uscita

Per configurare l'inserimento dei dati di certificazione nei messaggi in uscita, è necessario disporre di uno o più CSP (Certification Service Provider) per la certificazione della posta. MDaemon Technologies offre ai propri clienti un servizio di certificazione. Per ulteriori informazioni, visitare: www.mdaemon.com.

Per utilizzare la certificazione dei messaggi di posta in uscita con MDaemon, eseguire la registrazione presso un provider CSP, quindi procedere come segue:

1. Aprire la finestra di dialogo Certificazione VBR: fare clic su Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR.
2. Fare clic su "*Inserisci dati certificazione nei messaggi in uscita*."
3. Fare clic su "*Configura dominio per certificazione messaggi*". Verrà aperta la finestra di dialogo Impostazione certificazione.
4. Digitare il *Nome dominio* per il quale si desidera inserire i dati di certificazione nei messaggi in uscita.
5. Scegliere nell'elenco a discesa *Tipo di posta* il tipo di posta certificata dal CSP per il dominio oppure inserire un nuovo tipo di posta se quello desiderato non è presente.
6. Inserire uno o più CSP che certificheranno la posta in uscita del dominio. Separare i nomi dei CSP con uno spazio.
7. Fare clic su "*OK*".
8. Configurare il server in modo da firmare i messaggi in uscita del dominio con DKIM 536 oppure verificare che questi vengano inviati da un server SPF 533 approvato. Questa operazione è necessaria per garantire che l'origine del

messaggio sia legittima, ossia che il messaggio proviene dal server MDaemon in uso. Un messaggio non può essere certificato a meno che il server ricevente sia prima in grado di determinare che il messaggio è autentico.

La tecnologia VBR non richiede che i messaggi siano firmati o che vengano trasmessi al CSP, perché quest'ultimo non si occupa della firma o della convalida di messaggi specifici, ma solo di garantire la conformità a procedure ottimali relative alla posta elettronica utilizzate da uno specifico dominio.

Per ulteriori informazioni sui servizi di certificazione forniti da MDaemon Technologies, visitare il sito:

http://www.mdaemon.com/email-certification/

Specifiche VBR - RFC 5518:

http://tools.ietf.org/html/rfc5518

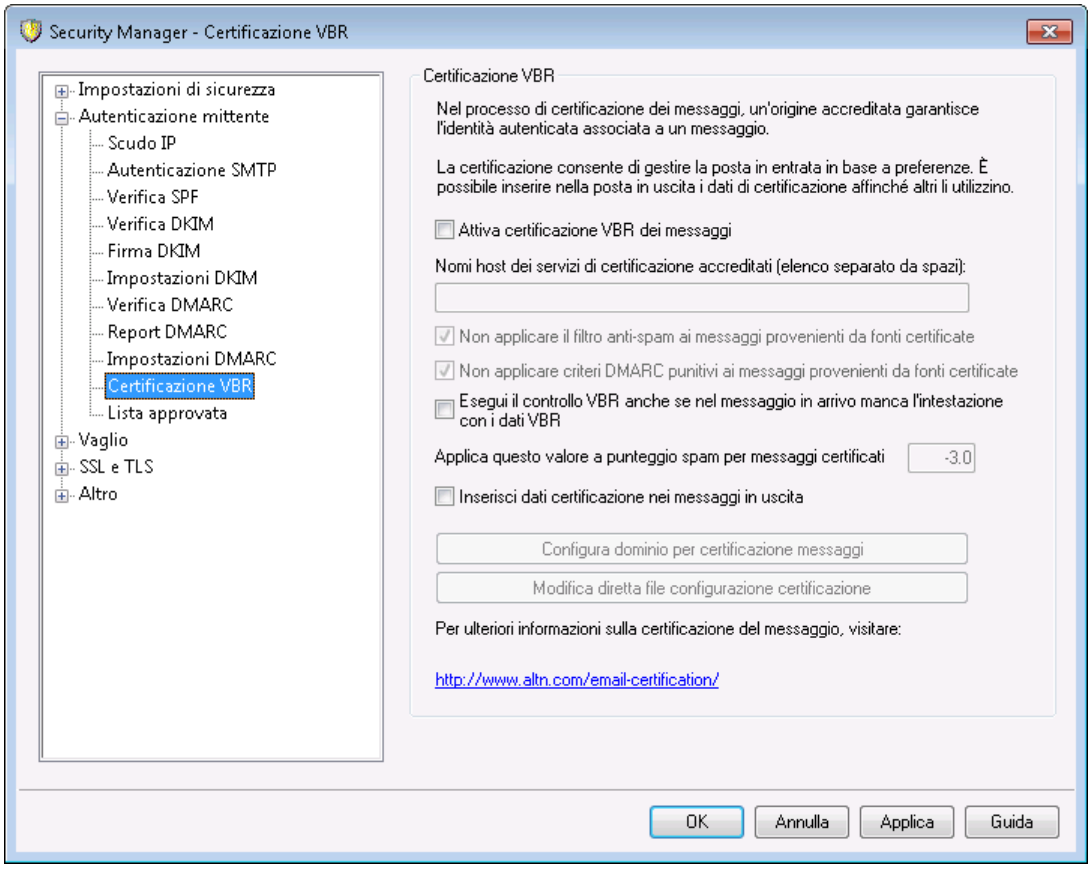
Per ulteriori informazioni su DKIM, vedere:

http://www.dkim.org/

Per ulteriori informazioni, vedere:

Certificazione VBR 563

4.1.2.6.1 Certificazione VBR



La finestra di dialogo Certificazione VBR si trova in: Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR.

Certificazione VBR

Attiva certificazione VBR dei messaggi
Selezionare questa casella di controllo per abilitare la certificazione dei messaggi in entrata. Quando viene ricevuto un messaggio in entrata per il quale è richiesta la certificazione, MDaemon interroga il CSP (Certification Service Provider, provider di servizi di certificazione) accreditato per verificare se il messaggio possa essere considerato "certificato" o meno. In caso affermativo, a seconda dell'opzione selezionata il messaggio viene escluso dal filtro spam oppure viene corretto il punteggio assegnato da Spam Filter 691 al messaggio.

Nomi host dei servizi di certificazione accreditati (elenco separato da spazi):
Inserire in questa casella i nomi degli host accreditati per il servizio di certificazione. Nel caso di più host, separarne i nomi con uno spazio.

Non applicare il filtro anti-spam ai messaggi provenienti da fonti certificate
Selezionare questa opzione se si desidera escludere dal filtro spam i messaggi provenienti da fonti certificate.

Non applicare criteri DMARC punitivi ai messaggi provenienti da fonti certificate
Questa opzione assicura che i messaggi verificati provenienti da fonti certificate non vengano penalizzati se il dominio di invio applica criteri DMARC 552 restrittivi (ad esempio p=quarantine o p=reject) e il messaggio non supera il controllo DMARC. L'opzione è abilitata per impostazione predefinita.

Esegui il controllo VBR anche se nel messaggio in arrivo manca l'intestazione con i dati VBR
Abilitare questa opzione se si desidera eseguire controlli VBR anche sui messaggi in arrivo in cui manca l'intestazione con i dati VBR. Di norma questa intestazione è necessaria, ma VBR funziona bene anche senza. Quando l'intestazione manca, MDaemon interroga i CSP accreditati utilizzando il tipo di posta "all". L'opzione è disabilitata per impostazione predefinita.

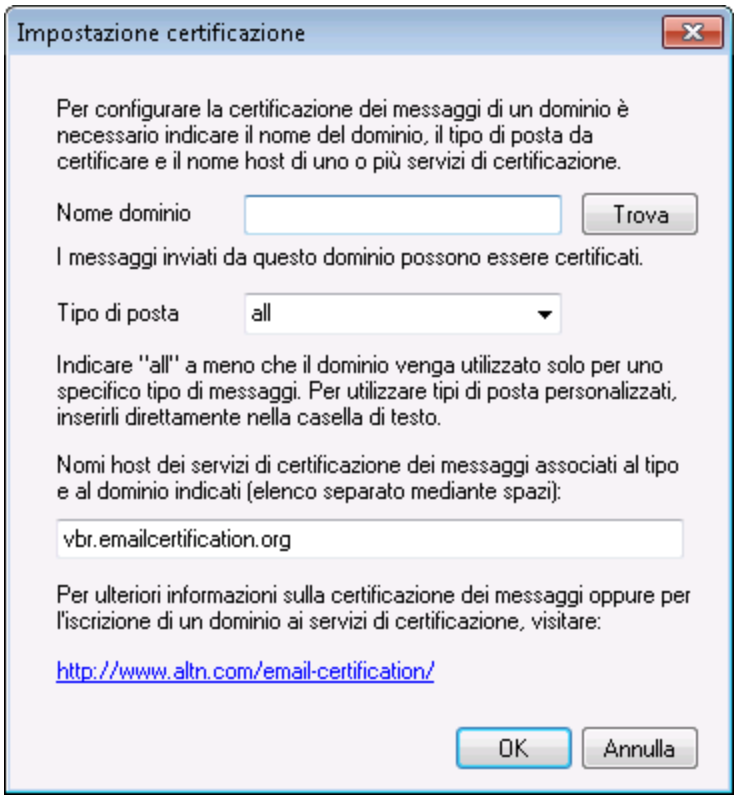
Applica questo valore a punteggio spam per messaggi certificati
Se non si desidera escludere dal filtro spam i messaggi certificati, questa opzione consente di specificare il valore utilizzato per la rettifica del punteggio spam del messaggio. In genere, questo valore è un numero negativo che rappresenta una rettifica in senso positivo del punteggio spam. Il valore predefinito è "-3.0".

Inserisci dati certificazione nei messaggi in uscita
Fare clic su questa casella di controllo per inserire i dati di certificazione nei messaggi in uscita. Fare quindi clic sul pulsante *Configura dominio per certificazione messaggi* per aprire la finestra di dialogo Impostazione certificazione al fine di specificare i domini da certificare e i relativi CSP.

Configura dominio per certificazione messaggi
Dopo aver selezionato l'opzione *Inserisci dati certificazione nei messaggi in uscita*, fare clic su questo pulsante per aprire la finestra di dialogo Impostazione certificazione. Nella finestra di dialogo è possibile specificare il dominio associato ai messaggi in uscita da certificare, i tipi di posta da certificare e i CSP associati al dominio.

Modifica diretta file configurazione certificazione
Dopo aver selezionato l'opzione *Inserisci dati certificazione nei messaggi in uscita*, fare clic su questo pulsante per aprire il file di configurazione VBR (Vouch-by-Reference). Il file include tutti i domini configurati nella finestra di dialogo Impostazione certificazione per l'uso di VBR, unitamente ai relativi dati VBR. È possibile utilizzare questo file per modificare le voci precedentemente create o per crearne di nuove.

Impostazione certificazione



Dopo aver abilitato l'opzione *Inserisci dati certificazione nei messaggi in uscita* della finestra di dialogo Certificazione, fare clic sul pulsante *Configura dominio per certificazione messaggi* per aprire la finestra di dialogo Impostazione certificazione. Nella finestra di dialogo è possibile specificare il dominio associato ai messaggi in uscita da certificare, i tipi di posta da certificare e i CSP associati al dominio.

Impostazione certificazione

Nome dominio
Utilizzare questa opzione per inserire il dominio per il quale certificare i messaggi in uscita.

Trova
Se la funzione di certificazione dei messaggi è stata già configurata per uno specifico dominio, digitare il *Nome dominio* e fare clic su questo pulsante per inserire nella finestra di dialogo le opzioni già definite.

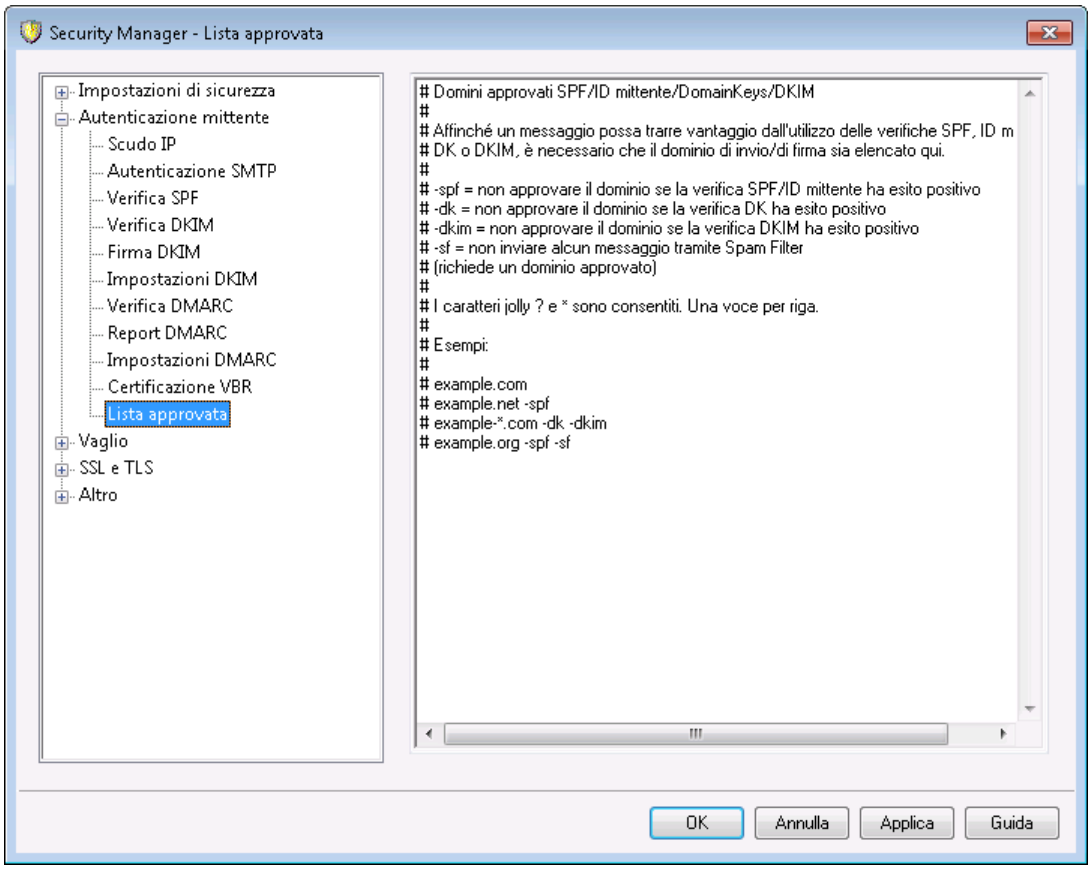
Tipo di posta
Utilizzare la casella di riepilogo a discesa per scegliere il tipo di posta certificata in relazione al dominio dal CSP associato. Se il tipo desiderato non è presente, inserirne uno manualmente.

Nomi host dei servizi...
Inserire i nomi degli host dei CSP accreditati per la certificazione dei messaggi in uscita del dominio, ad esempio `vbr.emailcertification.org`. Nel caso di più CSP, separarne i nomi con uno spazio.

Per ulteriori informazioni, vedere

Certificazione dei messaggi 560

4.1.2.7 Lista approvata



Poiché alcuni spammer e mittenti di e-mail di massa hanno iniziato a utilizzare SPF o a firmare i messaggi con una firma DKIM valida, il fatto che un messaggio sia firmato e verificato non è una garanzia che il messaggio che si riceve non sia effettivamente spam, anche se il messaggio proviene da una fonte considerata valida. Per questo motivo il punteggio spam di un messaggio non viene ridotto a seguito della verifica SPF o DKIM, a meno che il dominio estratto dalla firma non sia nell'Elenco approvato. Questo è in sostanza una lista consentiti che si può utilizzare per designare i domini autorizzati a ottenere una riduzione del punteggio spam all'atto della verifica dei messaggi di posta in arrivo.

Quando un messaggio firmato da uno di questi domini viene verificato da SPF o DKIM, il relativo punteggio di spam viene ridotto in base alle impostazioni che si trovano nelle

schermate SPF[533] e Verifica DKIM[537]. È comunque possibile allegare uno qualsiasi dei flag elencati di seguito, se si desidera impedire a uno di tali metodi di verifica di ridurre il punteggio. È inoltre disponibile un flag che consente di impedire ai messaggi verificati il passaggio attraverso Spam Filter.

-spf Non ridurre il punteggio spam dopo la verifica SPF per i messaggi inviati da questo dominio.

-dkim Non ridurre il punteggio spam dopo la verifica DKIM per i messaggi provenienti da questo dominio.

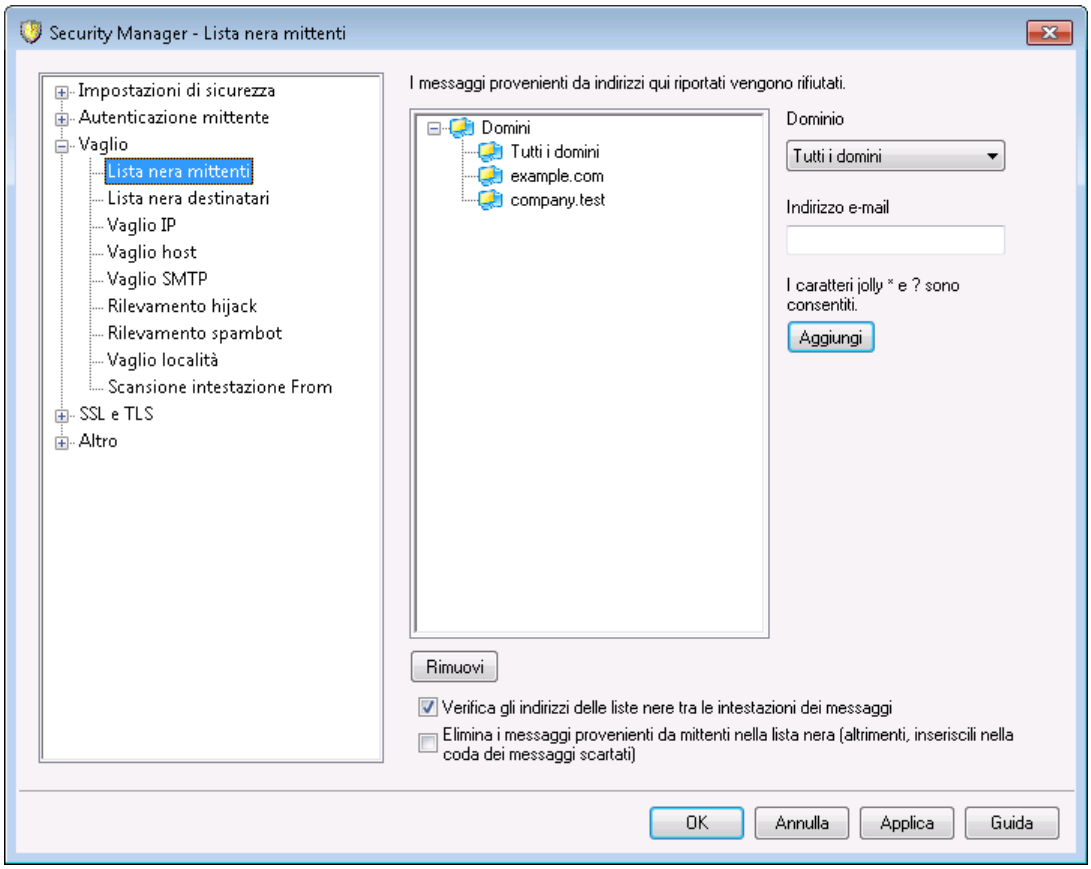
-sf Non elaborare i messaggi verificati da questo dominio tramite Spam Filter.

DMARC e l'elenco approvato

Verifica DMARC[552] utilizza allo stesso modo questo Elenco approvato, che consente di disporre delle esenzioni in base a identificatori DKIM e percorsi SPF verificati da fonti ritenute affidabili. Se, ad esempio, arriva un messaggio che non supera la verifica DMARC ma ha una firma DKIM valida da un dominio sull'elenco approvato, il messaggio non è soggetto ai criteri di DMARC (ovvero, il messaggio viene trattato come se il criterio fosse "`p=none`"). Lo stesso accade se la verifica del percorso SPF corrisponde a un dominio presente nell'elenco approvato.

4.1.3 Vaglio

4.1.3.1 Lista mittenti bloccati



Lista bloccati mittenti è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Questo elenco contiene gli indirizzi che non sono autorizzati a inviare posta mediante il server. I messaggi provenienti da uno degli indirizzi della lista nera vengono respinti durante la sessione SMTP. Questo metodo è utile per limitare alcuni dei problemi degli utenti. Gli indirizzi possono essere bloccati per singolo dominio o su base globale (tutti i domini di MDaemon).

I messaggi provenienti dagli indirizzi elencati vengono rifiutati
In questa finestra sono visualizzati tutti gli indirizzi attualmente bloccati, elencati in base al dominio che li blocca.

Dominio
Scegliere il dominio a cui sarà associato questo indirizzo bloccato. ossia il dominio che non deve più ricevere posta proveniente dall'indirizzo specificato. Scegliere "Tutti i domini" da questo elenco per bloccare l'indirizzo a livello globale.

Indirizzo e-mail
Immettere l'indirizzo che si desidera bloccare. Poiché sono consentiti i caratteri jolly, la sintassi "*@esempio.net" sopprime tutti i messaggi provenienti da tutti gli utenti di "esempio.net" e la sintassi "utente1@*" sopprime tutti i messaggi da tutti gli indirizzi

che iniziano con "utente1", indipendentemente dal dominio di partenza del messaggio.

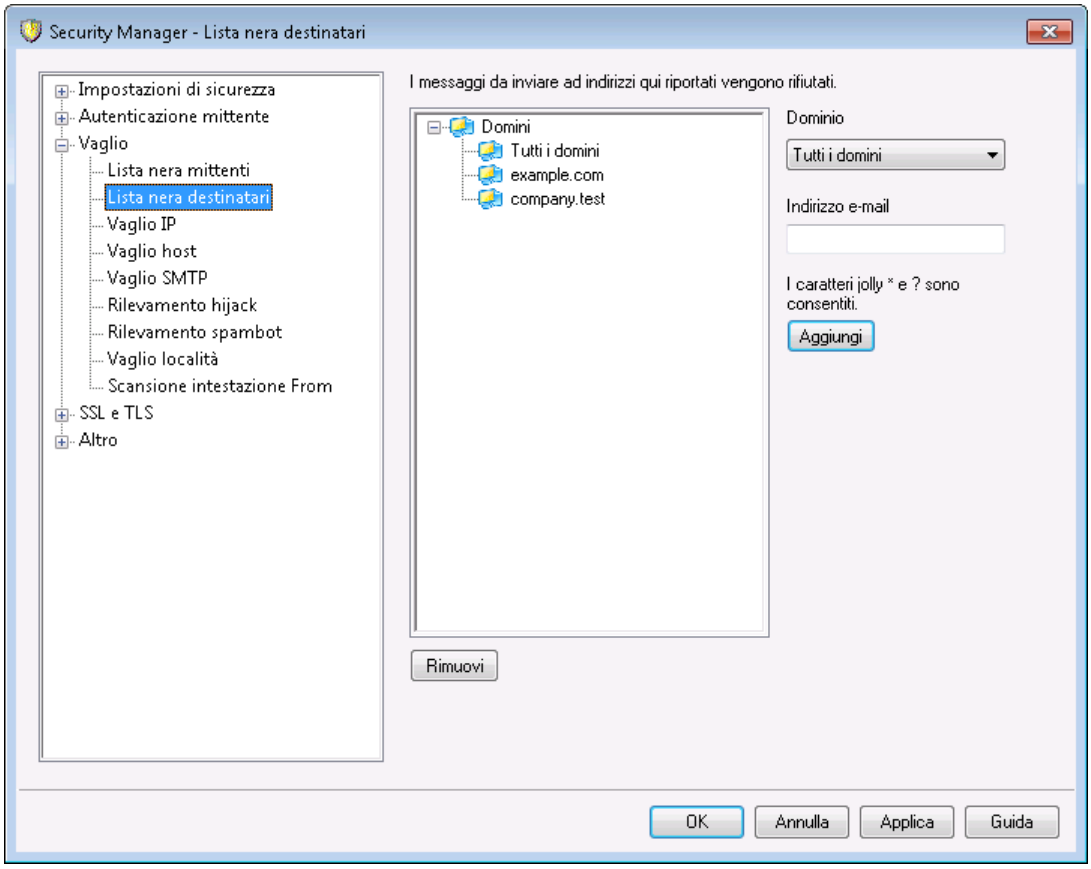
Aggiungi
Fare clic su questo pulsante per aggiungere l'indirizzo designato all'elenco bloccati.

Rimuovi
Fare clic su questo pulsante per rimuovere dall'elenco la voce selezionata.

Controlla presenza di indirizzi della lista bloccati nelle intestazioni dei messaggi
Per impostazione predefinita, MDaemon applica la lista bloccati ai valori estratti dalle intestazioni From/Sender del messaggio durante la sessione SMTP. Ciò evita che il messaggio venga coinvolto e spostato nella coda dei messaggi scartati dal thread MTA.

Elimina i messaggi inviati da mittenti nella lista bloccati (altrimenti, aggiungi a coda messaggi scartati)
Attivare questa opzione per impostare MDaemon in modo che elimini i messaggi in arrivo da mittenti inclusi nella lista bloccati. Oltre alla posta normale, questa opzione viene applicata anche ai messaggi che arrivano via MultiPOP e DomainPOP. Quando questa opzione è disattivata, il messaggio viene inserito nella coda dei messaggi scartati anziché essere eliminato. L'opzione è disattivata per impostazione predefinita.

4.1.3.2 Lista bloccati destinatari



Lista bloccati destinatari è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Questo elenco contiene gli indirizzi e-mail che non sono autorizzati a ricevere posta mediante il server. I messaggi provenienti da uno degli indirizzi della lista nera verranno respinti. Gli indirizzi possono essere bloccati per singolo dominio o su base globale (tutti i domini di MDaemon). La lista bloccati destinatari opera solo sui dati RCPT delle buste SMTP (non sulle intestazioni dei messaggi).

I messaggi da recapitare agli indirizzi elencati vengono rifiutati
In questa finestra sono visualizzati tutti gli indirizzi attualmente bloccati, elencati in base al dominio che li blocca.

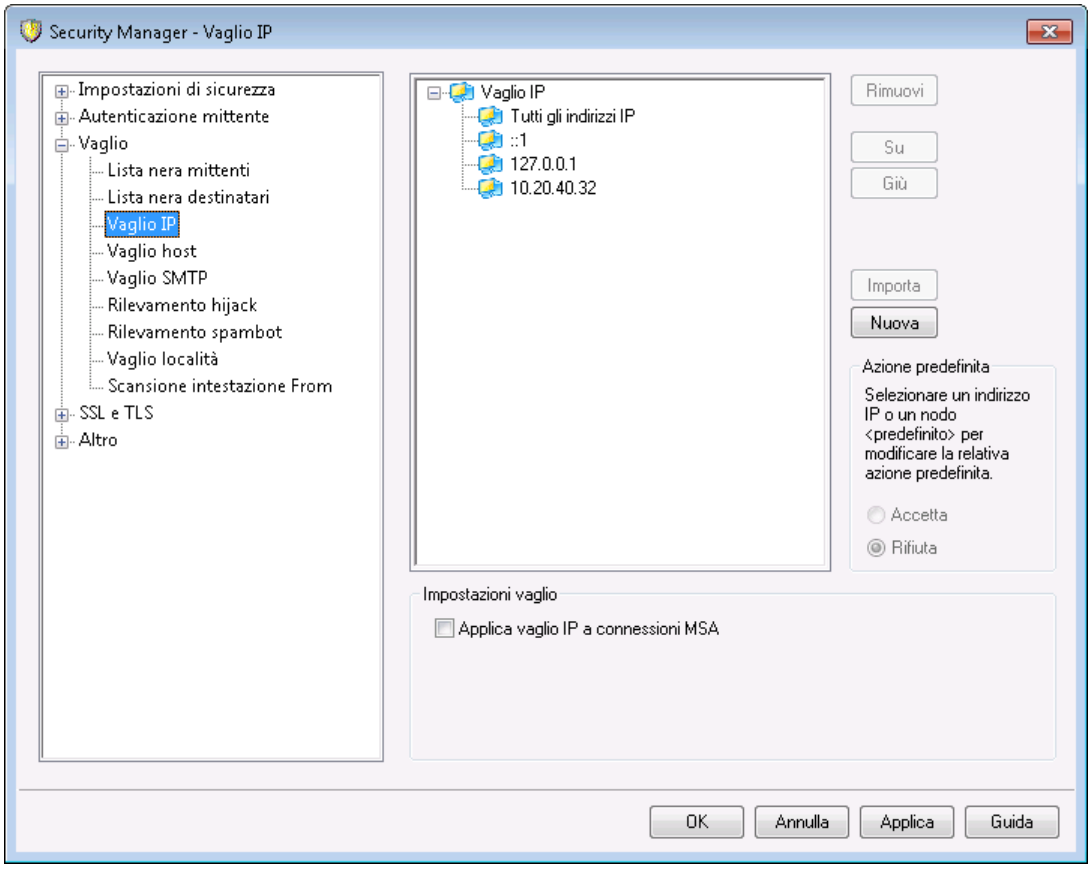
Dominio
Scegliere il dominio a cui sarà associato questo indirizzo bloccato. ossia il dominio che non deve più ricevere posta proveniente dall'indirizzo specificato. Scegliere "Tutti i domini" da questo elenco per bloccare l'indirizzo a livello globale.

Indirizzo e-mail
Immettere l'indirizzo che si desidera bloccare. Poiché sono consentiti i caratteri jolly, la sintassi "*@esempio.net" sopprime tutti i messaggi per tutti gli utenti di "esempio.net" e la sintassi "utente1@*" sopprime tutti i messaggi per gli indirizzi che iniziano con "utente1", indipendentemente dal dominio di destinazione del messaggio.

Aggiungi
Fare clic su questo pulsante per aggiungere l'indirizzo designato all'elenco bloccati.

Rimuovi
Fare clic su questo pulsante per rimuovere dall'elenco la voce selezionata.

4.1.3.3 Vaglio IP



Vaglio IP è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Vaglio IP consente di definire indirizzi IP remoti specifici autorizzati o meno a connettersi con gli indirizzi IP locali. Gli indirizzi IP remoti inseriti in Vaglio IP possono essere associati con tutti gli indirizzi IP locali o con singoli indirizzi IP. È consentito l'uso della notazione CIDR e dei caratteri jolly *, # e ?.

Ad esempio:

..*.*	Corrisponde a tutti gli indirizzi IP
#.#.#.#	Corrisponde a tutti gli indirizzi IP
192.*.*.*	Corrisponde a tutti gli indirizzi IP che iniziano con 192
192.168.*.239	Corrisponde agli indirizzi IP da 192.168.0.239 a 192.168.255.239
192.168.0.1??	Corrisponde agli indirizzi IP da 192.168.0.100 a 192.168.0.199

Nuova voce vaglio IP

Per creare una nuova voce di vaglio IP, fare clic su **Nuovo**. Si apre la finestra di dialogo Nuova voce vaglio IP in cui è possibile creare la voce.

IP locale
Scegliere dall'elenco a discesa "Tutti gli IP" o l'IP specifico a cui applicare la voce.

IP remoto (CIDR, caratteri jolly * ? e # sono accettati)
Inserire l'indirizzo IP remoto da aggiungere all'elenco, associato con l'IP locale indicato in precedenza.

Accetta connessioni
Selezionando questa opzione, si autorizza la connessione degli indirizzi IP remoti specificati con l'indirizzo IP locale associato.

Rifiuta connessioni
Selezionando questa opzione, NON si autorizza la connessione degli indirizzi IP remoti specificati con l'indirizzo IP locale associato. La connessione verrà rifiutata o eliminata.

Aggiungi
Dopo aver inserito le informazioni relative alle opzioni precedenti, fare clic su questo pulsante per aggiungere la voce all'elenco.

Importa

Selezionare un indirizzo IP e fare clic su questo pulsante se si desidera importare i dati dell'indirizzo IP da un file APF o .htaccess. Il supporto di questi file da parte di MDaemon attualmente è limitato a quanto segue:

- vengono supportati "deny from" e "allow from"
- vengono importati solo i valori IP (non i nomi di dominio)
- è possibile usare la notazione CIDR, ma non gli indirizzi IP parziali.
- Ogni riga può contenere un qualsiasi numero di indirizzi IP separati da spazi o virgole. Ad esempio, "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5" e simili.
- Le righe che iniziano per # vengono ignorate.

Rimuovi

Per rimuovere una voce, selezionarla dall'elenco e fare clic su **Rimuovi**.

Azione predefinita

Per specificare l'azione predefinita per le connessioni da indirizzi IP remoti che non sono stati definiti, scegliere un indirizzo IP dall'elenco e fare clic su **accetta** o **rifiuta**. Una volta specificata un'azione predefinita, è possibile modificarla selezionando il nodo "<default>" sotto l'indirizzo IP e selezionando quindi la nuova impostazione predefinita.

accetta
Scegliendo questa opzione, verranno accettate le connessioni provenienti da qualsiasi indirizzo IP non espressamente definito nella schermata Vaglio IP.

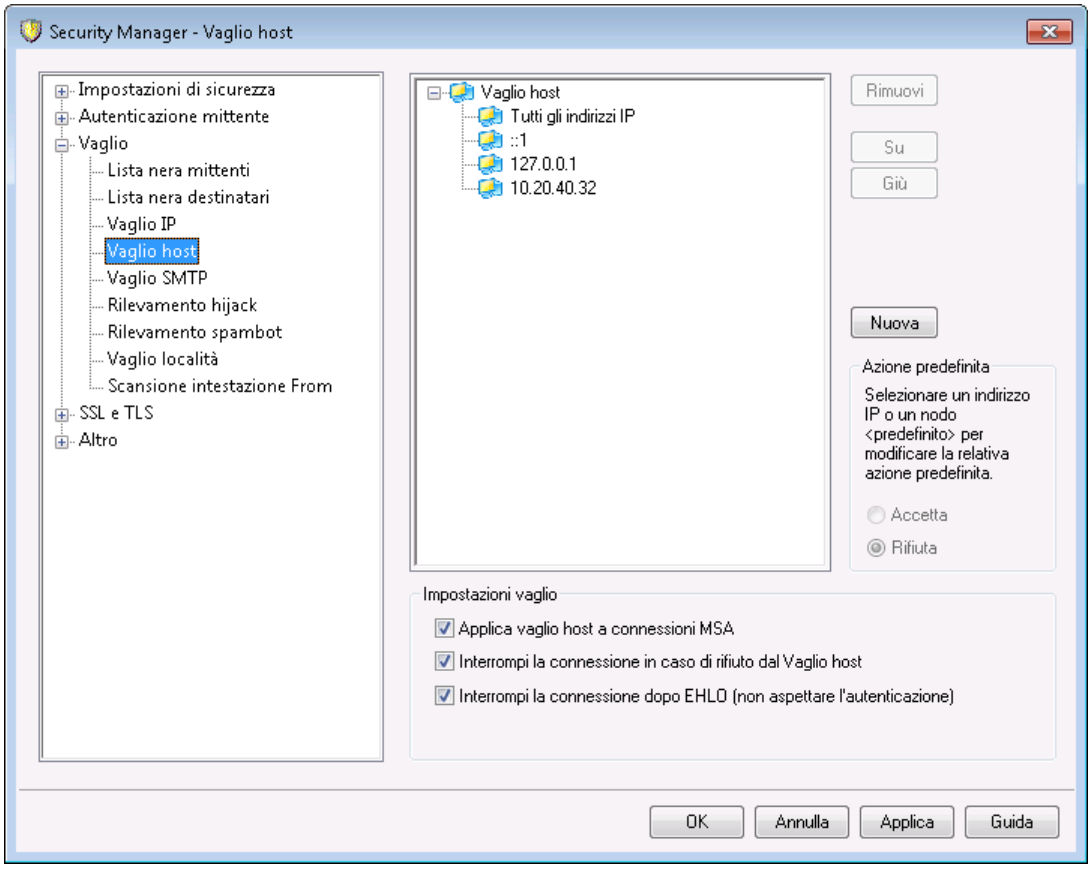
rifiuta
Scegliendo questa opzione, verranno respinte o eliminate le connessioni provenienti da qualsiasi indirizzo IP non espressamente definito nella schermata Vaglio IP.

Vaglio IP non bloccherà in nessun caso gli indirizzi IP accreditati 526 o locali.

Impostazioni di vaglio

Applica vaglio IP a connessioni MSA
Utilizzare questa opzione per applicare il vaglio IP alle connessioni eseguite alla porta MSA 110 del server. In genere questo non è necessario, Questa impostazione è abilitata per impostazione predefinita.

4.1.3.4 Vaglio host



Vaglio host è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Questo consente di definire gli host remoti autorizzati a connettersi agli indirizzi IP locali. È possibile specificare un elenco di host e configurare il server in modo che autorizzi o rifiuti le connessioni dagli host indicati. Vaglio host esegue un confronto tra i valori EHLO e PTR, determinati nel corso della sessione SMTP, e i valori indicati in questa schermata.

Nuova voce vaglio host

Per creare una nuova voce di vaglio host, fare clic su **Nuovo**. Si apre la finestra di dialogo Nuova voce vaglio host in cui è possibile creare la voce.

IP locale
Con questo elenco a discesa è possibile scegliere l'indirizzo IP locale al quale applicare questa voce di Vaglio host. Per applicarla a tutti gli indirizzi IP locali, selezionare "All IPs".

Host remoto (caratteri jolly * e # accettati)
Inserire l'host remoto da aggiungere all'elenco, associato con l'IP locale indicato in precedenza.

Accetta connessioni
Selezionando questa opzione, si autorizza la connessione dell'host remoto specificato con l'indirizzo IP locale associato.

Rifiuta connessioni
Selezionando questa opzione, NON si autorizza la connessione dell'host remoto specificato con l'indirizzo IP locale associato. La connessione verrà rifiutata o eliminata.

Rimuovi

Per rimuovere una voce, selezionarla dall'elenco e fare clic su **Rimuovi**.

Azione predefinita

Per specificare l'azione predefinita per le connessioni da host remoti che non sono stati definiti, scegliere un indirizzo IP dall'elenco e fare clic su **accetta** o **rifiuta**. Una volta specificata un'azione predefinita, è possibile modificarla selezionando il nodo "<default>" sotto l'indirizzo IP e selezionando quindi la nuova impostazione predefinita.

accetta
Scegliendo questa opzione, verranno accettate le connessioni provenienti da qualsiasi host non espressamente definito nella schermata Vaglio host.

rifiuta
Scegliendo questa opzione, verranno rifiutate le connessioni provenienti da qualsiasi host non espressamente definito nella schermata Vaglio host.

La schermata relativa a Vaglio host non bloccherà in nessun caso gli host accreditati 526 o quelli locali.

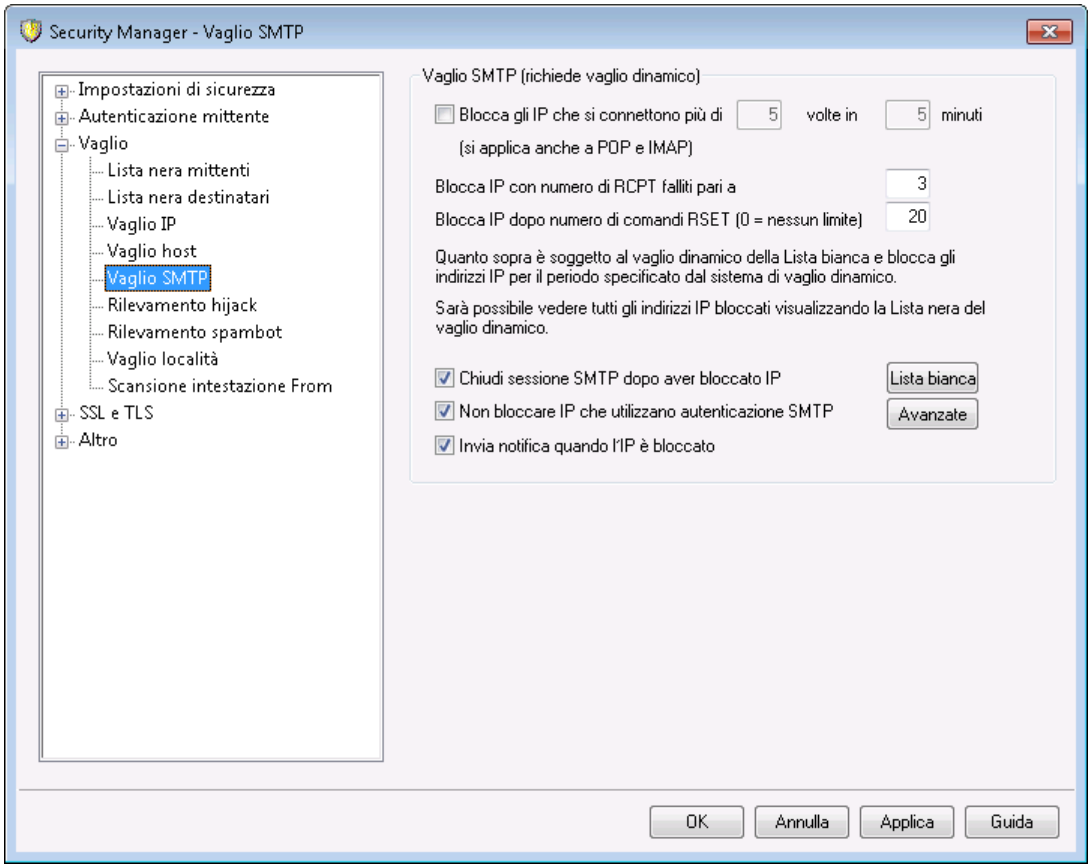
Impostazioni di vaglio

Applica vaglio host a connessioni MSA
Utilizzare questa opzione per applicare il vaglio host alle connessioni eseguite alla porta MSA 110 del server. Questa opzione è attivata per impostazione predefinita.

Interrompi connessione al rifiuto del vaglio host
Quando si attiva questa opzione, la connessione viene interrotta immediatamente in caso di rifiuto da parte del vaglio host.

Interrompi la connessione dopo EHLO (non aspettare l'autenticazione)
Attivare questa opzione se si desidera interrompere immediatamente le connessioni escluse dopo EHLO/HELO. In genere si attende l'autenticazione. Questa opzione è attivata per impostazione predefinita.

4.1.3.5 Schermo SMTP



Con lo Schermo SMTP è possibile bloccare gli indirizzi IP che si connettono a MDaemon troppe volte entro un numero di minuti specificato. È inoltre possibile bloccare gli indirizzi che causano troppi RCPT non riuscite e quelli che inviano troppo comandi RSET. Il Vaglio SMTP richiede il Vaglio dinamico e utilizza la Lista bloccati dinamica 638 e la Lista consentiti dinamica 636.

Blocca gli IP che si connettono più di [X] volte in [X] minuti
Selezionare questa casella di controllo se si desidera bloccare momentaneamente i siti che si connettono un numero eccessivo di volte al proprio server in un intervallo di tempo limitato. Specificare il numero di minuti e di connessioni consentiti durante questo intervallo. Gli indirizzi vengono bloccati per il tempo specificato nella schermata Controllo errori di autenticazione 627. L'opzione si applica anche alle connessioni POP e IMAP.

Blocca gli IP che provocano questo numero di errori di RCPT
Quando un indirizzo IP provoca un determinato numero di errori di tipo "Destinatario sconosciuto" durante una sessione di posta, verrà automaticamente bloccato per la quantità di tempo specificato nella schermata Controllo errori di autenticazione 627. Frequenti errori di tipo "Destinatario sconosciuto" rappresentano spesso un indizio del fatto che il mittente sia uno "spammer" in quanto, generalmente, in questo caso i messaggi vengono inviati a indirizzi obsoleti o errati.

Blocca gli IP che inviano questo numero di comandi RSET (0 = nessun limite)
Questa opzione consente di bloccare un indirizzo IP che abbia prodotto, durante una singola sessione di posta, il numero di comandi RSET indicato. Inserire "0" se non si desidera impostare alcun limite. Nella schermata Server 94 in Impostazioni Server esiste un'opzione simile che consente di limitare il numero di comandi RSET consentito. Un indirizzo IP resterà bloccato per il tempo specificato nella schermata Controllo errori di autenticazione 627.

Chiudi sessione SMTP dopo aver bloccato l'IP
Attivando questa opzione, MDaemon chiude la sessione SMTP dopo il blocco dell'indirizzo IP. Per impostazione predefinita, questa opzione è abilitata.

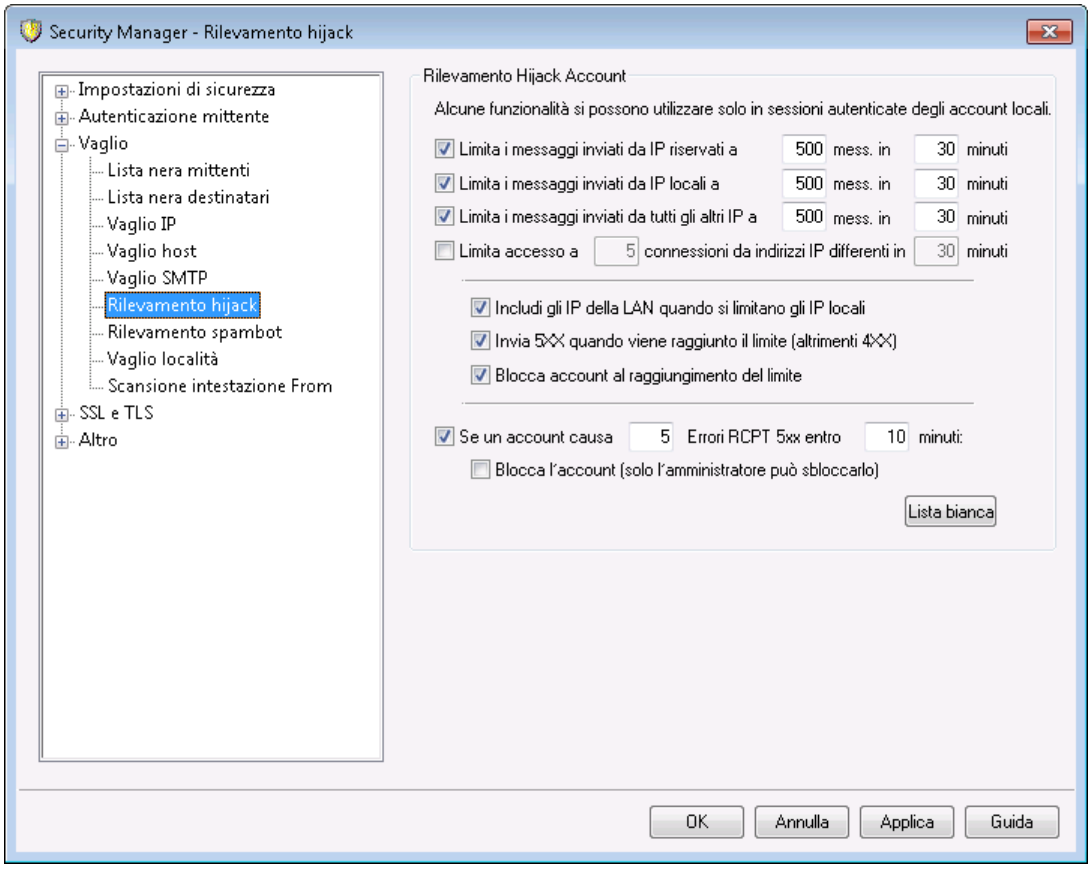
Non bloccare gli IP quando si utilizza l'autenticazione SMTP
Selezionando questa casella di controllo, i mittenti che autenticano le sessioni di posta prima dell'invio non vengono interessati dal vaglio dinamico. Per impostazione predefinita, questa opzione è abilitata.

Invia notifica quando l'IP è bloccato
Per impostazione predefinita, quando un indirizzo IP viene automaticamente bloccato dal sistema di vaglio dinamico, vengono utilizzate le opzioni *Resoconti blocco indirizzo IP* 631 di Vaglio dinamico per notificare tale azione all'utente. Deselezionare questa casella di controllo se non si desidera ricevere notifiche quando un indirizzo IP viene bloccato a causa della funzionalità di Vaglio SMTP.

Lista consentiti
Fare clic su questo pulsante per aprire la Lista consentiti dinamica 636. Gli indirizzi IP inclusi nell'elenco vengono esclusi dalle funzioni dello Schermo SMTP.

Avanzate
Questo pulsante apre la finestra di dialogo Vaglio dinamico 623.

4.1.3.6 Rilevamento hijack



Rilevamento hijack account

Le opzioni di questa schermata consentono di rilevare potenziali hijack dell'account MDaemon impedendo automaticamente l'invio di messaggi tramite il server. Ad esempio, nel caso in cui uno spammer sia entrato in possesso di indirizzo di e-mail e password di un account, questa funzionalità consente di evitare che lo spammer utilizzi l'account per inviare posta indesiderata in massa mediante il sistema. È possibile specificare il numero massimo di messaggi che un account può inviare in un determinato numero di minuti, in base all'indirizzo IP da cui viene eseguita la connessione. Si può anche determinare la disattivazione di un account che abbia raggiunto il limite. È inoltre disponibile un *Elenco esenzioni* che può essere utilizzato per esentare alcuni indirizzi da questa restrizione. Il rilevamento hijack dell'account è attivato per impostazione predefinita.

Il rilevamento hijack account viene applicato solo agli account locali con una sessione autenticata e l'account Postmaster viene escluso automaticamente.

Limita messaggi inviati da IP riservati a [xx] messaggi in [xx] minuti
Utilizzare questa opzione se si desidera impedire agli account MDaemon che si connettono da IP riservati di inviare un numero di messaggi superiore a quello

specificato in un determinato numero di minuti. Gli indirizzi IP riservati sono per la maggior parte quelli definiti dalle RFC (ad esempio, 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10 e FE80::/64).

Limita messaggi inviati da IP locali a [xx] messaggi in [xx] minuti
Utilizzare questa opzione se si desidera impedire agli account MDaemon che si connettono da IP locali di inviare un numero di messaggi superiore a quello specificato in un determinato numero di minuti. Gli indirizzi IP locali sono gli indirizzi IP configurati per i propri domini MDaemon.

Limita messaggi inviati da tutti gli altri IP a [xx] messaggi in [xx] minuti
Utilizzare questa opzione se si desidera impedire agli account MDaemon che si connettono dagli altri IP di inviare un numero di messaggi superiore a quello specificato in un determinato numero di minuti.

Limita accesso a [xx] connessioni provenienti da IP diversi in [xx] minuti
Utilizzare questa opzione per limitare il numero di connessioni provenienti da indirizzi IP diversi consentite in un determinato numero di minuti. Ad esempio, in circostanze normali se si accede all'account da dieci indirizzi IP diversi nel giro di pochi minuti, è probabile si sia verificato l'hijack dell'account. L'opzione è disabilitata per impostazione predefinita.

Includi gli IP della LAN quando si limitano gli IP locali
Per impostazione predefinita gli IP della LAN[620] vengono inclusi quando si utilizza l'opzione "*Limita i messaggi inviati dagli IP locali...*" descritta sopra. Deselezionare questa casella per non includere gli IP della LAN quando si limitano gli IP locali.

Invia 5XX quando viene raggiunto il limite (altrimenti 4XX)
Per impostazione predefinita, raggiunto uno dei limiti, MDaemon invierà un codice risposta 5XX all'account con hijack. Disattivare questa opzione per inviare invece un codice 4XX.

Blocca account al raggiungimento del limite
Selezionare questa casella di controllo se si desidera bloccare gli account che tentano di inviare un numero di messaggi superiore a quello consentito. In tal caso, il server invia l'errore 552, la connessione viene chiusa e l'account viene bloccato immediatamente. L'account bloccato non sarà più in grado di inviare o controllare la posta, ma MDaemon continuerà ad accettare la relativa posta in arrivo. Infine, quando l'account viene bloccato, viene inviato un messaggio al postmaster corrispondente all'account. Il postmaster può riabilitare l'account semplicemente rispondendo al messaggio.

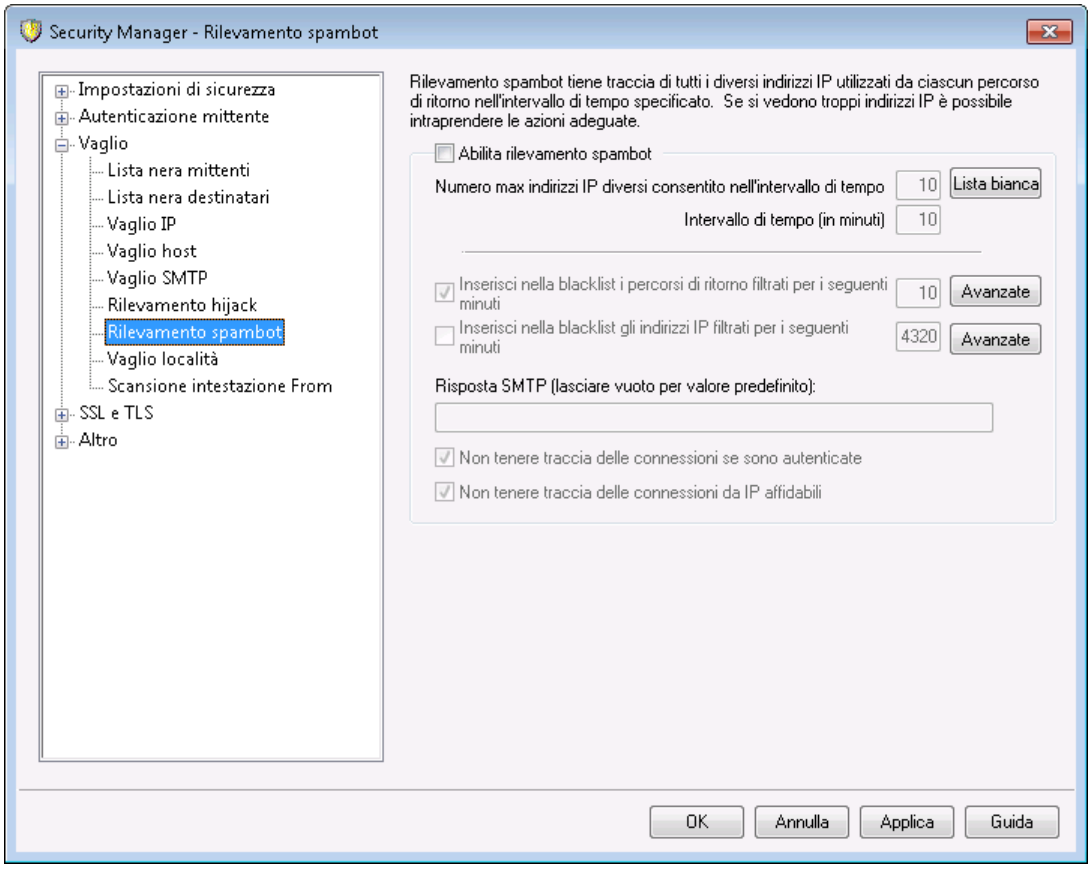
Se un account causa [xx] errori RCPT 5xx entro [xx] minuti
Questa opzione consente di monitorare quante volte un account tenta di inviare messaggi a un destinatario non valido entro un periodo di tempo specifico. Una caratteristica comune dei messaggi di spam è che vengono spesso inviati a un elevato numero di destinatari non validi, perché lo spammer tenta di inviarli a vecchi

indirizzi e-mail oppure tenta di indovinare nuovi indirizzi. Per questo motivo, se un account MDaemon inizia a inviare messaggi a un numero elevato di account non validi in un breve periodo di tempo, questa è una buona indicazione che l'account è stato sottoposto a hijack e viene utilizzato per l'invio di spam. Utilizzare questa opzione con l'opzione "*Blocca l'account...*" riportata di seguito può consentire di bloccare un account violato prima che vengano fatti troppi danni. Nota: Per questa opzione, un destinatario non valido è definito come codice di errore 5xx in risposta a un comando RCPT quando si tenta di inviare la posta dell'utente.

Blocca l'account (solo l'amministratore può sbloccarlo)
Utilizzare questa opzione se si desidera bloccare un account quando viene raggiunta la soglia indicata in "*Se un account causa [xx] errori RCPT 5xx...*". In questo caso viene inviata una e-mail di notifica all'amministratore, in modo che possa indagare sul problema e sbloccare l'account.

Elenco esenzioni
Utilizzare l'*Elenco esenzioni* per designare gli indirizzi da escludere dal rilevamento hijack account. I caratteri jolly sono accettati. Ad esempio, "`newsletter@esempio.com`" consente di escludere l'account MDaemon "newsletter" di esempio.com", mentre "`*@newsletter.esempio.com`" consente di escludere tutti gli account MDaemon appartenenti al dominio newsletter.esempio.com. L'account Postmaster è escluso automaticamente dal rilevamento hijack account.

4.1.3.7 Rilevamento spambot



Il rilevamento spambot tiene traccia degli indirizzi IP che ciascun valore `SMTP MAIL` (percorso restituzione) utilizza in un determinato periodo di tempo. Se lo stesso percorso restituzione viene utilizzato da un numero eccessivo di indirizzi IP diversi in un breve periodo di tempo, è possibile che indichi una rete spambot. Quando viene rilevato uno spambot, la connessione corrente viene immediatamente interrotta e il valore di return-path può essere facoltativamente bloccato per un periodo di tempo specificato dall'utente È inoltre possibile bloccare tutti gli indirizzi IP noti per essere spambot per un periodo di tempo specificato.

Abilita rilevamento spambot
Selezionare questa casella per attivare il rilevamento spambot. Questa opzione è disabilitata per impostazione predefinita.

Numero massimo di indirizzi IP diversi consentiti durante l'intervallo di tempo
Numero di indirizzi IP diversi da cui può connettersi un determinato percorso restituzione durante l'intervallo di tempo specificato.

Intervallo di tempo (in minuti)
Specificare l'intervallo di tempo (in minuti) da utilizzare durante il tentativo di rilevamento delle reti spambot.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni di Rilevamento spambot. Qui è possibile specificare indirizzi IP, mittenti e destinatari esclusi dal rilevamento spambot.

Blocca i return-path che causano problemi per questo numero di minuti
Utilizzare questa opzione se si desidera bloccare i return-path degli spambot rilevati. MDaemon non accetterà i messaggi con un return-path bloccato per il numero di minuti specificato. L'opzione è abilitata per impostazione predefinita.

Avanzate
Fare clic su questo pulsante per aprire la finestra File mittenti spambot. Visualizza i return-path attualmente bloccati e il numero di minuti rimanenti prima della rimozione dalla lista bloccati.

Blocca gli IP che causano problemi per questo numero di minuti
Utilizzare questa opzione se si desidera bloccare gli indirizzi IP degli spambot rilevati. MDaemon non accetterà i messaggi provenienti da un indirizzo IP bloccato per il numero di minuti specificato. L'opzione è disabilitata per impostazione predefinita.

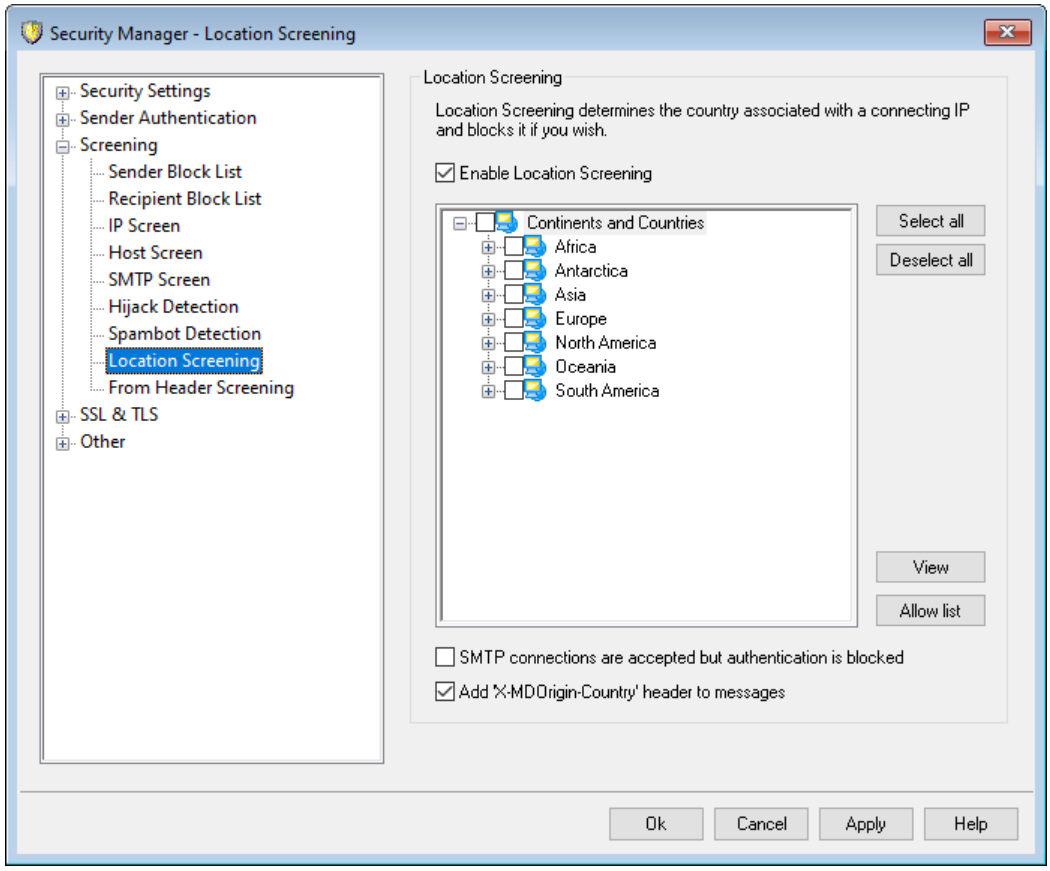
Avanzate
Fare clic su questo pulsante per aprire la finestra di dialogo File IP spambot. Visualizza gli indirizzi IP attualmente bloccati e il numero di minuti rimanenti prima della rimozione dalla lista bloccati.

Risposta SMTP (lasciare vuoto per valore predefinito)
Utilizzare questa opzione per personalizzare la risposta SMTP agli spambot che tentano di inviare messaggi da un return-path o indirizzo IP bloccato. MDaemon restituirà la risposta SMTP, "`551 5.5.1 <testo personalizzato>`", anziché la risposta predefinita. Lasciare il campo vuoto per utilizzare la risposta predefinita di MDaemon.

Se sono autenticate, non tenere traccia delle connessioni
Per impostazione predefinita MDaemon non terrà traccia delle sessioni autenticate 531 per il rilevamento spambot. Se non si desidera escludere le connessioni autenticate, deselezionare questa casella di controllo.

Non tenere traccia delle connessioni provenienti da IP affidabili
Per impostazione predefinita il rilevamento spambot non terrà traccia delle connessioni provenienti da indirizzi IP accreditati 527. Se non si desidera escludere gli IP affidabili, deselezionare questa casella di controllo.

4.1.3.8 Screening posizione



Screening posizione

La funzione Screening posizione (o vaglio località) è un sistema di blocco geografico che consente di bloccare connessioni SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 79, XML API, Remote Administration, CalDAV/CardDAV, XMPP e Minger in ingresso da regioni non autorizzate. MDaemon individua il paese associato all'indirizzo IP che si connette e blocca la connessione se questa proviene da un'area non autorizzata, aggiungendo quindi una riga al registro dello screening. Nel caso del SMTP, lo Screening posizione può bloccare solo le connessioni che utilizzano AUTH. La funzione è particolarmente utile, ad esempio, quando non esistono utenti che risiedono in determinato paese ma si desidera comunque ricevere posta da tale nazione. In questo modo si bloccano solo le persone che tentano di accedere al server.

La cartella `\MDaemon\Geo\` contiene i file del database utilizzato come database master degli IP nazionali. I file sono stati forniti da MaxMind (www.maxmind.com) ed è possibile scaricare gli aggiornamenti dal loro sito, se necessario.

Attiva screening posizione
Il vaglio della posizione è attivato per impostazione predefinita, ma nessuna regione o paese viene bloccato: MDaemon si limita a registrare il paese o la regione che esegue la connessione. Per bloccare una posizione, fare clic sulla casella di fianco alle regioni o paesi che si desidera bloccare e selezionare **OK** o **Applica**. Quando è attivo lo screening o il vaglio della posizione, indipendentemente dal fatto che

esistano delle posizioni bloccate o meno, MDaemon inserirà l'intestazione "X-MDOrigin-Country" nei messaggi, per filtrare i contenuti o per altri scopi. Questa intestazione contiene i codici ISO 3166 a due lettere di paesi e continenti.

Seleziona/Deseleziona tutti
Utilizzare questi pulsanti per selezionare o deselezionare tutte le posizioni dell'elenco.

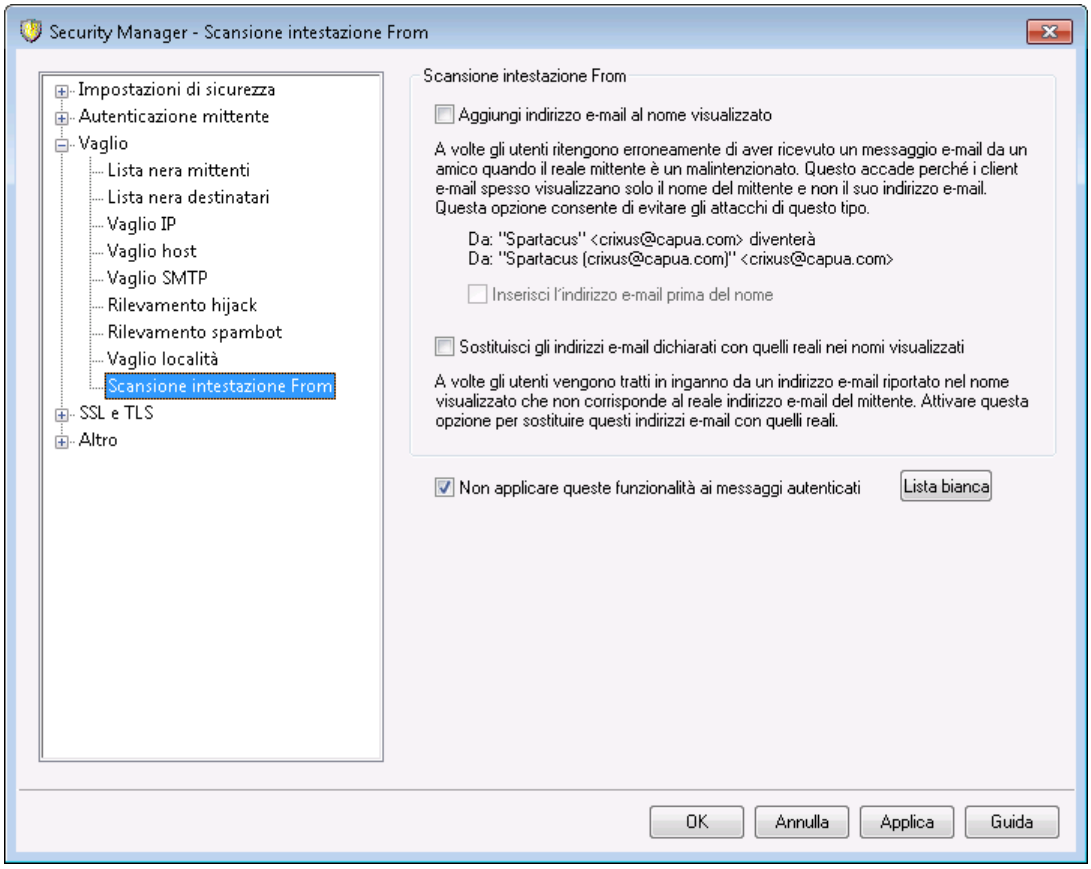
Visualizza
Fare clic su questo pulsante per visualizzare il file di testo di tutte le posizioni attualmente bloccate da Screening posizione. Se si seleziona/deseleziona una casella nell'elenco delle posizioni, il pulsante *Visualizza* sarà disponibile solo dopo un clic su **Applica**.

Lista consentiti
Questo pulsante consente di aprire la Lista consentiti del vaglio dinamico 636, che viene utilizzata anche per lo Screening posizione. Per esentare un indirizzo IP dallo Screening posizione, fare clic su questo pulsante e specificare l'indirizzo IP e la scadenza dell'esenzione.

Le connessioni SMTP sono accettate ma l'autenticazione è bloccata
Selezionare questa casella di controllo se, per le connessioni SMTP, si desidera bloccare solo le connessioni che tentano di utilizzare l'autenticazione.

Aggiungi intestazione "X-MDOrigin-Country" ai messaggi
Per impostazione predefinita, quando si attiva lo Screening posizione, MDaemon inserisce l'intestazione "X-MDOrigin-Country" nei messaggi, per filtrare i contenuti o per altri scopi. Questa intestazione contiene i codici ISO 3166 a due lettere di paesi e continenti invece dei nomi completi. Se non si desidera che l'intestazione venga inserita nei messaggi, deselezionare la casella di controllo.

4.1.3.9 Scansione intestazione From



Scansione intestazione From

Questa funzione di sicurezza modifica l'intestazione "From:" dei messaggi in entrata in modo che la parte dell'intestazione che indica solo il nome, ora contenga sia il nome che l'indirizzo e-mail. Questo metodo serve a fronteggiare la tattica comunemente utilizzata nello spam e negli attacchi in cui il messaggio sembra provenire da altro destinatario. Quando si visualizza un elenco di messaggi, i client di posta elettronica in genere visualizzano solo il nome del mittente anziché nome e indirizzo e-mail. Per visualizzare l'indirizzo e-mail, il destinatario deve prima aprire il messaggio o eseguire altre azioni analoghe, ad esempio fare clic con il pulsante destro del mouse sulla voce, posizionare il puntatore sul nome o altro. Per questo motivo i responsabili degli attacchi di solito creano una e-mail in modo che un nome di persona o di azienda legittimi siano visualizzati nella parte visibile dell'intestazione "From:" mentre l'indirizzo e-mail non legittimo risulti nascosto. Ad esempio, l'intestazione "From:" di un messaggio dovrebbe effettivamente essere, `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, ma è possibile che il client visualizzi solo `"Honest Bank and Trust"` come mittente. Questa funzione consente di modificare la parte visibile dell'intestazione in modo da visualizzare entrambe le parti. Nell'esempio sopra riportato il mittente viene ora visualizzato come `"Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>`, fornendo così un'indicazione chiara che il messaggio non è affidabile.

Aggiungi indirizzo e-mail al nome visualizzato
Selezionare questa opzione per modificare la parte visibile del client in modo tale che l'intestazione "From:" dei messaggi in entrata includa sia il nome che l'indirizzo e-mail del destinatario. La struttura della nuova intestazione cambierà da `"Nome mittente" <cassettaPostale@esempio.com>` in `"Nome mittente (cassettaPostale@esempio.com)" <cassettaPostale@esempio.com>`. Questa funzione è valida solo per i messaggi inviati a utenti locali ed è disattivata per impostazione predefinita. Prima di attivare questa opzione, tener conto del fatto che alcuni utenti potrebbero non aspettarsi o desiderare la modifica dell'intestazione From: nonostante sia utile a identificare le e-mail illegittime.

Inserisci l'indirizzo e-mail prima del nome
Quando si utilizza l'opzione *Aggiungi indirizzo e-mail al nome visualizzato* sopra descritta, abilitare l'opzione quando si desidera scambiare nome e indirizzo e-mail nell'intestazione "From:" modificata, in modo che l'indirizzo e-mail sia riportato per primo. Sempre secondo l'esempio sopra riportato, `"Nome utente" <cassettaPostale@esempio.com>` diventa: `"cassettaPostale@esempio.com (Nome mittente)" <cassettaPostale@esempio.com>`.

Sostituisci gli indirizzi e-mail dichiarati con quelli reali nei nomi visualizzati
Un'altra tattica utilizzata nei messaggi spam è l'inserimento di un nome e un indirizzo e-mail dall'apparenza legittima nella parte visibile dell'intestazione "From:" anche se non si tratta dell'indirizzo reale del mittente. Utilizzare questa opzione se si desidera sostituire l'indirizzo e-mail visibile in messaggi come questo con l'effettivo indirizzo e-mail del mittente.

Non applicare queste funzionalità ai messaggi autenticati
Selezionare questa casella di controllo se non si desidera applicare le opzioni di Scansione intestazione From ai messaggi in arrivo autenticati da MDaemon.

Elenco esenzioni
Utilizzare questa opzione per aggiungere indirizzi all'elenco esenzioni di Scansione intestazione From. Per i messaggi inviati agli indirizzi elencati l'intestazione "From:" non verrà modificata.

4.1.4 SSL e TLS

MDaemon supporta il protocollo Secure Sockets Layer (SSL)/Transport Layer Security (TLS) per SMTP, POP e IMAP 587 e per MDaemon Remote Administration 594 e il server Web di Webmail 590. Il protocollo SSL, sviluppato da Netscape Communications Corporation, è il metodo standard per la protezione delle comunicazioni Web tra server e client e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché SSL è integrato in tutti i principali browser attualmente sul mercato, la semplice installazione di un

certificato digitale valido sul server attiverà le funzionalità SSL del browser che si connette a MDRA o Webmail.

Se si esegue la connessione alle porte di posta standard mediante un client e-mail invece di utilizzare Webmail, MDaemon supporta l'estensione STARTTLS su TLS per SMTP e IMAP e l'estensione STLS per POP3. Tuttavia, è necessario che il client sia configurato per l'uso di SSL e che supporti queste estensioni, dal momento che non tutti i client prevedono tale supporto. Utilizzare le pagine Lista nessun STARTTLS 599 e Lista STARTTLS 600 per designare host e indirizzi specifici che non devono o devono, rispettivamente, usare STARTTLS.

La finestra di dialogo SSL & TLS contiene anche una pagina in cui è possibile attivare DNSSEC 604 (DNS Security Extensions), la pagina Estensioni SMTP 601 in cui attivare Richiedi TLS, MTA-STA e report TLS e la paginaLet's Encrypt 605 per i casi in cui si utilizza Let's Encrypt come autorità di certificazione (CA, Certificate Authority).

Le opzioni che consentono di abilitare e configurare il protocollo SSL si trovano nella sezione SSL e TLS della finestra di dialogo Impostazioni sicurezza, disponibile in Sicurezza » Security Manager » SSL & TLS. Le impostazioni delle porte SSL per i protocolli SMTP, POP3 e IMAP si trovano nella finestra Porte 110, accessibile dal percorso: Impostazioni » Impostazioni server » DNS e IP. Le porte HTTPS per Webmail 590 e Remote Administration 594 sono disponibili nelle rispettive schermate.

Per ulteriori informazioni sulla creazione e l'uso dei certificati SSL, vedere:

Creazione e uso dei certificati SSL 928

—

Il protocollo TLS/SSL è descritto in RFC-4346: Transport Layer Security (TLS) Protocol Versione 1.1

L'estensione STARTTLS per SMTP è descritta in RFC-3207: Estensione del servizio SMTP per connessioni SMTP protette su Transport Layer Security

L'uso di TLS con i protocolli IMAP e POP3 è descritto in RFC-2595: Uso di TLS con IMAP, POP3 e ACAP

DNSSEC (DNS Security Extensions) è definita in: RFC-4033: Introduzione e requisiti della sicurezza DNS e RFC-4035: Modifiche del protocollo per le estensioni di sicurezza DNS as

Per una descrizione completa di RequireTLS, vedere: RFC 8689: Opzione SMTP Richiedi TLS.

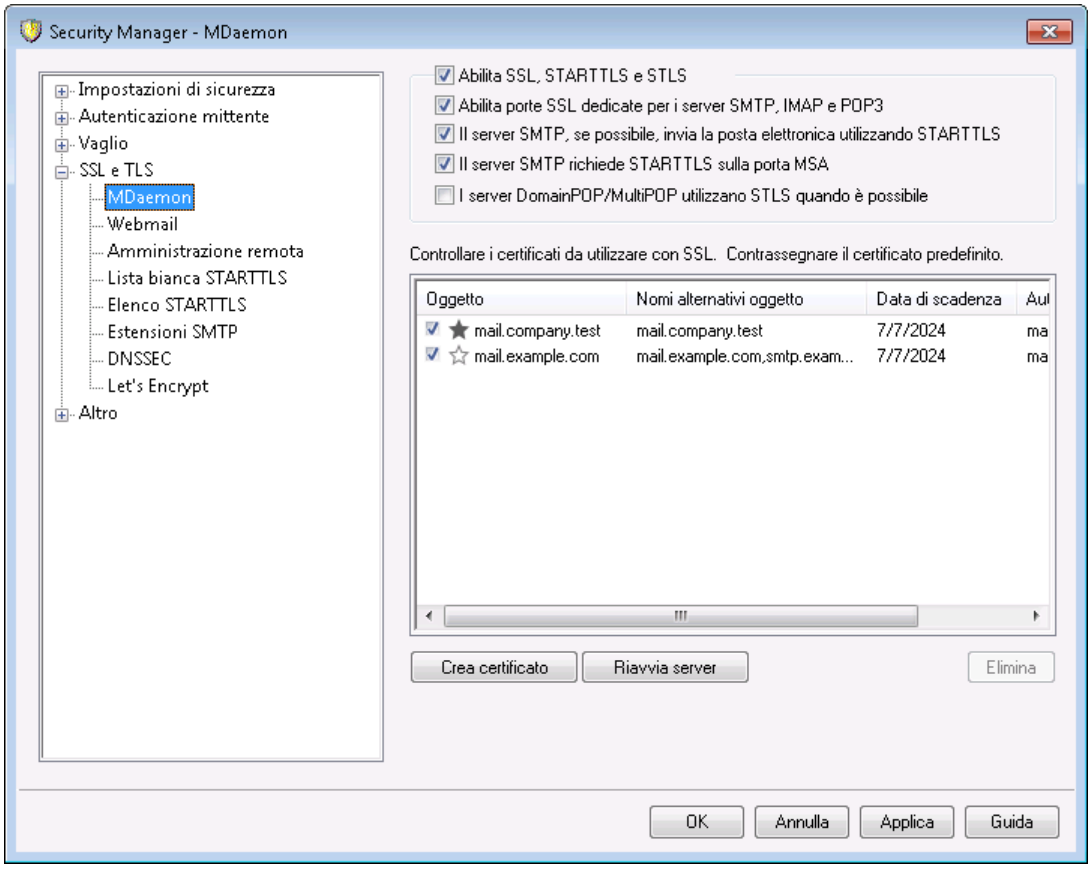
Il supporto di MTA-STS è descritto in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

I report TLS sono illustrati in RFC 8460: Report TLS SMTP.

Per ulteriori informazioni, vedere:

SSL e TLS » MDaemon 587
SSL & TLS » Webmail 590
SSL & TLS » Remote Administration 594

4.1.4.1 MDaemon



Abilita SSL, STARTTLS e STLS
Selezionare questa casella di controllo per attivare il supporto per i protocolli SSL/TLS e le estensioni STARTTLS e STLS, quindi scegliere il certificato che si desidera utilizzare nell'elenco successivo.

Abilita porte SSL dedicate per i server SMTP, IMAP e POP3
Attivare questa opzione per abilitare le porte SSL dedicate, specificate nella finestra Porte 110 di Dominio predefinito/server. Ciò non condiziona l'uso da parte dei client di STARTTLS e STLS con le porte di posta predefinite, ma fornisce solo un livello di supporto maggiore per il protocollo SSL.

Il server SMTP, se possibile, invia la posta elettronica utilizzando STARTTLS
Selezionare questa opzione per tentare di utilizzare l'estensione STARTTLS per tutti i messaggi SMTP inviati. Se il server al quale ci si connette non supporta l'estensione STARTTLS, il messaggio viene consegnato normalmente senza utilizzare il protocollo SSL. Utilizzare Lista nessun STARTTLS 599 se si desidera impedire l'uso di STARTTLS per determinati domini.

Il server SMTP richiede STARTTLS sulla porta MSA
Attivare questa opzione per richiedere STARTTLS per le connessioni al server eseguire mediante la porta MSA 110.

I server DomainPOP/MultiPOP utilizzano STLS laddove è possibile
Selezionare questa casella di controllo per fare in modo che i server DomainPOP e MultiPOP utilizzino l'estensione STLS ogniqualvolta sia possibile.

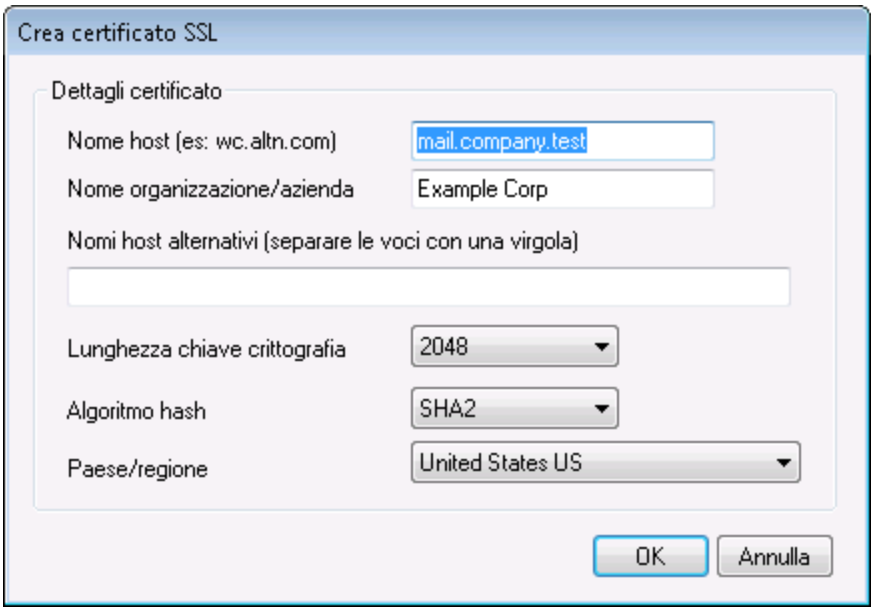
Seleziona certificato da utilizzare con SSL

Questa casella consente di visualizzare i certificati SSL. Selezionare la casella di controllo accanto ai certificati che si intende attivare. Fare clic sulla stella accanto a quello che si desidera impostare come certificato predefinito. MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito. Fare doppio clic su un certificato per aprirlo nella finestra di dialogo Certificato di Windows e visualizzarne i dettagli (funzionalità disponibile solo nell'interfaccia dell'applicazione, non nell'amministrazione remota basata su browser).

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Viene visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Crea certificato

Fare clic su questo pulsante per aprire la finestra di dialogo Crea certificato SSL.



Dettagli certificato

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "mail.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto. Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Algoritmo hash
Scegliere l'algoritmo hash che si desidera utilizzare: SHA1 o SHA2. L'impostazione predefinita è SHA2.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

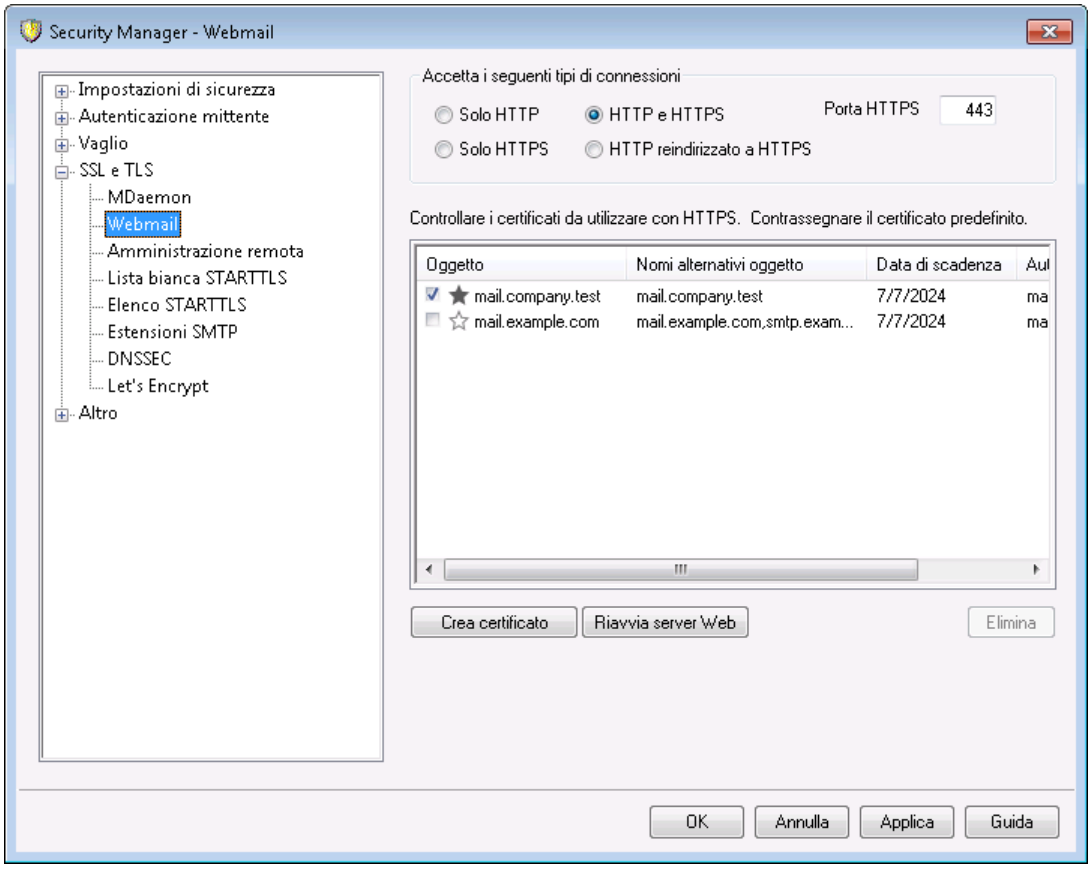
Riavvia server

Per riavviare i server SMTP/IMAP/POP, fare clic su questa opzione. Quando vengono apportate delle modifiche al certificato, è necessario riavviare i server.

Vedere:

SSL e TLS 585
Creazione e uso dei certificati SSL 928

4.1.4.2 Webmail



Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). SSL è il metodo standard per la protezione delle comunicazioni

Web tra server e client. e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare Webmail per l'utilizzo di HTTPS si trovano nella schermata SSL & HTTPS accessibile da Impostazioni » Web e Servizi IM » Webmail". Per comodità, tuttavia, queste opzioni sono anche riportate in "Sicurezza » Security Manager » SSL & TLS » Webmail".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 585

Questa finestra di dialogo è valida per Webmail solo quando si utilizza il server Web incorporato di MDaemon. Se si configura Webmail per l'uso con un altro server Web come IIS, queste opzioni non saranno utilizzate. Il supporto SSL/HTTPS dovrà essere configurato utilizzando gli altri strumenti per i server web.

Accetta i seguenti tipi di connessioni

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a Webmail. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in Webmail e non si desidera imporre agli utenti di Webmail l'utilizzo di HTTPS. Webmail rimane in attesa di connessioni sulla porta HTTPS indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta TCP di Webmail definita nella schermata Server Web 330 di Webmail.

Solo HTTPS
Scegliere questa opzione se si desidera che HTTPS sia il protocollo richiesto al momento della connessione a Webmail. Se si attiva questa opzione, Webmail risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da Webmail per le connessioni SSL. Il valore predefinito della porta SSL è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di Webmail (vale a dire, "https://example.com" è equivalente a "https://example.com:443").

Questa porta è diversa dalla porta di Webmail definita nella scheda Server Web 330. Se le connessioni HTTP a Webmail sono consentite, devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

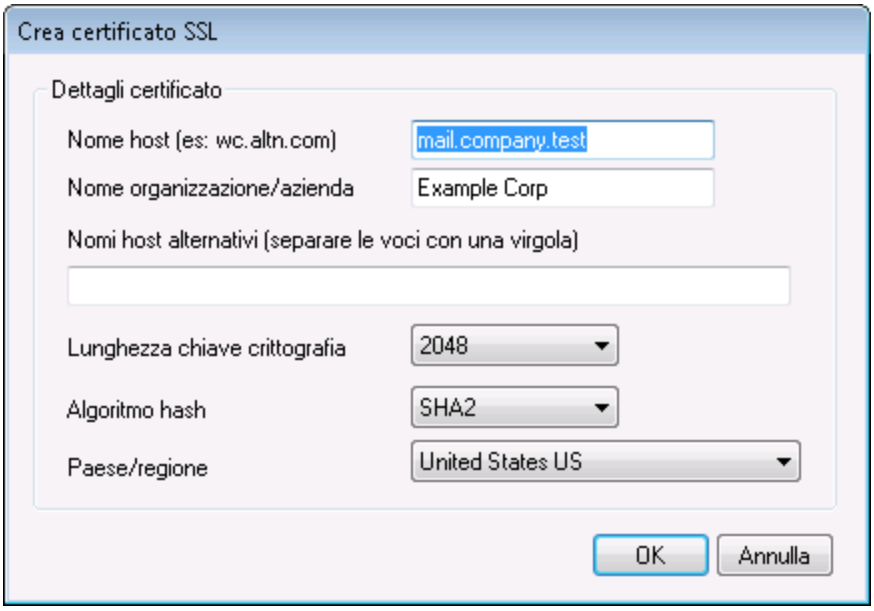
Seleziona certificato da usare per HTTPS/SSL

Questa casella consente di visualizzare i certificati SSL. Selezionare la casella di controllo accanto ai certificati che si intende attivare. Fare clic sulla stella accanto a quello che si desidera impostare come certificato predefinito. MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito. Fare doppio clic su un certificato per aprirlo nella finestra di dialogo Certificato di Windows e visualizzarne i dettagli (funzionalità disponibile solo nell'interfaccia dell'applicazione, non nell'amministrazione remota basata su browser).

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Crea certificato

Fare clic su questo pulsante per aprire la finestra di dialogo Crea certificato SSL.



Dettagli certificato

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto. Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Algoritmo hash
Scegliere l'algoritmo hash che si desidera utilizzare: SHA1 o SHA2. L'impostazione predefinita è SHA2.

Riavvia server Web

Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare un nuovo certificato, è necessario riavviare il server Web.

Utilizzo di Let's Encrypt per la gestione del certificato

Let's Encrypt è un'autorità di certificazione (CA) che fornisce certificati gratuiti mediante un processo automatizzato che si pone la finalità di eliminare i processi più complessi di creazione, convalida, firma, installazione e rinnovo manuali dei certificati per i siti Web sicuri.

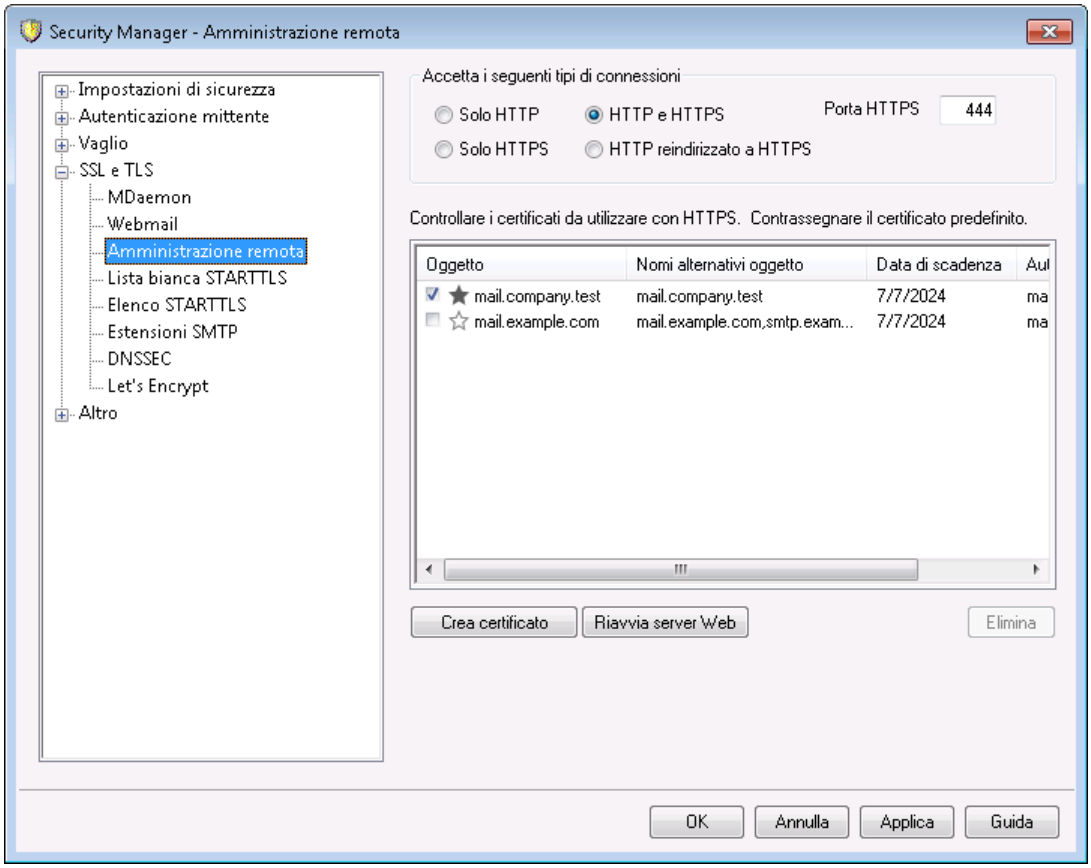
Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un

certificato, è disponibile la schermata Let's Encrypt[605] che consente di configurare ed eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP[188] del dominio predefinito[185] come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica. Vedere l'argomento Let's Encrypt[605] per ulteriori informazioni.

Vedere:

SSL e certificati[585]
Creazione e uso dei certificati SSL[928]

4.1.4.3 Remote Administration



Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). SSL è il metodo standard per la protezione delle comunicazioni Web tra server e client. e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare Remote Administration per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in Impostazioni » Web e Servizi IM » Remote Administration. Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » Remote Administration".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 585

Questa schermata è valida per Remote Administration solo quando si utilizza il server Web incorporato di MDaemon. Se si configura Remote Administration per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Accetta i seguenti tipi di connessioni

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a Remote Administration. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in Remote Administration e non si desidera imporre agli utenti di Remote Administration l'utilizzo di HTTPS. Remote Administration rileva le connessioni sulla porta HTTPS designata di seguito, ma risponde comunque alle normali connessioni http sulla porta TCP di Remote Administration della schermata Server Web 361.

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a Remote Administration. Se si attiva questa opzione, Remote Administration risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da Remote Administration per le connessioni SSL. La porta SSL predefinita è 444. Se si utilizza la porta SSL predefinita, non sarà necessario includere il numero di porta nell'URL di Remote

Administration per la connessione via HTTPS (ovvero, "https://esempio.com" equivale a https://esempio.com:444").

> Non si tratta della stessa porta di Remote Administration designata nella schermata Server Web. Se consentite, le connessioni HTTP a Remote Administration devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

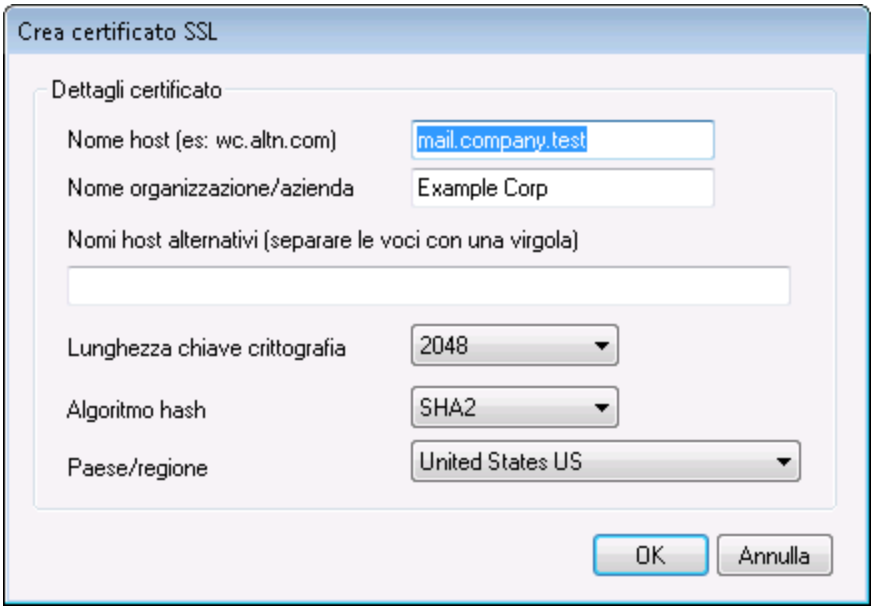
Seleziona certificato da usare per HTTPS/SSL

Questa casella consente di visualizzare i certificati SSL. Selezionare la casella di controllo accanto ai certificati che si intende attivare. Fare clic sulla stella accanto a quello che si desidera impostare come certificato predefinito. MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto (è possibile specificare i nomi alternativi quando si crea il certificato). Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito. Fare doppio clic su un certificato per aprirlo nella finestra di dialogo Certificato di Windows e visualizzarne i dettagli (funzionalità disponibile solo nell'interfaccia dell'applicazione, non nell'amministrazione remota basata su browser).

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Crea certificato

Fare clic su questo pulsante per aprire la finestra di dialogo Crea certificato SSL.



Dettagli certificato

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

MDaemon supporta l'estensione Server Name Indication (SNI) del protocollo TLS, che consente di utilizzare un certificato diverso per ciascun nome host del server. MDaemon analizzerà i certificati attivi e sceglierà quello con il nome host richiesto nel campo Nomi alternativi oggetto. Se il client non richiede un nome host oppure se non viene individuato alcun certificato corrispondente, viene utilizzato il certificato predefinito.

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Algoritmo hash
Scegliere l'algoritmo hash che si desidera utilizzare: SHA1 o SHA2. L'impostazione predefinita è SHA2.

Riavvia server Web

Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare un nuovo certificato, è necessario riavviare il server Web.

Utilizzo di Let's Encrypt per la gestione del certificato

Let's Encrypt è un'autorità di certificazione (CA) che fornisce certificati gratuiti mediante un processo automatizzato che si pone la finalità di eliminare i processi più complessi di creazione, convalida, firma, installazione e rinnovo manuali dei certificati per i siti Web sicuri.

Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un certificato, è disponibile la schermata Let's Encrypt 605 che consente di configurare ed

eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP[188] del dominio predefinito[185] come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica. Vedere l'argomento Let's Encrypt[605] per ulteriori informazioni.

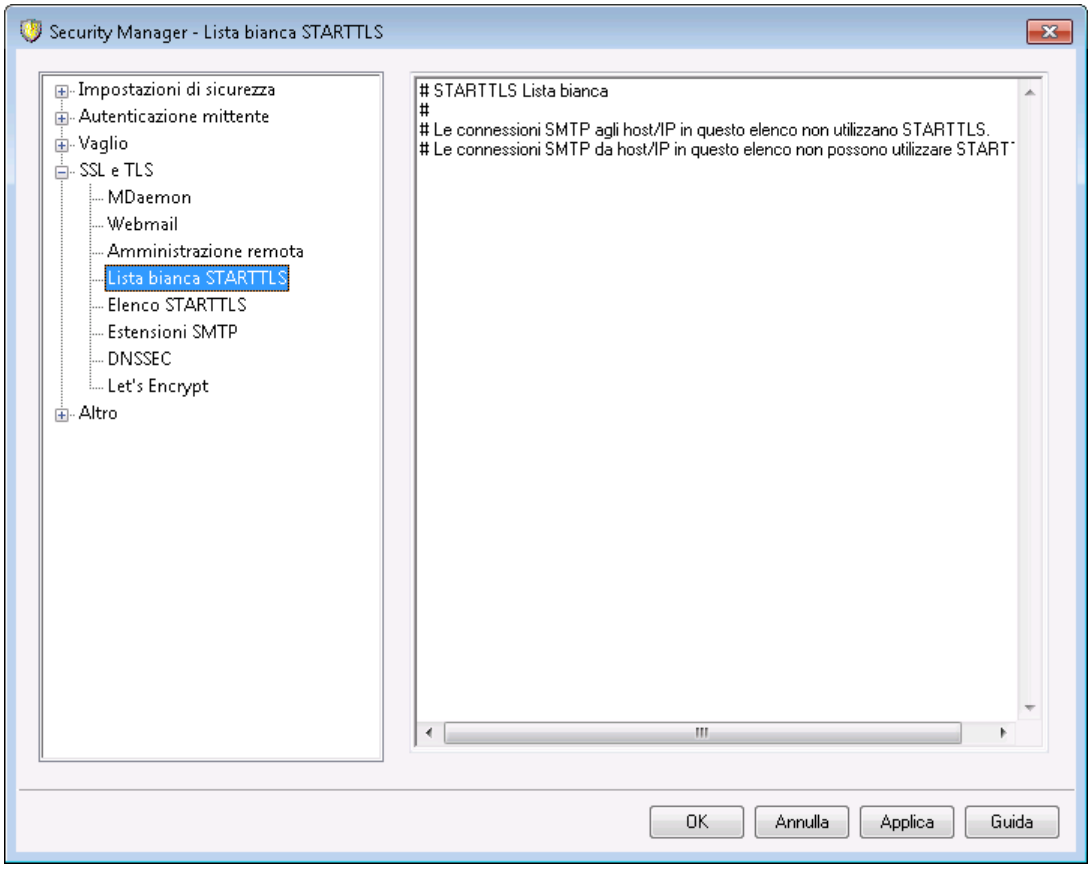
Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere:

Esecuzione di Remote Administration in IIS[368]
SSL e certificati[585]
Creazione e uso dei certificati SSL[928]

Per ulteriori informazioni su Remote Administration, vedere:

Configurazione remota[359]
Remote Administration » Server Web[361]
Valori predefiniti di accesso Web[814]
Account Editor » Accesso Web[735]

4.1.4.4 Lista nessun STARTTLS



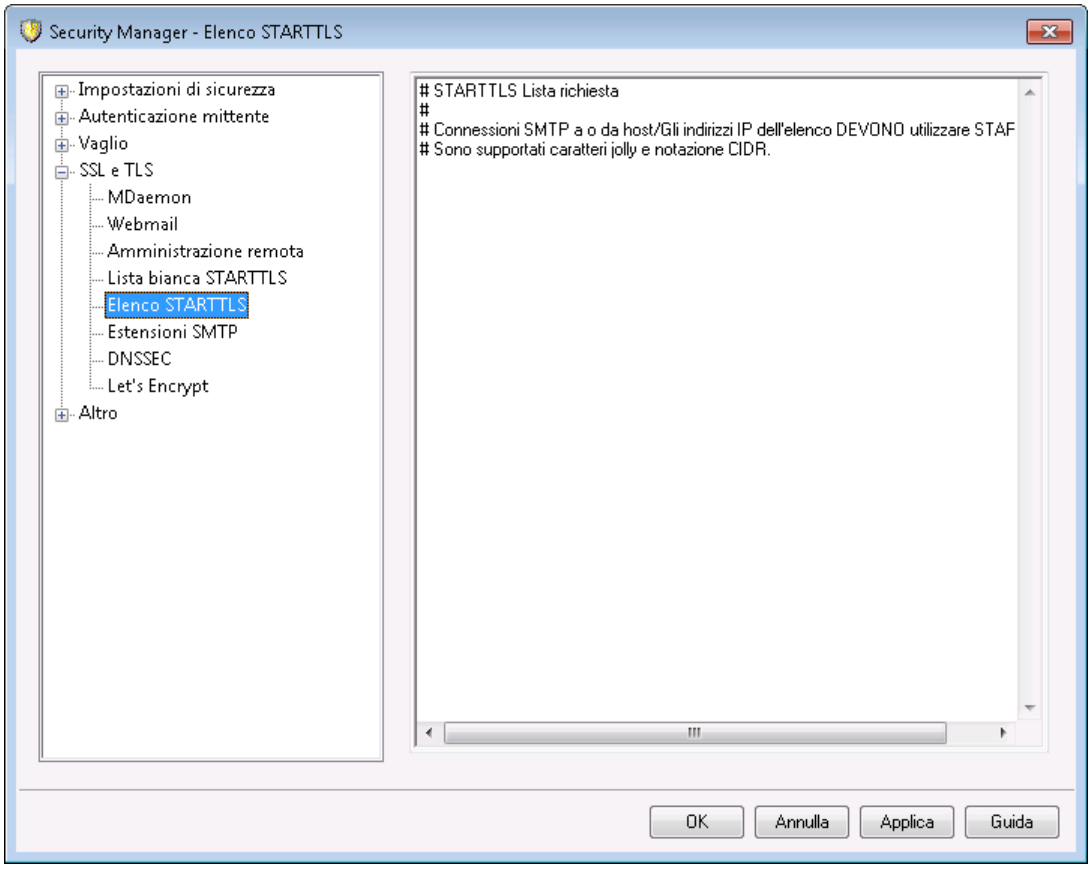
Utilizzare questa lista per impedire l'uso di STARTTLS quando si invia o si riceve posta da o verso determinati host o indirizzi IP.

La Lista nessun STARTTLS è prioritaria rispetto alla Lista obbligatoria STARTTLS 600 e all'opzione *Per il server SMTP è obbligatoria la STARTTLS sulla porta MSA.* 587

L'estensione STARTTLS per SMTP viene descritta nella RFC-3207, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc3207.txt.

4.1.4.5 Elenco STARTTLS

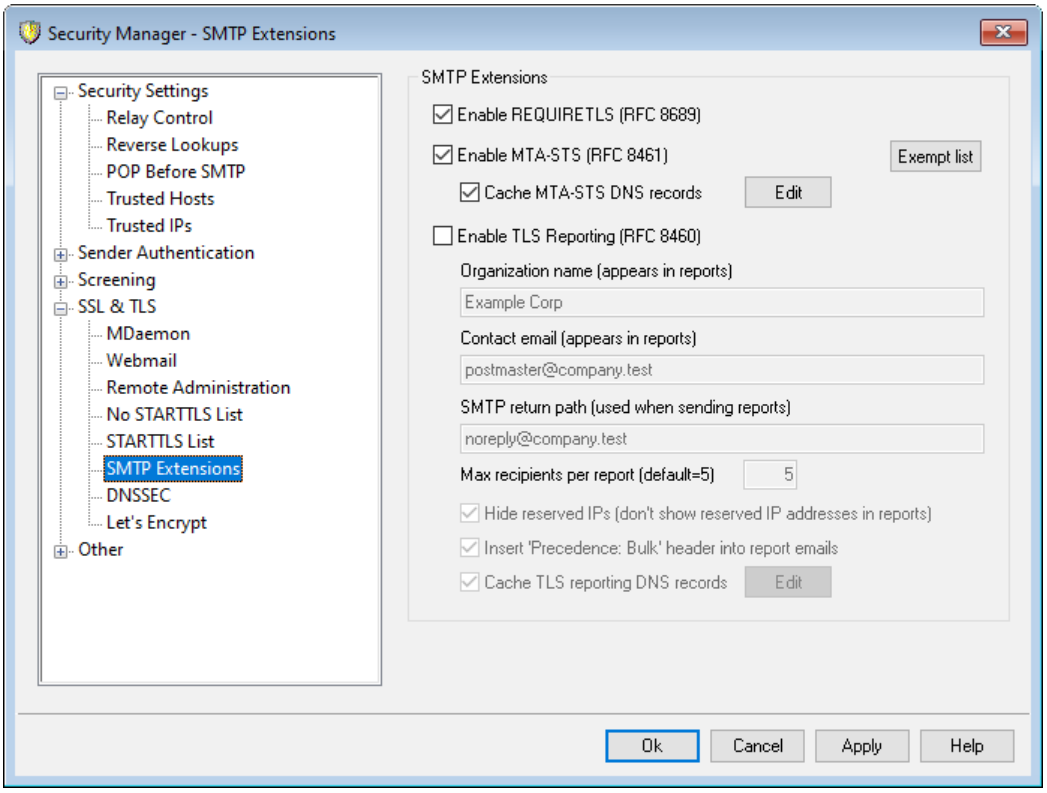


Utilizzare questa schermata per indicare host, indirizzi IP e indirizzi MAIL FROM che richiedono l'utilizzo dell'estensione STARTTLS, per poter ricevere posta dal server.

L'estensione STARTTLS per SMTP viene descritta nella RFC-3207, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc3207.txt.

4.1.4.6 Estensioni SMTP



Estensioni SMTP

Attiva REQUIRETLS (RFC 8689)
RequireTLS consente di contrassegnare i messaggi che **devono** essere inviati usando TLS. Se l'invio tramite TLS non è possibile (o se i parametri dello scambio del certificato TLS sono inaccettabili) i messaggi torneranno al mittente invece di essere consegnati in modo non sicuro. Per una descrizione completa di RequireTLS, vedere: RFC 8689: Opzione SMTP Richiedi TLS.

RequireTLS è attivato per impostazione predefinita, ma solo i messaggi contrassegnati in modo specifico con una regola creata usando una nuova azione ContentFilter 661, "*Contrassegna messaggi per REQUIRETLS...*", o i messaggi inviati a `<local-part>+requiretls@domain.tld` (ad esempio, `arvel+requiretls@mdaemon.com`) sono sottoponibili all'elaborazione RequireTLS. Tutti gli altri messaggi vengono trattati come se il servizio fosse disattivato. Esistono diversi requisiti da soddisfare perché un messaggio possa essere inviato usando RequireTLS. In mancanza di alcuni di essi i messaggi non saranno inviati e torneranno al mittente invece di essere inviati in modo non sicuro. I requisiti sono:

- RequireTLS deve essere attivato.
- Il messaggio deve essere contrassegnato come richiedente l'uso di RequireTLS, mediante l'azione di filtro contenuti o l'indirizzo "`<localpart>+requiretls@....`

- Le ricerche DNS degli host MX destinatari devono utilizzare DNSSEC[604] (vedere di seguito) oppure MX deve essere convalidato da MTA-STS.
- La connessione all'host ricevente deve utilizzare SSL (STARTTLS).
- Il certificato SSL dell'host ricevente deve corrispondere al nome host MX e concatenarsi a una CA attendibile.
- Il server di posta ricevente deve supportare REQUIRETLS e dichiararlo nella risposta EHLO.

RequireTLS richiede la ricerca DNSSEC degli host di record MX, oppure MX deve essere convalidato da MTA-STS. È possibile configurare DNSSEC[604] specificando i criteri in base ai quali le ricerche richiederanno il servizio DNSSEC. Cache IP[115] di MDaemon ha un'opzione per l'accettazione delle asserzioni DNSSEC ed esistono istruzioni correlate a DNSSEC all'inizio del file degli host MX[108]. Infine, DNSSEC richiede server DNS configurati in modo appropriato, operazione che non viene illustrata nel presente file della Guida in linea.

Attiva MTA-STS (RFC 8461)
Il supporto di MTA-STS è attivato per impostazione predefinita ed è descritto in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP MTA Strict Transport Security (MTA-STS) è un meccanismo che consente ai fornitori di servizi di posta (SP) di dichiarare la propria idoneità a ricevere connessioni SMTP protette con Transport Layer Security (TLS) e di specificare se i server SMTP di invio si rifiuterebbero di recapitare posta a host MX che non offrono TLS con un certificato di server affidabile. Per impostare MTA-STS per il proprio dominio, è necessario disporre di un file di policy MTA-STS che si può scaricare via HTTPS dall'URL https://mta-sts.dominio.tld/.well-known/mta-sts.txt, dove per "dominio.tld" si intende il nome del proprio dominio. Il file di testo della policy deve contenere stringhe nel seguente formato:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

La modalità può essere "none", "testing" o "enforce". Deve essere presente una stringa "mx" per ciascuno dei nomi di host MX. È possibile utilizzare un carattere jolly per i sottodomini, ad esempio "*.dominio.tld". Il valore di max_age è espresso in secondi. I valori più comuni sono 86400 (1 giorno) e 604800 (1 settimana).

È inoltre necessario un record TXT DNS in _mta-sts.dominio.tld, dove per "dominio.tld" si intende il nome del proprio dominio. Deve essere presente un valore nel formato:

```
v=STSv1; id=20200206T010101;
```

Il valore di "id" deve essere modificato ogni volta che si cambia file di policy. Di solito si utilizza un indicatore di data e ora come id.

Elenco esenzioni
Utilizzare questo elenco per esentare specifici domini da MTA-STS.

Aggiungi record MTA-STS DNS in cache
Per impostazioni MDaemon aggiunge i record MTA-STS DNS in cache. Fare cli su **Modifica** per visualizzare o modificare il file della cache corrente.

Attiva report TLS (RFC 8460)
I report TLS sono disabilitati per impostazione predefinita e illustrati in RFC 8460: Report TLS SMTP.

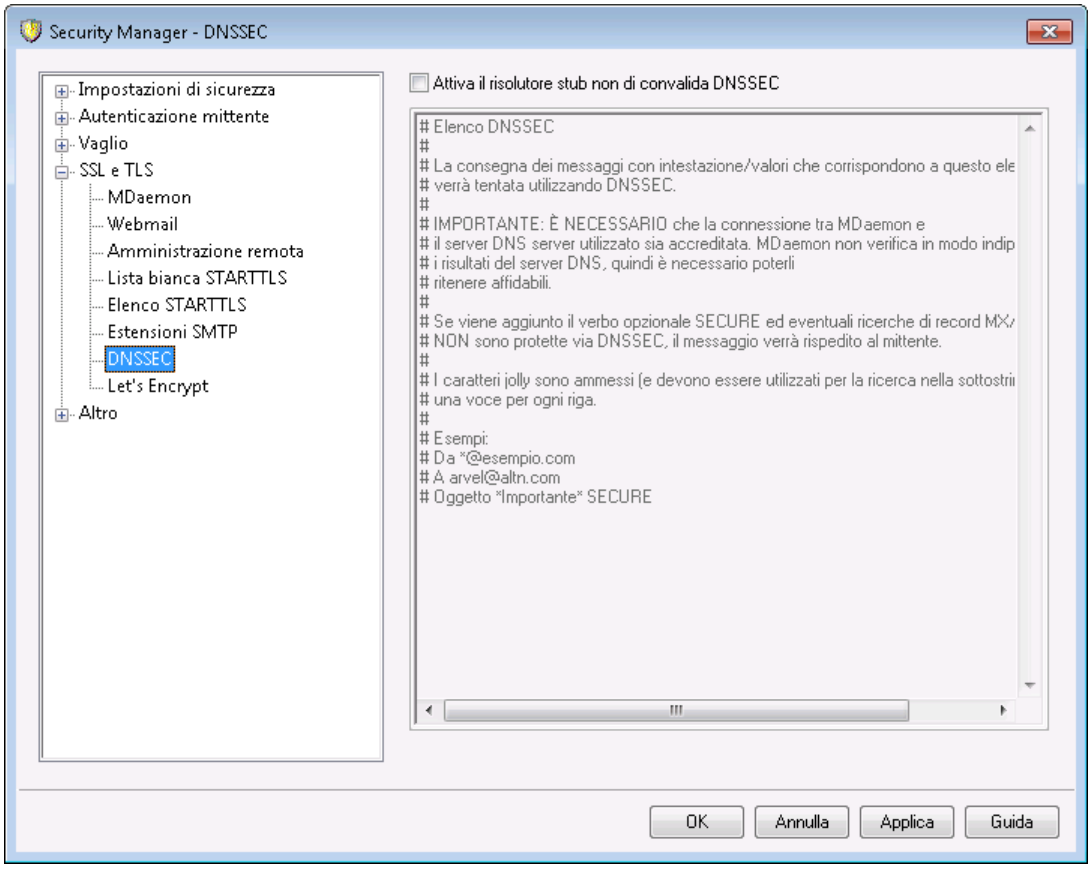
I report TLS consentono ai domini di che utilizzano MTA-STS di ricevere notifiche relative agli eventuali errori di recupero delle policy MTA-STS o di negoziazione di un canale sicuro che utilizzi STARTTLS. Quando i report sono abilitati, MDaemon invia un report giornaliero a ciascun dominio abilitato per STS a cui ha inviato (o tentato di inviare) posta durante la giornata. Sono disponibili diverse opzioni per configurare le informazioni che saranno contenute dai report.

Per abilitare i report TLS per il proprio dominio, è necessario attivare la firma DKIM 539 e creare un record TXT DNS in `_smtp._tls.dominio.tld`, dove per "dominio.tld" si intende il nome del proprio dominio, con un valore nel seguente formato:

```
v=TLSRPTv1; rua=mailto:mailbox@dominio.tld
```

Dove mailbox@dominio.tld è l'indirizzo e-mail a cui si desidera che vengano inviati i report per il proprio dominio.

4.1.4.7 DNSSEC



L'opzione DNSSEC (DNS Security Extensions) consente a MDaemon di agire come risolutore stub non di convalida in grado di riconoscere la sicurezza, definito in RFC 4033 e 4035 come "una entità che invia query DNS, riceve risposte DNS ed è in grado di stabilire un canale protetto in modo appropriato a un server dei nomi ricorsivo in grado di riconoscere la sicurezza che fornirà questi servizi per conto del risolutore stub in grado di riconoscere la sicurezza". Questo significa che durante le query DNS di MDaemon può essere richiesto il servizio DNSSEC dai propri server DNS, impostando il bit AD (Authentic Data) nelle query e verificandone la presenza nelle risposte. Questo può fornire un livello di sicurezza aggiuntivo durante il processo DNS per alcuni messaggi, anche se non per tutti, perché DNSSEC non è ancora supportato da tutti i server DNS o per tutti i domini di livello superiore.

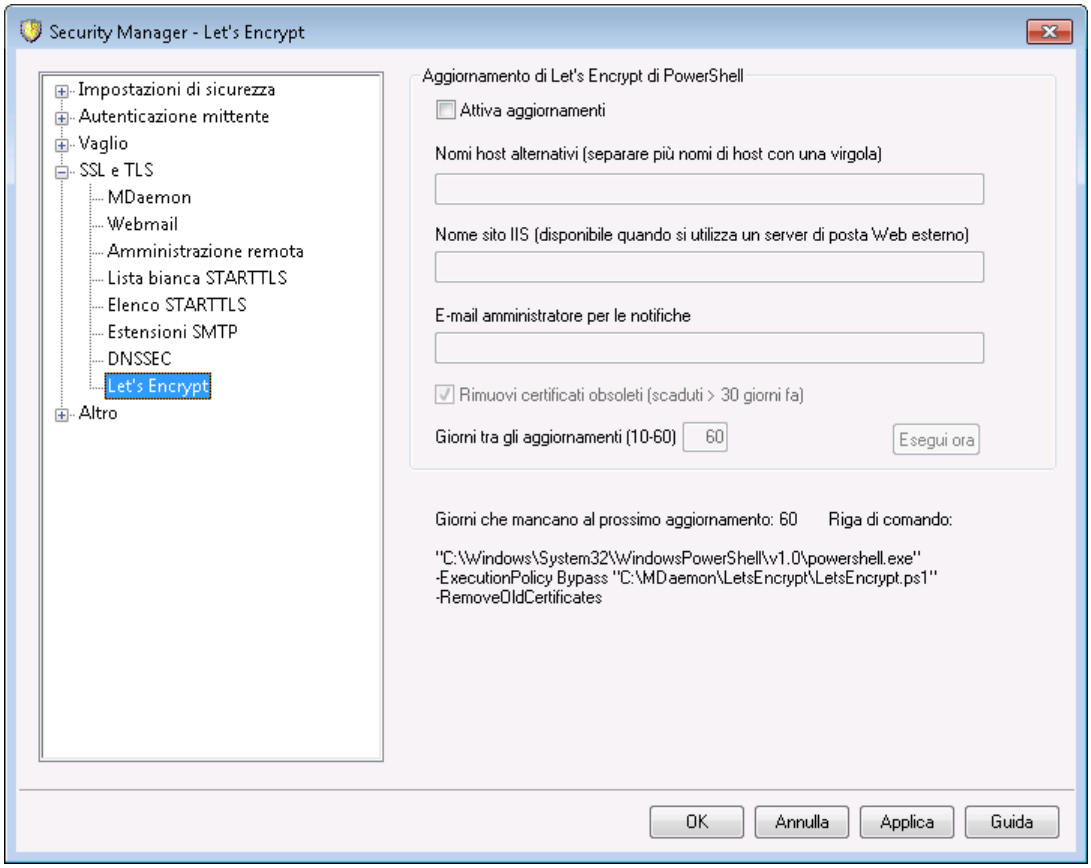
Quando abilitato, il servizio DNSSEC viene applicato solo ai messaggi che soddisfano i criteri di selezione. Può essere richiesto o essere considerato obbligatorio nei termini e modalità selezionati dall'utente. È sufficiente specificare le combinazioni "`intestazione/valore`" selezionate nella schermata e MDaemon richiederà il servizio DNSSEC per i messaggi che corrispondono al criterio ogni volta che esegue una query DNS. Quando i risultati DNS non includono dati autenticati, non ne derivano conseguenze negative; MDaemon torna semplicemente al normale comportamento DNS. Se tuttavia si desidera *richiedere* DNSSEC per specifici messaggi, aggiungere "SECURE" alla combinazione intestazione/valore (ad es. `To *@esempio.net SECURE`). Per questi messaggi, quando i risultati DNS non includono dati autenticati, il messaggio sarà restituito al mittente. **Nota:** poiché le ricerche DNSSEC impiegano più tempo e risorse e

dato che DNSSEC non è ancora supportato da tutti i server, MDaemon non è configurato per applicare DNSSEC a tutti i messaggi consegnati per impostazione predefinita. Tuttavia, se si desidera richiedere DNSSEC per tutti i messaggi, sarà necessario includere "`To *`" nei criteri.

Nei registri delle sessioni di posta sarà presente una riga all'inizio quando il servizio DNSSEC viene utilizzato con "DNSSEC" accanto ai dati protetti nei registri.

Poiché è un risolutore stub non di convalida, MDaemon richiede i dati autenticati al server DNS utilizzato ma non è in grado di verificare in modo indipendente che i dati ricevuti dal server siano sicuri. Ne consegue che per utilizzare in modo corretto l'opzione DNSSEC è necessario verificare che la connessione con il server DNS sia affidabile. Ad esempio, avviene su host locale o all'interno di una LAN o luogo di lavoro sicuro.

4.1.4.8 Let's Encrypt



Utilizzo di Let's Encrypt per la gestione del certificato

Per supportare SSL/TLS e HTTPS[585] per MDaemon[587], Webmail[590] e Remote Administration[594], è necessario un certificato SSL/TLS. I certificati sono file di piccole dimensioni emessi da un'autorità di certificazione (CA) utilizzati per verificare che un client o un browser siano connessi al server previsto e che consentono a SSL/TLS/HTTPS di proteggere la connessione a un determinato server. Let's Encrypt è l'autorità di certificazione CA che fornisce certificati gratuiti mediante un processo automatizzato che intende eliminare il meccanismo complesso con cui attualmente si procede alla creazione, convalida, firma, installazione e rinnovo manuali di certificati per siti Web sicuri.

Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un certificato, è disponibile questa schermata che consente di configurare ed eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP[188] del dominio predefinito[185] come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica.

Let's Encrypt richiede la presenza di PowerShell 5.1 e .Net Framework 4.7.2, non è quindi in grado di funzionare in Windows 2003. Inoltre, Webmail[330] deve essere impostato per l'ascolto sulla porta 80 e lo script non funziona se è stato configurato un nome host SMTP[188] (ovvero FQDN) che non punta al server MDaemon come dominio predefinito.

Aggiornamenti di Let's Encrypt con PowerShell

Attiva aggiornamenti
Selezionare questa casella di controllo per creare e aggiornare automaticamente una certificazione SSL/TLS mediante script di Let's Encrypt. Il certificato viene aggiornato ogni 10-60 giorni, a seconda dell'impostazione di *Frequenza aggiornamenti (10-60 giorni)*.

Nomi host alternativi (separare i nomi host con una virgola)
Per specificare nomi host alternativi nel certificato, specificare tali nomi host qui, separandoli con una virgola. Non è necessario includere il valore del nome host SMTP del dominio predefinito nell'elenco. Se, ad esempio, il dominio predefinito è "`esempio.com`", configurato con il nome host SMTP "`mail.esempio.com`", e si desidera utilizzare il nome host alternativo "`imap.esempio.com`", è sufficiente aggiungere "`imap.esempio.com`" come nome host alternativo. Se non si desidera utilizzare alcun nome host alternativo, lasciare il campo vuoto. **Nota:** se si aggiungono dei nomi host alternativi, è necessario completare una richiesta di

verifica HTTP da Let's Encrypt per ognuno per convalidare il controllo del server per tali nomi host. Se le richieste di verifica non vengono completate tutte il processo non si concluderà in modo corretto.

Nome sito IIS (disponibile quando si utilizza un server di posta Web esterno)
Se si esegue Webmail mediante IIS, immettere il nome del sito IIS qui. È necessario disporre degli strumenti di Web Scripting di Microsoft installati affinché il certificato venga impostato automaticamente in IIS.

E-mail amministratore per notifiche
Se si desidera ricevere una notifica in caso di errore durante un aggiornamento di Let's Encrypt, specificare un indirizzo e-mail dell'amministratore qui.

Rimuovi certificati obsoleti (scaduti > 30 giorni fa)
Per impostazione predefinita MDaemon rimuove i certificati obsoleti scaduti da più di 30 giorni. Per non rimuovere automaticamente i certificati, deselezionare la casella di controllo.

Frequenza aggiornamenti (10-60 giorni)
Utilizzare questa opzione per specificare la frequenza dell'aggiornamento del certificato, da 10 a 60 giorni. Il valore predefinito è 60 giorni.

Esegui ora
Fare clic su questo pulsante per avviare immediatamente lo script.

4.1.5 Altro

4.1.5.1 Protezione backscatter - Panoramica

Backscatter

Il termine "Backscatter" si riferisce ai messaggi di risposta ricevuti dagli utenti relativi a messaggi mai spediti. Ciò si verifica quando i messaggi spam o i messaggi inviati da virus includono un indirizzo di ritorno contraffatto. Di conseguenza, se uno di questi messaggi viene respinto dal server del destinatario o se all'account del destinatario è associata una risposta automatica relativa, ad esempio, all'assenza per vacanze o trasferimento, il messaggio di risposta viene diretto all'indirizzo contraffatto. Ciò provoca la ricezione di migliaia di messaggi fittizi relativi a notifiche dello stato di recapito, a vacanze o assenze, a risposte automatiche e così via. Gli spammer e i creatori di virus, inoltre, sfruttano spesso questo fenomeno e lo utilizzano per lanciare attacchi di tipo DoS (Denial of Service) contro i server di posta, determinando così la ricezione di innumerevoli messaggi e-mail non validi da server sparsi in tutto il mondo.

Soluzione di MDaemon

Per contrastare questo fenomeno, MDaemon include una funzionalità chiamata Protezione backscatter (BP, Backscatter Protection). Questa funzionalità utilizza un metodo di codifica hash di una chiave privata per generare e inserire nell'indirizzo del percorso di ritorno dei messaggi in uscita uno speciale codice con validità temporale

limitata, in modo da consentire la ricezione dei soli messaggi di riposta e di notifica di recapito legittimi. Quando uno di tali messaggi riscontra un problema di consegna e viene rispedito oppure quando viene ricevuto un messaggio di risposta automatica al quale è associato il percorso di ritorno "mailer-daemon@..." o NULL, MDaemon è in grado di individuare il codice speciale e di verificare che si tratta di una risposta automatica legittima a un messaggio spedito da uno degli account in uso. Se il messaggio include un indirizzo privo del codice speciale o se quest'ultimo ha più di sette giorni, l'evento viene registrato da MDaemon e il messaggio può essere rifiutato.

La funzione Protezione Backscatter 608 è disponibile in: Sicurezza » Impostazioni sicurezza » Altro » Protezione backscatter.

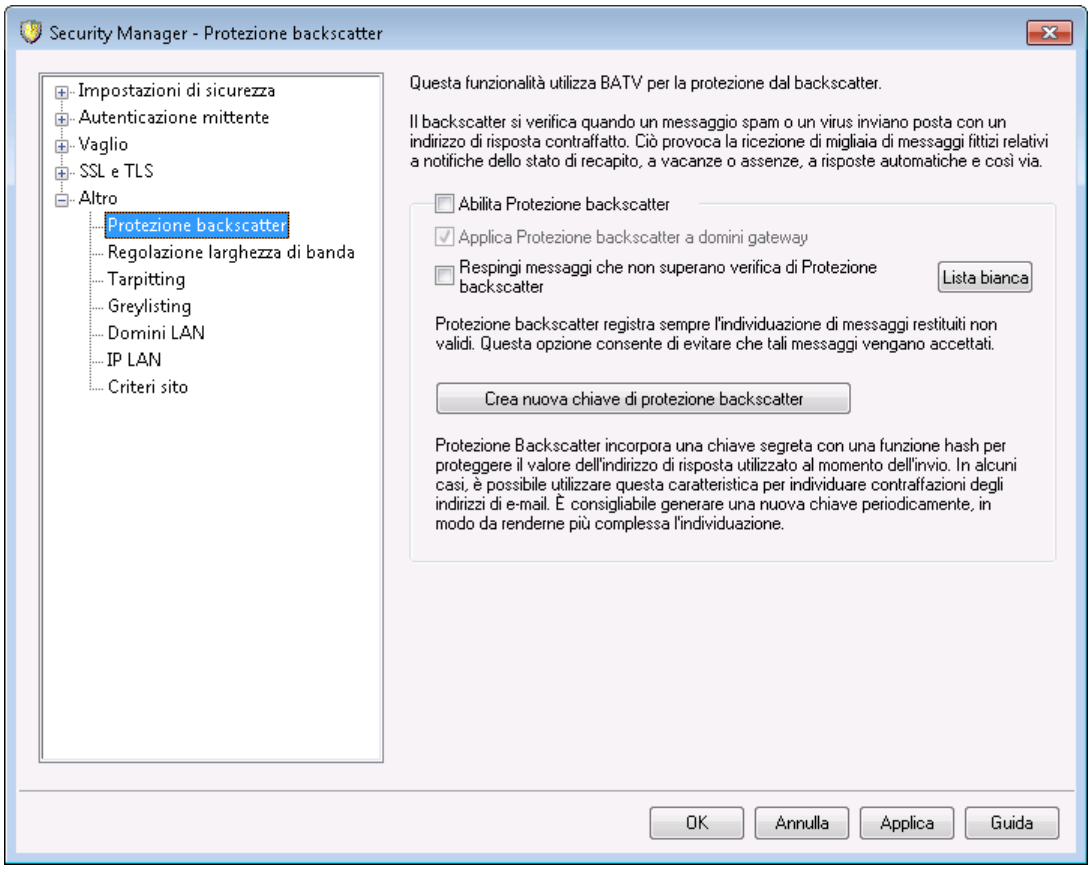
La funzionalità Protezione backscatter è un'implementazione della convalida BATV (Bounce Address Tag Validation). Per ulteriori informazioni su BATV, visitare il sito

http://www.mipassoc.org/batv/

Per ulteriori informazioni, vedere:

Protezione backscatter 608

4.1.5.1.1 Protezione backscatter



Protezione backscatter

Abilita Protezione backscatter
Selezionare questa casella di controllo se si desidera inserire un codice speciale di Protezione backscatter nell'indirizzo "Return-Path" di ciascun messaggio. Il codice viene generato utilizzando la chiave privata inclusa nel file `rsa.private` che si trova nella cartella `PEM\_batv\` di MDaemon. Il codice è valido per sette giorni. I messaggi DSN in entrata o di risposta automatica, ai quali è associato il percorso di ritorno "`mailer-daemon@...`" o `NULL` devono includere un codice Protezione backscatter valido; in caso contrario, la convalida ha esito negativo.

Se l'opzione viene disabilitata, il codice speciale di Protezione backscatter non viene inserito nei messaggi in uscita. La funzionalità rimane attiva, tuttavia, per verificare che i messaggi di notifica dello stato del recapito e di risposta automatica che includono un codice valido non vengano erroneamente respinti.

Applica Protezione backscatter a domini gateway
Quando è attiva la Protezione backscatter, fare clic su questa opzione se si desidera applicarla anche ai domini per i quali MDaemon funge da gateway o da server di backup. (vedere Gateway Manager 255).

Respingi messaggi che non superano la verifica di Protezione backscatter
Selezionare questa casella di controllo se si desidera rifiutare i messaggi di notifica dello stato del recapito o di risposta automatica che non superano la convalida di Protezione backscatter. I messaggi ai quali è associato il percorso di ritorno "`mailer-daemon@...`" o `NULL` non superano la verifica se sono privi del codice speciale o se quest'ultimo ha più di sette giorni. Grazie all'affidabilità della Protezione backscatter, non sono possibili falsi positivi né esistono aree di incertezza: un messaggio è valido oppure non lo è. È quindi possibile configurare MDaemon in modo che respinga i messaggi non validi, purché tutti i messaggi in uscita dagli account includano lo speciale codice di Protezione backscatter. Il risultato della verifica di Protezione backscatter viene sempre registrato nel file registro SMTP (entrata), anche se si sceglie di non respingere i messaggi che non superano la verifica. I messaggi in entrata relativi ai gateway non vengono respinti a meno che l'opzione *Applica Protezione backscatter a domini gateway* non sia stata selezionata.

Quando si abilita la funzionalità Protezione backscatter è opportuno attendere una settimana prima di attivare l'opzione che consente di scartare i messaggi di risposta automatica non validi. In questa finestra temporale, infatti, possono essere ricevuti messaggi di notifica dello stato del recapito o di risposta automatica inviati prima dell'attivazione di Protezione backscatter e attivando tale opzione alcuni messaggi di riposta legittimi potrebbero essere erroneamente respinti. Una settimana rappresenta un periodo di tempo ragionevole per l'attivazione dell'opzione di scarto dei messaggi non validi.

> Questa avvertenza è valida anche nel caso in cui si crei una nuova chiave di Protezione backscatter e si elimini immediatamente quella precedente, senza continuare a utilizzarla per una settimana. Per ulteriori informazioni, vedere l'opzione *Crea nuova chiave di protezione backscatter*.

Elenco esenzioni
Fare clic su questo pulsante per aprire l'elenco esenzioni di Protezione backscatter. In questa lista è possibile indicare gli indirizzi IP o i domini che si desidera escludere dalla protezione backscatter.

Crea nuova chiave di protezione backscatter
Fare clic su questo pulsante per creare una nuova chiave di protezione backscatter. Questa chiave viene utilizzata da MDaemon per creare e verificare i codici speciali inseriti nei messaggi. La chiave è inclusa nel file `rsa.private` che si trova nella cartella `PEM\_batv\` di MDaemon. Quando viene generata la nuova chiave, una finestra di messaggio segnala che la chiave precedente rimane operativa per sette giorni, a meno che non la si elimini immediatamente. Nella maggior parte dei casi è opportuno scegliere "**No**" e continuare a utilizzare la chiave per altri sette giorni. Se la chiave viene eliminata immediatamente, la verifica di alcuni dei messaggi legittimi in entrata potrebbe avere esito negativo perché rappresentano risposte a messaggi che includono il codice speciale generato dalla chiave precedente.

Se il traffico relativo all'e-mail è suddiviso tra più server, è possibile che il file contenente la chiave debba essere condiviso da tutti i server o da tutti gli MTA (Mail Transfer Agent) in uso.

Vedere:

Protezione backscatter - Panoramica 607

4.1.5.2 Regolazione larghezza di banda - Panoramica

La funzionalità di regolazione della larghezza di banda è una nuova funzione che consente di controllare la larghezza di banda utilizzata da MDaemon. È possibile controllare la velocità di avanzamento delle sessioni o dei servizi, impostando velocità diverse per ogni servizio principale di MDaemon in base al dominio, compresi i domini e i gateway di dominio. È inoltre possibile impostare i limiti per le connessioni locali selezionando "Traffico locale" in una casella a discesa. In questo modo, possono essere create particolari impostazioni per la larghezza di banda, che verranno applicate se la connessione ha origine o fine in un indirizzo IP locale o in un nome di dominio.

La funzione di regolazione della larghezza di banda può essere applicata sia in base alla sessione, sia in base al servizio. Se la funzione è applicata in base alla sessione, la velocità di ogni sessione viene regolata indipendentemente dalle altre. Di conseguenza, più sessioni dello stesso tipo di servizio attive contemporaneamente possono superare il

valore impostato per il servizio. Quando si configura la regolazione della larghezza di banda in base al servizio, MDaemon controlla l'utilizzo complessivo delle sessioni relative allo stesso tipo di servizio e suddivide equamente la larghezza di banda totale. Più sessioni quindi condividono equamente la larghezza di banda massima configurata. Questo consente di impostare un limite per l'intero servizio.

Quando si estende la funzione Regolazione larghezza di banda a un gateway di dominio, è necessario gestire il gateway in modo leggermente diverso dal solito, in quanto a questo non è associato un indirizzo IP. Per determinare se al gateway sia associata la sessione SMTP in entrata, MDaemon deve utilizzare il valore passato al comando RCPT. In caso affermativo, alla sessione SMTP in entrata viene applicata la regolazione della larghezza di banda. A causa dei limiti di SMTP, se uno dei destinatari di un messaggio è rappresentato da un gateway di dominio, la regolazione della larghezza di banda viene applicata all'intera sessione.

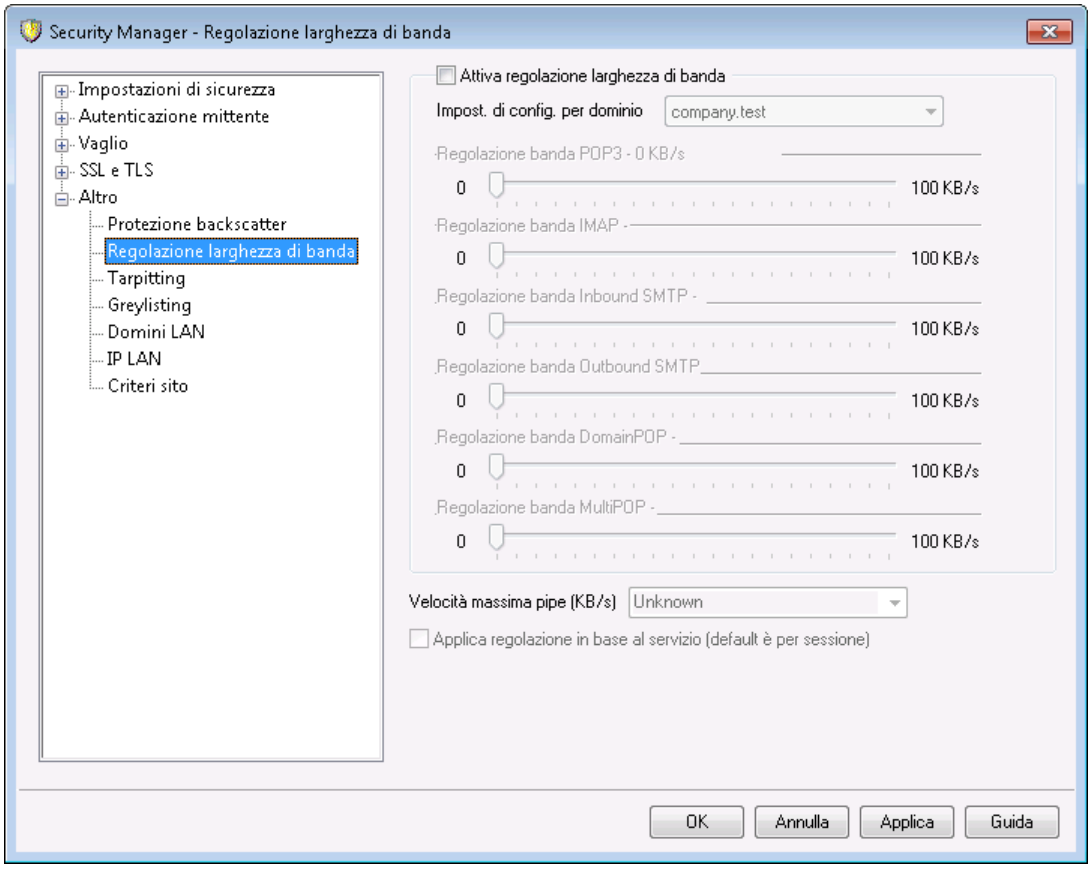
Il sistema Regolazione larghezza di banda opera in termini di kilobyte al secondo (KB/s). Il valore "0", indicando che non è previsto alcun limite alla velocità di avanzamento della sessione o del servizio, consente l'utilizzo della massima larghezza di banda disponibile. Il valore "10", ad esempio, impone a MDaemon di regolare la velocità di trasmissione in modo che questa si attesti su un valore uguale o leggermente superiore a 10 KB/s.

Gli impulsi di attività all'inizio di una sessione possono superare i limiti fissati. La regolazione ha luogo e diventa più precisa durante l'avanzamento della sessione.

Per ulteriori informazioni, vedere:

Regolazione larghezza di banda 612
IP LAN 620

4.1.5.2.1 Regolazione larghezza di banda



Attiva regolazione larghezza di banda
Questa casella di controllo consente di attivare la funzione Regolazione larghezza di banda.

Impost. di config. per dominio
Selezionare un dominio nell'elenco a discesa e impostare le opzioni relative ai vari servizi per configurare la regolazione della larghezza di banda del dominio selezionato. L'impostazione di un particolare controllo su "0" indica che per la larghezza di banda di quel tipo di servizio non è previsto alcun limite. L'ultima voce dell'elenco a discesa è *Traffico locale*. Impostando la regolazione della larghezza di banda per questa opzione, si determina un limite per il traffico locale, ovvero per le sessioni e i servizi che utilizzano la LAN locale. La schermata IP LAN 620 consente di indicare l'elenco dei domini e degli indirizzi IP da considerare locali.

Servizi

Regolazione della larghezza di banda - [tipo di servizio] - XX KB/s
Dopo aver selezionato un dominio nell'elenco a discesa, è possibile utilizzare questi controlli per impostare un limite alla larghezza di banda del dominio selezionato. L'impostazione del valore "0" indica che non è previsto alcun limite per la larghezza di banda del particolare tipo di servizio. Scegliendo un numero diverso da zero, si

imposta un limite sulla larghezza di banda, in kilobyte al secondo, per il servizio selezionato.

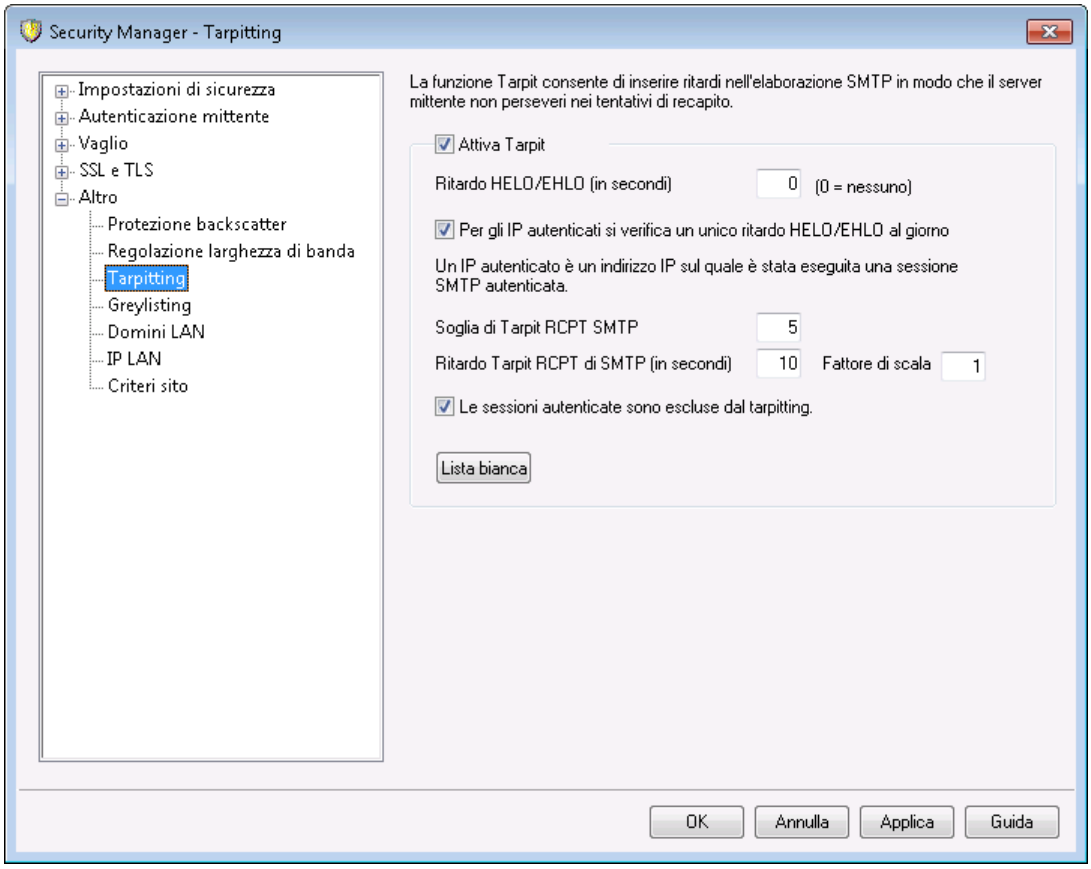
Velocità massima pipe (KB/s)
Scegliere la velocità massima di connessione, in kilobyte al secondo, dall'elenco a discesa.

Applica regolazione in base al servizio (default è per sessione)
Abilitare questa casella di controllo se si desidera applicare la regolazione della larghezza di banda in base al servizio anziché la sessione, secondo l'impostazione predefinita. Quando la regolazione è impostata in base al servizio, la quantità di larghezza di banda allocata viene suddivisa equamente tra tutte le sessioni attive di quel tipo di servizio. Di conseguenza, la quantità totale di larghezza di banda utilizzata, ad esempio, da più client IMAP connessi contemporaneamente non può mai superare la quantità indicata, indipendentemente dal numero dei client connessi. Se la regolazione è impostata in base alla *sessione*, il limite indicato non può essere superato da una singola sessione IMAP, ma solo dal totale di più sessioni attive contemporaneamente.

Per ulteriori informazioni, vedere:

Regolazione larghezza di banda - Panoramica 610

4.1.5.3 Tarpitting



La funzione Tarpitting è disponibile in: `Sicurezza » Impostazioni sicurezza » Altro » Tarpitting`.

Questa funzione consente di rallentare deliberatamente una connessione a seguito della ricezione di un determinato numero di comandi `RCPT` dal mittente. Ciò consente di scoraggiare l'utilizzo del server da parte di coloro che inviano messaggi di posta elettronica indesiderati ("spam"). È possibile specificare il numero di comandi `RCPT` consentiti prima dell'inizio del tarpitting e il numero di secondi di ritardo della connessione ogni volta che si riceve il successivo comando dall'host. L'assunto che sottende a questa tecnica consiste nell'imporre ai mittenti di messaggi indesiderati un periodo di attesa lungo e variabile per l'invio di ogni messaggio, scoraggiandoli così a riutilizzare in futuro il server per questa operazione.

Attiva Tarpit
Per attivare le funzionalità Tarpit di MDaemon, selezionare questa casella di controllo.

Ritardo HELO/EHLO (in secondi)
Utilizzare questa opzione per ritardare la risposta del server ai comandi SMTP `EHLO/HELO`. Un ritardo di risposta pari anche a solo dieci secondi consente di ridurre significativamente il tempo di elaborazione grazie alla riduzione della posta spam ricevuta. Spesso i propagatori di spam fanno affidamento sul rapido recapito dei loro messaggi e, di conseguenza, non restano a lungo in attesa di una risposta ai

comandi EHLO/HELO. Con un ritardo anche minimo, gli strumenti di spam spesso desistono e proseguono con altre attività invece di attendere una risposta. Le connessioni sulla porta MSA (contrassegnate nella schermata Porte 110 sotto Impostazioni server) sono sempre esentate da questo ritardo. L'impostazione predefinita di questa opzione è pari a "0" e indica che i comandi EHLO/HELO non verranno ritardati.

Per gli IP autenticati si verifica un solo ritardo HELO/EHLO al giorno
Selezionare questa casella di controllo se si desidera applicare il ritardo EHLO/HELO una sola volta al giorno nel caso di sessioni autenticate provenienti da specifici indirizzi IP. Il ritardo verrà applicato al primo messaggio proveniente dall'indirizzo IP, ma tutti i messaggi successivi provenienti dallo stesso indirizzo IP non subiranno ritardi.

Soglia di Tarpit RCPT SMTP
Indicare il numero di comandi RCPT del protocollo SMTP consentiti in una sessione di posta prima che MDaemon attivi il tarpitting dell'host. Ad esempio, se si imposta il valore 10 e l'host mittente tenta di inviare un messaggio a 20 indirizzi (ossia utilizza 20 comandi RCPT), MDaemon consentirà il normale inoltro dei primi 10 e si interromperà dopo ogni comando successivo per il numero di secondi specificato nella casella *Ritardo tarpit RCPT di SMTP*.

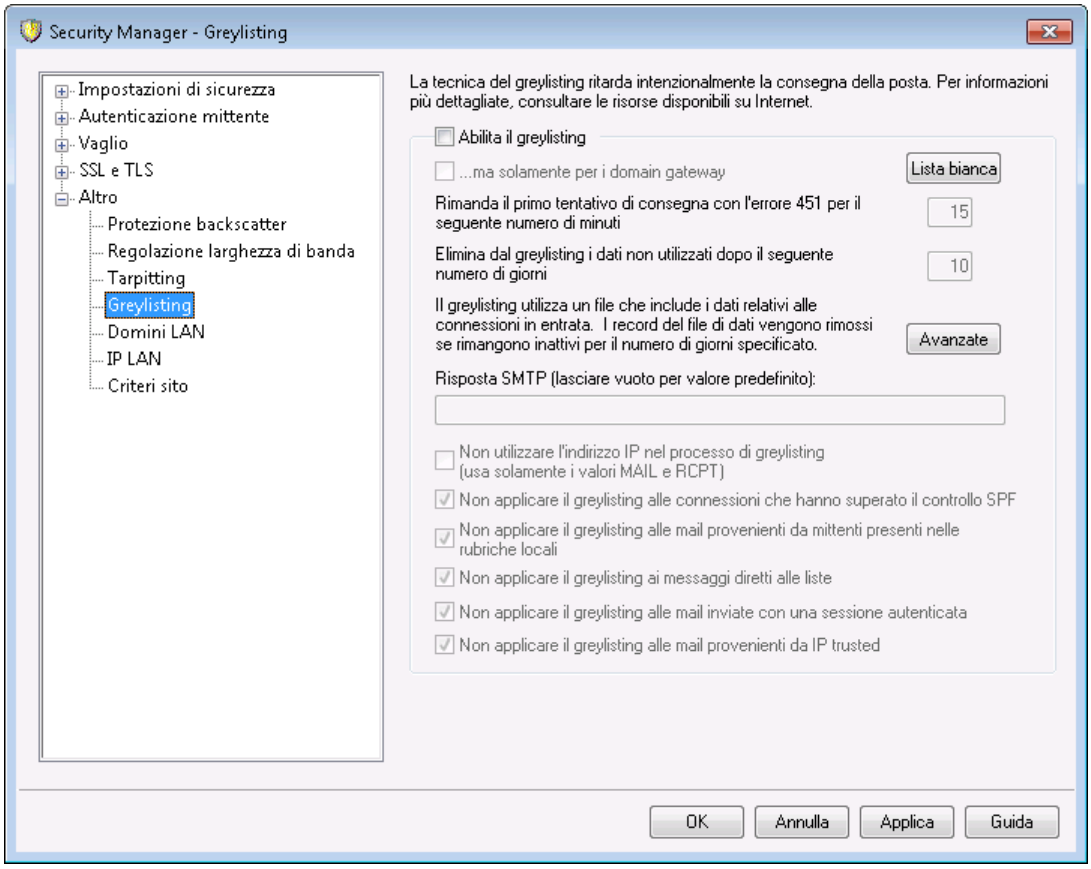
Ritardo Tarpit RCPT di SMTP (in secondi)
Quando viene raggiunto il valore indicato per l'host nel campo *Soglia di Tarpit RCPT SMTP*, MDaemon resterà in attesa per il numero di secondi indicato in questo campo dopo la ricezione di ogni successivo comando RCPT inviato dall'host durante la sessione di posta.

Fattore di scala
Rappresenta il coefficiente in base al quale aumenta il ritardo tarpit nel tempo. Una volta raggiunta la soglia tarpit e applicato alla sessione il ritardo tarpit, la durata del successivo ritardo nella sessione viene determinata moltiplicando questo coefficiente per la durata del ritardo precedente. Ad esempio, se il ritardo tarpit è impostato su 10 e il fattore di scala su 1,5, il primo ritardo sarà di 10 secondi, il secondo di 15, il terzo di 22,5 e il quarto di 33,75, poiché 10 x 1,5 = 15; 15 x 1,5 = 22,5 e così via. Il valore predefinito del fattore di scala è 1 e indica che il ritardo non viene incrementato.

Le sessioni autenticate sono escluse dal tarpitting
Selezionando questa casella di controllo, i mittenti che autenticano le sessioni non vengono interessati dalla funzione di Tarpitting.

Elenco esenzioni
Fare clic su questo pulsante per aprire la Lista consentiti dinamica 636, utilizzata anche per il Tarpitting. all'interno della quale è possibile inserire gli indirizzi IP che si desidera escludere dalla funzione di Tarpitting.

4.1.5.4 Greylisting



La funzione Greylisting è disponibile nella finestra di dialogo Sicurezza, in: `Sicurezza » Impostazioni sicurezza » Altro » Greylisting`. Il Greylisting è una tecnica antispam che sfrutta il fatto che i server SMTP ritentano la consegna di qualsiasi messaggio riceva un codice di errore temporaneo del tipo "riprovare più tardi". Con questa tecnica, quando arriva un messaggio da un mittente non presente nella lista consentiti o comunque sconosciuto, il mittente, il destinatario e l'indirizzo IP del server mittente verranno registrati e il messaggio verrà rifiutato come previsto dal processo di Greylisting durante la sessione SMTP con un codice di errore temporaneo. Ogni successivo tentativo di consegna verrà temporaneamente rifiutato per un intervallo di tempo prestabilito (ad esempio 15 minuti). Dal momento che gli "spammer" in genere non eseguono ulteriori tentativi di consegna una volta che un messaggio viene rifiutato, questa funzione consente di ridurre considerevolmente il numero di messaggi spam ricevuti. Tuttavia, anche se dovessero pensare di ritentare la consegna in un secondo momento, è possibile che a quel punto gli spammer siano stati già identificati e che siano disponibili altre opzioni per la lotta allo spam (ad esempio le Liste bloccati DNS 717) in grado di bloccarli con efficacia. È importante sottolineare, tuttavia, che questa tecnica può ritardare il ricevimento di posta "non spam" insieme a quella indesiderata. I messaggi considerati legittimi vengono comunque consegnati una volta scaduto il periodo di tempo stabilito per il greylisting. È importante anche sottolineare che non esiste un modo per determinare i tempi di attesa dei server di invio prima di ulteriori tentativi di consegna. È possibile che il rifiuto di messaggi con un codice di errore temporaneo determini ritardi di durata indeterminata, compresa tra pochi minuti e un'intera giornata.

Esistono numerosi problemi comuni ed effetti collaterali negativi associati al greylisting. La schermata Greylisting offre una serie di opzioni che consentono di gestire tali problemi.

In primo luogo, per l'invio della posta in uscita alcuni domini utilizzano un insieme di server. Poiché ogni tentativo di consegna può essere effettuato da un server differente, la funzione greylisting considererebbe ogni tentativo come una nuova connessione. Ciò potrebbe aumentare il tempo impiegato per superare il blocco applicato da questa funzione, perché ogni tentativo verrebbe considerato come un messaggio diverso anziché un nuovo tentativo di consegna di un messaggio precedente. Utilizzando un'opzione di ricerca SPF, nel caso di domini di invio che pubblicano i propri dati SPF questo problema può essere risolto. Esiste inoltre un'opzione che consente di ignorare completamente l'indirizzo IP del server di posta. L'utilizzo di questa opzione riduce l'efficienza della funzione greylisting, ma risolve completamente i problemi legati all'invio da server differenti.

In secondo luogo, la funzione greylisting richiede generalmente un database di grandi dimensioni poiché è necessario tenere traccia di ogni connessione in entrata. In MDaemon, la quantità di connessioni di cui tenere traccia è ridotta perché la funzione Greylisting viene applicata in prossimità della fine della sequenza di elaborazione SMTP. Ciò consente di applicare al messaggio tutte le altre opzioni di filtro di MDaemon prima che questo raggiunga la fase di greylisting. Di conseguenza, le dimensioni del file dati per la funzione greylisting vengono significativamente diminuite. Poiché tale file è residente in memoria, inoltre, l'impatto sulle prestazioni è minimo.

Infine, sono disponibili numerose opzioni che consentono di ridurre l'impatto della funzione greylisting sui messaggi "non spam". Innanzitutto, è possibile escludere i messaggi inviati alle liste di distribuzione. Il Greylisting dispone di un proprio elenco di esenzioni in cui è possibile designare indirizzi IP, mittenti e destinatari che si desidera escludere dal processo di Greylisting. Infine, Greylisting offre un'opzione per l'utilizzo della rubrica di ciascun account come elenco esenzioni. È quindi possibile escludere dalla funzione greylisting la posta proveniente da utenti contenuti nella rubrica.

Per ulteriori informazioni generali sulla funzione Greylisting, visitare il sito Internet di Even Harris all'indirizzo:

http://projects.puremagic.com/greylisting/.

Greylisting

Abilita il greylisting
Selezionare questa opzione per attivare la funzione Greylisting.

...ma solamente per i domain gateway
Selezionare questa opzione se si desidera attivare la funzione solo per i messaggi destinati a domini gateway.

Elenco esenzioni
Questo pulsante consente di aprire l'elenco esenzioni dal Greylisting, in cui è possibile designare mittenti, destinatari e indirizzi IP che saranno esenti dal greylisting.

Rimanda il primo tentativo di consegna con l'errore 451 per il seguente numero di minuti
Consente di definire per quanti minuti un tentativo di consegna deve rimanere bloccato dopo il tentativo iniziale. Durante questo intervallo, ogni successivo tentativo di consegna eseguito dalla stessa combinazione server/mittente/destinatario (definita anche come "tripletta Greylist") verrà rifiutato con un altro codice di errore temporaneo. Una volta scaduto l'intervallo di tempo, per la tripletta non verrà implementato alcun ulteriore ritardo a meno che il record di database corrispondente non sia stato eliminato perché scaduto.

Elimina dal database del greylisting i record non utilizzati dopo il seguente numero di giorni
Una volta scaduto il periodo iniziale per una determinata tripletta, ai successivi messaggi relativi alla stessa tripletta non verranno applicati altri ritardi. Tuttavia, se non viene ricevuto alcun messaggio corrispondente alla tripletta per il numero di giorni indicato in questa opzione, il relativo record di database viene eliminato. I tentativi di consegna successivi eseguiti dalla stessa tripletta generano un nuovo record e, di conseguenza, il periodo di ritardo iniziale viene applicato nuovamente.

Avanzate
Fare clic su questo pulsante per aprire il database Greylisting e rivedere o modificare le triplette.

Risposta SMTP (lasciare vuoto per valore predefinito)
Se si immette una stringa di testo personalizzato in questo spazio, MDaemon restituirà la risposta SMTP, "`451 <testo personalizzato immesso>`" invece del messaggio predefinito "`451 Greylisting abilitato. Riprovare tra X minuti`". L'opzione è utile, ad esempio, quando si desidera immettere una stringa che contenga un URL per una descrizione del greylisting.

Non utilizzare l'indirizzo IP nel processo di greylisting (usa solo i valori MAIL e RCPT)
Selezionare questa casella di controllo se non si desidera utilizzare l'indirizzo IP del server di invio come parametro per la funzione greylisting. Ciò consente di risolvere eventuali problemi causati dagli insiemi di server, ma riduce le prestazioni della funzione Greylisting.

Non applicare il greylisting alle connessioni che hanno superato il controllo SPF
Quando si utilizza questa opzione, se un messaggio in arrivo corrisponde al mittente e al destinatario di una tripletta ma non al server di invio e se l'elaborazione SPF indica quest'ultimo come un'alternativa valida a quello elencato nella tripletta, il messaggio viene gestito come una consegna successiva relativa alla stessa tripletta, anziché come una nuova connessione per cui creare un nuovo record Greylisting.

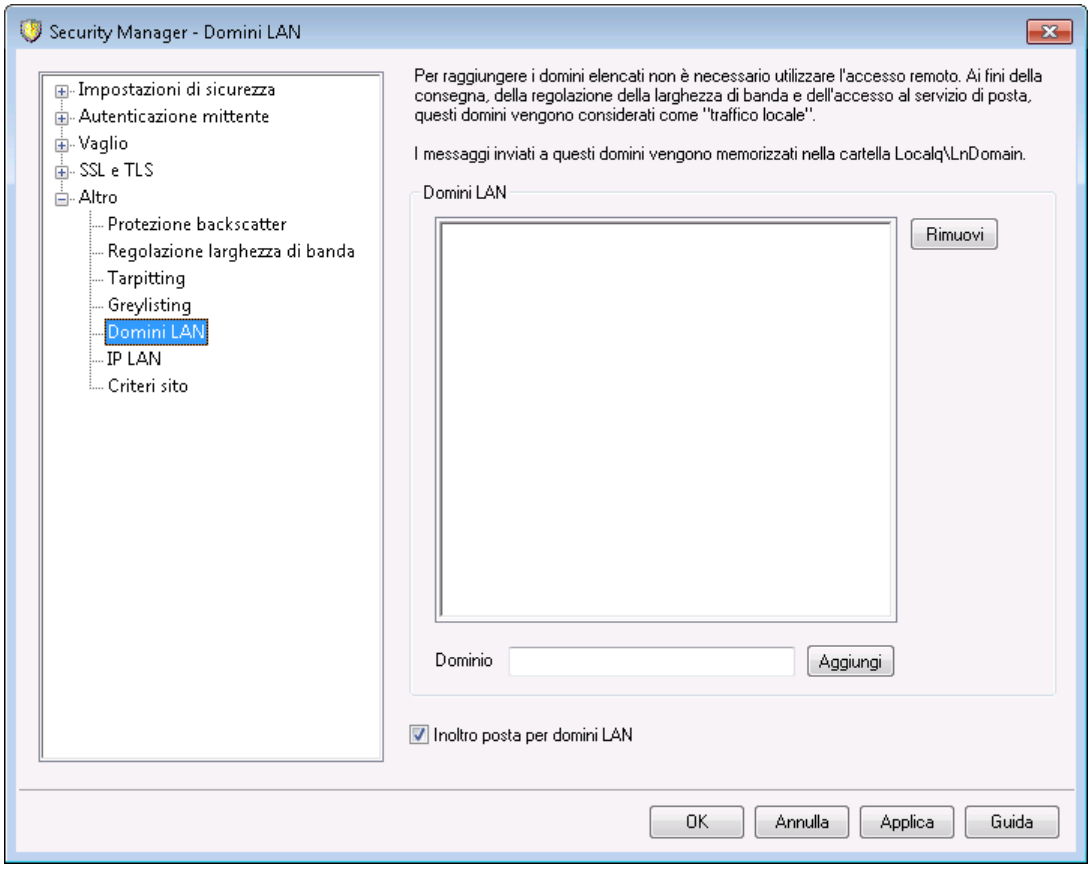
Non applicare il greylisting alle mail provenienti da mittenti presenti nelle rubriche locali
Selezionare questa opzione se si desidera escludere un messaggio dalla funzione Greylisting quando il mittente è presente nella rubrica del destinatario.

Non applicare il greylisting ai messaggi diretti alle liste
Selezionare questa casella di controllo se si desidera escludere dalla funzione Greylisting i messaggi delle liste di distribuzione.

Non applicare il greylisting alle mail inviate con una sessione autenticata
Utilizzare questa opzione se si desidera escludere dalla funzione Greylisting tutti i messaggi in arrivo durante una sessione autenticata.

Non applicare il greylisting alle mail provenienti da IP accreditati
Utilizzare questa opzione se si desidera escludere dalla funzione Greylisting tutti i messaggi provenienti da indirizzi IP accreditati.

4.1.5.5 Domini LAN



Domini LAN

MDaemon considera i domini elencati in questa finestra come parti della rete LAN locale. Di conseguenza, non è necessaria alcuna connessione remota o connessione Internet per consegnare un messaggio a uno di questi domini.

Dominio
Per inserire un nome di dominio nell'elenco, indicarne il nome e fare clic su *Aggiungi*.

Aggiungi
Dopo aver specificato un dominio nell'opzione *Dominio*, fare clic su questo pulsante per aggiungerlo all'elenco.

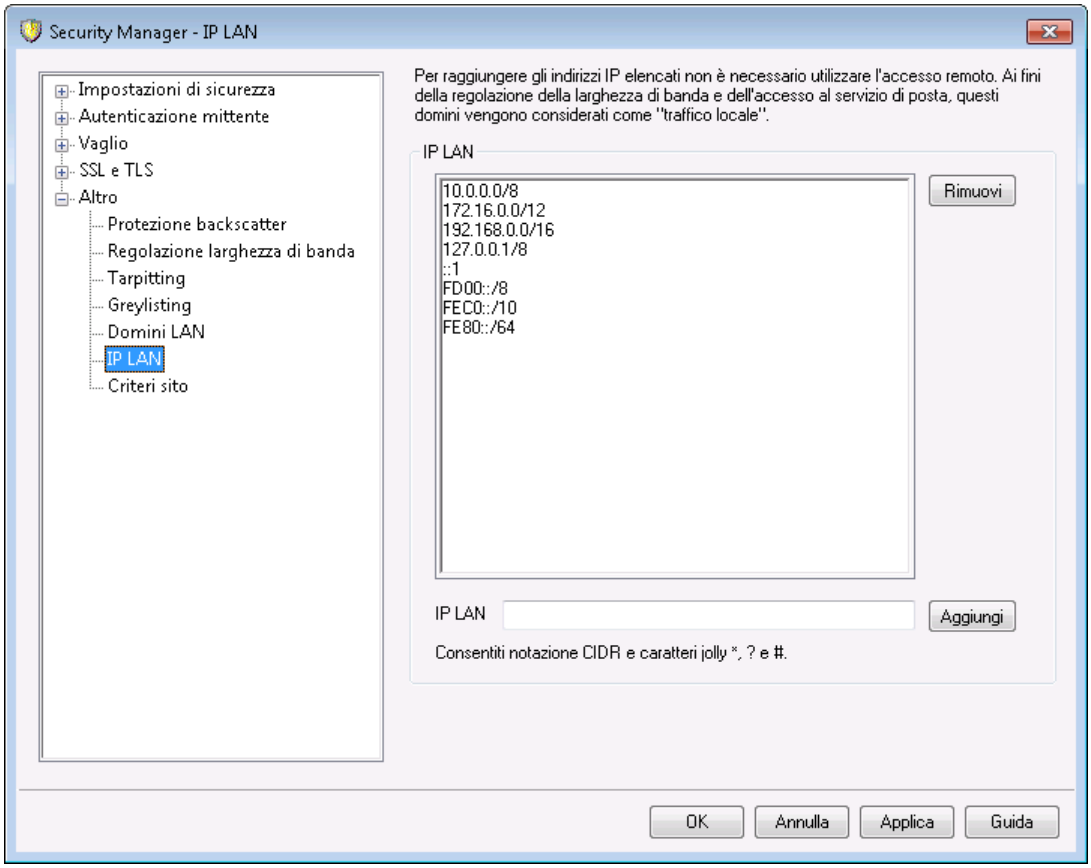
Rimuovi
Selezionare un dominio nell'elenco, quindi fare clic su questo pulsante per rimuoverlo.

Inoltrare posta per i domini LAN
La selezione di questa opzione consente l'inoltro della posta relativa ai domini e offre una forma di controllo sul traffico in entrata e in uscita dai domini.

Vedere:

IP LAN 620

4.1.5.6 IP LAN



IP LAN

Questa schermata, analoga alla schermata Domini LAN 619, consente di specificare gli indirizzi IP presenti sulla rete LAN locale. Questi indirizzi non richiedono una connessione remota o Internet e sono quindi considerati come "traffico locale" ai fini della limitazione della larghezza di banda. Agli indirizzi locali non vengono inoltre applicate numerose limitazioni relative al blocco della posta spam e alla sicurezza.

Rimuovi
Selezionare un indirizzo IP nell'elenco, quindi fare clic su questo pulsante per rimuoverlo.

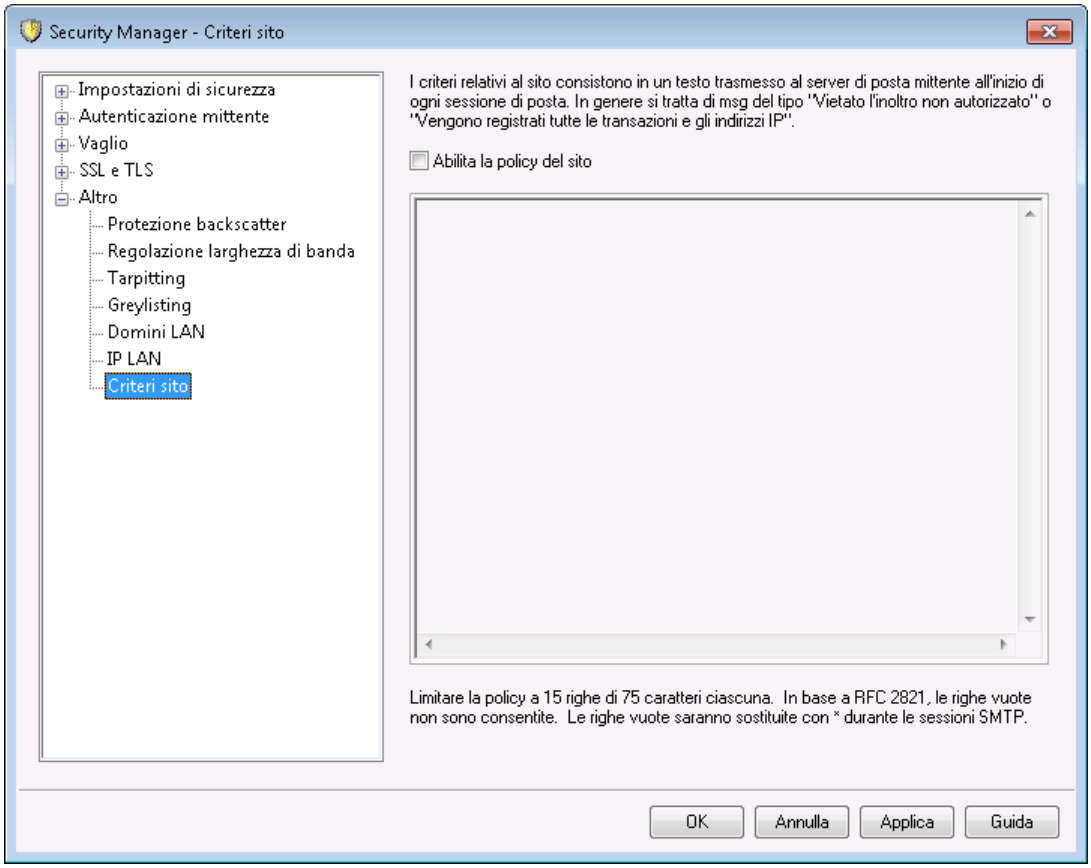
IP LAN
Immettere un indirizzo IP da aggiungere all'elenco degli indirizzi IP locali, quindi fare clic su *Aggiungi*. È possibile utilizzare i caratteri jolly, ad esempio "127.0.*.*".

Aggiungi
Dopo aver immesso un indirizzo IP nel controllo *IP LAN*, fare clic su questo pulsante per aggiungerlo all'elenco.

Vedere:

Domini LAN 619

4.1.5.7 Criteri sito



Creazione di un'informativa relativa alla protezione delle sessioni SMTP
Questa finestra di dialogo consente di specificare un'informativa relativa ai criteri di utilizzo (policy) del sito. Il testo viene memorizzato nel file `policy.dat` che si trova

nella sottocartella \app\ di MDaemon e viene trasmesso ai server di invio all'inizio di ogni sessione di posta SMTP. Esempi comuni di criterio di utilizzo del sito potrebbero essere i seguenti: "Questo server non provvede all'inoltro" oppure "L'uso non autorizzato è vietato". Non è necessario inserire all'inizio di ciascuna riga "220" oppure "220-". MDaemon gestisce di conseguenza ciascuna riga, con o senza il prefisso relativo ai codici.

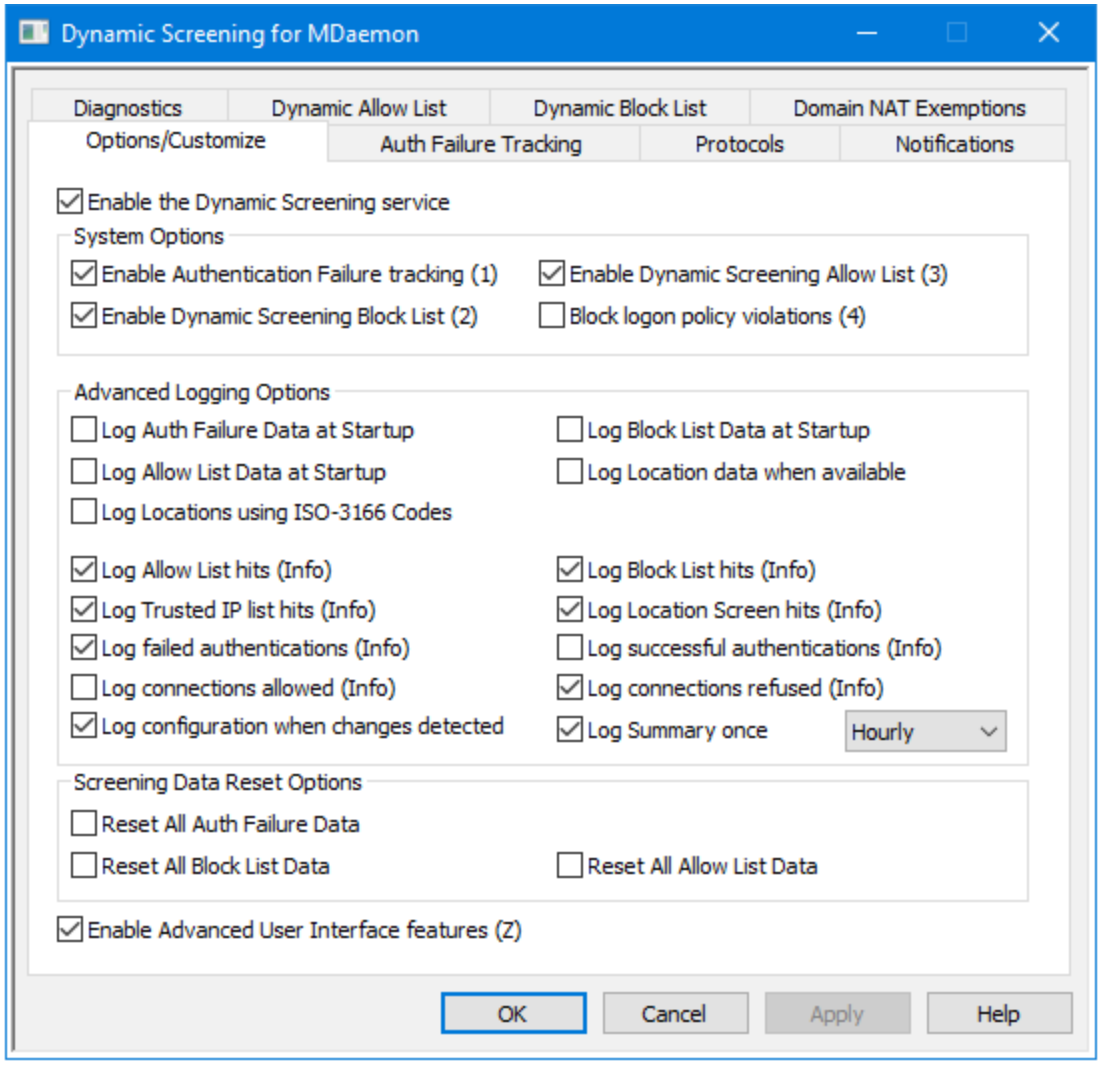
Durante la transazione SMTP, un'informativa relativa ai criterio di utilizzo del sito contenente un'istruzione relativa alla consegna della posta sarà simile a quanto segue:

```
220-MDaemon Technologies ESMTP MDaemon
220-Questo sito non inoltra posta non autorizzata.
220-Agli utenti del server non autorizzati
220-non è consentito consegnare posta attraverso questo sito.
220
HELO esempio.com...
```

Il file POLICY.DAT deve essere composto solo da testo ASCII stampabile e non deve superare i 512 caratteri per riga. Tuttavia, è consigliabile non superare mai i 75 caratteri per riga. Questo file può avere la dimensione massima di 5.000 byte. MDaemon non visualizzerà file la cui dimensione superi i 5.000 byte.

4.2 Vaglio dinamico

4.2.1 Opzioni/Personalizza



Utilizzando Vaglio dinamico, MDaemon è in grado di tenere traccia del comportamento delle connessioni in ingresso per identificare attività sospette e rispondere di conseguenza. È possibile bloccare un indirizzo IP 627 (o un intervallo di indirizzi) dalla connessione quando non supera l'autenticazione per il numero di volte specificato entro il periodo di tempo indicato. È anche possibile bloccare gli account 627 che tentano di autenticarsi quando non superano l'autenticazione troppe volte e troppo rapidamente. Inoltre, quando un indirizzo IP o un account è bloccato, non si tratta di un blocco permanente. L'indirizzo IP che si connette sarà bloccato per il numero di minuti, ore o giorni specificati e gli account bloccati possono essere sbloccati automaticamente dopo un periodo di tempo specificato, oppure manualmente dall'amministratore.

Abilita il servizio di vaglio dinamico
Selezionare questa casella per abilitare il servizio di vaglio dinamico. È possibile abilitare/disabilitare il servizio anche nella sezione Server del riquadro di spostamento nell'interfaccia utente principale di MDaemon.

Opzioni di sistema

Abilita controllo errori di autenticazione
Quando questa opzione è abilitata, il servizio Vaglio dinamico controllerà gli errori di autenticazione per i protocolli indicati nella scheda Protocolli 630 ed eseguirà le azioni determinate dalle opzioni nella scheda Controllo errori di autenticazione 627. L'opzione è abilitata per impostazione predefinita.

Attiva vaglio dinamico su lista bloccati
Questa opzione attiva la capacità del servizio di vaglio dinamico di bloccare indirizzi e intervalli di indirizzi IP. È possibile gestire la lista bloccati dalla scheda Lista bloccati dinamica 638. La lista bloccati è attivata per impostazione predefinita.

Attiva vaglio dinamico su lista consentiti
Questa opzione attiva la funzionalità del servizio di vaglio dinamico Lista consentiti dinamica 636, che si può utilizzare per esentare indirizzi e intervalli di indirizzi IP dal filtro del vaglio dinamico. La lista consentiti è attivata per impostazione predefinita.

Blocca violazioni criteri di accesso
Per impostazione predefinita, MDaemon richiede agli account di utilizzare l'indirizzo e-mail completo per effettuare l'accesso, anziché solo la parte dell'indirizzo relativa alla cassetta postale (ad esempio, devono usare "`utente1@esempio.com`" e non soltanto "`utente1`"). Questo comportamento è controllato dall'opzione "*I server richiedono l'indirizzo e-mail completo per l'autenticazione*" disponibile nella pagina Sistemi 501. Quando l'opzione è attiva, è possibile attivare anche l'opzione *Blocca violazioni criteri di accesso* se si desidera bloccare qualsiasi indirizzo IP che tenti di accedere senza utilizzare l'indirizzo e-mail completo. Questa opzione è disattivata per impostazione predefinita.

Opzioni di registrazione avanzate

Registra dati errori di autorizzazione all'avvio
Questa opzione abilita la scrittura di tutti i dati degli errori di autenticazione 627 correntemente memorizzati da Vaglio dinamico nel file di registro all'avvio. È disabilitata per impostazione predefinita.

Registra dati lista bloccati all'avvio
Abilita la scrittura di tutti i dati della Lista bloccati dinamica 638 che sono archiviati nel file di registro all'avvio. È disabilitata per impostazione predefinita.

Registra dati lista consentiti all'avvio
Attiva la scrittura di tutti i dati della Lista consentiti dinamica 636 che sono archiviati nel file di registro all'avvio. È disabilitata per impostazione predefinita.

Registra dati sulla posizione se disponibili
Selezionare questa casella per registrare i dati sulla posizione di ogni connessione, se disponibili.

Registra posizioni utilizzando i codici ISO-3166
Selezionare questa casella se si desidera utilizzare i codici nazionali ISO-3166 a due lettere quando si registrano le località, anziché i nomi.

Registra tutte le corrispondenze con la lista consentiti
Aggiunge una voce al registro del vaglio dinamico ogni volta che una connessione in entrata proviene da un indirizzo presente nella Lista consentiti dinamica 636.

Registra tutte le corrispondenze con la lista bloccati
Aggiunge una voce al registro del vaglio dinamico ogni volta che una connessione in entrata proviene da un indirizzo presente nella Lista bloccati dinamica 638.

Registra tutte le corrispondenze della lista di indirizzi IP accreditati
Questa opzione aggiunge una voce al registro di Vaglio dinamico ogni volta che una connessione in ingresso arriva da un indirizzo IP accreditato 527.

Registra tutte le corrispondenze dello screening posizione
Questa opzione aggiunge una voce al registro di Vaglio dinamico ogni volta che una connessione in ingresso viene rifiutata a causa dello screening posizione 582.

Registra tutte le autenticazioni non riuscite
Questa opzione aggiunge una voce al registro di Vaglio dinamico ogni volta che una connessione in ingresso non supera l'autenticazione.

Registra tutte le autenticazioni riuscite
Selezionare questa opzione per registrare tutti i tentativi di autenticazione in ingresso riusciti correttamente. È disabilitata per impostazione predefinita.

Registra tutte le connessioni consentite
Abilitare questa opzione se si desidera creare una voce di registro per ogni connessione che supera il Vaglio dinamico ed è autorizzata a procedere. È disabilitata per impostazione predefinita.

Registra tutte le connessioni rifiutate
Questa opzione aggiunge una voce al registro di Vaglio dinamico ogni volta che una connessione in ingresso viene rifiutata dal Vaglio dinamico.

Registra configurazione quando sono rilevate delle modifiche
Questa opzione aggiunge voci al registro per tutte le configurazioni di Vaglio dinamico quando sono rilevate delle modifiche da parte di origini esterne (ad esempio la modifica manuale del file INI). Le modifiche normali sono registrate a livello di Info.

Registra riepilogo una volta [Ogni giorno | Ogni ora | Ogni minuto]
Aggiunge al registro di Vaglio dinamico un riepilogo delle statistiche di Vaglio dinamico una volta al giorno, ogni ora o ogni minuto. Per impostazione predefinita il riepilogo viene registrato ogni ora.

Opzioni ripristino dati vaglio

Ripristina tutti i dati errori autorizzazione
Fare clic su questa casella di controllo se si desidera cancellare tutti i dati di autenticazione da Vaglio dinamico. È quindi necessario fare clic su **Applica** o su **OK** perché avvenga il ripristino.

Reimposta tutti i dati della lista bloccati
Fare clic su questa casella di controllo per cancellare tutti i dati della lista bloccati del vaglio dinamico. È quindi necessario fare clic su **Applica** o su **OK** perché avvenga il ripristino.

Reimposta tutti i dati della lista consentiti
Fare clic su questa casella di controllo per cancellare tutti i dati della lista consentiti del vaglio dinamico. È quindi necessario fare clic su **Applica** o su **OK** perché avvenga il ripristino.

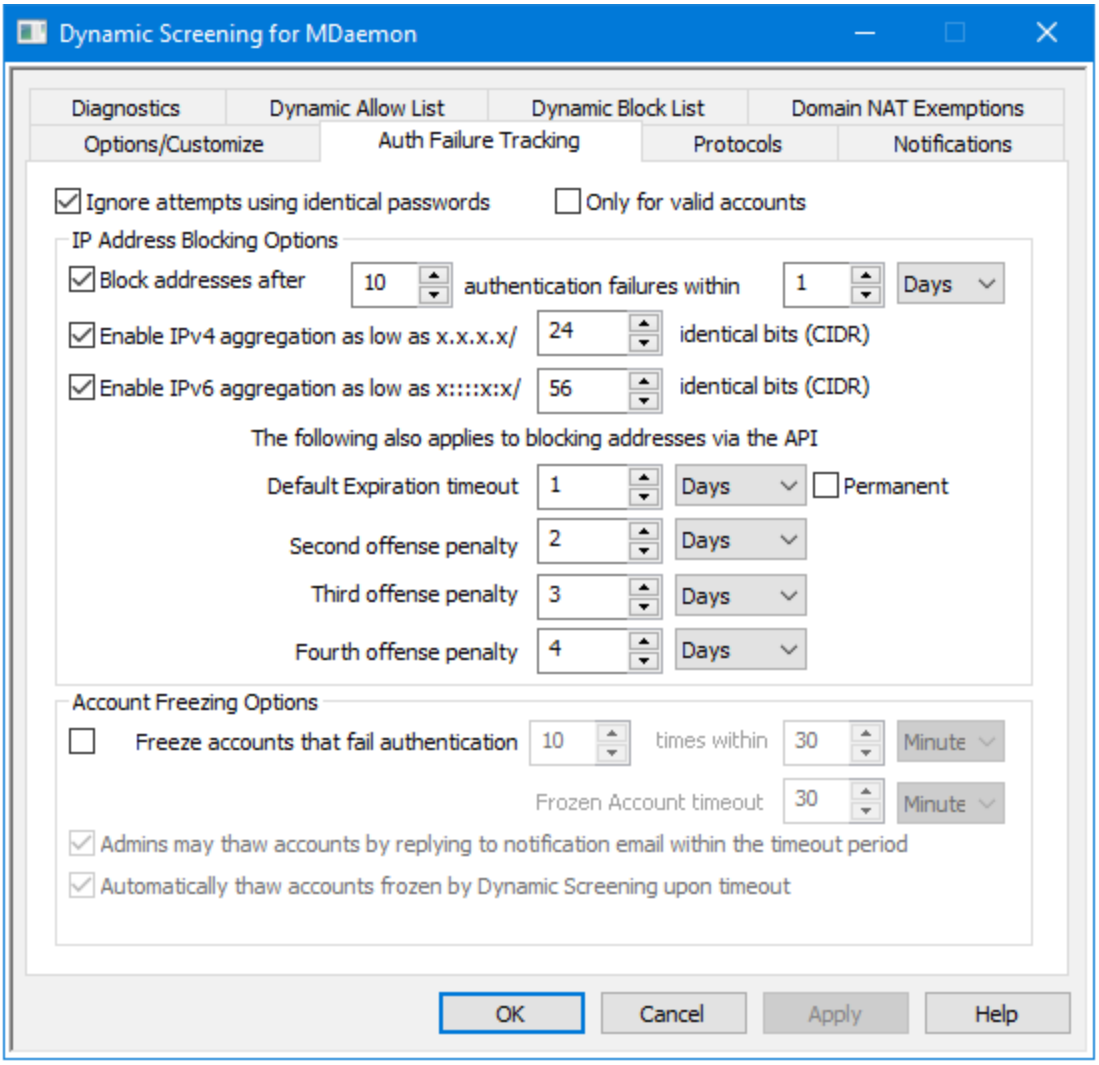
Abilita funzioni interfaccia utente avanzata

Selezionare questa casella e chiudere/riaprire l'interfaccia di configurazione di MDaemon per aggiungere alcune funzionalità avanzate del Vaglio dinamico. Una schermata Esenzioni NAT dominio 640 è stata aggiunta alla finestra di dialogo Vaglio dinamico e si può utilizzare per designare specifiche combinazioni di indirizzo IP/dominio da esentare dal blocco del vaglio dinamico quando gli utenti validi a tale indirizzo IP non riescono ad autenticarsi con la password. Sono state inoltre aggiunte alcune scelte rapide del vaglio dinamico alla sezione corrispondente della barra degli strumenti ed è stata aggiunta un'opzione al menu di scelta rapida Vaglio dinamico nella sezione Server dell'interfaccia principale che consente di mettere in pausa, piuttosto che disattivare, il servizio di vaglio dinamico, per impedire ai client di accedere al servizio durante la gestione delle opzioni.

Vedere:

Controllo errori di autenticazione 627
Lista consentiti dinamica 636
Lista bloccati dinamica 638
Esenzioni NAT dominio 640
Protocolli 630
Screening posizione 582
Schermo SMTP 575

4.2.2 Controllo errori di autenticazione



Ignora tentativi di autenticazione che usano la stessa password

Questa opzione si applica alle opzioni di blocco degli indirizzi IP e alle opzioni di blocco degli account riportate di seguito. Per impostazione predefinita, quando un tentativo di autenticazione fallisce, i tentativi di autenticazione successivi che utilizzano la stessa password saranno ignorati. Non saranno conteggiati nel numero di errori consentiti prima di bloccare l'indirizzo IP o l'account. Più tentativi di utilizzare la stessa password errata si verificano ad esempio quando la password e-mail dell'utente è stata modificata o è scaduta e il client sta tentando di eseguire l'accesso usando la vecchia password.

Solo per gli account validi
Attivare questa opzione per ignorare i tentativi di autenticazione con password duplicata solo quando i tentativi di accesso riguardano un account valido. Questo significa che se, ad esempio, un utente aggiorna la propria password in un client, ma un altro client è ancora in esecuzione con la vecchia password, i tentativi di accesso del vecchio client saranno comunque ignorati, poiché il nome di accesso del client è

corretto. Un bot che tentasse nomi di accesso casuali con una password simile non godrà dello stesso vantaggio e sarà bloccato non appena superata la soglia di errori di autenticazione.

Opzioni blocco indirizzi IP

Blocca indirizzi dopo [xx] errori di autenticazione in [xx] [minuti | ore | giorni]
Selezionare questa casella di controllo se si desidera bloccare momentaneamente un indirizzo IP quando non riesce a eseguire l'autenticazione sul server per un numero eccessivo di volte in un intervallo di tempo limitato. Specificare il numero di minuti, ore o giorno e il numero di errori consentiti durante questo intervallo.

Abilita aggregazione IPv4 fino a x.x.x.x/ [xx] bit identici (CIDR)
Questa opzione bloccherà un intervallo di indirizzi IPv4 quando gli errori di autenticazione provengono da indirizzi IP vicini gli uni agli altri invece che da un singolo indirizzo.

Abilita aggregazione IPv6 fino a x::::x:x/ [xx] bit identici (CIDR)
Questa opzione bloccherà un intervallo di indirizzi IPv6 quando gli errori di autenticazione provengono da indirizzi IP vicini gli uni agli altri invece che da un singolo indirizzo.

Penalità per più errori

Questa è la quantità di tempo per la quale un indirizzo o un intervallo di indirizzi IP saranno bloccati dal sistema Vaglio dinamico quando viene raggiunto il numero di errati tentativi di autenticazione specificato. Per impostazione predefinita la durata del blocco aumenta a ogni tentativo errato. Il che significa che ad esempio, se un indirizzo IP viola il limite di errori di autenticazione, sarà bloccato per un giorno. Se lo stesso indirizzo IP in seguito supera ancora il limite, verrà aggiunta la *Penalizzazione seconda trasgressione* all'*Intervallo predefinito di scadenza*, quindi sarà aggiunta la *Penalizzazione terza trasgressione* alla scadenza predefinita e così via. La lunghezza della penalizzazione raggiunge il suo massimo con l'aggiunta della *Penalizzazione quarta trasgressione*.

Timeout predefinito scadenza
Questa è la quantità di tempo per la quale la connessione a MDaemon per un indirizzo o un intervallo di indirizzi IP sarà bloccata quando viene raggiunto il limite di errati tentativi di autenticazione specificato sopra. Il valore predefinito è di 1 giorno.

Penalità per secondo errore
Questa è la quantità di tempo che viene aggiunta all'*Intervallo predefinito di scadenza* quando un indirizzo IP o un intervallo di indirizzi IP viene bloccato dal Vaglio dinamico per la seconda volta.

Penalità per terzo errore
Questa è la quantità di tempo che viene aggiunta all'*Intervallo predefinito di scadenza* quando un indirizzo IP o un intervallo di indirizzi IP viene bloccato dal Vaglio dinamico per la terza volta.

Penalità per quarto errore
Questa è la quantità di tempo che viene aggiunta all'*Intervallo predefinito di scadenza* quando un indirizzo IP o un intervallo di indirizzi IP viene bloccato dal Vaglio dinamico per la quarta volta e per tutte le volte successive.

Permanente
Fare clic su questa casella per bloccare in modo permanente gli indirizzi IP che violano il limite di errori di autenticazione, invece di bloccarli temporaneamente con le penalità sopra definite.

Opzioni di blocco account

Blocca account che non superano l'autenticazione [xx] volte entro [xx] [Minuti | Ore | Giorni]
Selezionare questa casella se si desidera impostare lo stato di un account 729 su BLOCCATO quando esegue il numero specificato di tentativi di autenticazione errati nel periodo di tempo indicato. MDaemon accetterà ancora i messaggi in arrivo per un account bloccato, ma non sarà possibile acceder all'account per inviare o raccogliere i messaggi fino a quando viene sbloccato (il che significa che lo stato dell'account torna a essere ABILITATO). L'opzione è abilitata per impostazione predefinita.

Timeout account bloccato
Periodo di tempo per il quale l'account resterà bloccato, se si è abilitata l'opzione sotto *Sblocca automaticamente gli account bloccati da Vaglio dinamico al timeout*.

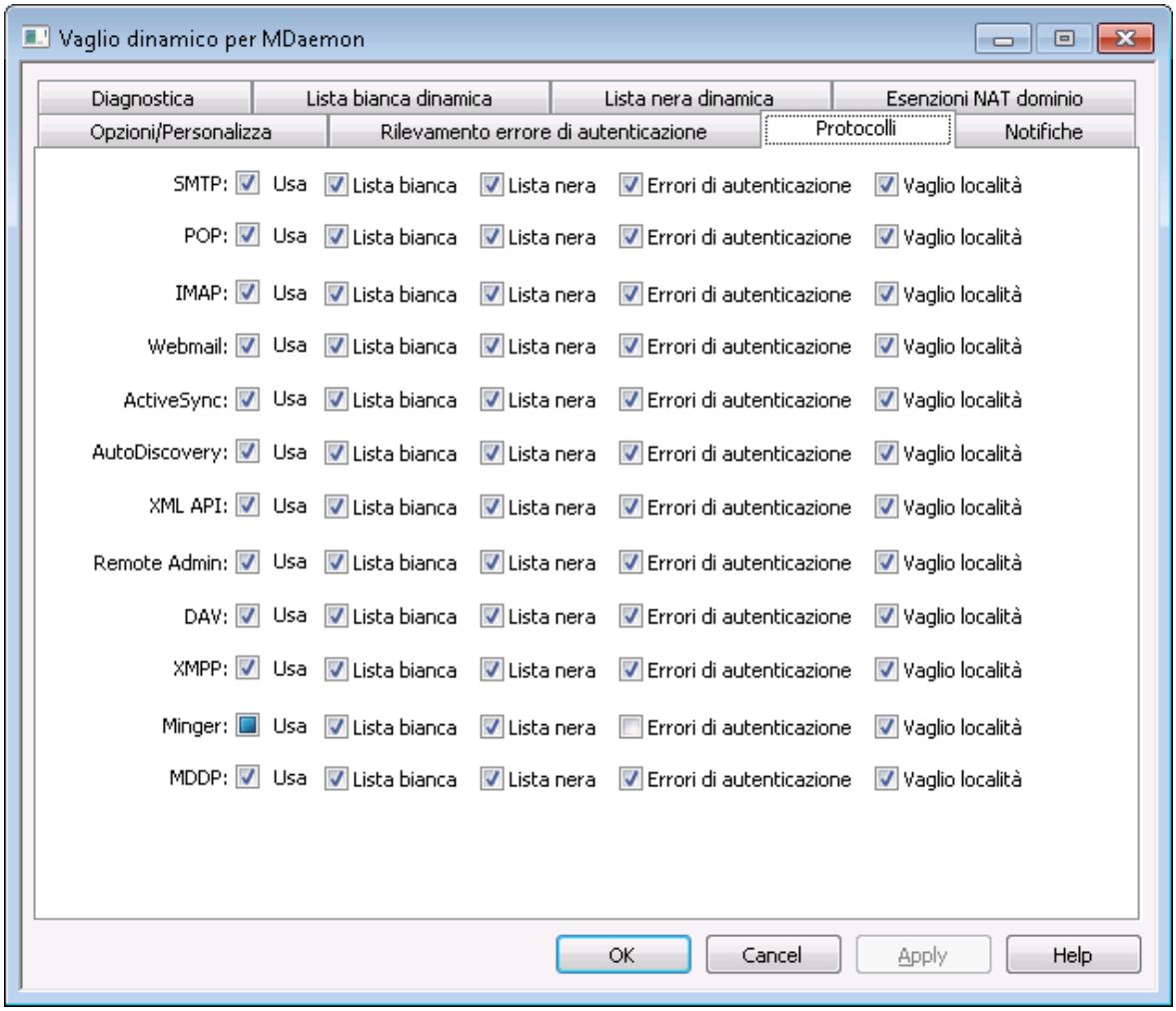
Gli amministratori possono sbloccare gli account rispondendo alle e-mail di notifica entro il periodo di timeout
Quando un account viene bloccato da Vaglio dinamico, per impostazione predefinita un amministratore riceverà un'e-mail di notifica. L'amministratore può quindi sbloccare l'account (riportarne lo stato su "Abilitato") semplicemente rispondendo all'e-mail, se questa opzione è abilitata. L'opzione è abilitata per impostazione predefinita e richiede che siano abilitate le opzioni Report account bloccati nella scheda Notifiche 631.

Sblocca automaticamente account bloccati da Vaglio dinamico al timeout
Selezionare questa casella se si desidera sbloccare automaticamente gli account bloccati una volta trascorso il periodo di *Timeout account bloccato*. L'opzione è disabilitata per impostazione predefinita.

Vedere:

Opzioni/Personalizza 623
Lista consentiti dinamica 636
Lista bloccati dinamica 638
Notifiche 631

4.2.3 Protocolli

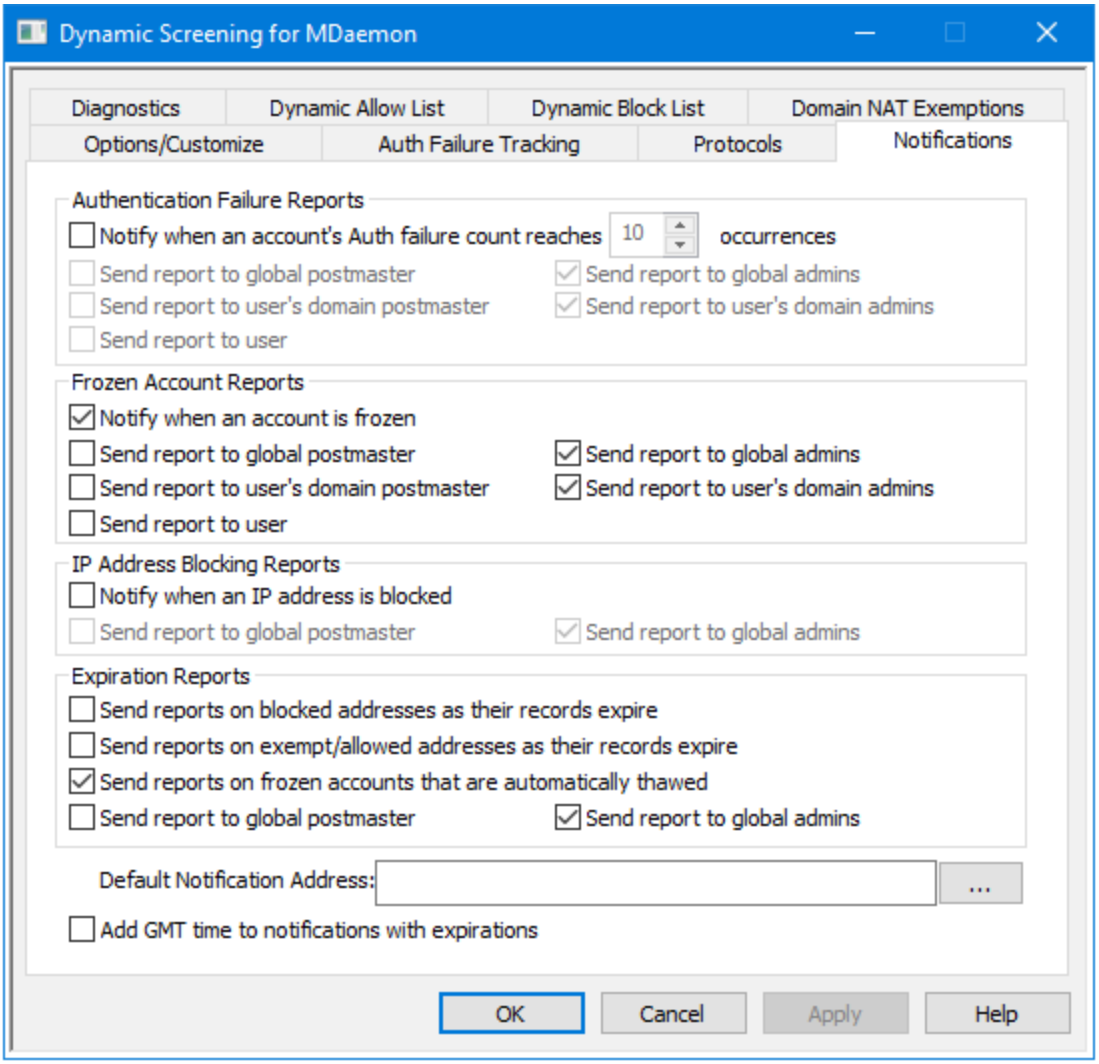


Per impostazione predefinita il servizio Vaglio dinamico è applicato ai seguenti protocolli: SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 79, il servizio Management API, MDaemon Remote Administration. WebDAV e CalDAV, XMPP e Minger. Usare le opzioni della scheda Protocolli per determinare quali protocolli devono essere controllati per le sessioni in ingresso a fronte della Lista consentiti dinamica 636 e della Lista bloccati dinamica 638, per i quali saranno registrati i tentativi di autenticazione non riusciti 627 e a cui sarà applicato il vaglio della posizione 582. Per impostazione predefinita tutte le opzioni in questa finestra di dialogo sono abilitate ad eccezione degli errori di autorizzazione di Minger.

Vedere:

Controllo errori di autenticazione 627
Lista consentiti dinamica 636
Lista bloccati dinamica 638

4.2.4 Notifiche



Report errori di autenticazione

Notifica quando il numero di errori di autenticazione di un account raggiunge [xx] occorrenze
Questa opzione fa sì che MDaemon invii un messaggio di notifica a un postmaster o a un altro destinatario selezionato quando un account non supera l'autenticazione un determinato numero di volte consecutive. Se nessuno degli indirizzi selezionati può essere risolto, MDaemon invierà il messaggio all'*Indirizzo di notifica predefinito* indicato di seguito. Se non è stato specificato nessun indirizzo, il messaggio non sarà inviato. L'opzione è abilitata per impostazione predefinita e impostata su 10 occorrenze.

Invia report a postmaster globale
Selezionare questa casella di controllo se si desidera inviare i report al postmaster globale 847. Per impostazione predefinita, questa opzione è abilitata.

Invia report a amministratori globali
Selezionare questa casella di controllo se si desidera inviare i report agli amministratori globali[773].

Inviare resoconto al postmaster del dominio utente
Selezionare questa casella se si desidera inviare i report al postmaster del dominio[847] per l'account che non ha superato i tentativi di autenticazione.

Inviare resoconto all'amministratore del dominio utente
Selezionare questa casella se si desidera inviare i report agli amministratori del dominio[773] per l'account che non ha superato i tentativi di autenticazione.

Inviare resoconto all'utente
Selezionare questa casella di controllo per inviare un resoconto degli errori all'utente il cui account non ha eseguito l'autenticazione.

Report account bloccati

Notifica quando un account è bloccato
Questa opzione fa sì che MDaemon invii un messaggio di notifica a un postmaster o a un altro destinatario selezionato quando un account viene bloccato per troppi errori di autenticazione[627]. Se nessuno degli indirizzi selezionati può essere risolto, MDaemon invierà il messaggio all'Indirizzo di notifica predefinito indicato di seguito. Se non è stato specificato nessun indirizzo, il messaggio non sarà inviato. L'opzione è abilitata per impostazione predefinita.

Invia report a postmaster globale
Selezionare questa casella di controllo se si desidera inviare i report al postmaster globale[847]. Per impostazione predefinita, questa opzione è abilitata.

Invia report a amministratori globali
Selezionare questa casella di controllo se si desidera inviare i report agli amministratori globali[773].

Inviare resoconto al postmaster del dominio utente
Selezionare questa casella se si desidera inviare i report al postmaster del dominio[847] per l'account bloccato.

Inviare resoconto all'amministratore del dominio utente
Selezionare questa casella se si desidera inviare i report agli amministratori del dominio[773] per l'account bloccato.

Inviare resoconto all'utente
Selezionare questa casella di controllo per inviare un resoconto all'account bloccato.

Report blocco indirizzi IP

Notifica quando un indirizzo IP è bloccato
Questa opzione fa sì che MDaemon invii un messaggio di notifica a un postmaster o a un altro destinatario selezionato quando un account viene bloccato dal sistema

Vaglio dinamico. Se nessuno degli indirizzi selezionati può essere risolto, MDaemon invierà il messaggio all'Indirizzo di notifica predefinito indicato di seguito. Se non è stato specificato nessun indirizzo, il messaggio non sarà inviato. L'opzione è abilitata per impostazione predefinita.

Invia report a postmaster globale
Selezionare questa casella di controllo se si desidera inviare i report al postmaster globale 847. Per impostazione predefinita, questa opzione è abilitata.

Invia report a amministratori globali
Selezionare questa casella di controllo se si desidera inviare i report agli amministratori globali 773.

Report scadenza

Invia report su indirizzi bloccati quando i record scadono
Questa opzione invia un rapporto agli indirizzi designati ogni volta che un indirizzo IP bloccato scade dalla Lista bloccati dinamica 638. L'opzione è abilitata per impostazione predefinita.

Invia resoconti su indirizzi esentati/consentiti allo scadere della registrazione
Questa opzione invia un rapporto agli indirizzi designati ogni volta che un indirizzo consentito scade dalla Lista consentiti dinamica 636. L'opzione è abilitata per impostazione predefinita.

Invia report su account bloccati che vengono sbloccati automaticamente
Questa opzione invia un report agli indirizzi indicati ogni volta che un account bloccato viene sbloccato automaticamente 627 una volta trascorso *il periodo di timeout account bloccato*. L'opzione è abilitata per impostazione predefinita.

Invia report a postmaster globale
Selezionare questa casella di controllo se si desidera inviare i report al postmaster globale 847. Per impostazione predefinita, questa opzione è abilitata.

Invia report a amministratori globali
Selezionare questa casella di controllo se si desidera inviare i report agli amministratori globali 773.

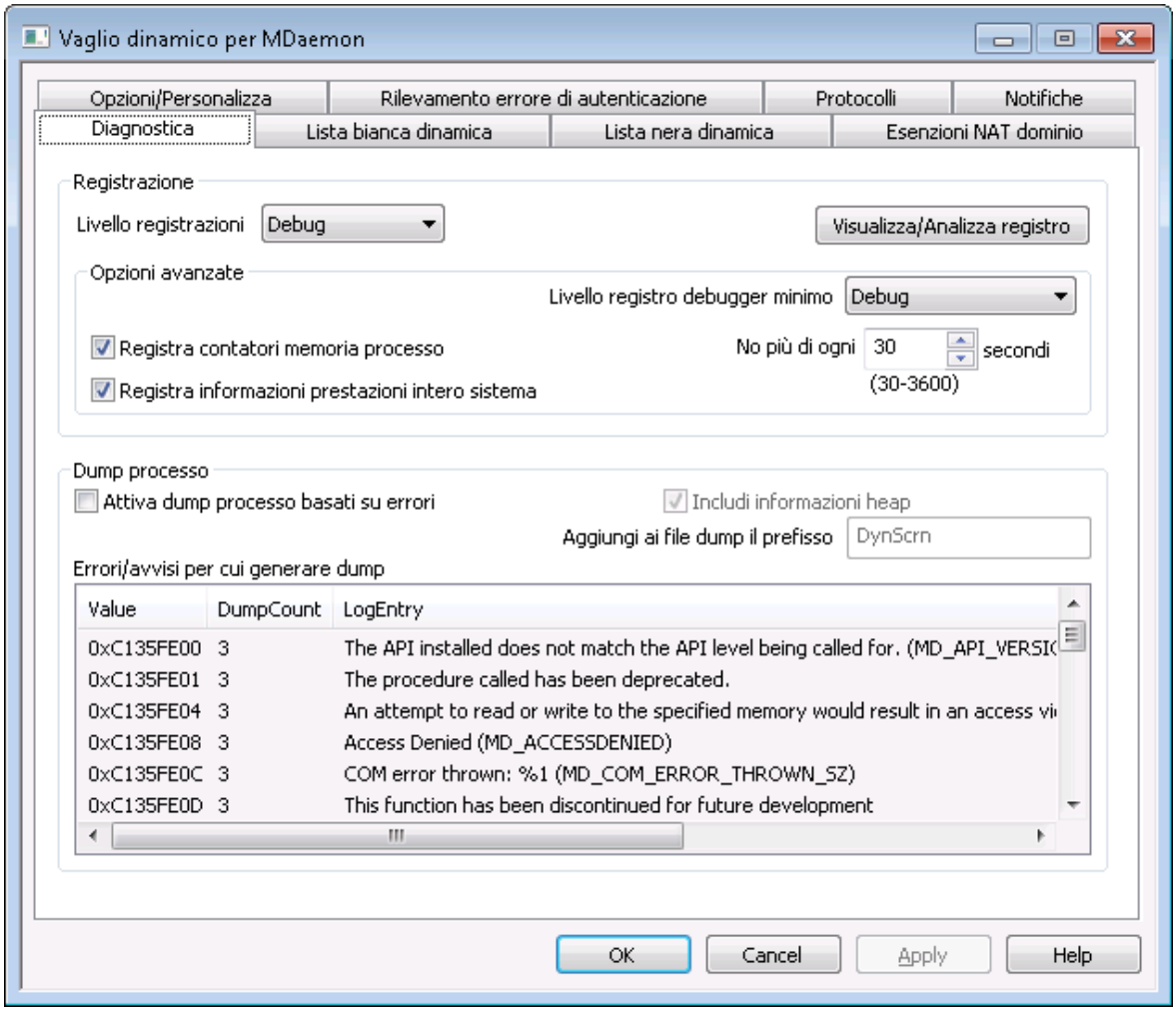
Indirizzo di notifica predefinito
Questo è l'indirizzo al quale verranno inviati i report di notifica quando non sono specificati altri indirizzi o quando nessuno degli indirizzi specificati può essere risolto. Se nessun indirizzo può essere risolto e non è indicato nessun *Indirizzo di notifica predefinito*, il report non sarà inviato.

Aggiungi ora GMT alle notifiche con scadenza
Per impostazione predefinita, quando vengono inviati i report di notifica che includono un'ora di scadenza, l'ora è quella del server locale. Abilitare questa opzione se si desidera includere l'ora GMT. Questo è utile quando gli amministratori e-mail si trovano in altri fusi orari.

Vedere:

Opzioni/Personalizza 623
Controllo errori di autenticazione 627

4.2.5 Diagnostica



In questa schermata sono disponibili le opzioni avanzate che nella maggior parte dei casi non sarà necessario utilizzare, se non per tentare di diagnosticare un problema del Vaglio dinamico o per una richiesta dell'assistenza tecnica.

Registrazione

Livello di registrazione

Sono supportati sei livelli di registrazione, dal più alto al più basso volume di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili ed è in genere usato per la diagnosi di un problema o

quando l'amministratore necessita di informazioni dettagliate.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Visualizza/Analizza registro
Fare clic su questo pulsante per aprire il Visualizzatore del registro di sistema avanzato di MDaemon. Per impostazione predefinita i registri vengono archiviati in: "..\MDaemon\Logs\"

Opzioni avanzate

Livello minimo registro debugger
Livello minimo di registrazione da inviare al debugger. I livelli di registrazione disponibili sono identici a quelli descritti in precedenza.

Registra contatori di memoria del processo
Selezionare questa casella per registrare informazioni specifiche del processo su Memoria, Handle e Thread nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Registra dati delle prestazioni dell'intero sistema
Selezionare questa casella per registrare le informazioni sulle prestazioni dell'intero sistema nel file di registro. Questa funzione è utile per individuare potenziali problemi di allocazione risorse e lead. Le voci di registro saranno emesse solo in caso di modifica dei dati successiva all'ultima registrazione.

Non più di ogni [xx] secondi
Utilizzare questa opzione per impostare il limite di frequenza della registrazione delle informazioni su processo e prestazioni.

Dump del processo

Attiva dump del processo in base agli errori
Attivare questa opzione per generare dump del processo ogni volta che si verifica un errore o un avviso specifico e indicata di seguito.

Includi informazioni heap nei dump
Per impostazione predefinita le informazioni heap sono incluse nei dump di

processo. Se non si desidera includerli, deselezionare questa casella di controllo.

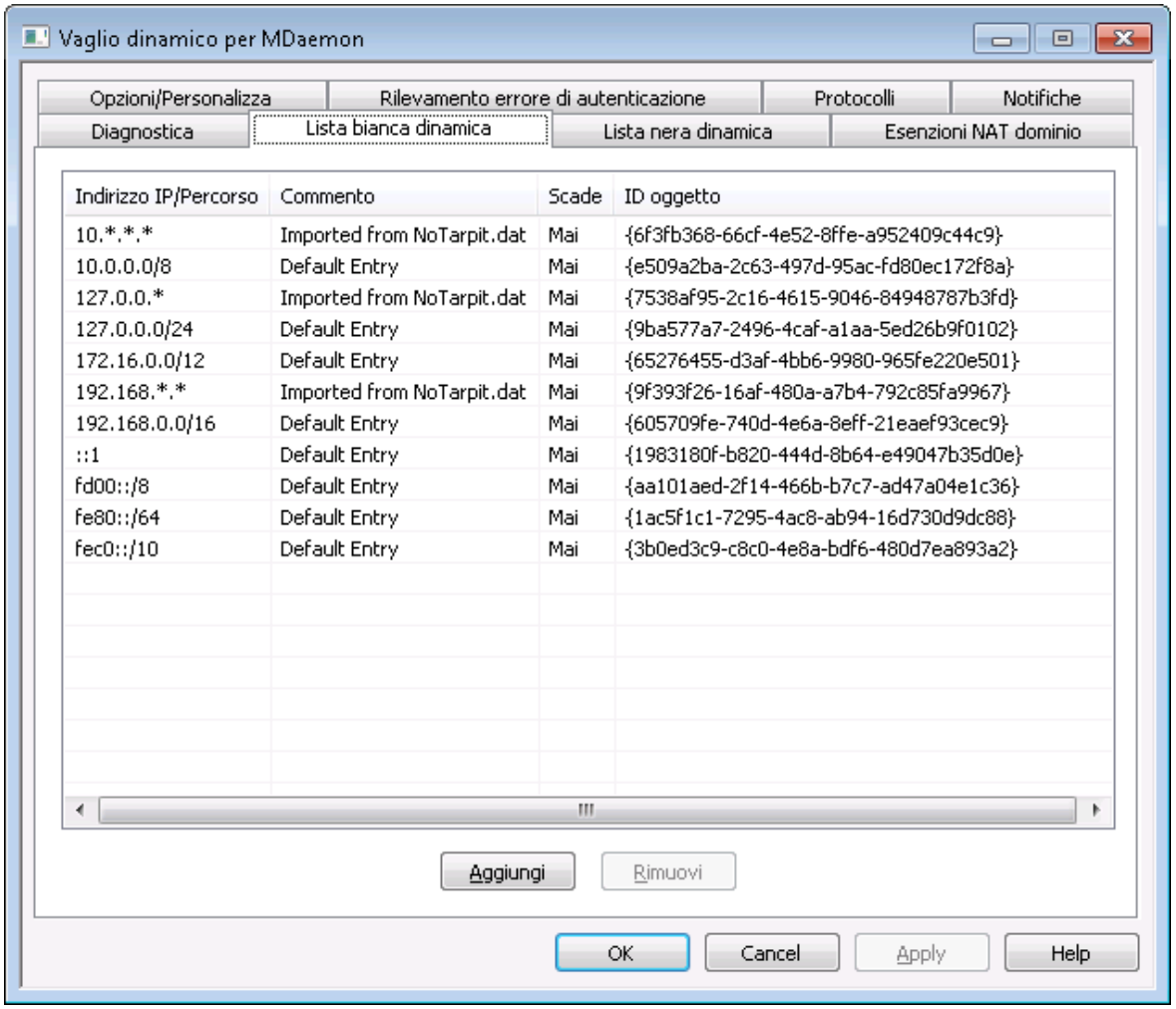
Prefisso file dump
I nomi dei file di dump del processo inizieranno con il prefisso indicato.

Errori/avvisi con generazione di dump
Fare clic con il pulsante destro del mouse in quest'area e utilizzare le opzioni *Aggiungi/Modifica/Elimina voce...* per gestire l'elenco degli errori o avvisi che avviano i dump del processo. Per ciascuna voce è possibile specificare il numero di dump di processo consentiti prima di essere disattivato.

Vedere:

Vaglio dinamico » Opzioni/Personalizza 623

4.2.6 Lista consentiti dinamica



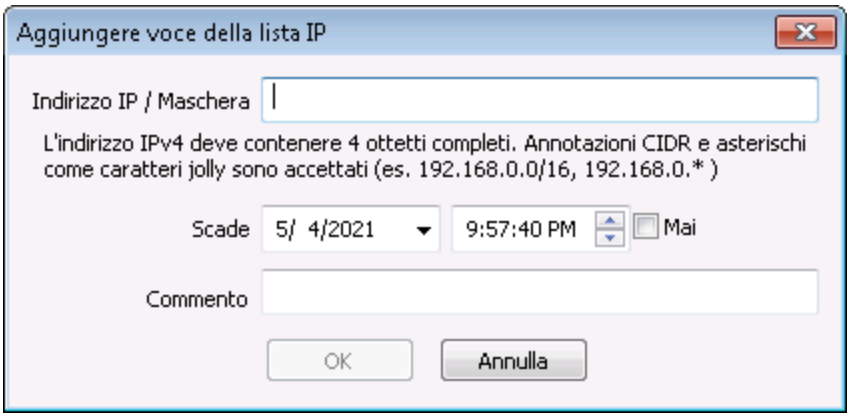
La Lista consentiti dinamica contiene l'elenco degli indirizzi o degli intervalli di indirizzi IP che saranno esentati dal blocco da parte del servizio di vaglio dinamico quando

tenteranno di connettersi a MDaemon. È possibile aggiungere indirizzi alla Lista consentiti dinamica facendo clic sul pulsante **Aggiungi**. Ogni voce contiene l'indirizzo o l'intervallo di indirizzi IP, la data e l'ora in cui la voce scadrà (oppure "Mai" se non scadrà), eventuali commenti che si desidera aggiungere alla voce e un ID oggetto. La Lista consentiti dinamica viene utilizzata anche da vaglio SMTP 575, vaglio località 582 e tarpitting 614.

Aggiunta di indirizzi o intervalli di indirizzi IP alla Lista consentiti dinamica

Per aggiungere una voce alla lista:

1. Fare clic su **Aggiungi**. Viene aperta la finestra di dialogo Aggiungi voce a elenco IP.



2. Immettere l'indirizzo IP o l'intervallo di indirizzi IP.
3. Selezionare la data e l'ora in cui si desidera che la voce scada, o fare clic su **Mai**.
4. Immettere un commento per la voce (opzionale).
5. Fare clic su **OK**.

Rimozione di una voce dall'elenco

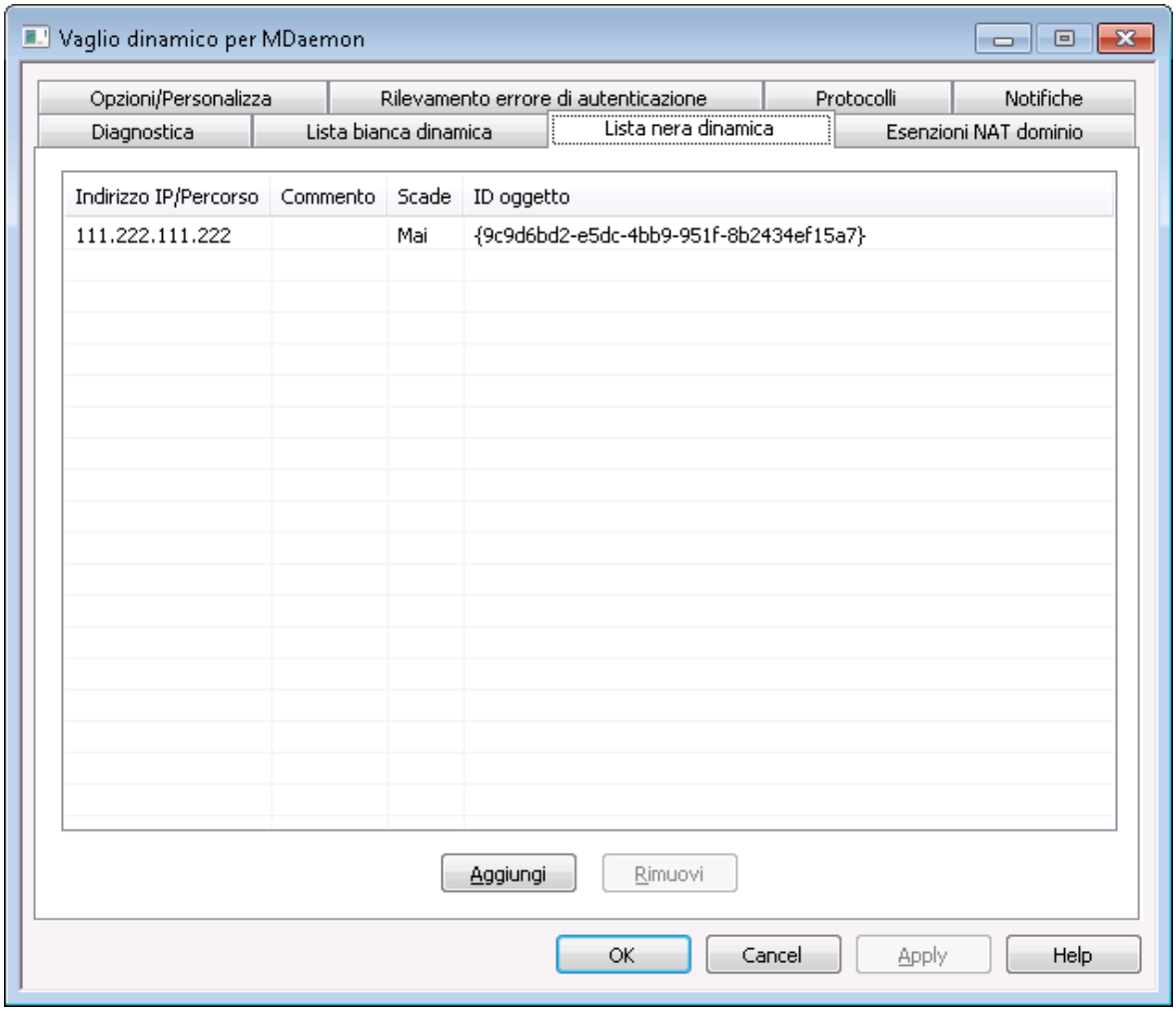
Per rimuovere una o più voci dall'elenco, procedere come indicato di seguito.

1. Selezionare la voce e o le voci che si desidera rimuovere dall'elenco (usare Ctrl+clic del mouse per selezionare più voci).
2. Fare clic su **Rimuovi**.

Vedere:

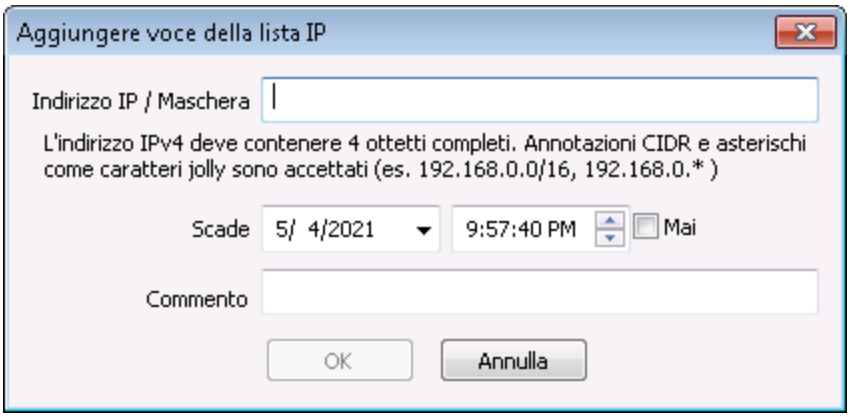
Opzioni/Personalizza 623
Controllo errori di autenticazione 627
Lista bloccati dinamica 638
Protocolli 630

4.2.7 Lista bloccati dinamica



La Lista Bloccati dinamica contiene l'elenco degli indirizzi o degli intervalli di indirizzi IP che saranno bloccati dal servizio di vaglio dinamico quando tenteranno di connettersi a MDaemon. Gli indirizzi possono essere aggiunti automaticamente mediante le opzioni Controllo errori di autenticazione 627 e Schermo SMTP 575 e aggiunti manualmente facendo clic sul pulsante **Aggiungi**. Ogni voce contiene l'indirizzo o l'intervallo di indirizzi IP, la data e l'ora in cui la voce scadrà (oppure "Mai" se non scadrà), eventuali commenti che si desidera aggiungere alla voce e un ID oggetto.

1. Fare clic su **Aggiungi**. Viene aperta la finestra di dialogo Aggiungi voce a elenco IP.



2. Immettere l'indirizzo IP o l'intervallo di indirizzi IP.
3. Selezionare la data e l'ora in cui si desidera che la voce scada, o fare clic su **Mai**.
4. Immettere un commento per la voce (opzionale).
5. Fare clic su **OK**.

Rimozione di una voce dall'elenco

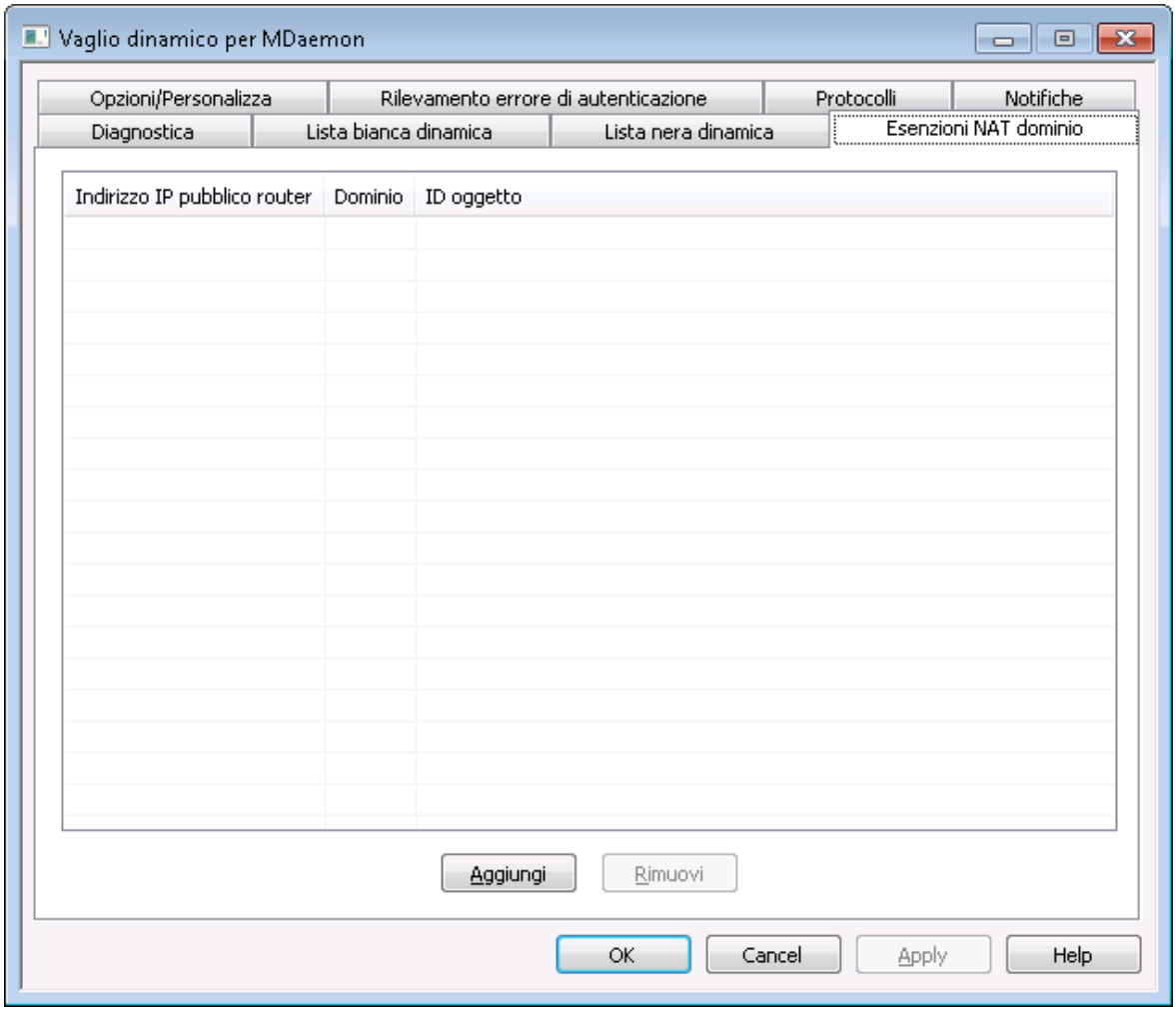
Per rimuovere una o più voci dall'elenco, procedere come indicato di seguito.

1. Selezionare la voce e o le voci che si desidera rimuovere dall'elenco (usare Ctrl+clic del mouse per selezionare più voci).
2. Fare clic su **Rimuovi**.

Vedere:

Opzioni/Personalizza 623
Controllo errori di autenticazione 627
Lista consentiti dinamica 636
Protocolli 630

4.2.8 Esenzioni NAT dominio



Questa schermata si rende disponibile quando si attiva l'opzione *per l'attivazione delle funzionalità avanzate dell'interfaccia utente* nella schermata Opzioni/Personalizza 623 del Vaglio dinamico.

Utilizzare questa funzione per accogliere un gruppo di utenti MDaemon che risiedono sulla stessa rete locale esterna (LAN), che utilizza la medesima traduzione degli indirizzi di rete (NAT) per offrire un singolo IP pubblico condiviso per tutti gli utenti. L'aggiunta dell'indirizzo IP pubblico della LAN e del dominio MDaemon a cui appartengono gli account consente di evitare il blocco dell'indirizzo IP da parte del Vaglio dinamico quando uno o più utenti non riescono ad eseguire l'autenticazione a causa di una password errata. Senza questa funzione, un utente valido con un client email configurato in modo errato potrebbe provocare il blocco dell'indirizzo IP della LAN e impedire di conseguenza a tutti gli utenti di accedere ai propri messaggi email. Questo può accadere, ad esempio, quando la password di un utente cambia ma l'utente dimentica di aggiornarla nel client e-mail.

Gli indirizzi IP elencati possono essere bloccati per altre ragioni, ad esempio bot che tentano di accedere ad account non validi, client con configurazione non corretta che tentano di accedere a un dominio MDaemon diverso da quello associato all'indirizzo IP e così via. Se si desidera escludere completamente un indirizzo IP dal vaglio dinamico, utilizzare la Lista consentiti dinamica 636.

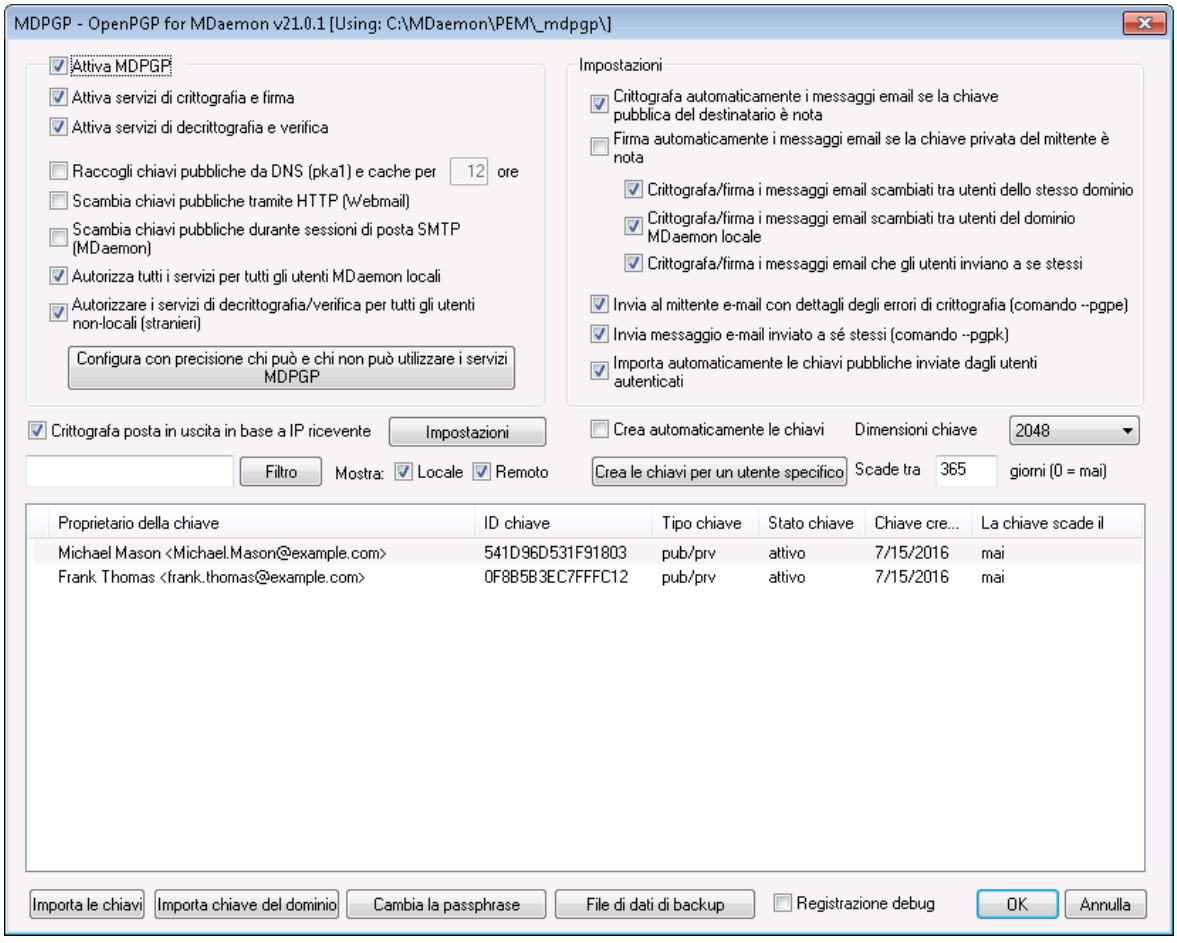
Aggiunta di un'esenzione NAT del dominio

Selezionare **Aggiungi**, immettere l'*Indirizzo IP pubblico router* della LAN esterna e selezionare il *Dominio* MDaemon i cui utenti eseguiranno l'accesso da quell'indirizzo IP. Infine, fare clic su **OK**.

Per ulteriori informazioni, vedere:

Opzioni/Personalizza 623

4.3 MDPGP



OpenPGP è un protocollo standard del settore per lo scambio di dati crittografati. Esistono molti plugin OpenPGP per i client di posta elettronica che consentono agli utenti di inviare e ricevere messaggi crittografati. MDPGP è il componente OpenPGP integrato di MDaemon che offre agli utenti servizi di crittografia, decrittografia e di gestione di base delle chiavi senza richiedere l'uso di un plugin per il client di posta elettronica.

MDPGP esegue la crittografia e la decrittografia dei messaggi di e-mail utilizzando un sistema chiave pubblica/chiave privata. A tale scopo, quando si desidera utilizzare MDPGP per inviare un messaggio privato e sicuro a qualcuno, MDPGP crittografa il messaggio utilizzando la "chiave" che in precedenza si è ottenuta da tale persona (la sua "chiave pubblica") e importata in MDPGP. Se, al contrario, si deve ricevere un messaggio privato da un altro utente, allora questi dovrà crittografare il messaggio utilizzando la chiave pubblica fornita dall'utente. L'invio della chiave pubblica al mittente è assolutamente necessaria, perché altrimenti questi non potrà inviare il messaggio crittografato con OpenPGP. La chiave pubblica univoca è necessaria per crittografare il messaggio perché MDPGP utilizzerà poi la chiave privata corrispondente per decrittografare il messaggio.

Per gestire la firma, la crittografia e la decrittografia dei messaggi, MDPGP gestisce due archivi di chiavi (definiti keyring): uno per le chiavi pubbliche e uno per le chiavi private. MDPGP può generare le chiavi degli utenti in modo automatico quando necessario oppure è possibile crearle manualmente per utenti specifici. È inoltre possibile importare delle chiavi create altrove. MDaemon può anche cercare le chiavi pubbliche allegate ai messaggi autenticati inviati da utenti locali e importare tali chiavi in modo automatico. Ne consegue che un utente può richiedere una chiave pubblica a qualcuno e inviarla quindi via posta elettronica a sé stesso, in modo che MDPGP la rilevi e la importi quindi nel keyring pubblico. MDPGP non memorizza in alcun caso più copie della stessa chiave, ma possono esistere più chiavi diverse per un singolo indirizzo. Infine, ogni volta che arriva un messaggio a un indirizzo che dispone di una chiave in un keyring, MDPGP firma, crittografa o decrittografa il messaggio secondo necessità e in base alle proprie impostazioni. Se un indirizzo dispone di più chiavi, MDPGP utilizzerà quella definita come chiave preferita per crittografare il messaggio. Se non è stata definita una chiave preferita, MDPGP utilizzerà la prima. Durante la decrittografia di un messaggio MDaemon proverà con ciascuna chiave.

È possibile configurare i servizi di firma e crittografia di MDPGP in modo che funzionino in modo automatico o manuale. Quando si imposta il funzionamento automatico, MDPGP quando possibile firma e crittografa i messaggi in modo automatico. Quando si imposta il funzionamento manuale, MDPGP firma o crittografa un messaggio solo quando il mittente inserisce un comando speciale nell'Oggetto del messaggio. In tutti i casi, i messaggi vengono firmati, crittografati o decrittografati solo quando all'account è stata garantita l'autorizzazione a utilizzare tali servizi.

Le specifiche di OpenPGP sono descritte nelle RFC 4880 e 3156.

Attivazione di MDPGP

Attiva MDPGP
MDPGP è attivato per impostazione predefinita, ma comunque non firmerà, crittograferà o decrittograferà alcun messaggio fino a quando non si creano o si importano le chiavi nei relativi keyring, o fino a quando non si userà l'opzione riportata di seguito per impostare MDPGP su *Crea automaticamente le chiavi*.

Attiva servizi di crittografia e firma
Per impostazione predefinita è possibile firmare e crittografare i messaggi non appena le chiavi necessarie sono nel keyring. Disattivare l'opzione se non si desidera consentire a MDPGP di firmare o crittografare i messaggi.

È possibile firmare i messaggi senza crittografarli, ma tutti i messaggi che vengono crittografati con MDPGP saranno anche firmati.

Attiva servizi di decrittografia e verifica
Per impostazione predefinita i messaggi crittografati in arrivo daranno decrittografati se si conosce la chiave privata del destinatario. MDPGP inoltre verificherà le firme incorporate nei messaggi non crittografati. Si noti, comunque, che sia il mittente che il destinatario devono essere autorizzati a utilizzare i servizi di decrittografia e verifica, mediante le opzioni "*Autorizza tutti...*" o "*Configura con precisione chi può...*" (tutti sono autorizzati per impostazione predefinita). Disabilitare questa opzione se non si desidera verificare le firme incorporate o consentire a MDPGP di decrittografare i messaggi, ad esempio se si desidera che tutti gli utenti gestiscano le proprie funzioni di decrittografia mediante un plug-in del client di posta elettronica. Quando l'opzione è disabilitata, i messaggi crittografati in entrata vengono gestiti come messaggi normali e collocati nella cassetta postale del destinatario.

Raccogli chiavi pubbliche da DNS (pka1) e cache per [xx] ore
Attivare questa opzione se si desidera che MDPGP esegua una ricerca delle chiavi pubbliche su DNS del destinatario del messaggio mediante PKA1. Questo è utile perché automatizza il processo che consente di ottenere le chiavi pubbliche di alcuni destinatari, evitando la necessità di ottenerle e importarle manualmente per poter mandare messaggi crittografati. Quando vengono eseguite le query PKA1, tutti gli eventuali URI della chiave trovati vengono immediatamente raccolti, convalidati e aggiunti al keyring. Le chiavi raccolte e importate correttamente nel keyring mediante questo metodo sono tracciate in un file denominato `fetchedkeys.txt` e scadranno automaticamente dopo il numero di ore specificato in questa opzione o in base al valore TTL del record PKA1 che vi fa riferimento, a seconda di quale valore è il maggiore. Pertanto il valore specificato in questo campo è il periodo di tempo minimo per cui la chiave sarà memorizzata nella cache. Il valore predefinito è 12 ore e il valore minimo accettabile è 1 ora.

Per pubblicare le proprie chiavi pubbliche nel DNS è necessario creare record TXT speciali. Ad esempio, per l'utente

> franco@esempio.com con l'ID chiave: 0A2B3C4D5E6F7G8H, nel DNS del dominio "esempio.com" si creerebbe un record TXT in "franco._pka.esempio.com" (sostituendo la @ nell'indirizzo e-mail con la stringa "._pka."). I dati per il record TXT avranno un aspetto simile al seguente: "v=pka1; fpr=<key's full fingerprint>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H" dove <key's full fingerprint> è l'impronta digitale o fingerprint completo della chiave (40 caratteri che rappresentano il valore fingerprint completo di 20 byte). È possibile visualizzare un valore di fingerprint completo della chiave facendo doppio clic sulla chiave nell'interfaccia utente di MDPGP.

Scambia chiavi pubbliche mediante HTTP (Webmail)
Attivare questa opzione se si desidera utilizzare Webmail come server base a chiave pubblica; Webmail soddisferà le richieste di chiavi pubbliche degli utenti. Il formato dell'URL per sottoporre le richieste ha il seguente aspetto: "http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>". Dove <Webmail-URL> è il percorso al server Webmail (ad esempio, "http://wc.example.com") e <Key-ID> è l'ID chiave a sedici caratteri della chiave desiderata (ad esempio, "0A1B3C4D5E6F7G8H"). L'ID chiave è costituito dagli ultimi 8 byte del fingerprint della chiave: 16 caratteri in tutto.

Scambia chiavi pubbliche durante le sessioni di posta SMTP (MDaemon)
Selezionare questa casella se si desidera abilitare la trasmissione automatica di chiavi pubbliche come parte del processo di invio di messaggi SMTP. A tal fine, il server SMTP di MDaemon riconoscerà il comando SMTP RKEY. Quando invia un'e-mail a un server che supporta RKEY, MDaemon si offrirà di trasmettere la chiave pubblica attuale e preferita del mittente all'altro host. L'host risponderà indicando che già ha la chiave ("250 2.7.0 Key already known") o che ha bisogno della chiave, nel qual caso la chiave viene trasferita immediatamente in formato ASCII armored ("354 Enter key, end with CRLF.CRLF") proprio come un messaggio e-mail. Le chiavi scadute o revocate non vengono trasmesse. Se MDaemon dispone di più chiavi per il mittente, invierà sempre la chiave correntemente contrassegnata come preferita. Se nessuna chiave è contrassegnata come preferita, sarà inviata la prima trovata. Se non sono disponibili chiavi valide, non verrà effettuata alcuna operazione. Vengono offerte solo chiavi pubbliche che appartengono agli utenti locali.

I trasferimenti di chiavi pubbliche avvengono come parte della sessione di posta SMTP che consegna il messaggio dell'utente. Perché le chiavi pubbliche trasmesse in questo modo vengano accettate, la chiave deve essere inviata insieme a un messaggio con firma DKIM 539 originata dal dominio del proprietario della chiave con il parametro i= impostato sull'indirizzo del proprietario della chiave, indirizzo che inoltre corrispondere esattamente all'indirizzo dell'intestazione From: univoco. Il "proprietario della chiave" viene estratto dalla chiave stessa. Inoltre, il messaggio deve arrivare da un host al percorso SPF 533 del mittente. Infine, il proprietario della chiave (o il relativo intero dominio grazie all'uso dei caratteri jolly) deve disporre dell'autorizzazione per RKEY con l'aggiunta di una voce al file di regole MDPGP (nel file di regole sono presenti istruzioni a questo scopo) che indica che il dominio può essere ritenuto affidabile per lo scambio delle chiavi. L'intero controllo viene eseguito

automaticamente ma è necessario che DKIM 536 e la verifica SPF 533 siano abilitati o non sarà possibile effettuare alcuna operazione.

Il registro MDPGP mostra i risultati e i dettagli di tutte le chiavi importate o eliminate e anche il registro della sessione SMTP registra questa attività. Questo processo registra l'eliminazione delle chiavi esistenti e la selezione delle nuove chiavi preferite e aggiorna tutti i server che partecipano ai quali invia e-mail quando vengono effettuate modifiche in questo senso.

Autorizza tutti i servizi per tutti gli utenti MDaemon locali
Per impostazione predefinita tutti gli account locali MDaemon sono autorizzati a utilizzare i servizi MDPGP abilitati: firma, crittografia, decrittografia e verifica. Se vi sono utenti specifici per i quali non si desidera consentire l'uso di uno o più servizi, è possibile utilizzare l'opzione "*Configura con precisione chi può e chi non può utilizzare i servizi MDPGP*" per escluderli. Disattivare questa opzione se si desidera autorizzare solo utenti locali specifici. In quel caso utilizzare l'opzione "*Configura con precisione chi può e chi non può utilizzare i servizi MDPGP*" per garantire l'accesso a chi si desidera.

Autorizzare i servizi di decrittografia/verifica per tutti gli utenti non-locali (stranieri)
Per impostazione predefinita i messaggi crittografati in arrivo per un destinatario locale da un mittente non locale possono essere decrittografati se è nota la chiave privata del destinatario locale. In modo simile, MDPGP verificherà le firme incorporate nei messaggi in arrivo da parte di utenti non locali. Se vi sono mittenti non locali i cui messaggi non si desidera decrittografare o verificare, è possibile utilizzare l'opzione "*Configura con precisione chi può e chi non può utilizzare i servizi MDPGP*" per escludere tali mittenti da quei servizi. Disattivare questa opzione se non si desidera decrittografare i messaggi o verificare le firme incorporate quando il mittente è un indirizzo non locale. In quel caso è possibile utilizzare comunque l'opzione "*Configura con precisione chi può e chi non può utilizzare i servizi MDPGP*" per specificare le eccezioni a tale limitazione.

Configura con precisione chi può e chi non può utilizzare i servizi MDPGP
Fare clic su questo pulsante per aprire il file `rules.txt` e configurare le autorizzazioni degli utenti per MDPGP. Con questo file è possibile specificare quali sono gli utenti che possono firmare, crittografare e decrittografare i messaggi. È inoltre possibile escludere utenti specifici da queste opzioni. Ad esempio, si può usare la regola "`+*@esempio.com`" per consentire a tutti gli utenti di `esempio.com` di crittografare i messaggi, ma aggiungere quindi "`-franco@esempio.com`" per impedire a `franco@esempio.com` di eseguire le medesime operazioni. Vedere il testo nella prima parte del file `rules.txt` per leggere esempi e istruzioni.

Note e sintassi di rules.txt

- Solo i messaggi di e-mail autenticati con SMTP provenienti dagli utenti di questo server MDaemon possono utilizzare il servizio di crittografia. È comunque possibile specificare indirizzi non locali che si desidera escludere dal servizio di crittografia, il che significa che MDPGP **non** crittograferà i messaggi indirizzati a tali indirizzi, anche se la chiave pubblica è conosciuta.
- In caso di conflitto tra le impostazioni in `rules.txt` e l'opzione generale "*Autorizza tutti i servizi per tutti gli utenti MDaemon locali*", verrà utilizzata l'impostazione del file `rules.txt`.

- In caso di conflitto tra le impostazioni in `rules.txt` e l'opzione globale "*Autorizzare i servizi di decrittografia/verifica per tutti gli utenti non-locali (stranieri)*", verrà utilizzata l'impostazione del file `rules.txt`.
- Il testo di una stringa dopo il simbolo # viene ignorato.
- Se si inseriscono più indirizzi e-mail su una stringa, separarli con uno spazio.
- È possibile utilizzare i caratteri jolly (* e ?) all'interno degli indirizzi.
- Anche se i messaggi MDPGP crittografati sono **sempre** firmati, se si autorizza un utente a crittografare i messaggi non si concede necessariamente anche l'autorizzazione a firmare messaggi non crittografati. Per firmare un messaggio non crittografato, l'account deve disporre dell'autorizzazione alla firma.
- A ogni indirizzo e-mail deve essere anteposto uno dei seguenti tag:

+ (più) - l'indirizzo può usare il servizio di crittografia MDPGP.

- (meno) - l'indirizzo **non può** usare il servizio di crittografia MDPGP.

! (punto esclamativo) - l'indirizzo può usare il servizio di decrittografia MDPGP.

~ (tilde) - l'indirizzo **non può** usare il servizio di decrittografia MDPGP.

^ (accento circonflesso) - l'indirizzo può usare il servizio di firma MDPGP.

= (uguale) - l'indirizzo **non può** usare il servizio di firma MDPGP.

$ (dollaro) - l'indirizzo può usare il servizio di verifica MDPGP.

& (e commerciale) - l'indirizzo **non può** utilizzare il servizio di verifica MDPGP.

Esempi:

`+*@*` - Tutti gli utenti di tutti i domini possono crittografare.

`!*@*` - Tutti gli utenti di tutti i domini possono decrittografare.

`^*@*` - Tutti gli utenti di tutti i domini possono firmare.

`^*@esempio.com` - Tutti gli utenti di esempio.com possono firmare.

`+franco@esempio.com ~franco@esempio.com` - L'utente può crittografare ma non decrittografare.

`+GROUP:UtentiCrittografia` - I membri del gruppo `UtentiCrittografia` di MDaemon possono crittografare

`^GROUP:UtentiFirma` - I membri del gruppo `UtentiFirma` di MDaemon possono firmare

Modalità di crittografia/firma

Modalità automatica

Utilizzare le opzioni in Impostazioni per configurare MDPGP in modo che i messaggi vengano firmati e crittografati automaticamente, in base alle autorizzazioni concesse agli account. Quando un account invia un messaggio autenticato e MDPGP conosce la

chiave richiesta, il messaggio viene firmato o crittografato in base alle impostazioni riportate di seguito.

I codici speciali dell'Oggetto descritti nella sezione Modalità manuale di seguito hanno sempre la precedenza sulle opzioni della modalità automatica. Ne consegue che se una di queste opzioni viene disattivata, un account autorizzato a firmare o crittografare i messaggi può sempre definire la forma o la crittografia di un messaggio manualmente utilizzando uno dei codici.

Impostazioni

Crittografa automaticamente i messaggi e-mail se la chiave pubblica del destinatario è nota
Per impostazione predefinita, se a un account è consentito crittografare messaggi, MDPGP li crittografa automaticamente se la chiave pubblica dell'account del destinatario è nota. Disattivare questa opzione se non si desidera che i messaggi vengano crittografati automaticamente; i messaggi potranno essere comunque crittografati manualmente utilizzando i codici speciali descritti nella sezione Modalità manuale di seguito.

Firma automaticamente i messaggi e-mail se la chiave privata del mittente è nota
Fare clic su questa opzione se si desidera che MDPGP firmi automaticamente i messaggi quando la chiave privata dell'account del mittente è nota, se l'account è autorizzato a firmare i messaggi. Anche quando questa opzione è disattivata, i messaggi potranno essere comunque firmati manualmente utilizzando i codici speciali descritti nella sezione Modalità manuale di seguito.

Crittografa/firma i messaggi e-mail scambiati tra utenti dello stesso dominio
Se si imposta MDPGP in modo che crittografi o firmi automaticamente i messaggi, questa opzione fa in modo che MDPGP esegua questa operazione anche quando i messaggi vengono scambiati tra utenti dello stesso dominio, purché le chiavi richieste siano note. L'opzione è abilitata per impostazione predefinita.

Crittografa/firma i messaggi e-mail scambiati tra utenti dei domini locali MDaemon
Se si imposta MDPGP in modo che crittografi o firmi automaticamente i messaggi, questa opzione fa in modo che MDPGP esegua questa operazione anche quando i messaggi vengono scambiati tra utenti dei domini locali MDaemon, purché le chiavi richieste siano note. Se, ad esempio, i domini MDaemon comprendono "esempio.com" ed "esempio.net", i messaggi scambiati tra gli utenti di questi domini saranno automaticamente firmati o crittografati. L'opzione è abilitata per impostazione predefinita.

Crittografa/firma i messaggi e-mail che gli utenti inviano a se stessi
Se si imposta MDPGP in modo che crittografi o firmi automaticamente i messaggi, questa operazione verrà eseguita anche quando l'utente MDaemon invia un messaggio a sé stesso (ad esempio, franco@esempio.com invia un messaggio a franco@esempio.com). Pertanto, se l'account è autorizzato a utilizzare sia la crittografia che la decrittografia (impostazione predefinita), MDPGP accetterà il

messaggio dell'utente, lo crittograferà e lo decrittograferà immediatamente, collocandolo nella stessa cassetta postale dell'utente. Se, tuttavia, l'account non è stato configurato per la decrittografia, l'opzione fa in modo che il messaggio sia crittografato e collocato quindi nella stessa casetta postale dell'utente ancora crittografato. L'opzione è abilitata per impostazione predefinita.

Modalità manuale

Quando si disabilitano le opzioni *Firma automaticamente i messaggi...* e *Crittografa automaticamente i messaggi...* sopra descritte, si può utilizzare MDPGP in modalità manuale. MDPGP non firma né crittografa alcun messaggio, fatta eccezione per quelli autenticati e con uno dei seguenti odici nell'intestazione dell'oggetto del messaggio:

--pgps Se possibile, firma questo messaggio. Il codice si può posizionare alla fine o all'inizio dell'oggetto.

--pgpe Se possibile, crittografa questo messaggio. Il codice si può posizionare alla fine o all'inizio dell'oggetto.

--pgpx Il messaggio **DEVE** essere crittografato. Se non è possibile crittografarlo, (ad esempio, perché la chiave privata del destinatario non è nota), il messaggio torna al mittente. Il codice si può posizionare alla fine o all'inizio dell'oggetto.

--pgpk Inviami la mia chiave pubblica. L'utente inserisce questo codice all'inizio dell'oggetto e invia il messaggio a sé stesso. MDPGP invierà all'utente un messaggio e-mail con la sua chiave pubblica.

--pgpk<E-mail> Inviami la chiave pubblica di questo indirizzo. L'utente inserisce questo codice all'inizio dell'oggetto e invia il messaggio a sé stesso. MDPGP invierà all'utente un messaggio e-mail con la chiave pubblica dell'indirizzo.

Esempio:

```
Subject: --pgpk<franco@esempio.com>
```

Gestione delle chiavi

Le chiavi pubbliche e private si possono gestire utilizzando le opzioni nella metà inferiore della finestra di dialogo MDPGP. È presente una voce per ciascuna chiave ed è possibile fare clic con il pulsante destro del mouse su una voce per esportare la chiave, eliminarla, attivarla o disattivarla, impostarla come chiave preferita (vedere "*Scambia chiavi pubbliche durante sessioni di posta SMTP*" sopra), o impostarla come chiave di dominio (vedere di seguito). Quando si fa clic su **Esporta chiave**, questa viene salvata nella cartella `\MDaemon\Pem\_mdpgp\exports\` ed è possibile inviare via e-mail la chiave pubblica a un altro indirizzo e-mail. Le opzioni "Mostra locali/remoti" e "Filtro" facilitano l'individuazione di determinati indirizzi o gruppi.

Uso di una chiave di dominio

Se si desidera, è possibile utilizzare una singola chiave per crittografare tutti i messaggi destinati a un dominio specifico, indipendentemente dal mittente. Questo è utile, ad esempio, se uno dei propri domini e un dominio esterno desiderano crittografare tutti i messaggi e-mail scambiati reciprocamente, ma non vogliono configurare e controllare singole chiavi di crittografia per ogni account utente nel dominio. È possibile ottenere questo risultato in diversi modi:

- Se si dispone già di una chiave pubblica per un altro dominio e si desidera utilizzare quella chiave per la crittografia di tutti i messaggi in uscita diretti a tale dominio, fare clic con il pulsante destro del mouse sulla chiave e selezionare **Imposta come chiave di dominio**. Quindi immettere il nome del dominio e fare clic su **OK**. Questo consentirà di creare una regola del filtro contenuti per fare in modo che tutti i messaggi indirizzati a quel dominio ("To:" nome dominio) siano crittografati usando la chiave indicata.
- Se la chiave pubblica del dominio è stata fornita ma non è stata ancora inserita nell'elenco, selezionare **Importa chiave del dominio**, immettere il nome del dominio e fare clic su OK, quindi passare al file `public.asc` del dominio e selezionare **Apri**. In questo modo si creerà anche la regola del filtro contenuti per la crittografia dei messaggi indirizzati al dominio.
- Personalizzare le regole del filtro contenuti come necessario per specificare esattamente quali messaggi debbano essere crittografati prima di essere inviati ai domini.
- Per creare una nuova chiave per uno dei domini da inviare a un altro dominio per la crittografia dei messaggi inviati, seguire le istruzioni riportate per l'opzione "*Crea le chiavi per un utente specifico*" riportata di seguito, selezionando "`_Domain Key (domain.tld)_ <anybody@domain.tld>`" dall'elenco.

Per crittografare i messaggi in uscita non utilizzare una chiave per la quale si dispone anche della chiave privata corrispondente. Se la si utilizza, MDPGP crittograferà il messaggio e vedrà subito che la chiave di decrittografia è nota e quindi decrittograferà immediatamente lo stesso messaggio.

Invia al mittente una e-mail con i dettagli degli errori di crittografia (comando --pgpe)
Quando viene utilizzato il comando `--pgpe` per l'invio di messaggi crittografati e la crittografia non riesce, ad esempio perché non è stata rilevata la relativa chiave, questa opzione farà in modo che una e-mail di notifica venga rispedita al mittente per informarlo dell'esito negativo. Questa opzione è disattivata per impostazione predefinita, ovvero non verrà inviato alcun messaggio di notifica degli errori.

Invia messaggio e-mail inviato a sé stessi (comando --pgpk)
Quando un utente invia a se stesso un messaggio e-mail con "`--pgpk<indirizzo e-mail>`" come oggetto (ad es. `--pgpk<frank@example.com>`). Se esiste una chiave pubblica di <indirizzo e-mail> verrà rispedita al richiedente.

Importa automaticamente le chiavi pubbliche inviate da utenti autenticati
Per impostazione predefinita, quando un utente autenticato invia un messaggio e-mail con una chiave pubblica in formato ASCII armored allegata, MDPGP importa la chiave pubblica nel keyring. Si tratta di un modo semplice per ottenere la chiave pubblica di un utente in MDPGP, inviando via e-mail la chiave pubblica a sé stessi come allegato. Disattivare questa opzione se non si desidera importare automaticamente le chiavi pubbliche.

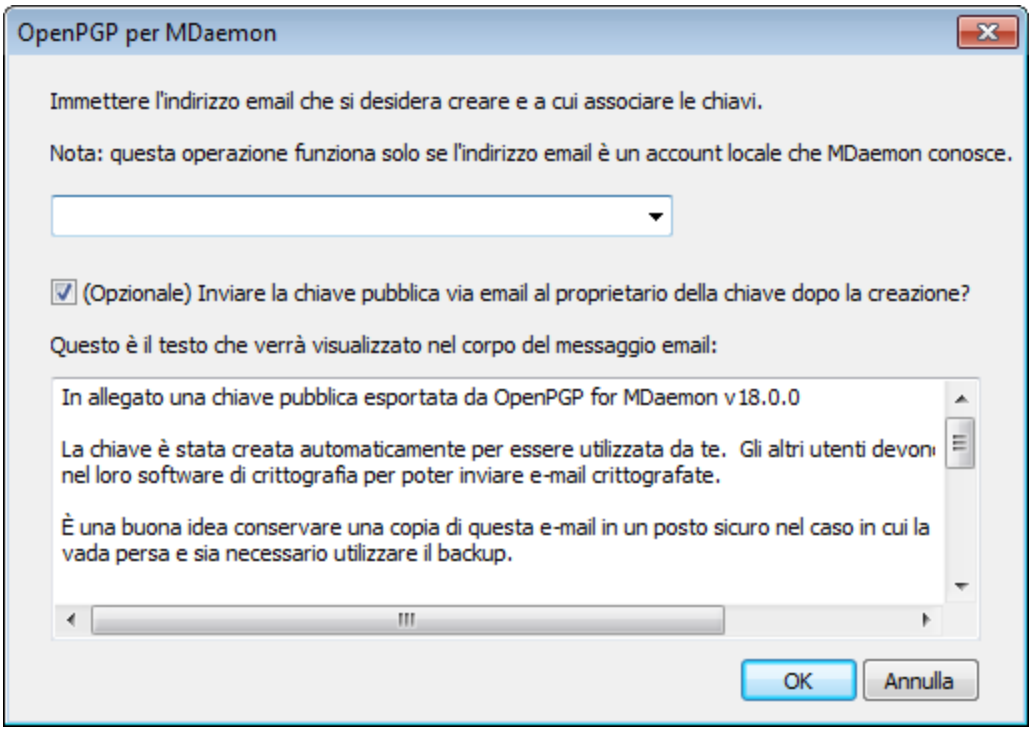
Crea automaticamente le chiavi
Attivare questa opzione se si desidera che MDPGP crei automaticamente una coppia di chiavi privata/pubblica per ognuno degli utenti MDaemon. Invece di generarle tutte in una volta, tuttavia, MDPGP le creerà di volta in volta, creando la coppia di chiavi di ciascun utente alla successiva elaborazione di un messaggio per tale utente. L'opzione è disattivata per impostazione predefinita, per risparmiare risorse ed evitare le generazione non necessaria di chiavi per account che non utilizzeranno mai MDPGP.

Dimensioni della chiave
Utilizzare questa opzione per specificare le dimensioni delle chiavi generate da MDPGP. Le dimensioni delle chiavi possono essere impostate su 1024, 2048 o 4096. L'impostazione predefinita è chiavi di 2048 byte.

Scade tra [xx] giorni (0=mai)
Utilizzare questa opzione per specificare il numero di giorni dalla data di creazione in cui una chiave generata da MDPGP sarà valida prima della scadenza. Impostare l'opzione su "0" se non si desidera alcuna scadenza delle chiavi. Il valore predefinito è 0.

Crea le chiavi per un utente specifico
Per generare manualmente una coppia di chiavi per un account:

1. Fare clic su **Crea le chiavi per un utente specifico**.
2. Scegliere l'account nell'elenco a discesa. Se si desidera creare un singola chiave da applicare a tutti gli account di un dominio, selezionare l'opzione "_Domain Key (domain.tld)_ <anybody@domain.tld>" dall'elenco.
3. **Facoltativamente:** Selezionare la casella **Inviare la chiave pubblica via email al proprietario della chiave...** per inviare la chiave all'utente come allegato a un messaggio e-mail.
4. Fare clic su **OK**.



Crittografa posta in uscita in base a IP ricevente
Se si desidera utilizzare una chiave di crittografia specifica per crittografare tutti i messaggi destinati a uno specifico indirizzo IP, attivare questa opzione e selezionare **Impostazioni** per aprire il file MTE (Message Transport Encryption) di MDaemon, in cui è possibile elencare l'indirizzo IP e l'ID della chiave associata. Qualsiasi sessione SMTP in uscita per la consegna di un messaggio a uno degli indirizzi IP elencati crittograferà il messaggio usando la chiave associata immediatamente prima della trasmissione. Se il messaggio è già crittografato in base a una chiave diversa, questo passaggio non verrà eseguito.

Importa le chiavi
Per importare manualmente un file di chiave in MDPGP, fare clic su questo pulsante, individuare il file della chiave e scegliere **Apri**. Quando si importa un file di chiave privata, non è necessario importare la chiave pubblica corrispondente, perché questa è inclusa nella chiave privata. Se si importa una chiave privata protetta da una passphrase, MDPGP chiederà di immettere la passphrase. Non sarà possibile importare la chiave privata senza prima immettere la passphrase. Dopo l'importazione di una chiave privata, MDaemon modifica la passphrase di tale chiave impostando la passphrase attualmente utilizzata da MDPGP.

Importa chiave del dominio
Se è stata fornita una chiave di crittografia pubblica per crittografare tutti i messaggi inviati a uno specifico dominio, fare clic su questo pulsante, immettere il nome del dominio, scegliere **OK** e passare al file `public.asc` del dominio e selezionare **Apri**. In questo modo si aggiungerà la chiave pubblica del dominio all'elenco e si creerà una regola del filtro contenuti per crittografare tutti i messaggi in uscita per quel dominio, indipendentemente dal mittente.

Cambia la passphrase
Le chiavi private sono sempre protette da una passphrase. Quando si tenta di importare una chiave privata, è necessario immettere la passphrase corrispondente. Quando si esporta una chiave privata, tale chiave è sempre protetta dalla passphrase e non può essere utilizzata o importata altrove senza prima immettere la passphrase. La passphrase predefinita di MDPGP è **MDaemon**. Per motivi di sicurezza è necessario modificare la passphrase dopo aver iniziato a utilizzare MDPGP, poiché in caso contrario tutte le chiavi create o importate in MDPGP avranno **MDaemon** come passphrase impostata (o modificata). È possibile modificare la passphrase in qualsiasi momento facendo clic su **Cambia la passphrase** nella schermata di MDPGP. Quando si cambia la passphrase, tutte le chiavi private del keyring vengono aggiornate con la nuova passphrase.

File di dati di backup
Fare clic su questo pulsante per eseguire un backup dei file di keyring `Keyring.private` e `Keyring.public`. Per impostazione predefinita, i file di backup saranno copiati in: "`\MDaemon\Pem\_mdpgp\backups`" e saranno caratterizzati da una data e dall'estensione `.bak` dopo il nome del file.

- I messaggi inoltrati non vengono crittografati.
- I messaggi del risponditore automatico non vengono crittografati.
- I server delle chiavi e la revoca delle chiavi non sono supportate, ad eccezione di quanto indicato per le opzioni "*Raccogli chiavi pubbliche da DNS (pka1) e cache per [xx] ore*" e "*Invia chiavi pubbliche mediante HTTP (Webmail)*".
- L'azione di crittografia Filtro contenuti non ha effetto sui messaggi già crittografati e le azioni di crittografia e decrittografia sono soggette a tutti i requisiti di configurazione di MDPGP.
- Gli elenchi a discesa in cui sono riportati gli account MDaemon mostrano, per impostazione predefinita, i primi 500 account. Per visualizzare tutti gli account, è possibile impostare `MaxUsersShown=0` in `plugins.dat`. In caso di liste molto lunghe, il caricamento potrebbe richiedere più tempo.
- `MDPGPUtil.exe` è uno strumento che consente di crittografare e decrittografare mediante delle opzioni della riga di comando. Per ulteriori informazioni, eseguire il comando MDPGPUtil senza argomenti da una shell a riga di comando.

4.4 Outbreak Protection

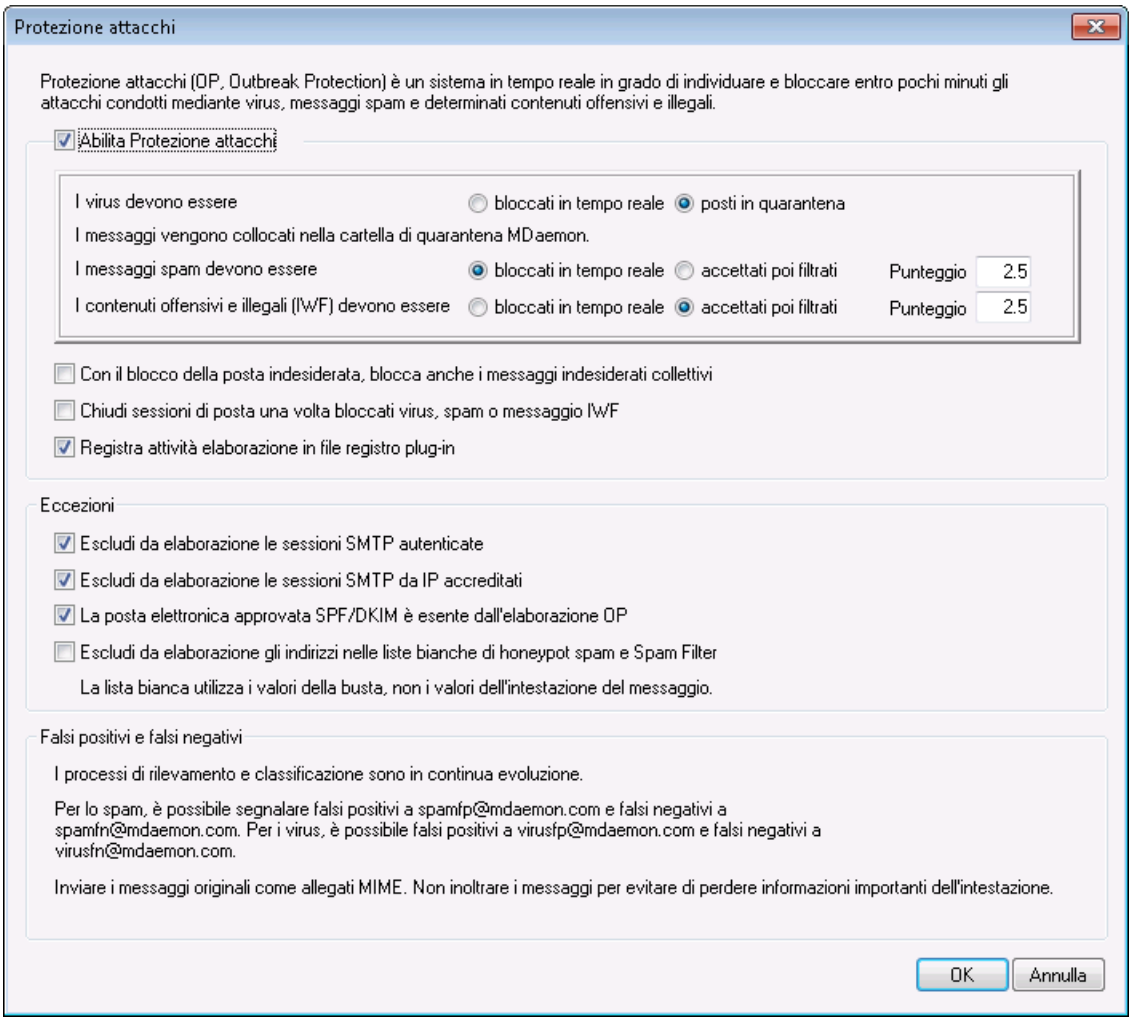
Outbreak Protection fa parte della funzionalità opzionale MDaemon AntiVirus 684. Quando si abilita MDaemon AntiVirus per la prima volta viene avviato un periodo di prova di 30 giorni. Se si desidera acquistare questa funzionalità, contattare il rivenditore MDaemon autorizzato o visitare il sito all'indirizzo: www.mdaemon.com.

Outbreak Protection (OP) è accessibile dal menu di MDaemon' Sicurezza (Sicurezza » Outbreak Protection... o Ctrl+Shift+1). È una rivoluzionaria tecnologia antispam, antivirus e antiphishing che consente di proteggere automaticamente e in tempo reale una infrastruttura di posta elettronica MDaemon entro pochissimi minuti dall'inizio di un attacco.

La funzione Outbreak Protection è completamente indipendente dal contenuto, ossia non dipende dall'analisi lessicale del contenuto del messaggio e non richiede quindi regole euristiche, funzioni di filtro dei contenuti o aggiornamenti delle definizioni antivirus. Grazie a questa caratteristica, la funzione di protezione non viene disattivata dall'aggiunta di testo spurio, da astute modifiche ortografiche, da tattiche di ingegneria sociale, da ostacoli linguistici o da differenze di codifica. Invece, OP si basa sul rilevamento di schemi ricorrenti e su tecnologie zero-hour. Queste sono fondate sull'analisi matematica della struttura del messaggio e delle caratteristiche di distribuzione del messaggio su SMTP: vengono analizzati i "pattern" associati alla trasmissione di un messaggio e-mail che vengono quindi confrontati con pattern simili rilevati con milioni di messaggi in tutto il mondo, grazie a un campionamento e confronto in tempo reale. **Nota:** OP non trasmette mai il reale contenuto dei messaggi, né è possibile derivare il contenuto dei messaggi dai pattern estratti.

Poiché i messaggi vengono analizzati in tutto il mondo e in tempo reale, la protezione è disponibile in pochi minuti, spesso entro pochi secondi dall'inizio dell'attacco. Nel caso dei virus, questo livello di protezione è fondamentale perché la verifica e la pubblicazione di un aggiornamento delle definizioni virus a seguito di un nuovo attacco possono richiedere diverse ore e può trascorrere un tempo ancora superiore prima che l'aggiornamento venga installato. Durante questo periodo di tempo, i server privi di Outbreak Protection sono vulnerabili al nuovo attacco. Analogamente, è necessario molto tempo anche per l'analisi di un nuovo messaggio spam e per la creazione di un'apposita regola di filtro che ne consentano l'individuazione da parte dei tradizionali sistemi euristici o basati sul contenuto.

È opportuno tenere presente, tuttavia, che la funzione Outbreak Protection non rappresenta un'alternativa alle tradizionali tecniche antivirus, antispam e antiphishing. In effetti, OP offre un ulteriore livello di protezione specializzato in aggiunta agli strumenti euristici, di firma e di contenuto già presenti in MDaemon. Outbreak Protection è una funzione specificamente progettata per fronteggiare attacchi su vasta scala anziché singoli o specifici messaggi infetti da virus o malware già noto che vengono gestiti più efficacemente dagli strumenti tradizionali.



Outbreak Protection

Abilita Protezione attacchi

Fare clic su questa casella di controllo per abilitare Outbreak Protection nel server in uso. I messaggi in entrata verranno analizzati per verificare se sono relativi ad attacchi in corso di tipo virale, spam o phishing. Le rimanenti opzioni presenti nella scheda di dialogo consentono di definire il destino dei messaggi che rappresentano un attacco e di indicare i mittenti che vengono esclusi dall'elaborazione OP.

I virus devono essere...

bloccati in tempo reale

Selezionare questa opzione se si desidera bloccare durante l'elaborazione SMTP i messaggi che rappresentano un attacco di tipo virale. Questi messaggi non verranno posti in quarantena né recapitati ai destinatari previsti, ma verranno respinti direttamente dal server.

posti in quarantena

Selezionare questa opzione se si desidera accettare i messaggi che rappresentano un attacco di tipo virale. I messaggi non verranno respinti dal server, ma verranno

posti in quarantena anziché essere recapitati ai destinatari previsti. I messaggi in quarantena vengono archiviati nella relativa cartella.

I messaggi spam devono essere...

bloccati in tempo reale
Selezionare questa opzione se si desidera bloccare durante l'elaborazione SMTP i messaggi che rappresentano un attacco di tipo spam. Questi messaggi non verranno contrassegnati come spam né recapitati ai destinatari previsti, ma verranno respinti direttamente dal server. I messaggi classificati da Outbreak Protection come posta "bulk" non vengono bloccati da questa opzione, a meno che si attivi l'opzione *Con il blocco della posta indesiderata, blocca anche i messaggi indesiderati collettivi*. È possibile che i messaggi classificati come collettivi da OP siano parte di liste di distribuzione di grandi dimensioni o di altri contenuti ampiamente distribuiti; di conseguenza possono essere considerati o meno spam. Per questo motivo, non è consigliabile bloccare o assegnare un punteggio in senso negativo a questo tipo di messaggi mediante OP.

accettati poi filtrati
Selezionare questa opzione se si desidera accettare i messaggi che rappresentano un attacco di tipo spam, in modo da sottoporli alla successiva elaborazione di Spam filter e di Filtro contenuti. Questi messaggi non vengono bloccati da OP, ma il relativo punteggio spam viene corretto in base all'opzione *Punteggio*.

Se si utilizza l'opzione *accettati poi filtrati*, Outbreak Protection non blocca direttamente i messaggi spam. Questi ultimi, tuttavia, possono essere bloccati da MDaemon durante l'elaborazione SMTP se Spam Filter utilizza l'opzione *SMTP rifiuta i msg con punteggi superiori o uguali a [xx]* della schermata Spam Filter 692.

Se ad esempio l'opzione relativa al punteggio determina un punteggio Spam Filter pari a 15.0 per un messaggio, quest'ultimo viene comunque rifiutato come spam se l'opzione di Spam Filter "*SMTP rifiuta....*" prevede lo scarto dei messaggi con un punteggio pari o superiore a 15.0.

Punteggio
Se si utilizza l'opzione *accettati poi filtrati*, questo è il valore aggiunto al punteggio spam del messaggio assegnato da Spam Filter qualora Outbreak Protection accerti che il messaggio rappresenta un attacco spam.

Contenuti IWF

L'opzione seguente viene applicata ai contenuti segnalati dall'IWF (Internet Watch Foundation) perché associati a siti contenenti immagini di abusi sui bambini, ossia pedopornografiche. L'opzione consente di uilizzare un elenco di URL forniti dall'IWF per individuare e contrassegnare i messaggi che si riferiscono a tali contenuti. La fondazione IWF opera come servizio Internet indipendente per la segnalazione di contenuto potenzialmente illegale, incluse le immagini relative a pedopornografia o ad abusi compiuti sui bambini, in qualsiasi parte del mondo. La fondazione opera in

coordinamento con le forze dell'ordine, con i governi, con l'industria Internet nel suo complesso e con il pubblico per contrastare la disponibilità online di contenuto illegale. L'elenco di URL fornito dalla fondazione viene aggiornato quotidianamente con i nuovi siti che ospitano immagini relative ad abusi sui bambini.

Molte organizzazioni hanno definito regole di conformità interne che governano il contenuto dei messaggi e-mail inviati o ricevuti dai propri impiegati, in particolare per quanto riguarda il materiale illegale o pornografico. Molte nazioni, inoltre, hanno proibito per legge l'invio o la ricezione di tale contenuto. Questa funzionalità può semplificare la conformità a queste disposizioni.

Per ulteriori informazioni sulla fondazione IWF, vedere:

http://www.iwf.org.uk/

I contenuti offensivi e illegali (IWF) devono essere...

bloccati in tempo reale
Scegliere questa opzione se si desidera rifiutare, durante l'elaborazione SMTP, i messaggi in entrata con contenuto segnalato dalla fondazione IWF.

accettati poi filtrati
Scegliere questa opzione se si desidera aumentare il punteggio spam di un messaggio con contenuto segnalato dalla fondazione IWF anziché respingerlo. Il punteggio spam del messaggio viene aumentato del valore specificato nel campo *Punteggio*.

Punteggio
Se si utilizza l'opzione *accettati poi filtrati*, questo è il valore aggiunto al punteggio spam del messaggio assegnato da Spam Filter qualora contenga contenuto segnalato dalla fondazione IWF.

Con il blocco della posta indesiderata, blocca anche i messaggi indesiderati collettivi
OP talvolta individua messaggi che possono essere considerati spam ma non sono inviati da botnet o da spammer noti, situazione comune nel caso di invio di posta collettiva (bulk) e di newsletter. OP classifica questi messaggi come "*Spam (bulk)*" anziché ""*Spam (confirmed)*". Selezionare questa opzione se si desidera applicare la funzionalità di blocco di Outbreak Protection anche alla posta classificata "*Spam (bulk)*". Se l'opzione è disabilitata, la funzionalità di blocco interessa solo i messaggi classificati come "*Spam (confirmed)*". L'accettazione di questo tipo di spam per una successiva elaborazione può essere necessaria per i siti che desiderano ricevere mailing di massa ma che per qualche motivo non possono esentare le fonti o i destinatari.

Registra attività elaborazione in file registro plug-in
Attivare questa casella di controllo per registrare tutte le attività di elaborazione di OP nel file di registro del plugin di MDaemon.

Eccezioni

Escludi da elaborazione le sessioni SMTP autenticate
Se si abilita questa opzione, le sessioni SMTP autenticate vengono escluse dall'elaborazione di OP. In altre parole, i messaggi inviati durante tali sessioni non vengono verificati da Outbreak Protection.

Escludi da elaborazione le sessioni SMTP da IP accreditati
Abilitare questa opzione se si desidera escludere dall'elaborazione di OP gli indirizzi IP accreditati. In questo caso, i messaggi provenienti da un server al quale è associato un indirizzo IP accreditato non vengono sottoposti a verifica da OP.

La posta elettronica approvata da SPF/DKIM è esente dall'elaborazione OP
Fare clic su questa casella di controllo per esentare un messaggio dall'elaborazione di OP quando il dominio mittente è riportato nell'elenco approvato 566 ed è stato convalidato mediante SPF o DKIM.

Honeypot di spam e indirizzi consentiti di Spam Filter sono esentati dall'elaborazione di OP
Fare clic su questa opzione per esentare Honeypot spam 723 e liste consentiti di Spam Filter dalle elaborazioni di Protezione attacchi. La lista consentiti viene applicata al destinatario o al valore RCPT attribuito durante la sessione SMTP. La "Lista consentiti (da)" viene applicata al mittente o al valore MAIL attribuito durante la sessione SMTP. Queste operazioni non sono basate sui valori dell'intestazione del messaggio.

Falsi positivi e falsi negativi

I falsi positivi, ossia la classificazione come attacco di un messaggio in realtà legittimo, rappresentano un'eventualità estremamente rara. Qualora si verifichi una tale eventualità, tuttavia, è possibile inviare il messaggio falso positivo all'indirizzo **spamfp@mdaemon.com** nel caso di spam o di phishing oppure all'indirizzo **virusfp@mdaemon.com** nel caso di virus. Ciò consentirà di raffinare e perfezionare i processi di individuazione e classificazione.

I falsi negativi, ossia la classificazione come legittimo di un messaggio che in realtà è spam o è associato a un attacco, rappresentano un'eventualità più frequente. Tuttavia, è opportuno ricordare che OP non è progettato per individuare tutti i messaggi spam, gli attacchi da virus e simili, ma costituisce solo un livello di protezione specifico contro gli attacchi. I messaggi meno recenti, quelli con un obiettivo specifico e simili che non fanno parte di un attacco in corso, potrebbero superare le verifiche eseguite da OP, ma verrebbero comunque bloccati da AntiVirus e da altre funzionalità di MDaemon nelle fasi successive dell'elaborazione. Qualora si verifichi un falso negativo, tuttavia, è possibile inviare il messaggio in questione all'indirizzo **spamfn@mdaemon.com** nel caso di spam o di phishing oppure all'indirizzo **virusfn@mdaemon.com** nel caso di virus. Ciò consentirà di raffinare e perfezionare i processi di individuazione e classificazione.

Qualora si desideri inviare un messaggio classificato in modo inappropriato, non inoltrare il messaggio e-mail originale ma inviarlo sotto forma di allegato MIME. In caso contrario, le intestazioni e altre informazioni fondamentali ai fini della classificazione verrebbero perse.

4.5 Filtro contenuti e antivirus

Filtro contenuti

È possibile utilizzare il Filtro contenuti[659], accessibile da Sicurezza » Filtro contenuti, per configurare una vasta gamma di funzioni, tra cui: la prevenzione della posta indesiderata, l'intercettazione dei messaggi contenenti virus prima che raggiungano la destinazione finale, la copia di specifici messaggi e-mail per uno o più utenti aggiuntivi, l'inserimento di una nota o di una clausola alla fine dei messaggi, l'aggiunta e l'eliminazione delle intestazioni, la rimozione degli allegati, l'eliminazione dei messaggi e molto altro ancora. Poiché vengono create dall'amministratore, le regole di Filtro contenuti possono essere di molti tipi e applicabili alle situazioni più diverse. Se progettata e sperimentata con accortezza, questa funzione può rivelarsi molto utile.

MDaemon AntiVirus (MDAV)

Quando si utilizza il componente AntiVirus opzionale di MDaemon, è possibile accedere a due schermate aggiuntive nella finestra di dialogo Filtro contenuti: Scansione dei virus[684] e programma di aggiornamento AV[688]. Queste schermate consentono di controllare direttamente le funzioni AntiVirus e di specificare le operazioni da eseguire quando viene rilevato un virus. MDAV dispone di due motori di scansione dei virus: IKARUS Anti-Virus e ClamAV. È possibile eseguire la scansione dei messaggi con uno dei due motori o con entrambi, per un livello extra di sicurezza. MDAV è inoltre dotato della funzione Protezione attacchi[653], che non è a base euristica e non dipende dalle firme come gli strumenti di protezione tradizionali, ma è progettato per individuare spam, phishing e attacchi da virus inseriti nel contesto di un attacco globale in corso e che, a volte, non vengono rilevati dagli strumenti tradizionali.

Quando si abilita MDaemon AntiVirus[684] per la prima volta viene avviato un periodo di prova di 30 giorni. Se si desidera acquistare questa funzionalità, contattare il rivenditore MDaemon autorizzato o visitare il sito all'indirizzo: www.mdaemon.com.

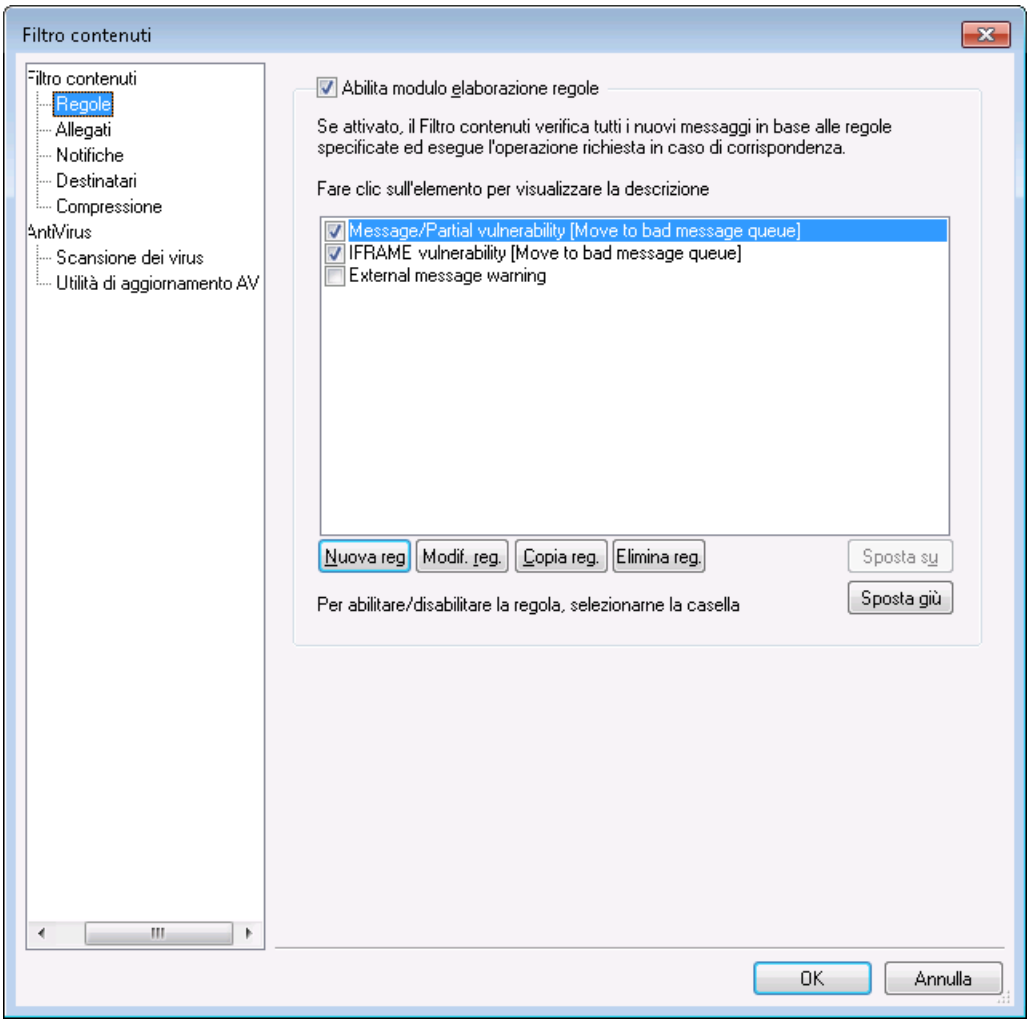
Per ulteriori informazioni, vedere:

Filtro contenuti[659]
Creazione di una nuova regola di filtro dei contenuti[661]
Modifica di una regola di Filtro contenuti esistente[666]
Uso di espressioni regolari nelle regole di filtro[667]

Scansione dei virus[684]
Utilità di aggiornamento AntiVirus[688]
Protezione attacchi[653]

4.5.1 Editor di Filtro contenuti

4.5.1.1 Regole



Ogni messaggio elaborato da MDaemon viene temporaneamente collocato in una delle code dei messaggi. Se la funzione Filtro contenuti è abilitata, ogni messaggio dovrà essere elaborato dalle regole di Filtro contenuti prima di poter lasciare la coda. Il risultato di questa procedura determina il destino del messaggio.

I messaggi con nome file che inizia con la lettera "P" vengono ignorati dal processo di Filtro contenuti. Tutti gli altri vengono invece elaborati in base a tale sistema. Al termine dell'elaborazione, il primo carattere del nome file dei messaggi viene sostituito con la lettera "P", in modo che il contenuto di ogni messaggio venga filtrato una sola volta.

Regole del filtro contenuti

Abilita modulo elaborazione regole
Selezionare questa casella di controllo per abilitare Filtro contenuti. Prima di essere consegnati, tutti i messaggi elaborati da MDaemon verranno filtrati mediante le regole di Filtro contenuti.

Elenco delle regole di Filtro contenuti

La casella di testo include tutte le regole di Filtro contenuti, ognuna associata a una casella di controllo che consente di abilitarla o disabilitarla. Per visualizzare una descrizione di ciascuna regola in base al formato script interno, selezionare la regola e attendere senza spostare il cursore del mouse per evitare di far scomparire la descrizione. Quando un messaggio viene elaborato da Filtro contenuti, le regole vengono applicate nell'ordine in cui sono elencate. L'ordine può essere modificato per ottenere un grado di flessibilità maggiore.

Ad esempio: se si dispone di una regola che impone l'eliminazione di tutti i messaggi contenenti le parole "Questa è posta indesiderata" e di una regola simile che causa l'invio di questi messaggi al postmaster, per poter applicare entrambe le regole al messaggio sarà sufficiente disporle nell'ordine appropriato. A questo scopo è necessario che in una posizione superiore all'interno dell'elenco non sia stata applicata la regola "Blocca elaborazione regole". Altrimenti, occorrerà utilizzare i pulsanti *Sposta su*/*Sposta giù* per posizionare la regola di interruzione dopo le altre due. Ogni messaggio contenente "Questa è posta indesiderata" verrà copiato e inviato al postmaster, quindi eliminato.

MDaemon consente di creare regole per effettuare più operazioni e di utilizzare gli operatori logici `and/or`. Nell'esempio precedente, anziché utilizzare più regole, sarebbe stato possibile eseguire tutte le operazioni con un'unica regola.

Nuova regola
Fare clic su questo pulsante per creare una nuova regola di Filtro contenuti. Verrà visualizzata la finestra di dialogo Crea regola 661.

Modifica regola
Fare clic su questo pulsante per visualizzare la regola selezionata nell'editor modifica regola 666.

Copia regola
Fare clic su questo pulsante per duplicare la regola di Filtro contenuti selezionata. Verrà creata e aggiunta all'elenco una regola identica a quella selezionata. Alla nuova regola viene automaticamente assegnato il nome predefinito "Copia di [nome della regola originale]". L'opzione si rivela particolarmente utile per creare più regole simili. È infatti sufficiente creare una singola regola, duplicarla più volte, quindi modificare le copie a seconda delle esigenze.

Elimina regola
Fare clic su questo pulsante per eliminare la regola di Filtro contenuti selezionata. Verrà chiesto di confermare l'eliminazione.

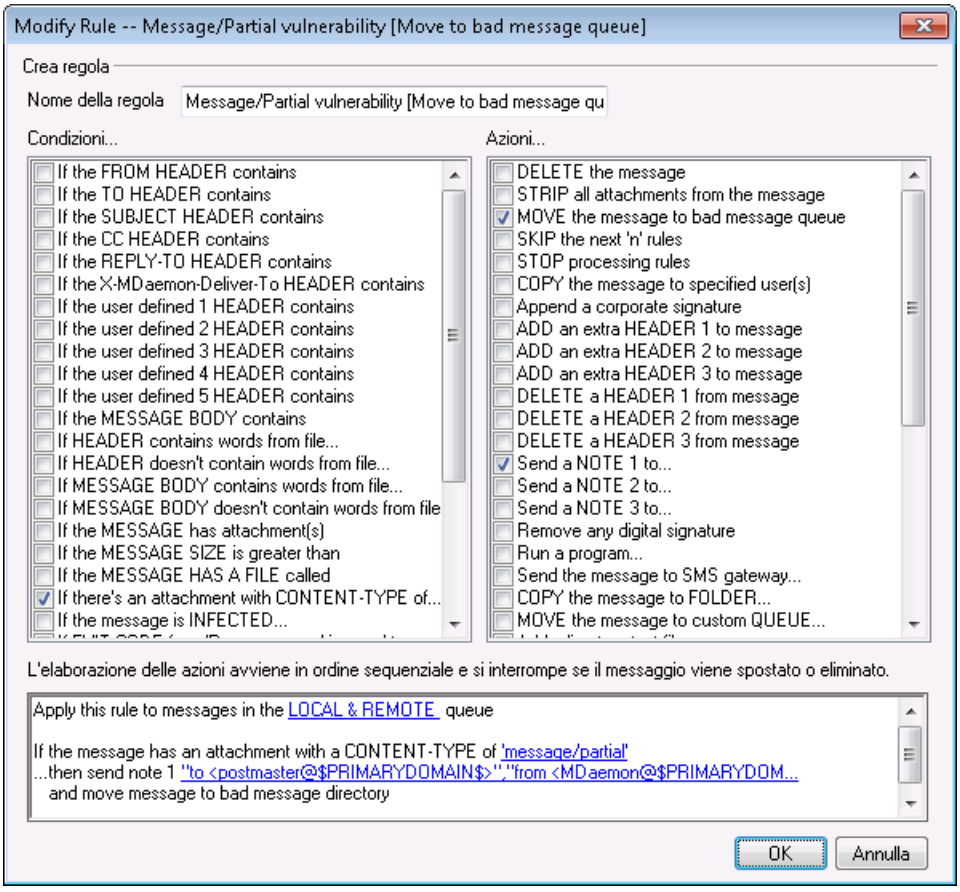
Sposta su
Fare clic su questo pulsante per spostare la regola selezionata verso l'alto.

Sposta giù
Fare clic su questo pulsante per spostare la regola selezionata verso il basso.

Per ulteriori informazioni, vedere:

Creazione di una nuova regola di Filtro contenuti 661
Modifica di una regola di Filtro contenuti esistente 666
Uso di espressioni regolari nelle regole di filtro 667

4.5.1.1.1 Creazione di una nuova regola di Filtro contenuti



La finestra di dialogo Crea regola consente di definire le regole di Filtro contenuti. Per visualizzarla, fare clic sul pulsante *Nuova regola* nella finestra di dialogo di Filtro contenuti.

Crea regola

Nome della regola
Digitare in questo campo un nome descrittivo da assegnare alla nuova regola. Per impostazione predefinita, la regola viene denominata "New Rule #n (Nuova regola n.)".

Condizioni

In questa casella vengono elencate le condizioni da applicare alla nuova regola. Selezionare la casella di controllo corrispondente alla condizione da applicare alla nuova regola. Ogni condizione abilitata verrà visualizzata nella sottostante casella di descrizione della regola. Per specificare le informazioni aggiuntive necessarie per la maggior parte delle condizioni, fare clic sul collegamento ipertestuale della condizione nella casella di descrizione della regola.

Se [HEADER] contiene - Selezionare una di queste opzioni per basare la regola sul contenuto di tali specifiche intestazioni dei messaggi. È necessario specificare il testo da ricercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 667.

Se [# HEADER] definita dall'utente contiene - Fare clic su una o più di queste opzioni per basare la regola sulle intestazioni dei messaggi che si definiranno. È necessario specificare la nuova intestazione e il testo da ricercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 667.

Se il CORPO DEL MESSAGGIO contiene - Questa opzione trasforma il corpo del messaggio in una nelle condizioni. È necessario specificare la stringa di testo da cercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 667.

Se il MESSAGGIO ha allegati - Quando questa opzione è selezionata, la regola verrà condizionata alla presenza di uno o più allegati del messaggio. Non è necessario fornire informazioni aggiuntive.

Se la DIMENSIONE DEL MESSAGGIO supera - Selezionare questa opzione per creare la regola in base alla dimensione del messaggio. La dimensione deve essere indicata in*KB*. L'impostazione predefinita è 10 KB.

Se il MESSAGGIO INCLUDE UN FILE denominato - Se questa opzione è selezionata, verrà eseguita la ricerca di un allegato con un nome particolare. Il nome del file deve essere specificato. Sono consentiti i caratteri jolly, ad esempio, *.exe e *.*.

Se il messaggio è INFETTO... - Questa condizione è VERA quando MDaemon determina che un messaggio è infetto da un virus.

Se il CODICE DI USCITA del programma precedente è uguale a - Se in una regola precedente dell'elenco viene utilizza l'azione *Esegui processo*, sarà possibile

avvalersi di questa condizione per cercare un determinato codice di uscita dal programma.

Se il MESSAGGIO CONTIENE UNA FIRMA DIGITALE - La condizione è valida per i messaggi provvisti di firma digitale. Non è necessario aggiungere ulteriori informazioni.

Se il MITTENTE è un membro del GRUPPO... - Questa condizione si applica a un messaggio quando viene inviato da un account che è membro del gruppo di account indicato nella regola.

Se il DESTINATARIO appartiene al GRUPPO - La condizione viene applicata ai messaggi i cui destinatari appartengono al gruppo di account specificato nella regola.

Se TUTTI I MESSAGGI - Selezionare questa opzione per applicare la regola a tutti i messaggi. Non è necessario aggiungere ulteriori informazioni. Questa regola ha effetto su tutti i messaggi, eccezione fatta per quelli a cui è stata applicata l'azione "Blocca elaborazione regole" o "Elimina messaggio" nell'ambito di una regola precedente.

Azioni

Consente di specificare le azioni da eseguire se un messaggio corrisponde alle condizioni della regola. Per alcune azioni sono necessarie informazioni aggiuntive, che possono essere specificate facendo clic sul collegamento ipertestuale relativo all'azione nella casella di descrizione della regola.

Elimina messaggio - Se si seleziona questa azione, il messaggio verrà eliminato.

Rimuovi tutti gli allegati dal messaggio - Se viene selezionata questa azione, gli allegati del messaggio verranno rimossi.

Sposta in coda messaggi scartati - Se viene selezionata questa azione, il messaggio verrà spostato nella coda dei messaggi scartati. Al messaggio viene aggiunta un'intestazione `X-MDBadQueue-Reason`.

Ignora n regole - Se è selezionata questa azione, verrà ignorato il numero di regole specificato. L'opzione è utile per applicare la regola in alcune circostanze ma non in altre.

Si supponga, ad esempio, di voler eliminare i messaggi che contengono le parole "Pubblicità non desiderata", ma non quelli con le parole "Pubblicità gradita". A tale scopo, è necessario creare una regola in base alla quale eliminare i messaggi contenenti le parole "Pubblicità non desiderata" e, in una posizione superiore nell'elenco delle regole, specificare una regola che stabilisce di ignorare la prima se il messaggio contiene le parole "Pubblicità gradita".

Interrompi l'elaborazione delle regole - Questa azione ignora tutte le regole rimanenti.

Copia messaggio per gli utenti specificati - Grazie a questa azione, una copia del messaggio verrà inviata a uno o più destinatari. È necessario specificare i destinatari del messaggio.

Aggiungi una firma aziendale - Questa azione consente di creare un breve testo da aggiungere come piè di pagina al messaggio. In alternativa, è possibile aggiungere il contenuto di un file di testo. È disponibile una casella di controllo *Usa HTML* per includere il codice HTML nel testo della firma. Questa azione supporta le macro firme $CONTACT...$*** 137.

Ad esempio, questa regola è utile per includere il testo "Questo messaggio e-mail è stato inviato da nomeazienda. Per commenti o domande, scrivere a utente01@esempio.com".

Aggiungi ulteriore intestazione al messaggio - Questa opzione consente di aggiungere un'ulteriore intestazione al messaggio. È necessario specificare il nome e il valore della nuova intestazione.

Elimina intestazione dal messaggio - Questa azione consente di rimuovere un'intestazione dal messaggio. È necessario specificare l'intestazione da eliminare.

Send Note To (Invia una nota a) - Questa azione consente di inviare un messaggio e-mail a un determinato indirizzo. Le opzioni disponibili consentono di specificare il destinatario, il mittente, l'oggetto e un breve testo. È inoltre possibile allegare alla nota il messaggio originale. **Nota:** questa azione consente di ignorare tutti i messaggi non dotati di percorso restituzione. Pertanto non può essere attivata, ad esempio, dai messaggi DSN (Delivery Status Notification).

È, ad esempio, possibile creare una regola in base a cui tutti i messaggi che contengono il testo "Questa è posta indesiderata" devono essere spostati nella directory dei messaggi scartati e un'altra regola che consente di inviarne notifica all'utente.

Rimuovi firma digitale - Fare clic su questa opzione per rimuovere una firma digitale dal messaggio.

Esegui processo... - Questa azione è utile per eseguire un particolare programma quando un messaggio corrisponde alle condizioni della regola. È necessario specificare il percorso del programma da eseguire. È possibile utilizzare la macro $MESSAGEFILENAME$ per passare il nome del messaggio al processo, nonché specificare se sospendere temporaneamente o indefinitamente le operazioni di MDaemon durante l'esecuzione. Inoltre, è possibile imporre la conclusione del processo e/o l'esecuzione in una finestra nascosta.

Invia il messaggio mediante un server gateway SMS - Questa opzione consente di inviare il messaggio mediante un server gateway SMS. È necessario specificare l'host o l'indirizzo IP e il numero di telefono SMS.

Copia il messaggio nella cartella... - Utilizzare questa opzione per archiviare una copia del messaggio in una cartella specifica.

SPOSTA i messaggi nella CODA personalizzata - Questa azione consente di spostare il messaggio in una o più code di posta personalizzate esistenti. Se si spostano i messaggi nelle code di posta remota personalizzate, è possibile utilizzare le opzioni di pianificazione personalizzata di Pianificazione eventi per controllare il momento in cui i messaggi vengono elaborati.

Aggiungi riga a file di testo - Questa opzione consente di aggiungere una riga a uno specifico file di testo. È necessario specificare il percorso del file e il testo da aggiungere. Nel testo possono essere utilizzate alcune macro, in modo che Filtro contenuti includa dinamicamente informazioni quali il mittente, il destinatario, l'ID messaggio e così via. Per visualizzare l'elenco delle macro consentite, fare clic sul pulsante Macro nella finestra di dialogo "Aggiungi riga a file di testo".

[Copia|Sposta] messaggio in cartelle pubbliche - Questa azione consente di copiare o spostare il messaggio in una o più cartelle pubbliche.

Trova e sostituisci in un'intestazione - Questa opzione consente di cercare determinate parole in un'intestazione specificata, quindi di eliminarle o sostituirle. Durante la creazione di questa regola, fare clic sul collegamento ipertestuale relativo alla specifica delle informazioni nella descrizione della regola per aprire la finestra "Intestazione – cerca e sostituisci", nella quale è possibile inserire l'intestazione e le parole da sostituire o eliminare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 667.

Trova e sostituisci nel corpo del messaggio - Questa opzione consente di cercare nel corpo del messaggio per sostituire il testo desiderato. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 667.

Passa a regola... - Utilizzare questa azione per passare direttamente a una regola successiva dell'elenco, saltando tutte le altre regole comprese tra le due.

Invio un messaggio istantaneo... - Questa azione invia un messaggio istantaneo a qualcuno quando il messaggio corrisponde ai criteri della regola. È possibile specificare l'indirizzo e-mail **A:**, l'indirizzo **Da:** e il contenuto del messaggio.

Aggiungi al Registro eventi di Windows... - Utilizzare questa azione per registrare una stringa di testo nel Registro eventi di Windows. È possibile utilizzare le macro nella stringa ed è disponibile un pulsante per visualizzare le macro consentite.

Estrai allegati nella cartella... - Utilizzare questa azione per estrarre allegati da un messaggio. È necessario specificare la cartella nella quale saranno copiati gli allegati ed è possibile scegliere di rimuovere l'allegato dal messaggio dopo averlo estratto. È anche possibile impostare delle condizioni per determinare quali allegati saranno estratti, in base al nome del file, al tipo di contenuto e alle dimensioni degli allegati.

Modifica priorità di elaborazione messaggio... - Questa azione è utilizzata per impostare la priorità di elaborazione del messaggio, da "10 (Urgente)" a "90 (Ritenta)". L'impostazione predefinita è "50 (normale)".

Firma con il selettore DKIM - Selezionando questa azione, nel messaggio verrà inserita una firma DKIM 539. L'opzione consente anche di firmare alcuni messaggi con un selettore diverso da quello indicato nella finestra di dialogo DKIM.

Contrassegna messaggi per REQUIRETLS... - Indica che il messaggio deve utilizzare REQUIRETLS 601.

[Firma|Crittografa|Decrittografa] il messaggio con la chiave [Privata|Pubblica] dell'utente... - Utilizzare queste azioni per firmare, crittografare o decrittografare un messaggio usando una chiave pubblica o privata. Vedere: MDPGP 641 per ulteriori informazioni. **Nota:** queste azioni verranno eseguite anche quando MDPGP è disattivato.

Aggiungi un'avvertenza all'inizio del messaggio... - Utilizzare questa azione se si desidera aggiungere un qualche tipo di avvertenza all'inizio del messaggio. È necessario immettere una stringa di testo semplice o codice HTML e selezionare la casella "Usa HTML". In alternativa, è possibile caricare il testo da un file.

Aggiungi un allegato... - Utilizzare questa azione se si desidera allegare un file a un messaggio che soddisfa i criteri della regola. Il file deve essere nella cartella `./MDaemon/CFilter/Attachments/`.

Estrai gli allegati e aggiungi i collegamenti... - Utilizzare questa azione se si desidera estrarre gli allegati dai messaggi che soddisfano i criteri della regola e aggiungere dei collegamenti. Vedere: Collegamento allegati 373.

Descrizione regola

In questa casella viene visualizzato il formato script interno della nuova regola. Fare clic su una delle condizioni o azioni della regola, rappresentate da collegamenti ipertestuali, per aprire l'editor appropriato e specificare le informazioni richieste.

Per ulteriori informazioni, vedere:

Editor di Filtro contenuti 659
Modifica di una regola di Filtro contenuti esistente 666
Uso di espressioni regolari nelle regole di filtro 667

4.5.1.1.2 Modifica di una regola di Filtro contenuti esistente

Per modificare una regola esistente, selezionarla e fare clic sul pulsante *Modifica regola* nella finestra di dialogo di Filtro contenuti. Verrà visualizzato l'editor che consente di modificare la regola. I comandi presenti in questo editor sono identici a quelli della finestra di dialogo Crea regola 661.

Per ulteriori informazioni, vedere:

Filtro contenuti 659
Creazione di una nuova regola di filtro dei contenuti 661
Uso di espressioni regolari nelle regole di filtro 667

4.5.1.1.3 Uso di espressioni regolari nelle regole di filtro

Il sistema di Filtro contenuti supporta le ricerche in base a *espressioni regolari*, una tecnica versatile che consente di cercare non solo stringhe di testo specifiche, ma anche *modelli* di testo. Le espressioni regolari contengono un insieme di testo semplice e di caratteri speciali che indicano il genere di corrispondenza da ricercare e, di conseguenza, rendono le regole di filtro dei contenuti più potenti e mirate.

Descrizione delle espressioni regolari
Un'espressione regolare (regular expression o regexp) è un modello di testo costituito da una combinazione di caratteri speciali, noti come *metacaratteri* e di caratteri di testo alfanumerici o "*letterali*", ad esempio abc, 123 e così via. Il modello viene utilizzato per confrontare le stringhe di testo. Le espressioni regolari vengono utilizzate principalmente per individuare corrispondenze di testo normale e per eseguire ricerche e sostituzioni.

I metacaratteri sono caratteri speciali utilizzati per funzioni e scopi specifici nell'ambito delle espressioni regolari. L'implementazione delle espressioni regolari nel sistema Filtro contenuti di MDaemon consente l'utilizzo dei seguenti metacaratteri:

```
\ | () [] ^ $ * + ? . <>
```

Metacaratteri	Descrizione
****	Quando precede un metacarattere, la barra rovesciata ("\") fa sì che questo venga considerato come un carattere letterale. La barra è necessaria se si desidera che l'espressione regolare esegua la ricerca di uno dei caratteri speciali utilizzati come metacarattere. Ad esempio, per la ricerca di "+" le espressioni devono includere "\+".
|	Il carattere *disgiuntivo* (chiamato anche "*OR*" o "*barra verticale*") viene utilizzato per indicare che una delle espressioni ai lati del carattere deve corrispondere alla stringa di destinazione. Nella ricerca di una stringa di testo, l'espressione regolare "abc|xyz" troverà una corrispondenza con tutte le occorrenze di "abc" o "xyz".
[...]	Una serie di caratteri tra parentesi quadre ("[" e "]") indica che qualsiasi carattere della serie può corrispondere alla stringa di testo desiderata. Un trattino ("-") interposto tra i caratteri racchiusi da parentesi indica un intervallo di caratteri. Ad esempio, la ricerca della stringa "abc" con

l'espressione regolare "[a-z]" produrrà tre corrispondenze: "*a*", "*b*" e "*c*". L'utilizzo dell'espressione "[az]" determinerà una sola corrispondenza: "*a*".

^ Indica l'inizio di una riga. Nella stringa di destinazione "abc ab a", l'espressione "^a" produrrà una corrispondenza, ovvero il primo carattere della stringa di destinazione. Anche l'espressione regolare "^ab" produrrà una corrispondenza, con i primi *due* caratteri della stringa di destinazione.

[^...] L'accento circonflesso ("^") immediatamente successivo alla parentesi quadra sinistra ("[") ha un altro significato. Viene utilizzato per escludere gli altri caratteri tra parentesi dalla corrispondenza con la stringa di destinazione. L'espressione "[^0-9]" indica che il carattere di destinazione non deve essere un numero.

(...) Le parentesi interessano l'ordine di valutazione del modello e operano come espressione *racchiusa tra tag* da utilizzare per le espressioni di *ricerca e sostituzione*.

Il risultato di una ricerca eseguita con un'espressione regolare viene temporaneamente conservato e può essere utilizzato nell'espressione *sostitutiva* per creare una nuova espressione. Nell'espressione *replace* è possibile includere un carattere "$0", che sarà sostituito dalla sotto-stringa trovata nell'espressione regolare durante la ricerca. Quindi, se l'espressione *search* "a(bcd)e" rileva una sotto-stringa corrispondente, un'espressione *replace* di "123-$0-123" sostituirà il testo corrispondente con "123-abcde-123".

Allo stesso modo, è possibile utilizzare i caratteri speciali "$1", "$2", "$3" e così via nell'espressione *replace*. Questi caratteri vengono sostituiti solo dai risultati dell'espressione *racchiusa tra tag* anziché dall'intera sottostringa corrispondente. Se l'espressione regolare contiene più espressioni racchiuse da tag, il numero che segue la barra rovesciata indica l'espressione racchiusa tra tag alla quale si fa riferimento. Ad esempio, se l'espressione di *ricerca* è "(123)(456)" e l'espressione di *sostituzione* è "a-$2-b-$1", la sottostringa corrispondente verrà sostituita con "a-456-b-123" e, in questa, l'espressione di *sostituzione* "a-$0-b" verrà sostituita con "a-123456-b"

**$** Il simbolo di dollaro ("$") indica la fine della riga. Nella stringa di testo "13 321 123", l'espressione "3$" produrrà una corrispondenza, rappresentata dall'ultimo carattere della stringa. Anche l'espressione regolare "123$" produrrà una corrispondenza, con gli ultimi *tre* caratteri della stringa di destinazione.

*	L'asterisco ("*") di quantificazione indica che il carattere situato a sinistra deve corrispondere a *zero o più* occorrenze del carattere in una riga. Pertanto, "1*abc" produrrà una corrispondenza con il testo "111abc" e "abc".
+	Analogamente all'asterisco di quantificazione, il segno "+" di quantificazione indica che il carattere situato a sinistra deve corrispondere a *una o più* occorrenze del carattere in una riga. Pertanto, "1+abc" produrrà una corrispondenza con il testo "111abc", ma non con il testo "abc".
?	Il punto interrogativo ("?") di quantificazione indica che il carattere situato a sinistra deve corrispondere *zero o una* volta. "1?abc" produrrà quindi una corrispondenza con il testo "abc" e con la porzione "1abc" di "111abc".
.	Il metacarattere punto (".") indica una corrispondenza con qualsiasi altro carattere. ".+abc" produrrà una corrispondenza con "123456abc" e "a.c" con "aac", abc", acc" e così via.

Condizioni e azioni appropriate
È possibile utilizzare le espressioni regolari in qualsiasi *Condizione* della regola di filtro *Intestazione*. ad esempio in qualsiasi regola la cui condizione sia "`Se l'INTESTAZIONE FROM contiene`". Le espressioni regolari possono essere utilizzate anche nella condizione "`Se il CORPO DEL MESSAGGIO contiene`".

Le espressioni regolari possono essere utilizzate in due *azioni* delle regole di Filtro contenuti: "`Trova e sostituisci in un'intestazione`" e "`Trova e sostituisci nel corpo del messaggio`".

Le espressioni regolari utilizzate nelle *condizioni* delle regole di Filtro contenuti non tengono conto della distinzione tra maiuscole/minuscole. Una lettera maiuscola viene considerata identica alla stessa lettera minuscola.

Il riconoscimento di maiuscole e minuscole nelle espressioni regolari utilizzate nelle *azioni* delle regole di Filtro contenuti è facoltativo. Quando si crea un'espressione regolare nell'azione della regola, è possibile abilitare o disabilitare questa opzione.

Configurazione di un'espressione regolare nella condizione di una regola

Per configurare una condizione di intestazione o corpo del messaggio utilizzando un'espressione regolare, procedere come indicato di seguito.

1. Nella finestra di dialogo Crea regola, scegliere la casella di controllo corrispondente alla condizione di intestazione o corpo del messaggio da inserire nella regola.

2. Nell'area di riepilogo situata nella parte inferiore della finestra di dialogo Crea regola, scegliere il collegamento "**contiene stringhe specifiche**" corrispondente alla condizione selezionata nel passaggio 1. Verrà visualizzata la finestra di dialogo Specifica testo ricerca.

3. Fare clic sul collegamento "**contains (contiene)**" all'interno dell'area "Stringhe correnti".

4. Scegliere "**Matches Regular Expression (Corrisponde a espressione regolare)**" nella casella di riepilogo a discesa, quindi fare clic su **OK**.

5. Se si desidera assistenza per la creazione dell'espressione regolare o si intende controllarla, scegliere "**Prova espressione regolare**." Se non si desidera utilizzare la finestra di dialogo Test espressione regolare, inserire l'espressione regolare nella casella di testo, scegliere **Aggiungi** e proseguire con il passaggio 8.

6. Inserire l'espressione nella casella di testo "Cerca espressione". Per semplificare il processo, utilizzare il menu di scelta rapida, che consente di inserire agevolmente i metacaratteri desiderati nell'espressione. Per accedere al menu, scegliere il pulsante ">". Quando si seleziona un'opzione del menu, nell'espressione viene inserito il metacarattere corrispondente e il punto di inserimento viene spostato nella posizione appropriata per il carattere stesso.

7. Digitare il testo per il controllo dell'espressione nell'area di testo e scegliere **Test**. Al termine del controllo, scegliere **OK**.

8. Fare clic su **OK**.

9. Proseguire con la creazione della regola.

Configurazione di un'espressione regolare nell'azione di una regola

Per configurare un'azione di ricerca e sostituzione utilizzando un'espressione regolare, attenersi alla procedura indicata di seguito.

1. Nella finestra di dialogo Crea regola, scegliere la casella di controllo corrispondente all'azione "*Search and Replace... (Trova e sostituisci)*" da inserire nella regola.

2. Nell'area di riepilogo situata nella parte inferiore della finestra di dialogo Crea regola, scegliere il collegamento "**specifica informazioni**" corrispondente alla condizione selezionata nel passaggio 1. Verrà visualizzata la finestra di dialogo Trova e sostituisci.

3. Se nel passaggio 1 si è scelta l'azione "*Cerca in intestazione...*", nella casella di riepilogo a discesa selezionare l'intestazione desiderata oppure digitarla, se non disponibile. Se nel passaggio 1 non si è scelta l'azione "*Cerca in intestazione...*", ignorare questo passaggio.

4. Inserire l'espressione di *ricerca* desiderata. Per semplificare il processo, utilizzare il menu di scelta rapida, che consente di inserire agevolmente i metacaratteri desiderati nell'espressione. Per accedere al menu, scegliere il pulsante ">". Quando si seleziona un'opzione del menu, nell'espressione viene inserito il metacarattere

corrispondente e il punto di inserimento viene spostato nella posizione appropriata per il carattere stesso.

5. Inserire l'espressione *sostitutiva* desiderata. Come nel caso dell'espressione di *ricerca*, anche in questa situazione è possibile utilizzare un menu di scelta rapida. Per eliminare la sottostringa anziché sostituirla con un testo diverso, lasciare la casella di testo vuota.

6. Se si desidera che l'espressione tenga conto di maiuscole e minuscole, scegliere "**Maiuscole/minuscole**".

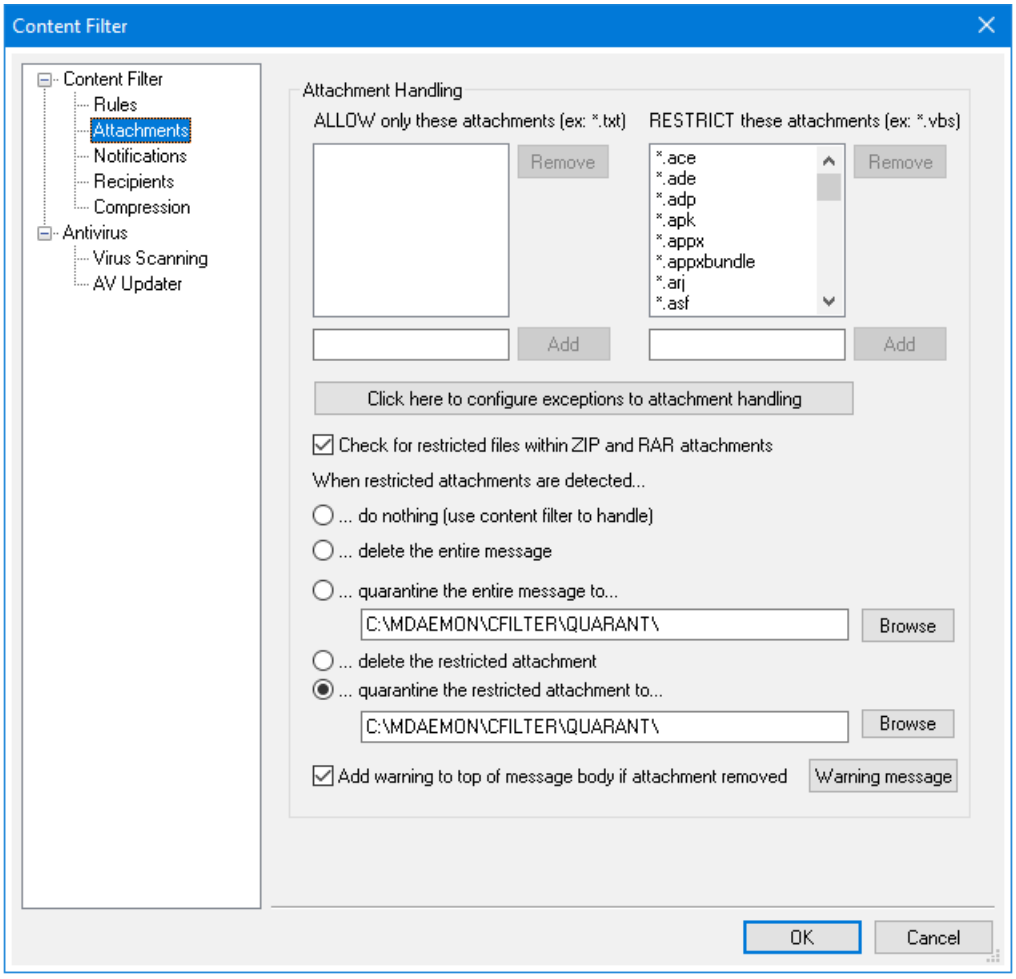
7. Per trovare e sostituire stringhe da considerare come espressioni regolari, scegliere Espressione regolare. In caso contrario, ogni stringa verrà considerata come semplice sottostringa di ricerca e sostituzione e verrà ricercata una corrispondenza letterale esatta del testo.

8. Se non si desidera controllare l'espressione, ignorare questo passaggio. Per controllare l'espressione, scegliere "**Esegui controllo**". Nella finestra di dialogo relativa al controllo delle operazioni di ricerca e sostituzione, inserire le espressioni e il testo da controllare, quindi scegliere **Controlla**. Al termine del controllo, scegliere **OK**.

9. Fare clic su **OK**.

10. Proseguire con la creazione della regola.

4.5.1.2 Allegati



Questa scheda consente di specificare gli allegati da classificare come ammessi o con restrizioni. Gli allegati non consentiti vengono rimossi automaticamente dai messaggi.

Gestione allegati

I nomi file specificati nell'elenco *APPL. RESTRIZIONI a questi allegati* vengono rimossi automaticamente dai messaggi. Se si inseriscono file nell'elenco *CONSENTI solo questi allegati*, verranno ammessi solo i file presenti nell'elenco e tutti gli altri allegati verranno rimossi. Dopo la rimozione dell'allegato, MDaemon consegna normalmente il messaggio, ma senza l'allegato. Le opzioni della scheda Notifiche possono essere utilizzate per inviare un messaggio di notifica a più indirizzi quando viene rilevato un allegato con restrizioni.

Nelle voci dell'elenco sono consentiti i caratteri jolly. Ad esempio, la voce "`*.exe`" determina l'ammissione o la rimozione di tutti gli allegati con estensione `EXE`. Per aggiungere una voce a un elenco, digitarne il nome file nell'apposito campo, quindi fare clic su Aggiungi.

Fare clic qui per configurare le eccezioni di gestione allegati
Fare clic su questo pulsante per specificare gli indirizzi da escludere dal controllo delle restrizioni imposte agli allegati. I messaggi destinati a questi indirizzi vengono elaborati anche se contengono un allegato con restrizioni.

Controlla file soggetti a limitazioni in allegati ZIP e RAR
Fare clic su questa opzione per controllare la presenza di file soggetti a limitazioni nel contenuto di allegati Zip, 7-Zip e RAR. Inoltre, verrà attivata qualsiasi altra regola del Filtro contenuti impostata per la ricerca di un nome file specifico all'interno di un allegato compresso.

Quando vengono rilevati allegati con restrizioni...
Fare clic sull'azione che si desidera venga intrapresa quando un messaggio contiene un allegato con restrizioni.

Nessuna azione (gestione con filtro contenuti)
Scegliere questa opzione se non si desidera intraprendere un'azione specifica in base alle impostazioni degli allegati, ma si desidera basare le azioni sulle regole di Filtro contenuti 659.

Elimina l'intero messaggio
Questa opzione prevede l'eliminazione dell'intero messaggio che contiene un allegato con restrizioni.

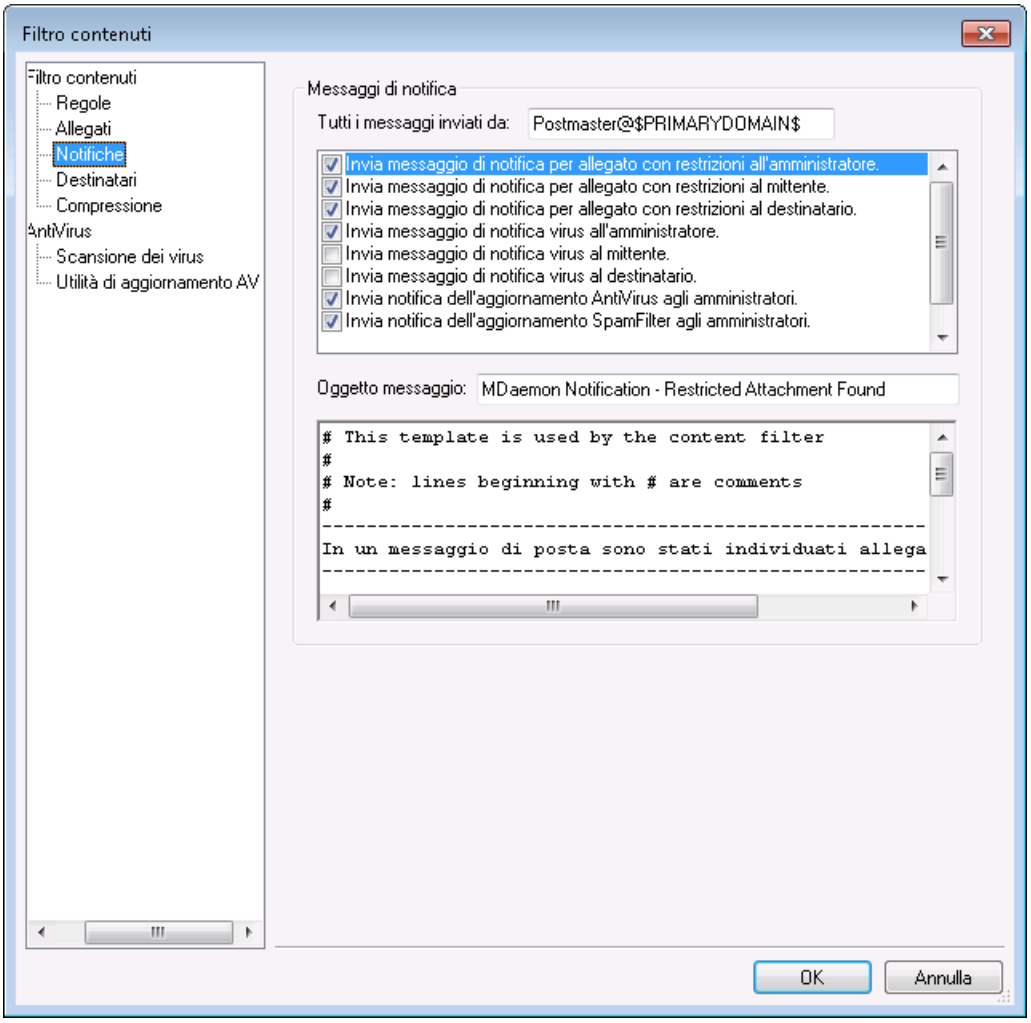
Poni in quarantena l'intero msg. in
Questa opzione consente di mettere in quarantena nella posizione specificata i messaggi con allegati con restrizioni.

Elimina l'allegato con restrizioni
Scegliere questa opzione se si desidera eliminare gli allegati con restrizioni invece di eliminare l'intero messaggio.

Poni in quarantena l'allegato con restrizioni in...
Per porre in quarantena gli allegati con limitazioni in una posizione specifica anziché eliminarli, selezionare questa opzione e indicare la posizione desiderata. Questa è l'impostazione predefinita.

Aggiungere un avviso all'inizio del corpo del messaggio se l'allegato è stato rimosso
Quando rimuove un allegato da un messaggio, ad esempio perché è stato rilevato un virus, MDaemon aggiunge un di avviso all'inizio del corpo del messaggio. Fare clic sul pulsante **Avviso** per rivedere o modificare il modello del messaggio di avviso. L'opzione è abilitata per impostazione predefinita.

4.5.1.3 Notifiche



Utilizzare questa schermata per designare le persone che devono ricevere messaggi di notifica quando viene rilevato un virus o un allegato limitato oppure quando vengono aggiornati i file dell'antivirus o di Spam Filter.

Messaggi di notifica

Tutti i messaggi inviati da:
Questa casella consente di specificare l'indirizzo da cui inviare i messaggi di notifica.

Invia messaggio di notifica virus a...
Quando viene recapitato un messaggio con un allegato contenente un virus, viene inviato un messaggio di avviso ai soggetti specificati in questa sezione. È possibile inviare un messaggio personalizzato al mittente, al destinatario e agli amministratori specificati nella schermata Destinatari 680. Per personalizzare il messaggio per una qualsiasi di queste tre voci, selezionarne una dall'elenco, quindi modificare il messaggio visualizzato nella metà inferiore della schermata. Ogni voce è associata a un messaggio diverso, anche se per impostazione predefinita alcuni sono identici.

Invia messaggio di notifica per allegato con restrizioni a...
Quando viene recapitato un messaggio con un allegato corrispondente a una voce con restrizioni (elencate nella scheda Allegati), viene inviato un messaggio di avviso ai soggetti specificati in questa sezione. È possibile inviare un messaggio personalizzato al mittente, al destinatario e agli amministratori specificati nella scheda Destinatari. Per personalizzare il messaggio per una qualsiasi di queste tre voci, selezionarne una dall'elenco, quindi modificare il messaggio visualizzato nella metà inferiore della scheda. Ogni voce è associata a un messaggio diverso, anche se per impostazione predefinita sono tutti e tre identici.

Invia notifica di aggiornamento Spam Filter agli amministratori
Utilizzare questa opzione se si desidera inviare agli amministratori ad ogni aggiornamento di Spam Filter un messaggio e-mail contenente i risultati dell'aggiornamento. Questa opzione è uguale all'opzione "*Invia messaggi di notifica con risultati aggiornamento*" disponibile in: `Spam Filter » Aggiornamenti`.

Oggetto messaggio:
Questo testo viene visualizzato nell'intestazione "Subject:" del messaggio di notifica inviato.

Messaggio
Si tratta del messaggio che verrà inviato alla voce selezionata nell'elenco descritto in precedenza, purché la casella di controllo corrispondente sia selezionata. Il messaggio può essere modificato direttamente nella casella in cui viene visualizzato.

I file effettivi che contengono questo testo si trovano nella directory `MDaemon\app\`. Questi sono:

`cfattrem[adm].dat` – Messaggio per allegati con restrizioni - Amministratori
`cfattrem[rec].dat` – Messaggio per allegato con restrizioni - Destinatario
`cfattrem[snd].dat` – Messaggio per allegato con restrizioni - Mittente
`cfvirfnd[adm].dat` – Messaggio per rilevamento virus - Amministratori
`cfvirfnd[rec].dat` – Messaggio per rilevamento virus - Destinatario
`cfvirfnd[snd].dat` – Messaggio per rilevamento virus - Mittente

Per ripristinare l'aspetto originale di uno di questi messaggi, è sufficiente eliminare il file desiderato perché MDaemon lo crei nuovamente nello stato predefinito.

Macro per i messaggi

Nei messaggi di notifica e in altri messaggi generati da Filtro contenuti è possibile utilizzare alcune macro. È possibile utilizzare le macro:

$ACTUALTO$	Alcuni messaggi possono contenere un campo "ActualTo" che, generalmente, rappresenta la casella postale e l'host di destinazione immessi dall'utente originale prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$AV_VERSION$	Elenca le versioni di AntiVirus utilizzate.
$CURRENTTIME$	Questa macro viene sostituita con l'ora corrente in cui il messaggio viene elaborato.
$ACTUALFROM$	Alcuni messaggi possono contenere un campo "ActualFrom" che, generalmente, rappresenta la casella postale e l'host di origine prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$FILTERRULENAME$	Questa macro viene sostituita dal nome della regola i cui criteri corrispondono al messaggio.
$FROM$	Espande l'indirizzo completo contenuto nell'intestazione "From:" del messaggio.
$FROMDOMAIN$	Questa macro inserisce il nome di dominio contenuto nell'indirizzo trovato nell'intestazione "From:" del messaggio (il valore a destra di "@" nell'indirizzo e-mail).
$FROMMAILBOX$	Riporta la parte relativa alla casella postale dell'indirizzo trovato nell'intestazione "From:" del messaggio (il valore a sinistra di "@" nell'indirizzo e-mail).
GEN_GUID	Viene generato un ID univoco con 11 caratteri alfanumerici. Esempio: 0XVBASADTZC
$HEADER:XX$	Questa macro viene sostituita nel messaggio riformattato dal valore dell'intestazione "xx". Ad esempio, Se nel messaggio originale è presente "`TO: utente01@esempio.com`", la macro `$HEADER:TO$` verrà espansa in "utente01@esempio.com". Se nel messaggio originale è presente "Subject: Questo è l'oggetto", la macro `$HEADER:SUBJECT$` verrà sostituita dal testo "Questo è l'oggetto".
$HEADER:MESSAGE-ID$	Analogamente alla macro `$HEADER:XX$`, questa macro viene sostituita dal valore dell'intestazione `Message-ID`.
$LIST_ATTACHMENTS_REMOVED$	Questa macro visualizza gli allegati rimossi dal messaggio.
$LIST_VIRUSES_FOUND$	Questa macro visualizza i virus rilevati in un

messaggio.

$MESSAGEFILENAME$	Questa macro restituisce il nome file del messaggio in corso di elaborazione.
$MESSAGEID$	Simile alla macro $HEADER:MESSAGE-ID$ precedente, a eccezione del fatto che rimuove i caratteri "<>" dal valore di message ID.
$PRIMARYDOMAIN$	Restituisce il nome del dominio predefinito di MDaemon, indicato nella schermata di Domain Manager 185.
$PRIMARYIP$	Questa macro restituisce l'indirizzo IPv4 188 del dominio predefinito 185.
$PRIMARYIP6$	Questa macro restituisce l'indirizzo IPv6 188 del dominio predefinito 185.
$RECIPIENT$	Questa macro viene sostituita dall'indirizzo completo del destinatario del messaggio.
$RECIPIENTDOMAIN$	Questa macro viene sostituita dal nome dominio del destinatario del messaggio.
$RECIPIENTMAILBOX$	Indica la casella postale del destinatario (il valore a sinistra di "@" nell'indirizzo di posta elettronica).
$REPLYTO$	Questa macro espande il valore dell'intestazione "Reply-to" del messaggio.
$SENDER$	Questa macro restituisce l'indirizzo completo da cui è stato inviato il messaggio.
$SENDERDOMAIN$	Questa macro viene sostituita dal nome dominio del mittente del messaggio (il valore a destra di "@" nell'indirizzo di posta elettronica).
$SENDERMAILBOX$	Indica la casella postale del mittente (il valore a sinistra di "@" nell'indirizzo di posta elettronica).
$SUBJECT$	Visualizza il testo contenuto nell'oggetto del messaggio.

4.5.1.3.1 Macro per i messaggi

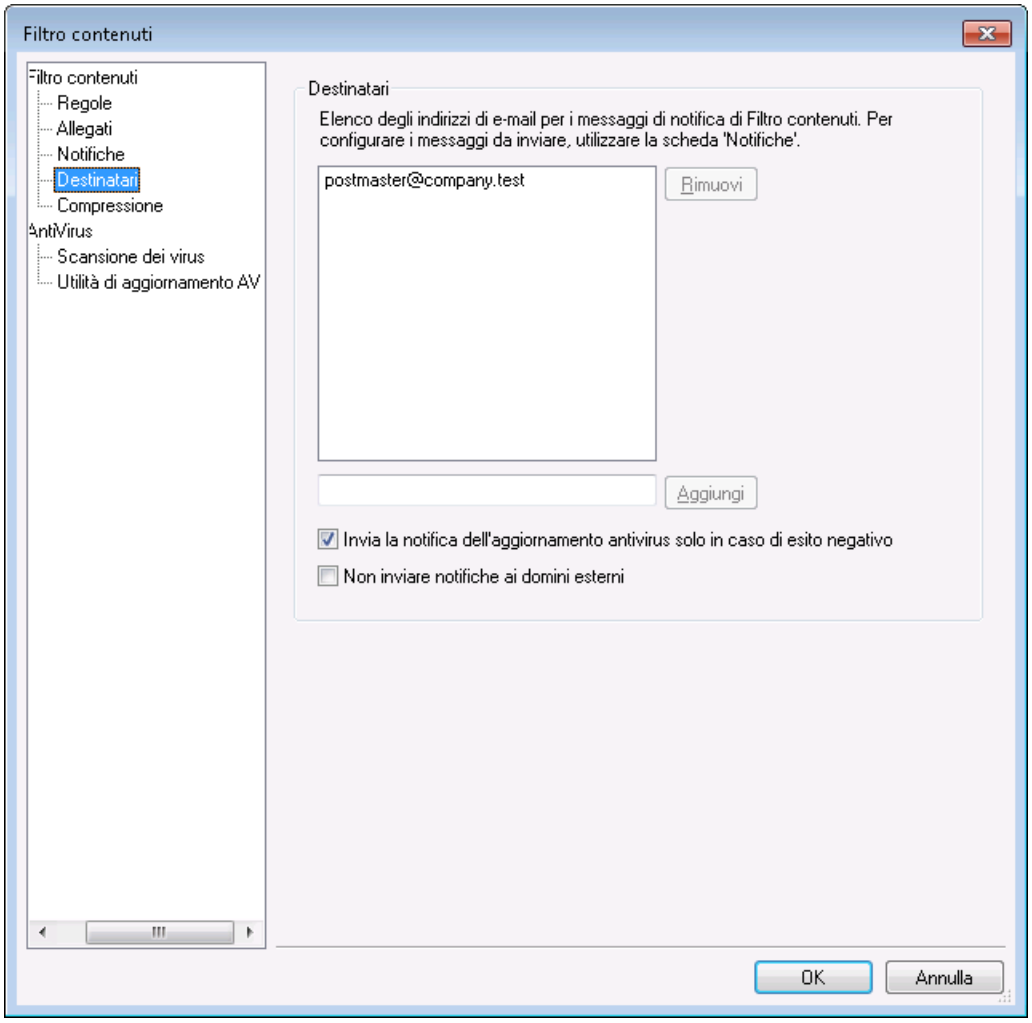
Nei messaggi di notifica e in altri messaggi generati da Filtro contenuti è possibile utilizzare alcune macro. È possibile utilizzare le macro:

$ACTUALTO$	Alcuni messaggi possono contenere un campo "ActualTo" che, generalmente, rappresenta la

	casella postale e l'host di destinazione immessi dall'utente originale prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$AV_VERSION$	Elenca le versioni di AntiVirus utilizzate.
$CURRENTTIME$	Questa macro viene sostituita con l'ora corrente in cui il messaggio viene elaborato.
$ACTUALFROM$	Alcuni messaggi possono contenere un campo "ActualFrom" che, generalmente, rappresenta la casella postale e l'host di origine prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$FILTERRULENAME$	Questa macro viene sostituita dal nome della regola i cui criteri corrispondono al messaggio.
$FROM$	Espande l'indirizzo completo contenuto nell'intestazione "From:" del messaggio.
$FROMDOMAIN$	Questa macro inserisce il nome di dominio contenuto nell'indirizzo trovato nell'intestazione "From:" del messaggio (il valore a destra di "@" nell'indirizzo e-mail).
$FROMMAILBOX$	Riporta la parte relativa alla casella postale dell'indirizzo trovato nell'intestazione "From:" del messaggio (il valore a sinistra di "@" nell'indirizzo e-mail).
GEN_GUID	Viene generato un ID univoco con 11 caratteri alfanumerici. Esempio: 0XVBASADTZC
$HEADER:XX$	Questa macro viene sostituita nel messaggio riformattato dal valore dell'intestazione "xx". Ad esempio, Se nel messaggio originale è presente "`TO: utente01@esempio.com`", la macro `$HEADER:TO$` verrà espansa in "utente01@esempio.com". Se nel messaggio originale è presente "Subject: Questo è l'oggetto", la macro `$HEADER:SUBJECT$` verrà sostituita dal testo "Questo è l'oggetto".
$HEADER:MESSAGE-ID$	Analogamente alla macro `$HEADER:XX$`, questa macro viene sostituita dal valore dell'intestazione `Message-ID`.
$LIST_ATTACHMENTS_REMOVED$	Questa macro visualizza gli allegati rimossi dal messaggio.
$LIST_VIRUSES_FOUND$	Questa macro visualizza i virus rilevati in un messaggio.

$MESSAGEFILENAME$	Questa macro restituisce il nome file del messaggio in corso di elaborazione.
$MESSAGEID$	Simile alla macro $HEADER:MESSAGE-ID$ precedente, a eccezione del fatto che rimuove i caratteri "<>" dal valore di message ID.
$PRIMARYDOMAIN$	Restituisce il nome del dominio predefinito di MDaemon, indicato nella schermata di Domain Manager 185.
$PRIMARYIP$	Questa macro restituisce l'indirizzo IPv4 188 del dominio predefinito 185.
$PRIMARYIP6$	Questa macro restituisce l'indirizzo IPv6 188 del dominio predefinito 185.
$RECIPIENT$	Questa macro viene sostituita dall'indirizzo completo del destinatario del messaggio.
$RECIPIENTDOMAIN$	Questa macro viene sostituita dal nome dominio del destinatario del messaggio.
$RECIPIENTMAILBOX$	Indica la casella postale del destinatario (il valore a sinistra di "@" nell'indirizzo di posta elettronica).
$REPLYTO$	Questa macro espande il valore dell'intestazione "Reply-to" del messaggio.
$SENDER$	Questa macro restituisce l'indirizzo completo da cui è stato inviato il messaggio.
$SENDERDOMAIN$	Questa macro viene sostituita dal nome dominio del mittente del messaggio (il valore a destra di "@" nell'indirizzo di posta elettronica).
$SENDERMAILBOX$	Indica la casella postale del mittente (il valore a sinistra di "@" nell'indirizzo di posta elettronica).
$SUBJECT$	Visualizza il testo contenuto nell'oggetto del messaggio.

4.5.1.4 Destinatari

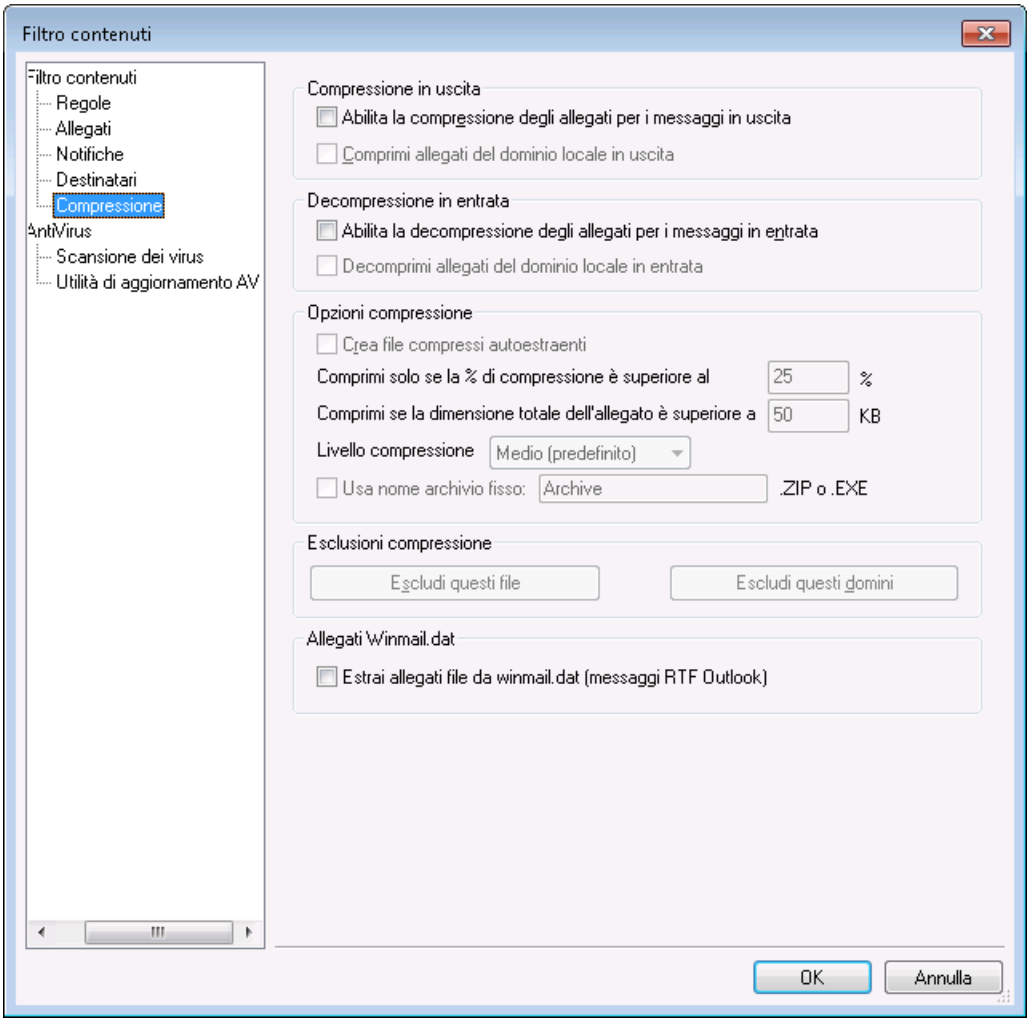


Destinatari

Questo elenco di destinatari corrisponde alle diverse opzioni della scheda *Notifiche* utilizzate per inviare messaggi agli amministratori. Sono gli indirizzi ai quali viene inviato un messaggio di notifica quando viene selezionata un'opzione di tipo amministrativo della scheda Notifiche. Per aggiungere un indirizzo in questa sezione, digitarlo nell'apposita casella e fare clic su *Aggiungi*. Per rimuovere un indirizzo, selezionarlo dall'elenco e fare clic su *Rimuovi*.

Non inviare notifiche ai domini esterni
Selezionare questa casella se si desidera limitare i messaggi di notifica del Filtro contenuti ai destinatari del dominio locale. L'opzione è disabilitata per impostazione predefinita.

4.5.1.5 Compressione



I comandi di questa scheda consentono di comprimere o decomprimere automaticamente gli allegati prima della consegna del messaggio. È possibile controllare il livello di compressione, nonché altri parametri e criteri di esclusione. Questa funzione può ridurre sensibilmente la larghezza di banda e il throughput necessari per consegnare i messaggi in uscita.

Compressione in uscita

Abilita la compressione degli allegati per i messaggi in uscita
Scegliere questa casella di controllo per abilitare la compressione automatica degli allegati dei messaggi remoti in uscita. Selezionando questo comando non verranno compressi tutti gli allegati, ma si attiverà semplicemente la funzione. Per determinare la compressione dei file è necessario specificare le altre impostazioni della scheda.

Comprimi allegati del dominio locale in uscita
Specificare questo comando per applicare le impostazioni di compressione a tutta la posta in uscita, compresi i messaggi destinati a un altro indirizzo locale.

Compressione in entrata

Abilita la decompressione degli allegati per i messaggi in entrata
Selezionare questa casella di controllo per attivare la decompressione automatica degli allegati dei messaggi di posta remota in entrata. Quando viene recapitato un messaggio con un allegato compresso, quest'ultimo verrà decompresso prima che il messaggio venga consegnato nella casella postale dell'utente locale.

Decomprimi allegati del dominio locale in entrata
Selezionare questa casella di controllo per applicare la funzione di decompressione automatica anche agli allegati della posta locale.

Opzioni compressione

Crea file compressi autoestraenti
Fare clic su questa casella di controllo per abbinare alla compressione la creazione di file zip a estrazione automatica con estensione `EXE`. L'opzione si rivela utile quando i destinatari non dispongono di un'utilità di decompressione. I file autoestraenti possono essere decompressi facendo doppio clic sull'icona del file.

Comprimi solo se la % di compressione è superiore al XX%
MDaemon comprimerà l'allegato di un messaggio prima di inviarlo solo se la percentuale di compressione supera il valore specificato in questo campo. Se ad esempio il valore specificato è 20 e la percentuale di compressione di un determinato allegato non raggiunge il 21%, questo non verrà compresso prima dell'invio.

Per determinarne la percentuale di compressione, un file deve essere innanzitutto compresso. Pertanto, la funzione non impedisce che i file vengano compressi, ma consente solo di evitare che vengano inviati allegati in formato compresso quando la relativa percentuale di compressione non raggiunge il valore specificato. In altri termini, se i file non possono essere compressi più del valore specificato, la compressione non verrà eseguita e il messaggio verrà inviato con gli allegati invariati.

Comprimi se la dimensione totale dell'allegato è superiore a XX KB
Se la funzione di compressione automatica dell'allegato è abilitata, verranno compressi solo gli allegati con dimensione complessiva superiore al valore specificato in questo campo. I messaggi associati ad allegati con dimensione inferiore a questa soglia vengono di norma consegnati senza alcuna modifica degli allegati.

Livello compressione
In questa casella di riepilogo a discesa è possibile scegliere il livello di compressione da applicare agli allegati compressi automaticamente. Sono disponibili tre livelli di compressione: minimo (compressione più rapida ma limitata), medio (valore predefinito) e massimo (compressione meno rapida ma più efficiente).

Usa nome archivio fisso: [nome archivio]
Se si desidera che agli allegati compressi automaticamente corrisponda uno specifico nome file, selezionare questa casella di controllo e scegliere il nome.

Esclusioni compressione

Escludi questi file
Fare clic sul pulsante fornito per specificare i file da escludere dalle funzioni di compressione automatica. Se l'allegato di un messaggio corrisponde a uno di questi nomi file, la compressione non verrà applicata, indipendentemente dalle impostazioni specificate. I caratteri jolly sono consentiti nelle voci dell'elenco. Ad esempio, se si specifica "*.exe", i file con estensione "exe" non verranno compressi.

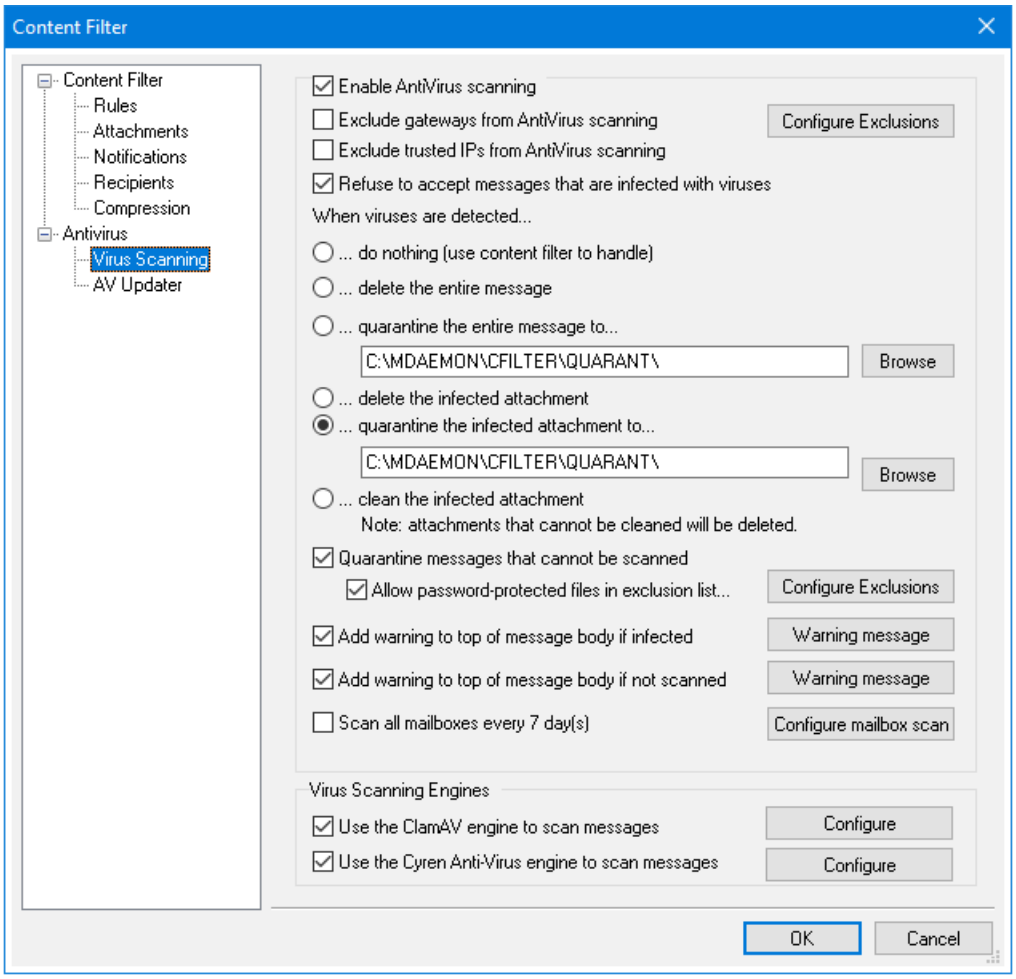
Escludi questi domini
Fare clic sul pulsante fornito per specificare i domini dei destinatari i cui messaggi devono essere esclusi dalla compressione automatica. Gli allegati dei messaggi associati a questi domini non verranno compressi, indipendentemente dalle impostazioni specificate.

Allegati winmail.dat

Estrazione di file allegati da winmail.dat (messaggi Outlook RTF)
Attivare questa opzione per estrarre i file dall'interno degli allegati winmail.dat e trasformarli in allegati al messaggio MIME standard.

4.5.2 AntiVirus

4.5.2.1 Scansione dei virus



Le opzioni di questa schermata saranno disponibili solo quando si utilizza la funzionalità MDaemon AntiVirus 684 opzionale. Quando si abilita MDaemon AntiVirus per la prima volta viene avviato un periodo di prova di 30 giorni. Se si desidera acquistare questa funzionalità, contattare il rivenditore MDaemon autorizzato o visitare il sito all'indirizzo: www.mdaemon.com.

Abilita scansione AntiVirus

Selezionare questa casella di controllo per abilitare la scansione antivirus dei messaggi. Quando riceve un messaggio contenente degli allegati, MDaemon lo analizza alla ricerca di virus prima di consegnare il messaggio alla destinazione finale.

Escludi gateway dalla scansione AntiVirus
Selezionare questa casella di controllo per escludere dalla scansione antivirus i messaggi associati a uno o più gateway di dominio di MDaemon. L'opzione è utile se si preferisce delegare la scansione di questi messaggi al server di posta del dominio. Per ulteriori informazioni sui gateway di dominio, vedere Gestore gateway 255.

Configura esclusioni
Fare clic sul pulsante Configura esclusioni per specificare gli indirizzi dei destinatari da escludere dalla scansione antivirus. MDaemon AntiVirus non esegue la scansione dei messaggi associati. È consentito utilizzare i caratteri jolly negli indirizzi. La funzione può pertanto essere utilizzata per escludere interi domini o determinate caselle postali di qualsiasi dominio, ad esempio "*@esempio.com" o "ArchivioVirus@*".

Escludi IP attendibili dalla scansione AntiVirus
Fare clic su questa casella di controllo se si desidera esentare i messaggi dalla scansione dell'AntiVirus quando provengono da uno degli Indirizzi IP attendibili 527.

Rifiuta messaggi infettati da virus
Selezionare questa casella di controllo per eseguire la scansione antivirus durante la sessione SMTP anziché al suo completamento e rifiutare i messaggi infettati. Poiché ogni messaggio in entrata viene analizzato prima che MDaemon lo accetti ufficialmente e termini la sessione, per il messaggio, che a livello tecnico non è stato ancora consegnato, risponde il server di invio. Il messaggio può essere rifiutato non appena viene rilevato un virus. In caso di rifiuto, non verrà intrapresa alcuna delle azioni specificate in questa finestra di dialogo. Non sarà eseguita la procedura di pulitura o quarantena, né verranno inviati messaggi di notifica. Questo comportamento consente di ridurre la diffusione di messaggi infettati e di notifica di virus.

Il file registro SMTP include i risultati dell'elaborazione AntiVirus. È possibile visualizzare i risultati seguenti:

- Il messaggio è stato analizzato ed è stata rivelata la presenza di un virus.
- Il messaggio è stato analizzato e non è stato rilevato alcun virus.
- Non è stato possibile analizzare il messaggio (solitamente perché è impossibile accedere o aprire un allegato in formato ZIP o di altro tipo).
- Non è stato possibile eseguire la scansione del messaggio (supera il limite di dimensione massima).
- Si è verificato un errore durante la scansione.

Quando viene rilevato un virus
Selezionare una delle opzioni in questa sezione per indicare l'azione che MDaemon dovrà intraprendere quando viene rilevato un virus.

Nessuna azione (gestione con filtro contenuti)
Scegliere questa opzione se nessuna delle azioni descritte in precedenza deve essere eseguita e si preferisce impostare le regole di Filtro contenuti per specificare una soluzione alternativa.

Elimina l'intero messaggio
Specificando questa opzione, verrà eliminato l'intero messaggio anziché il solo allegato. Poiché viene eliminato l'intero messaggio, l'opzione "*Aggiungi un messaggio di avviso...*" non è applicabile. È comunque possibile inviare una notifica al destinatario utilizzando i comandi della scheda Notifiche.

Poni in quarantena l'intero msg. in
Questa opzione è simile all'opzione "*Elimina l'intero messaggio*" descritta in precedenza, ma in questo caso il messaggio viene posto in quarantena nella posizione specificata e non viene eliminato.

Elimina l'allegato infettato
Scegliendo questa opzione, l'allegato infettato verrà eliminato. Il messaggio viene comunque consegnato al destinatario, ma senza l'allegato infettato. Il comando "*Aggiungi un messaggio di avviso*", visualizzato nella parte inferiore della finestra di dialogo, consente di aggiungere un testo al messaggio per segnalare all'utente l'eliminazione di un allegato infettato.

Poni in quarantena l'allegato infettato in
Questa opzione consente di specificare una posizione in cui porre in quarantena gli allegati infettati, in alternativa all'eliminazione o alla pulizia. Analogamente all'opzione "*Elimina l'allegato infettato*", il messaggio viene consegnato al destinatario senza l'allegato.

Elimina l'allegato infettato
Quando viene selezionata questa opzione, AntiVirus tenterà di pulire (disabilitare) l'allegato infetto. Se l'allegato non può essere pulito, verrà eliminato.

Poni in quarantena messaggi non scansionabili
Quando questa opzione è abilitata, vengono messi in quarantena tutti i messaggi di cui non è possibile eseguire la scansione, ad esempio i messaggi contenenti file protetti da password.

Consenti file protetti da password in elenco esclusioni...
Utilizzare questa opzione per consentire l'elaborazione di un messaggio con un file non sottoponibile a scansione e protetto da password tramite il programma AntiVirus, se il nome o il tipo di file si trova nell'elenco delle esclusioni.

Configura esclusioni
Fare clic su questo pulsante per aprire e gestire l'elenco delle esclusioni dei file. I nomi e i tipi di file inclusi in questo elenco non verranno sottoposti a scansione.

Aggiungi un messaggio di avviso all'inizio del corpo del messaggio infetto
Se è selezionata una delle opzioni "*...allegato*" illustrate in precedenza, è possibile specificare questa casella di controllo per aggiungere un testo di avviso all'inizio del messaggio associato all'allegato infettato prima di consegnarlo al destinatario. In questo modo, è possibile notificare al destinatario l'eliminazione dell'allegato e indicarne il motivo.

Messaggio avviso
Fare clic su questo pulsante per visualizzare il testo di avviso da aggiungere ai messaggi quando si utilizza la funzione "*Aggiungi un messaggio di avviso...*". Dopo aver apportato le modifiche desiderate al testo, fare clic su **OK** per chiudere la finestra di dialogo e salvare le modifiche.

Aggiungi un messaggio di avviso all'inizio del corpo del messaggio se non sottoposto a scansione
Quando si attiva questa opzione, MDaemon aggiunge un avviso nella parte superiore dei messaggi che non riesce ad analizzare.

Messaggio avviso
Fare clic su questo pulsante per visualizzare il testo di avviso da aggiungere ai messaggi che non è possibile analizzare. Dopo aver apportato le modifiche desiderate al testo, fare clic su **OK** per chiudere la finestra di dialogo e salvare le modifiche.

Controlla tutte le cassette postali ogni *n* giorni
Selezionare questa casella se si desidera eseguire la scansione periodica di tutti i messaggi memorizzati, per rilevare eventuali messaggi infetti che possono essere passati attraverso il sistema prima che l'aggiornamento delle definizioni dei virus sia stato in grado di rilevarlo. I messaggi infetti vengono spostati nella cartella della quarantena con l'intestazione `X-MDBadQueue-Reason` , in modo da rendere evidente la spiegazione quando visualizzati in MDaemon. I messaggi che non possono essere sottoposti a scansione non vengono messi in quarantena.

Configura scansione cassette postali.
Fare clic su questo pulsante per specificare la frequenza con cui si desidera sottoporre a scansione le caselle di posta e se si desidera sottoporre a scansione tutti i messaggi o solo quelli a partire da una determinata data. È anche possibile eseguire subito manualmente una scansione della cassetta postale.

Motori di scansione dei virus

MDaemon AntiVirus è dotato di due diversi motori di scansione dei virus: ClamAV e IKARUS Anti-Virus. Quando si attivano entrambi i motori, i messaggi vengono analizzati da tutti e due i motori; prima da IKARUS Anti-Virus quindi da ClamAV. In questo modo si costituisce un ulteriore livello di protezione, poiché un virus potrebbe essere identificato da un motore prima che venga eseguito l'aggiornamento delle definizioni dei virus dell'altro motore.

Utilizza il motore di ClamAV per eseguire la scansione sui messaggi
Fare clic su questa casella di controllo per utilizzare il motore di ClamAV per eseguire la scansione sui messaggi.

Configura
Fare clic su questo pulsante per accedere all'opzione per attivare la registrazione di debug per ClamAV. Il file di registro sarà archiviato nella cartella del registro di MDaemon.

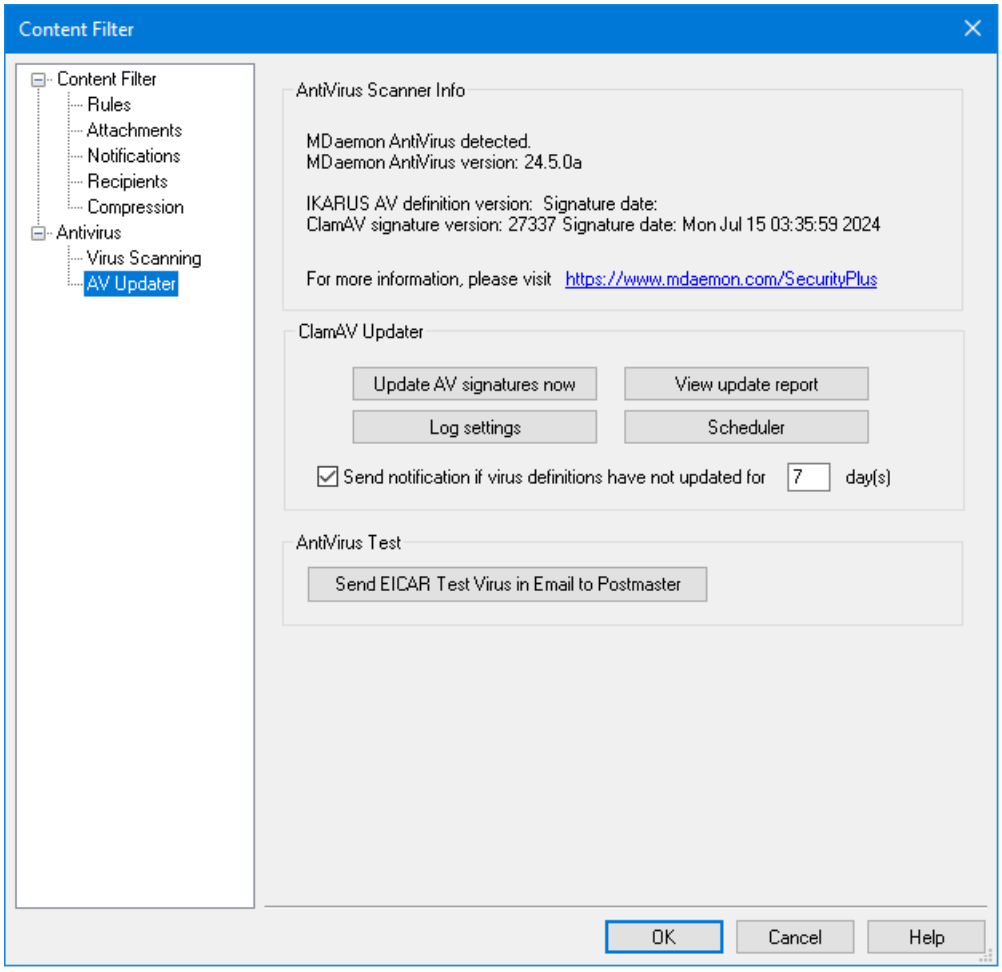
Utilizza il motore di IKARUS Anti-Virus per eseguire la scansione sui messaggi
Fare clic su questa casella di controllo per utilizzare il motore di IKARUS Anti-virus per eseguire la scansione sui messaggi.

Configura
Utilizzare questa opzione se si desidera contrassegnare come virus gli allegati con documenti che contengono macro. È possibile impostare un livello euristico da -1 a 5. "-1" corrisponde ad automatico, "0" a disabilitato e 1-5 dal livello euristico più basso al più alto.

Per ulteriori informazioni, vedere:

Utilità di aggiornamento AntiVirus 688
Filtro contenuti e antivirus 658

4.5.2.2 Utilità di aggiornamento AntiVirus



Alcune delle opzioni di questa schermata sono disponibili solo se si utilizza la funzionalità opzionale MDaemon AntiVirus 684. Quando si abilita MDaemon AntiVirus per la prima volta viene avviato un periodo di prova di 30 giorni. Se si desidera acquistare questa funzionalità, contattare il rivenditore MDaemon autorizzato o visitare il sito all'indirizzo: www.mdaemon.com.

I comandi di questa schermata consentono di aggiornare in modo manuale o automatico le definizioni dei virus. Le funzioni disponibili includono un'utilità di aggiornamento automatico, un visualizzatore di report per il monitoraggio dello scaricamento degli aggiornamenti e un'utilità che consente di verificare il corretto funzionamento della scansione antivirus.

Informazioni sull'analisi AntiVirus

Questa sezione informa se AntiVirus è disponibile e sulla versione in esecuzione. È inoltre riportata la data dell'ultimo aggiornamento delle definizioni dei virus.

Programma di aggiornamento di ClamAV

Aggiorna definizioni AntiVirus
Fare clic su questo pulsante per eseguire l'aggiornamento manuale delle definizioni dei virus. L'utilità di aggiornamento si connetterà immediatamente.

Configura aggiornamenti
Fare clic su questo pulsante per aprire la finestra di dialogo Configurazione utilità di aggiornamento Security Plus per MDaemon 690. Nella finestra di dialogo sono presenti quattro schede: URL aggiornamento, Connessione, Proxy e Varie.

Visualizza report aggiornamento
Il pulsante *Visualizza report aggiornamento* consente di aprire la finestra di visualizzazione del registro di AntiVirus. in cui sono elencati gli orari, le azioni eseguite e altre informazioni relative a ogni aggiornamento.

Pianificazione
Questo pulsante consente di aprire la schermata Pianificazione AntiVirus 386, utilizzata per pianificare le verifiche di disponibilità di aggiornamenti delle definizioni dei virus in giorni e orari specifici o in base a intervalli regolari.

Invia una notifica se le definizioni dei virus non sono state aggiornate per xx giorni.
Per impostazione predefinita, l'amministratore riceverà una notifica se le definizioni dei virus di ClamAV non sono state aggiornate per il numero di giorni specificato.

Test AntiVirus

Invia virus test EICAR nell'e-mail al postmaster
Fare clic su questo pulsante per inviare al postmaster un messaggio di testo infettato con EICAR. Si tratta di un allegato innocuo, utilizzato per il test dell'antivirus. Per controllare il comportamento di MDaemon alla ricezione del

messaggio, osservare la finestra del registro di Filtro contenuti nell'interfaccia principale di MDaemon. A seconda delle impostazioni, le righe del registro possono essere le seguenti:

```
Mon 25.02.08 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 25.02.08 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 25.02.08 18:14:49: > Message from: postmaster@esempio.com
Mon 25/02/2008 18:14:49: > Message to: postmaster@esempio.com
Mon 25.02.08 18:14:49: > Message subject: EICAR Test Message
Mon 25.02.08 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@esempio.com>
Mon 25.02.08 18:14:49: Performing viral scan...
Mon 25.02.08 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 25.02.08 18:14:50: > eicar.com was removed from message
Mon 25.02.08 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 25.02.08 18:14:50: > Total attachments scanned : 1 (including
multipart/alternatives)
Mon 25.02.08 18:14:50: > Total attachments infected : 1
Mon 25.02.08 18:14:50: > Total attachments disinfected: 0
Mon 25.02.08 18:14:50: > Total attachments removed : 1
Mon 25.02.08 18:14:50: > Total errors while scanning : 0
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@esempio.com (sender)
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@esempio.com (recipient)
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@esempio.com (admin)
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 25.02.02 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

Per ulteriori informazioni, vedere:

Finestra di dialogo Configurazione aggiornamento AntiVirus 690
AntiVirus 684
Filtro contenuti e antivirus 658

4.5.2.2.1 Finestra di dialogo Configurazione aggiornamento AntiVirus

Fare clic sul pulsante *Configura aggiornamenti* nella schermata Aggiornamento AV 688 per aprire la finestra di dialogo Configurazione utilità di aggiornamento Security Plus per MDaemon. Comprende le quattro schede seguenti:

Aggiorna URL
La scheda URL aggiornamento consente di indicare i server in cui AntiVirus cercherà gli aggiornamenti. È possibile impostare l'ordine in cui saranno controllati i server o scegliere un ordine casuale.

Connessione
La scheda Connessione consente di specificare il profilo di connessione a Internet che l'AntiVirus utilizzerà quando si connette ai siti di aggiornamento. Se si specifica l'opzione "*Utilizza la configurazione Internet specificata nel Pannello di controllo*", verranno utilizzate le impostazioni Internet predefinite. L'opzione "*Configura manualmente la connessione a Internet*" e i controlli utente successivi possono essere utilizzati per selezionare manualmente un profilo di connessione e per definire le impostazioni relative a nome utente e password.

Proxy
Nella scheda Proxy sono presenti le opzioni che consentono di specificare le impostazioni del server HTTP o FTP necessarie alla configurazione di rete corrente per la connessione ai siti di aggiornamento.

Varie
Le opzioni della scheda Varie consentono di configurare la registrazione delle attività dell'utilità di aggiornamento, specificando se registrare tali attività in un file e indicando la dimensione massima di quest'ultimo.

Per ulteriori informazioni, vedere:

Utilità di aggiornamento AntiVirus 688
AntiVirus 684
Filtro contenuti e antivirus 658

4.6 Spam Filter

4.6.1 Spam Filter

Spam Filter è una delle principali funzionalità della vasta gamma di strumenti per la prevenzione dello spam disponibile in MDaemon. Spam Filter incorpora una logica di elaborazione euristica che esamina i messaggi e-mail in arrivo calcolando un "punteggio" basato su un sistema complesso di regole. Questo punteggio viene utilizzato per determinare la probabilità che un messaggio sia di tipo spam e per intraprendere alcune operazioni come, ad esempio, rifiutare un messaggio, contrassegnarlo come possibile spam e così via.

Gli indirizzi possono essere consentiti o bloccati oppure designati come completamente esentati dal controllo dello Spam Filter. È possibile includere nei messaggi un report spam che mostra i punteggi di spam e la modalità con cui sono stati calcolati, oppure creare un report in una e-mail distinta che contiene in allegato il messaggio spam originale. Inoltre, è possibile utilizzare anche l'apprendimento bayesiano 696 per consentire a Spam Filter di incrementare con il tempo l'efficacia di identificazione dello spam aumentando, così, la sua affidabilità.

Infine, dopo aver esaminato diverse migliaia di messaggi spam, le regole sono state ottimizzate con il tempo diventando sempre più affidabili nel rilevare messaggi spam. Tuttavia, per soddisfare ogni specifica esigenza, è possibile personalizzare o aggiungere nuove regole modificando i file di configurazione di Spam Filter.

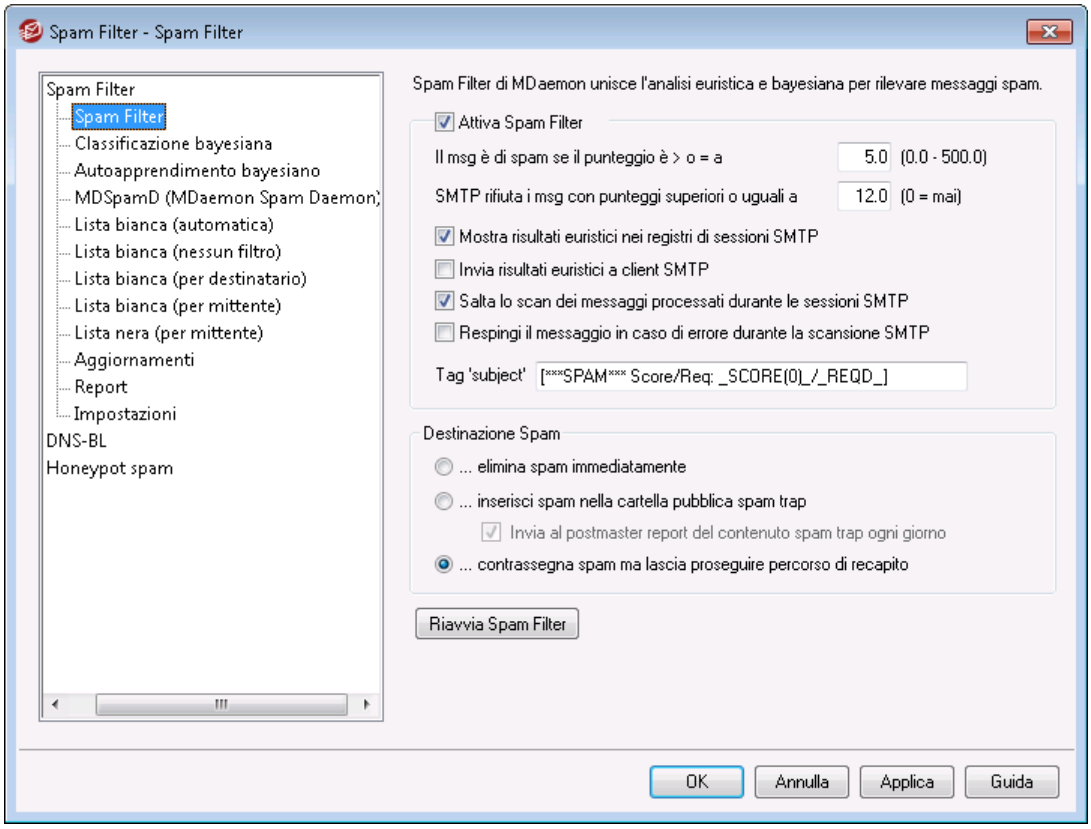
Spam Filter di MDaemon usa una tecnologia open-source integrata di tipo euristico molto diffusa. La home page del relativo progetto open-source è disponibile all'indirizzo

```
http://www.spamassassin.org
```

Per ulteriori informazioni, vedere:

Spam Filter 692
Liste bloccati DNS 717

4.6.1.1 Spam Filter



Attiva Spam Filter

Selezionare questa casella di controllo per attivare il sistema euristico per il filtro spam e il punteggio messaggi. Finché non viene abilitata questa opzione, non è disponibile alcuna delle opzioni Spam Filter della schermata.

Il msg è spam se il punteggio è > o = a XX (0,0-500,0)
Il valore specificato in questo campo indica la soglia di spam confrontata con i singoli punteggi di spam. Ogni messaggio con un punteggio maggiore o uguale a questo valore è considerato spam e determina, dunque, l'esecuzione delle operazioni previste in base alle impostazioni di Spam Filter.

SMTP rifiuta i msg con punteggi superiori o uguali a XX (0=mai)
Usare questa opzione per determinare una soglia di punteggio di spam, superata la quale i messaggi vengono respinti. Quando il punteggio è maggiore o uguale a questo valore, il messaggio viene respinto direttamente anziché procedere con le altre opzioni ed essere eventualmente consegnato. È opportuno che il valore di questa opzione sia sempre maggiore del valore che corrisponde all'opzione "*Il messaggio è spam se il punteggio è...*" descritta in precedenza. In caso contrario, il messaggio non è mai considerato spam, vengono applicate tutte le altre opzioni di Spam Filter e il messaggio viene respinto direttamente durante la consegna. Inserire in questo campo il valore "0" se si desidera disattivare l'analisi durante la sessione SMTP e respingere tutti i messaggi, ignorando i punteggi. Se la scansione SMTP è disattivata, sui messaggi accettati viene eseguita un'analisi basata sulle code. L'impostazione predefinita di questo campo è "12.0".

Esempio:

Se la soglia del punteggio di spam è impostata su 5.0 e quella affinché un messaggio venga respinto è impostata su 10.0, allora tutti i messaggi con un punteggio di spam maggiore o uguale a 5.0 ma inferiore a 10.0 vengono considerati spam e gestiti in base alle altre impostazioni di Spam Filter. Durante la consegna, ciascun messaggio con un punteggio di spam maggiore o uguale a 10.0 viene respinto.

È opportuno controllare le prestazioni di Spam filter nel tempo e, se necessario, modificare i valori delle soglie che consentono di considerare un messaggio spam o respingerlo. La maggior parte degli utenti, tuttavia, considera che la soglia del punteggio di spam impostata a 5.0 cattura più spam, con un numero relativamente basso di messaggi considerati erroneamente negativi, denominati anche "falsi negativi" (ovvero spam che non viene riconosciuto come tale), e raramente messaggi considerati erroneamente positivi, denominati anche "falsi positivi" (ovvero messaggi contrassegnati come spam ma che in realtà non lo sono). Una soglia di rifiuto impostata tra 10 e 15 fa sì che vengano respinti solo i messaggi che quasi certamente sono spam. È molto difficile che un messaggio di posta accettabile abbia un punteggio tanto alto. Il valore predefinito della soglia di rifiuto è 12.

Mostra risultati euristici nei registri delle sessioni SMTP
Questa opzione consente di registrare nei registri delle sessioni SMTP 178 i risultati dell'elaborazione euristica eseguita durante le sessioni SMTP.

Invia risultati euristici a client SMTP
Fare clic su questa opzione per mostrare i risultati dell'elaborazione euristica direttamente nelle trascrizioni delle sessioni SMTP. Questa opzione non è disponibile se il valore della soglia di rifiuto del punteggio di spam è impostato a "0", poiché ciò vorrebbe dire che lo spam non viene mai rifiutato per via del punteggio. Per ulteriori informazioni, consultare la precedente sezione "*SMTP rifiuta i msg con punteggi superiori o uguali a XX (0=mai)*".

Salta lo scan dei messaggi processati durante le sessioni SMTP
Per impostazione predefinita, durante la sessione SMTP viene eseguita l'analisi di tutti i messaggi al fine di determinarne il punteggio di spam e scartarli se il punteggio supera la soglia prevista. MDaemon esegue un'ulteriore ricerca in base alle code sui messaggi accettati per definirne la gestione in base ai punteggi e alla configurazione di Spam Filter. Selezionare questa opzione se si desidera escludere la ricerca basata sulle code e considerare definitivi i risultati della ricerca Spam Filter iniziale. Ciò consente di ridurre considerevolmente l'utilizzo della CPU aumentando le prestazioni del sistema antispam. Se si esclude la ricerca basata sulle code, ai messaggi vengono aggiunte solo le intestazioni SpamAssassin predefinite. Le modifiche alle intestazioni SpamAssassin predefinite o l'aggiunta di specifiche intestazioni personalizzate nel file `local.cf` verranno ignorate.

Respingi il messaggio in caso di errore durante la scansione SMTP
Abilitare questa opzione se si desidera che un messaggio venga rifiutato qualora venga riscontrato un errore durante la sua scansione SMTP.

Tag 'subject'
Questo tag viene inserito all'inizio dell'intestazione Subject (Oggetto) di tutti i messaggi che presentano un valore maggiore o uguale alla soglia del punteggio di spam richiesto. Questa può anche contenere informazioni relative al punteggio di spam ed è possibile utilizzare i filtri dei messaggi IMAP per cercarla e di conseguenza filtrare il messaggio (supponendo che Spam Filter sia configurato in modo da proseguire la consegna dei messaggi spam). Questo è un metodo semplice per instradare automaticamente i messaggi spam in una apposita cartella. Se si desidera inserire dinamicamente il punteggio di spam del messaggio e il valore della soglia richiesta, utilizzare il tag "`_HITS_`" per il punteggio del messaggio e "`_REQD_`" per la soglia. In alternativa, è possibile utilizzare "`_SCORE(0)_`" al posto di "`_HITS_`"; in questo modo viene aggiunto uno zero iniziale ai punteggi più bassi. Ciò consente di ordinare i messaggi in base all'oggetto in alcuni client e-mail.

Esempio:

Un tag oggetto impostato come `***SPAM*** Score/Req: _HITS_/_REQD_` - determina un messaggio spam con un punteggio di 6,2 e la modifica dell'oggetto da "Hey, here's some spam!" a "***SPAM*** Score/Req: 6.2/5.0 – Hey, here's some spam!"

Se "`_SCORE(0)_`" venisse sostituito con "`_HITS_`", verrebbe modificato con "***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"

Se non si desidera alterare l'intestazione, lasciare il campo vuoto in modo da non inserire alcun tag oggetto.

Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. La configurazione del tag "Subject" sarà determinata dalle impostazioni di un altro server. Vedere: Spam Daemon 702, per ulteriori informazioni.

Destinazione Spam

Se il punteggio di spam di un messaggio è maggiore o uguale a quello specificato sopra, Spam Filter esegue l'azione riportata di seguito.

Elimina immediatamente
Scegliere questa opzione se si desidera eliminare direttamente tutti i messaggi in arrivo il cui punteggio di spam supera il limite stabilito.

Inserisci messaggio in cartella pubblica spam trap
Scegliere questa opzione se si desidera contrassegnare i messaggi come spam e spostarli nella cartella pubblica spam anziché consentire la loro consegna.

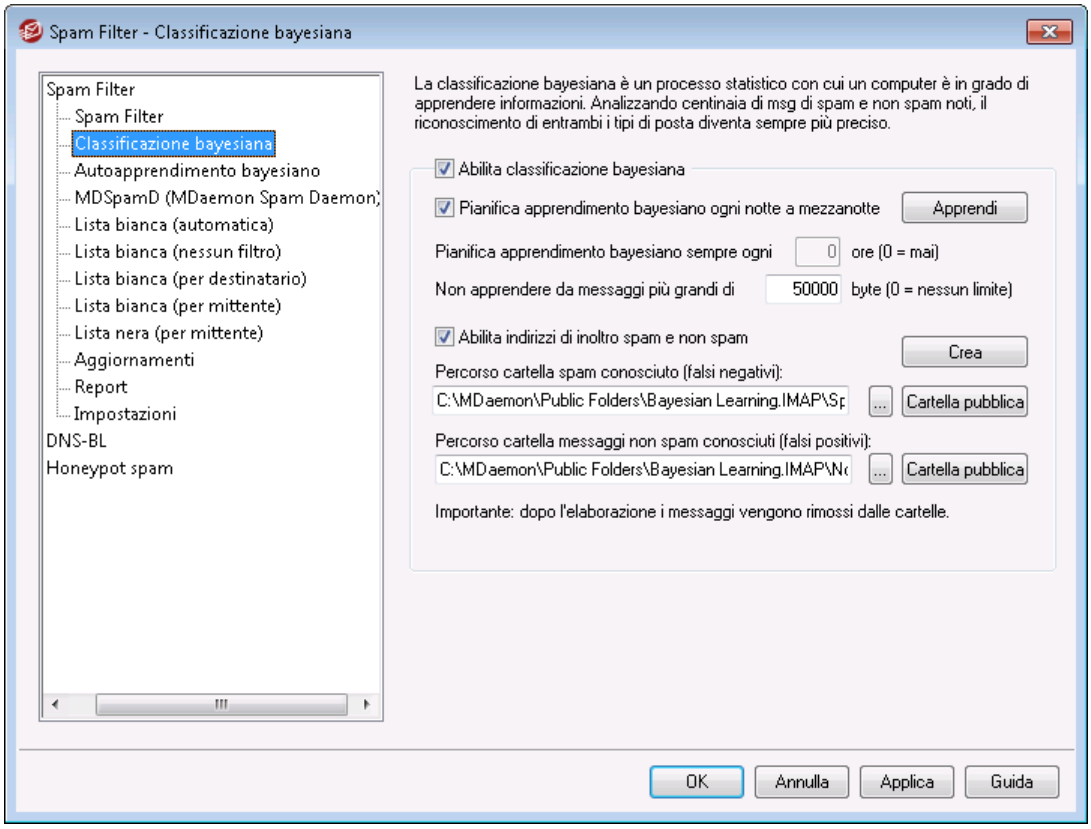
Invia ogni giorno il rapporto spam trap al postmaster
Se si utilizza l'opzione *Inserisci messaggio in cartella pubblica spam trap*, selezionare questa casella di controllo per far sì che il postmaster riceva un messaggio giornaliero con un riepilogo del contenuto della cartella.

...contrassegna spam ma lascia proseguire percorso di recapito
Scegliere questa opzione se si desidera proseguire con la consegna di tutti i messaggi spam al destinatario, ma si intende contrassegnarli come tali inserendo le varie intestazioni spam e/o i tag indicati nella schermata Report 713. Questa è l'opzione predefinita e consente di utilizzare opzioni quali lo spostamento della posta in una cartella spam per una revisione successiva evitando così la perdita di messaggi che potrebbero venire contrassegnati erroneamente come indesiderati, ossia dei falsi positivi.

Riavvia Spam Filter

Fare clic su questo pulsante per Riavviare il motore di Spam Filter

4.6.1.2 Classificazione bayesiana



Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Tutti gli apprendimenti bayesiani saranno eseguiti sull'altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon 702.

Spam Filter supporta l'apprendimento bayesiano, ovvero un processo statistico che può essere utilizzato per analizzare i messaggi spam e non spam allo scopo di accrescerne nel tempo l'affidabilità nel riconoscimento. È possibile utilizzare una cartella per i messaggi spam e non spam di cui viene effettuata una scansione manualmente oppure automaticamente, a intervalli regolari. Tutti i messaggi contenuti in queste cartelle vengono analizzati e indicizzati in modo da poterli confrontare con i nuovi messaggi e stabilire statisticamente la probabilità che si tratti di messaggi spam. Spam Filter può, quindi, aumentare o diminuire il punteggio di spam del messaggio sulla base dei risultati del confronto bayesiano.

Spam Filter non applica ai messaggi una classificazione bayesiana finché non viene effettuata un'analisi bayesiana sul numero di messaggi spam e non spam specificati nella schermata Autoapprendimento bayesiano 700. Ciò serve a fare sì che Spam Filter abbia un insieme di statistiche sufficientemente ampio per iniziare il confronto bayesiano. Una volta ricevuti dal sistema i messaggi da analizzare, questo è pienamente in grado di iniziare ad applicare i dati del confronto bayesiano a ciascun punteggio di spam del messaggio in arrivo. Continuando ad analizzare sempre più messaggi, le classificazioni bayesiane diventano sempre più accurate nel tempo.

Classificazione Bayesiana

Abilita classificazione bayesiana
Fare clic su questa casella di controllo se si desidera che il punteggio di spam di ciascun messaggio venga regolato in base al confronto con le statistiche bayesiane correntemente note.

Pianifica apprendimento bayesiano ogni notte a mezzanotte
Quando questa opzione è attivata, ogni giorno a mezzanotte Spam Filter analizzerà ed eliminerà tutti i messaggi contenuti nelle cartelle Spam e non Spam indicate di seguito. Se si desidera programmare l'apprendimento bayesiano per un altro intervallo di tempo, deselezionare questa opzione e utilizzare l'opzione *Pianifica apprendimento bayesiano sempre ogni XX ore*. Se non si desidera che l'apprendimento bayesiano avvenga automaticamente, deselezionare questa opzione e specificare "0" ore nell'opzione seguente.

Pianifica apprendimento bayesiano sempre ogni XX ore (0 = mai)
Se si desidera che l'apprendimento bayesiano avvenga in un intervallo di tempo diverso da quello di ogni notte a mezzanotte, deselezionare l'opzione descritta in precedenza e specificare un numero di ore in questa opzione. Quando il numero di ore indicato è trascorso, Spam Filter analizzerà e eliminerà tutti i messaggi contenuti nelle cartelle Spam e non Spam indicate di seguito. Se non si desidera che l'apprendimento bayesiano avvenga sempre automaticamente, deselezionare l'opzione precedente e specificare "0" ore in questa opzione.

Se si desidera conservare i messaggi dopo l'analisi, è possibile creare una copia di `LEARN.BAT` salvandola come `MYLEARN.BAT` nella sottocartella `\MDaemon\App\` ed eliminare quindi le due righe che iniziano con "`if exist`" che si trovano alla fine del file. Se la cartella include il file `MYLEARN.BAT`, MDaemon utilizzerà quest'ultimo anziché il file `LEARN.BAT`. Per ulteriori informazioni, consultare il file `SA-Learn.txt`, situato nella sottocartella `\MDaemon\SpamAssassin\`.

> Per informazioni più dettagliate sulla tecnologia euristica dei filtri spam e sull'apprendimento bayesiano, visitare l'indirizzo:
>
> http://www.spamassassin.org/doc/sa-learn.html

Non apprendere da messaggi più grandi di XX byte (0 = senza lim.)
Questa opzione consente di specificare la dimensione massima del messaggio ai fini dell'analisi bayesiana. I messaggi più grandi di tale dimensione non saranno analizzati. Specificare "0" in questa opzione se non si desidera inserire alcuna limitazione di dimensione.

Apprendi
Fare clic su questo pulsante per avviare manualmente l'analisi bayesiana delle cartelle specificate anziché attendere l'analisi automatica.

Abilita indirizzi di inoltro spam e non spam
Fare clic su questa casella di controllo se si desidera consentire agli utenti l'inoltro di messaggi spam e non spam (ham) a determinati indirizzi per consentire al sistema bayesiano di apprendere da essi. Gli indirizzi predefiniti utilizzati da MDaemon sono "SpamLearn@<dominio>" e "HamLearn@<dominio>". I messaggi inviati a questi indirizzi devono essere ricevuti mediante SMTP da una sessione autenticata con SMTP AUTH. Inoltre, MDaemon prevede l'inoltro dei messaggi agli indirizzi sopra riportati come allegati di tipo "message/rfc822". Ogni altro tipo di messaggio inviato a questi indirizzi e-mail non verrà elaborato.

È possibile cambiare gli indirizzi utilizzati da MDaemon aggiungendo la seguente chiave nel file CFilter.INI:

```
[SpamFilter]
SpamLearnAddress=IndirizzoApprendimentoSpam@
HamLearnAddress=IndirizzoApprendimentoNonSpam@
```

Nota: l'ultimo carattere di questi valori deve essere "@".

Crea
Fare clic su questo pulsante per creare automaticamente Cartelle IMAP pubbliche spam e non spam e configurarne l'uso da parte di MDaemon. Verranno create le cartelle riportate di seguito.

\Bayesian Learning.IMAP\	Cartella IMAP principale
\Bayesian Learning.IMAP\Spam.IMAP\	Questa cartella è destinata ai falsi negativi, ossia ai messaggi spam con un punteggio non abbastanza elevato per essere considerati tali.
\Bayesian Learning.IMAP\Non-Spam.IMAP\	Questa cartella è destinata ai falsi positivi, ossia ai messaggi non spam con un punteggio errato

sufficientemente elevato per essere considerati tali.

Per impostazione predefinita, le autorizzazioni di accesso a queste cartelle sono garantite solo agli utenti di domini locali e sono limitate alle funzioni di ricerca e inserimento. Le autorizzazioni predefinite dell'utente postmaster consentono le funzioni di ricerca, lettura, inserimento ed eliminazione.

Percorso cartella spam conosciuto (falsi negativi)
Questo è il percorso per la cartella usata per l'analisi bayesiana di messaggi spam noti. Copiare in questa cartella solamente i messaggi che si ritengono spam. È opportuno evitare di automatizzare la copia dei messaggi nella cartella, se non utilizzando le opzioni di Autoapprendimento bayesiano 700 o Honeypot spam 723. Se si automatizza tale processo, messaggi non spam potrebbero essere analizzati come spam e ciò diminuirebbe l'affidabilità delle statistiche bayesiane.

Percorso cartella messaggi non spam conosciuti (falsi positivi)
Questo è il percorso per la cartella usata per l'analisi bayesiana di messaggi sicuramente **non** spam. È opportuno copiare in questa cartella solo i messaggi che **non** si ritengono spam. È opportuno evitare di automatizzare la copia dei messaggi nella cartella, se non utilizzando le opzioni di Autoapprendimento bayesiano 700. Se si automatizza tale processo, messaggi spam potrebbero essere analizzati come non spam e ciò diminuirebbe l'affidabilità delle statistiche bayesiane.

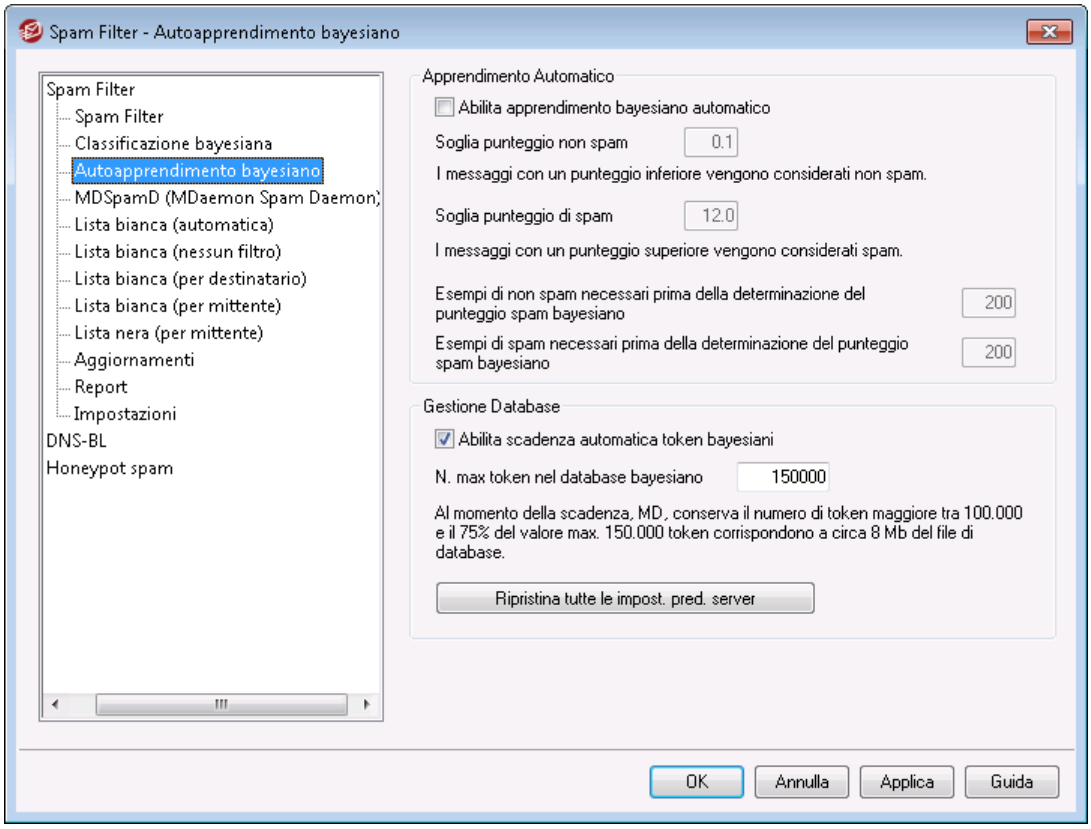
Cartella pubblica
Fare clic su uno dei pulsanti per definire come directory bayesiana una delle cartelle pubbliche esistenti. Si tratta di un metodo semplice per spostare i messaggi erroneamente segnalati come spam o non spam nelle directory bayesiane per l'analisi. Si noti, tuttavia, che autorizzando l'accesso a più persone aumenta la probabilità di inserire i messaggi nelle cartelle errate, alterando le statistiche e diminuendone l'affidabilità.

Se si rinomina una cartella pubblica mediante un client e-mail, Esplora risorse o con altri metodi, è necessario reimpostare manualmente il percorso inserendo il nome corretto della nuova cartella. Se si rinomina una cartella ma non si modifica il percorso nel relativo campo, Spam Filter continua a utilizzare per la cartella bayesiana il vecchio percorso anziché il nuovo.

Per ulteriori informazioni, vedere:

Autoapprendimento bayesiano 700
Honeypot spam 723

4.6.1.3 Autoapprendimento bayesiano



L'autoapprendimento bayesiano non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Tutti gli apprendimenti bayesiani saranno eseguiti sull'altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon 702.

Apprendimento automatico

Abilita apprendimento bayesiano automatico
Con l'apprendimento bayesiano automatico è possibile indicare le soglie del punteggio spam e non spam che consentono al sistema l'apprendimento automatico dai messaggi, senza la necessità di smistarli manualmente nelle cartelle spam e non spam. Tutti i messaggi con un punteggio inferiore alla soglia non spam sono trattati dall'apprendimento automatico come messaggi accettati mentre i messaggi con un punteggio superiore alla soglia spam sono trattati come messaggi indesiderati. Con l'apprendimento automatico, i vecchi token scaduti e rimossi dal database (vedere *Gestione database* vengono sostituiti automaticamente. In questo modo non è necessario intervenire manualmente per sostituire i token scaduti.

L'autoapprendimento risulta utile e vantaggioso se le soglie sono impostate con attenzione, in modo da evitare che i messaggi vengano collocati nelle cartelle con una classificazione impropria.

Soglia punteggio non spam
Il sistema di Classificazione bayesiana tratta i messaggi con un punteggio di spam inferiore a questo valore come messaggi non spam.

Soglia punteggio di spam
Il sistema di Classificazione bayesiana tratta i messaggi con un punteggio di spam superiore a questo valore come messaggi spam.

Esempi di non spam necessari prima della determinazione del punteggio spam bayesiano
Spam Filter non applica ai messaggi alcuna classificazione bayesiana finché il sistema bayesiano non ha analizzato il numero di messaggi non spam indicati in questo campo e di messaggi spam indicati nell'opzione seguente. Ciò serve a fare sì che Spam Filter abbia un insieme di statistiche sufficientemente ampio per iniziare il confronto bayesiano. Una volta ricevuti dal sistema i messaggi da analizzare, questo è pienamente in grado di iniziare ad applicare i dati del confronto bayesiano a ciascun punteggio di spam del messaggio in arrivo. Continuando ad analizzare sempre più messaggi, le classificazioni bayesiane diventano sempre più accurate nel tempo.

Esempi di spam necessari prima della determinazione del punteggio spam bayesiano
Come per l'opzione precedente relativa ai messaggi non spam, questa definisce il numero di messaggi *spam* da analizzare prima che Spam Filter inizi ad applicare la classificazione bayesiana.

Gestione database

Abilita scadenza automatica token bayesiani
Fare clic su questa opzione se si desidera che i token del database scadano automaticamente una volta raggiunto il numero indicato nel campo successivo. Impostando un limite di token è possibile evitare che il database bayesiano raggiunga dimensioni troppo grandi.

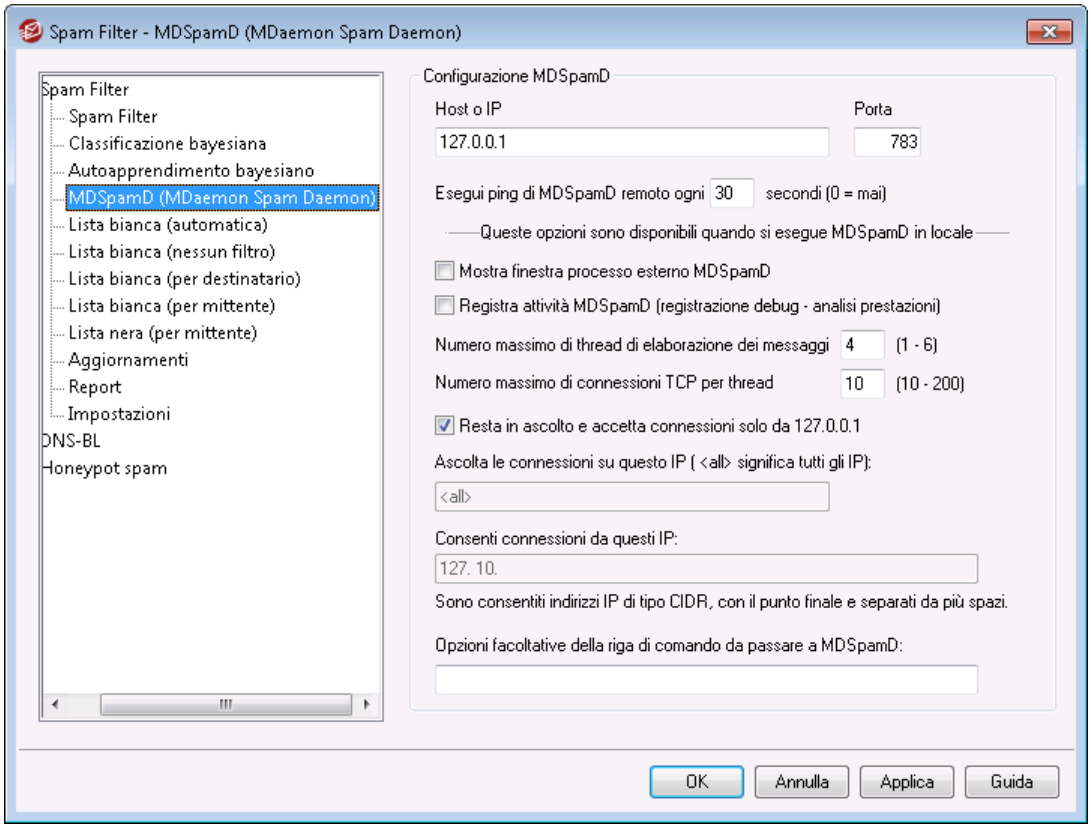
N. max token nel database bayesiano
Questo valore corrisponde al numero massimo di token bayesiani consentiti nel database. Una volta raggiunto tale numero, il sistema bayesiano elimina i token meno recenti riducendone il numero fino al valore più elevato tra il 75% del valore precedente o 100.000 token. Il numero di token non scende mai al di sotto di questi due valori, indipendentemente dal numero di token scaduti. Nota: 150.000 token del database corrispondono a circa 8 MB.

Ripristina tutte le impostazioni predefinite server
Facendo clic su questo pulsante è possibile ripristinare tutti i valori predefiniti delle opzioni bayesiane avanzate.

Vedere:

Classificazione Bayesiana 696
Honeypot spam 723

4.6.1.4 Spam Daemon (MDSpamD)



Il sistema per il filtro spam di MDaemon viene eseguito come sistema separato, MDSpamD (MDaemon Spam Daemon), a cui vengono inviati i messaggi tramite TCP/IP per la scansione. In questo modo è possibile aumentare le prestazioni di Spam Filter, nonché eseguire MDSpamD nel computer locale, in un altro computer oppure utilizzare un altro servizio MDSpamD (o un qualunque altro prodotto compatibile Spam Daemon) in esecuzione su un'altra postazione. Per impostazione predefinita, MDSpamD viene eseguito localmente e riceve i messaggi sulla porta 783 all'indirizzo 127.0.0.1, ma è possibile configurare una porta e un indirizzo IP differenti se si desidera inviare i messaggi ad un altro Spam Daemon in esecuzione in una postazione diversa o su una porta diversa.

Configurazione MDSpamD

Host o IP
Corrisponde all'host o all'indirizzo IP a cui MDaemon invierà i messaggi da analizzare con MDSpamD. Utilizzare `127.0.0.1` se MDSpamD viene eseguito localmente.

Porta
Corrisponde alla porta a cui il messaggio viene inviato. Il valore predefinito della porta MDSpamD è 783.

Esegui ping di MDSpamD remoto ogni XX secondi (0=mai)
Se si utilizza un servizio antispam (spam daemon) in esecuzione in una postazione remota, questa opzione consente di verificare periodicamente tramite ping se tale servizio è attivo. Inserire "0" se non si desidera effettuare il ping della postazione.

Opzioni disponibili se MDSpamD viene eseguito localmente

Mostra finestra processo esterno MDSpamD
Quando MDSpamD viene eseguito localmente, attivare questa opzione se si desidera eseguirlo in una finestra di processo esterno. Se si abilita questa opzione, l'output generato da MDSpamD viene inviato tramite pipe alla finestra di processo esterno anziché al sistema di registrazione o all'interfaccia utente interna di MDaemon. Questa opzione consente di migliorare le prestazioni perché i dati di MDSpamD non vengono gestiti e registrati da MDaemon. Tuttavia, in questo caso non viene creato alcun file di registro. Di conseguenza, non è possibile utilizzare questa funzione unitamente all'opzione di registrazione descritta successivamente e i dati di MDSpamD non verranno visualizzati nella scheda *Sicurezza»MDSpamD* della finestra principale di MDaemon.

Registra attività MDSpamD (registrazione debug - analisi prestazioni)
Selezionare questa casella di controllo per registrare tutte le attività di MDSpamD. Questa opzione non è disponibile se si utilizza l'opzione *Mostra finestra processo esterno MDSpamD*. Se si utilizzano le credenziali utente specificate nella finestra di dialogo Servizio Windows 416 invece di eseguire MDaemon nell'account SYSTEM, non verrà registrata alcuna attività relativa a MDSpamD.

Se si utilizza questa opzione di registrazione, è possibile che le prestazioni del sistema di posta risultino ridotte, in base al computer in uso e al livello di attività. In genere, è opportuno utilizzare questa opzione solo a scopo di debug.

Numero massimo di thread di elaborazione dei messaggi (1-6)
Corrisponde al numero massimo di thread che saranno utilizzati da MDaemon per l'elaborazione interna. È possibile impostare un valore compreso tra 1 e 6.

Numero massimo di connessioni TCP per thread (10-200)
Corrisponde al numero massimo di connessioni TCP accettate da un thread MDSpamD prima che si dirami in un altro thread. È possibile impostare un valore compreso tra 10 e 200.

Resta in ascolto e accetta connessioni solo da 127.0.0.1
Fare clic su questa opzione se non si desidera consentire al servizio MDSpamD locale di accettare connessioni di qualsiasi origine esterna. Saranno consentite solo connessioni derivanti dalla stessa postazione su cui viene eseguito MDSpamD.

Attendi connessioni su questo IP
Se l'opzione precedente è disattivata, è possibile utilizzare questa opzione per associare o limitare le connessioni ad uno specifico indirizzo IP. Saranno consentite solo le connessioni all'indirizzo IP indicato. Utilizzare "<all> (tutti)" se non si desidera limitare MDSpamD ad un particolare indirizzo IP.

Consenti connessioni da questi IP
Si tratta degli indirizzi IP da cui MDSpamD accetta le connessioni in entrata. Le connessioni da altri indirizzi IP saranno rifiutate. Questa opzione si rivela utile se si desidera consentire connessioni da un altro server per condividere l'elaborazione di Spam Filter.

Opzioni facoltative della riga di comando da passare a MDSpamD:

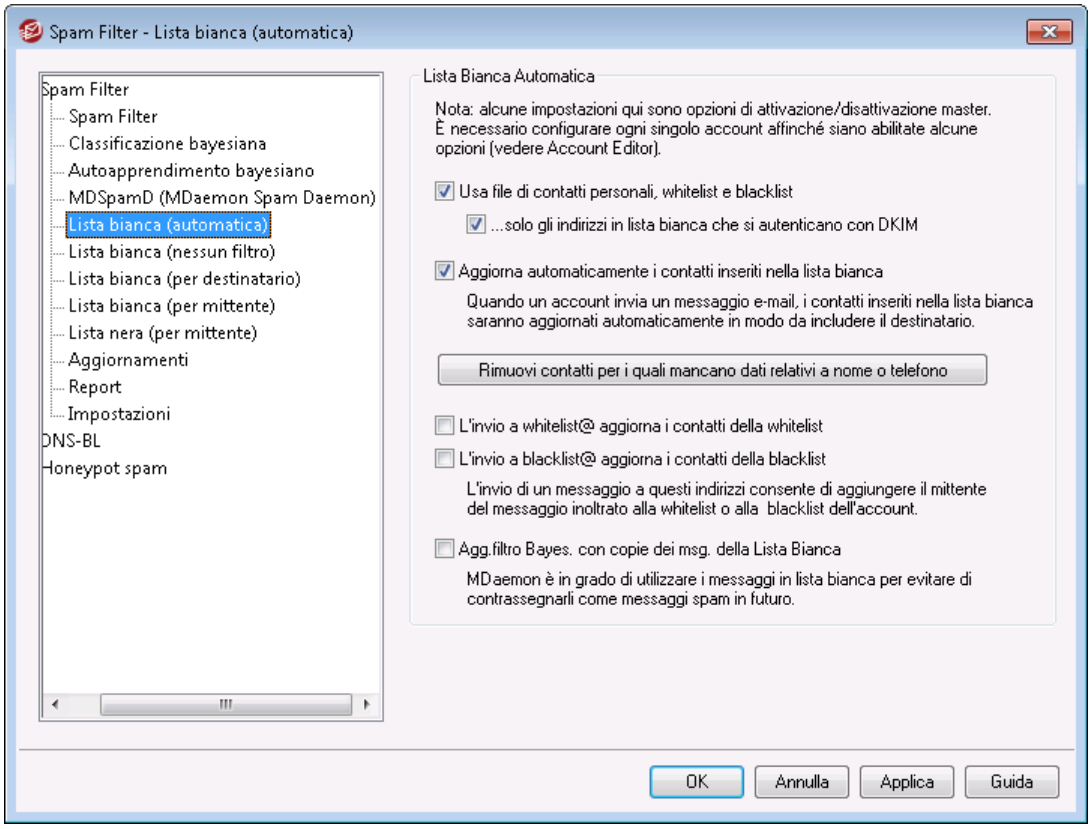
MDSpamD può accettare molte opzioni della riga di comando, descritte nel sito:

http://spamassassin.apache.org/

Se si desidera utilizzare una di queste opzioni, creare una stringa che comprenda le opzioni desiderate e inserirle in questa casella di testo.

È possibile configurare alcune opzioni utilizzando le impostazioni disponibili in questa finestra di dialogo. Di conseguenza, non è necessario impostarle manualmente tramite le opzioni della riga di comando.

4.6.1.5 Lista consentiti (automatica)



Lista consentiti automatica

Utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati
Fare clic su questa opzione per utilizzare i contatti personali di ciascun utente e i mittenti consentiti e bloccati per filtrare i messaggi spam per l'utente. Per ciascun messaggio in arrivo, MDaemon eseguirà una ricerca del mittente del messaggio tra i contatti e nelle liste consentiti e bloccati dell'account del destinatario. Se il mittente viene individuato, il messaggio viene automaticamente autorizzato o bloccato. Se non si desidera applicare automaticamente le liste consentiti e bloccati per tutti gli utenti di MDaemon, è possibile disabilitare l'opzione per i singoli utenti deselezionando *Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati* nella schermata Lista consentiti 774 dell'Account Editor.

...solo gli indirizzi in lista consentiti che si autenticano con DKIM
Quando si attiva questa opzione, MDaemon non inserisce i messaggi nella lista consentiti a meno che il mittente non sia stato autenticato mediante DomainKeys Identified Mail 536 (DKIM). Questa opzione consente di evitare l'inserimento nella lista consentiti di messaggi con indirizzi falsificati. L'opzione è disattivata per impostazione predefinita.

Aggiungi automaticamente i destinatari di posta ai mittenti consentiti
Quando questa opzione è attivata, ogni volta che un utente invia posta a un indirizzo e-mail non locale, MDaemon aggiungerà automaticamente il destinatario all'elenco dei mittenti consentiti dell'utente. Se utilizzata insieme all'opzione *Utilizza i*

contatti personali, i mittenti consentiti e i mittenti bloccati, consente di ridurre drasticamente il numero di falsi positivi di Spam Filter.

Se non si desidera applicare questa opzione a tutti gli utenti di MDaemon, è possibile disattivarla per i singoli utenti deselezionando la casella di controllo "*Aggiungi automaticamente i destinatari di posta ai mittenti consentiti*" nella schermata Lista consentiti 774 dell'Account Editor.

Questa opzione è disattivata per gli account che usano risposte automatiche.

Rimuovi contatti per i quali mancano dati relativi a nome o telefono
Questo pulsante consente di rimuovere dalla cartella Contatti predefinita degli utenti tutti i contatti che contengono solo l'indirizzo di posta elettronica. I contatti privi del nome o dei dati telefonici vengono rimossi. L'opzione serve principalmente ad aiutare coloro che hanno utilizzato l'opzione di inserimento automatico nella lista consentiti di MDaemon nelle versioni precedenti alla versione 11 a eliminare i contatti aggiunti solo come risultato della funzionalità della lista consentiti. Nelle versioni precedenti di MDaemon gli indirizzi venivano aggiunti ai contatti principali invece che a una cartella di mittenti consentiti dedicata. Ciò può comportare un esubero di voci nella cartella dei contatti degli utenti che sarebbe preferibile evitare.

È consigliabile utilizzare questa opzione con grande cautela, perché i contatti contenenti solo l'indirizzo di posta elettronica potrebbero essere legittimi.

L'inoltro ad allowlist@ aggiorna i mittenti consentiti
Quando questa opzione è attivata, gli account che utilizzano l'opzione "*Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati*" nella schermata Impostazioni di Account Editor possono inoltrare i messaggi ad `allowlist@<dominio>` e ottenere che MDaemon aggiunga il mittente del messaggio originale ai mittenti consentiti dell'account. L'indirizzo consentito viene ricavato dall'intestazione `From` del messaggio inoltrato.

I messaggi inoltrati ad `allowlist@<dominio>` devono essere allegati di tipo `message/rfc822` e devono pervenire a MDaemon tramite SMTP da una sessione autenticata. I messaggi inoltrati che non soddisfano tali requisiti non vengono elaborati.

È possibile cambiare gli indirizzi utilizzati da MDaemon modificando la seguente chiave nel file `CFILTER.INI`:

```
[SpamFilter]
WhiteListAddress=MyAllowListAddress@
```

Nota: l'ultimo carattere deve essere "@".

L'inoltro a blocklist@ aggiorna i mittenti bloccati
Quando questa opzione è attivata, gli account che utilizzano l'opzione "*Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati*" nella schermata Impostazioni di Account Editor possono inoltrare i messaggi a `blocklist@<dominio>` e ottenere che MDaemon aggiunga il mittente del messaggio originale ai mittenti bloccati dell'account. L'indirizzo bloccato viene ricavato dall'intestazione `From` del messaggio inoltrato.

I messaggi inoltrati a `blocklist@<dominio>` devono essere allegati di tipo `message/rfc822` e devono pervenire a MDaemon tramite SMTP da una sessione autenticata. I messaggi inoltrati che non soddisfano tali requisiti non vengono elaborati.

Aggiorna il motore bayesiano con le copie di dei messaggi in lista consentiti
Fare clic su questa casella per copiare automaticamente i messaggi autorizzati nella cartella di apprendimento bayesiano non spam, specificata nella schermata Bayesiano 696. Ciò consente di offrire automaticamente al motore bayesiano esempi di posta non spam. Fornendo regolarmente al motore bayesiano esempi di non spam da cui apprendere, se ne accresce nel tempo l'affidabilità e ciò consente di ridurre il numero di messaggi erroneamente classificati come spam.

Per utilizzare questa funzione, un messaggio in arrivo deve essere indirizzato a un utente locale e il mittente deve essere una persona presente nella sua rubrica. o nella cartella dei mittenti consentiti. Se il messaggio è in uscita, è il destinatario che deve essere presente nella rubricao tra i mittenti consentiti. Se si desidera che nessun messaggio in uscita si qualifichi, utilizzare Blocco note per modificare le impostazioni seguenti nel file `CFILTER.INI`:

```
[SpamFilter]
UpdateHamFolderOutbound=No (valore predefinito = Yes)
```

Se il messaggio è autorizzato, viene copiato nella cartella di apprendimento bayesiano non spam anche se non è stato attivato l'apprendimento pianificato nella schermata Bayesiano. In questo modo, se l'apprendimento pianificato o quello manuale vengono successivamente attivati, sarà pronto un insieme di messaggi non spam per l'analisi. Tuttavia, non tutti i messaggi autorizzati vengono copiati nella cartella di apprendimento. Se è stata attivata questa funzione, MDaemon copia i messaggi autenticati fino al raggiungimento di un numero stabilito e successivamente copia i messaggi a intervalli prestabiliti. Per impostazione predefinita, inizialmente vengono copiati i primi 200 messaggi autenticati e poi, successivamente, dieci alla volta. Il numero iniziale di copie è identico al numero specificato nell'opzione, "*Esempi di non spam necessari prima della determinazione del punteggio spam bayesiano*" all'interno della schermata Autoapprendimento bayesiano 700. Modificando l'impostazione si modifica anche questo valore. Per modificare l'intervallo con cui vengono copiati i messaggi successivi, modificare la seguente impostazione del file `MDaemon.ini`:

```
[SpamFilter]
HamSkipCount=10 (valore predefinito = 10)
```

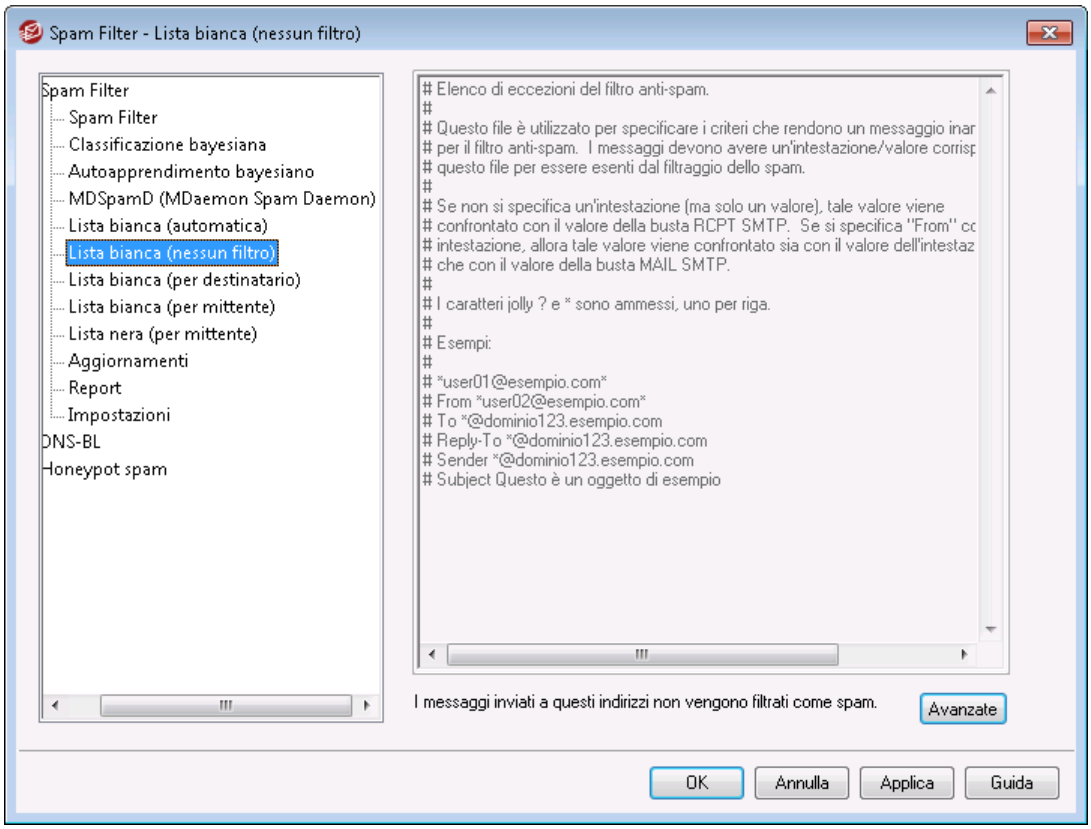
Infine, al termine della copia dei messaggi specificati, l'intero processo riprende nuovamente; inizialmente ne vengono copiati 200 e poi dieci alla volta o un altro

valore se questa impostazione è stata modificata. Per impostazione predefinita, il processo viene riavviato dopo che sono stati copiati 500 messaggi autenticati. È possibile modificare questo valore cambiando la seguente impostazione nel file `MDaemon.ini`:

```
[SpamFilter]
HamMaxCount=500 (valore predefinito = 500)
```

Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. Tutte le funzioni di apprendimento bayesiano vengono specificate dalle impostazioni dell'altro server e vengono eseguite su di esso. Per ulteriori informazioni, vedere Spam Daemon 702.

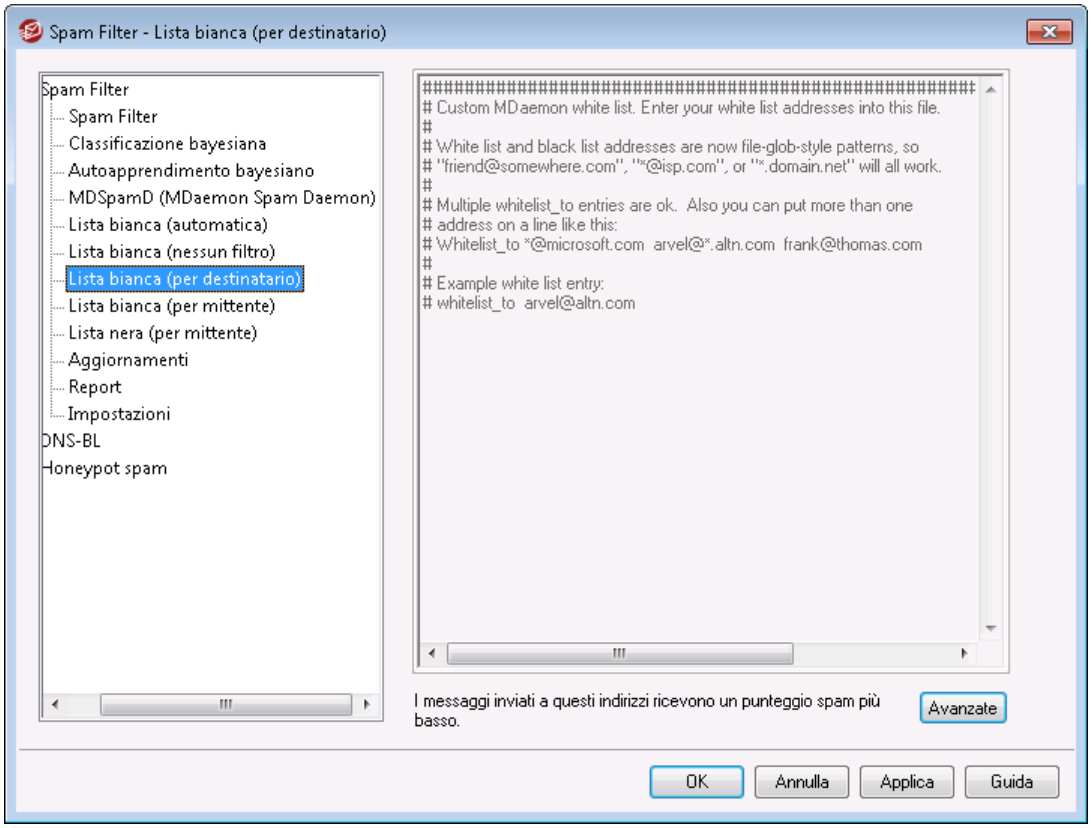
4.6.1.6 Lista consentiti (nessun filtro)



I messaggi inviati a questi indirizzi non vengono filtrati.
Fare clic su **Avanzate** in questa schermata per designare gli indirizzi del destinatario che si desidera esentare dall'applicazione filtro anti-spam. I messaggi destinati a questi indirizzi non vengono elaborati mediante filtri spam.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 702.

4.6.1.7 Lista consentiti (per destinatario)

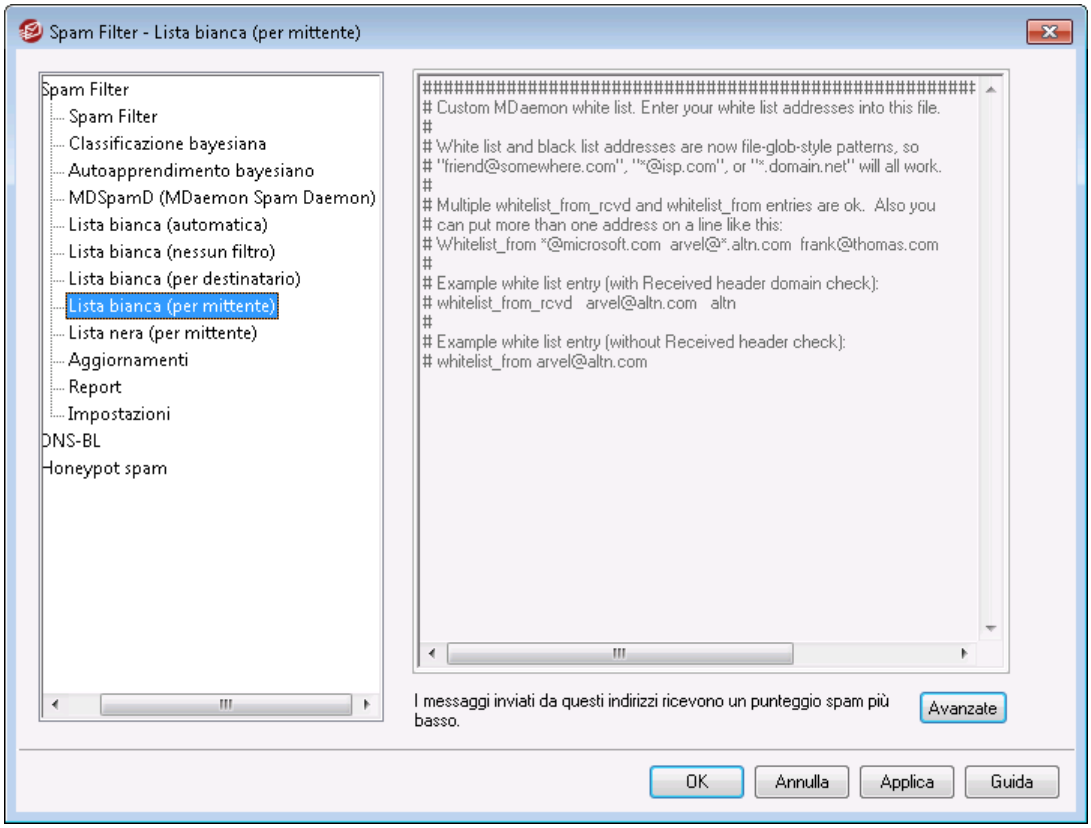


Il punteggio dei messaggi inviati a questi indirizzi viene corretto in senso positivo. Fare clic su **Avanzate** per aggiungere indirizzi a questa lista. Questa lista è simile alla *Lista consentiti (nessun filtro)* 708, con la differenza che, invece di esentare i messaggi indirizzati al destinatario dall'elaborazione dello Spam Filter, tale elaborazione avviene comunque ma il punteggio di Spam Filter 692 viene ridotto della quantità specificata nella schermata Impostazioni Spam Filter 715. Ne consegue che l'inserimento di un indirizzo in questa lista consentiti non garantisce automaticamente che un messaggio inviato a tale indirizzo non venga considerato spam. Ad esempio, se la soglia del punteggio spam è impostata su 5,0 e il valore della lista consentiti è impostato su 100 e arriva un messaggio di spam particolarmente eccessivo che ottiene un punteggio di 105,0 o superiore prima che il valore della lista consentiti venga sottratto, il punteggio finale di spam del messaggio sarà di almeno 5,0 e il messaggio verrà quindi considerato spam. Questa è tuttavia un'eventualità molto

improbabile, perché è raro che lo spam abbia un valore così alto, a meno che non contenga qualche altro elemento con un punteggio eccezionalmente alto, ad esempio un indirizzo bloccato.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 702.

4.6.1.8 Lista consentiti (per mittente)

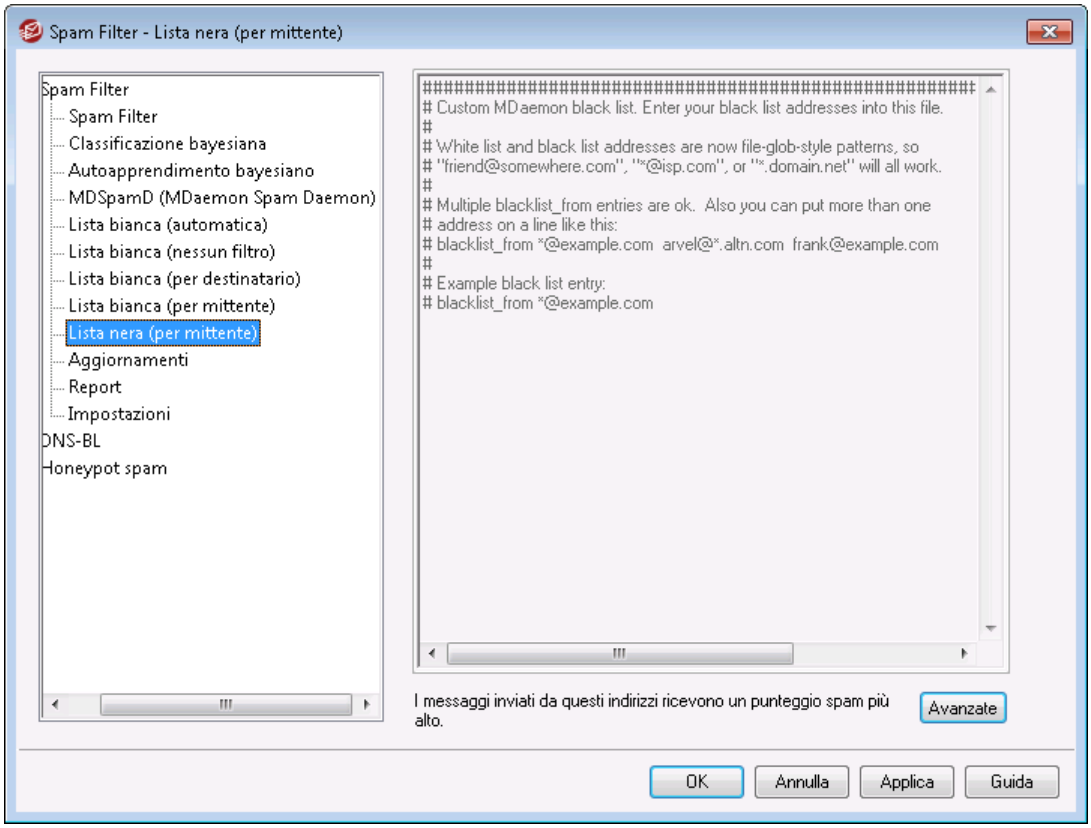


Il punteggio dei messaggi provenienti da questi indirizzi viene corretto in senso positivo. Fare clic su **Avanzate** per aggiungere indirizzi a questa lista. Questa lista consentiti è simile alla *Lista consentiti (per destinatario)* 709, tranne che per il fatto che la riduzione del punteggio spam si basa su chi *invia* il messaggio piuttosto che su chi lo riceve. Ai messaggi inviati da questi mittenti viene attribuito un punteggio di Spam Filter 692 ridotto della quantità specificata nella schermata Impostazioni Spam Filter 715. Ne consegue che l'inserimento di un indirizzo in questa lista consentiti non garantisce automaticamente che un messaggio inviato a tale indirizzo non venga considerato spam. Ad esempio, se la soglia del punteggio spam è impostata su 5,0 e

il valore della lista consentiti è impostato su 100 e arriva un messaggio di spam particolarmente eccessivo che ottiene un punteggio di 105,0 o superiore prima che il valore della lista consentiti venga sottratto, il punteggio finale di spam del messaggio sarà di almeno 5,0 e il messaggio verrà quindi considerato spam. Questa è tuttavia un'eventualità molto improbabile, perché è raro che lo spam abbia un valore così alto, a meno che non contenga qualche altro elemento con un punteggio eccezionalmente alto, ad esempio un indirizzo bloccato.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. Questo elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 702.

4.6.1.9 Lista bloccati (per mittente)

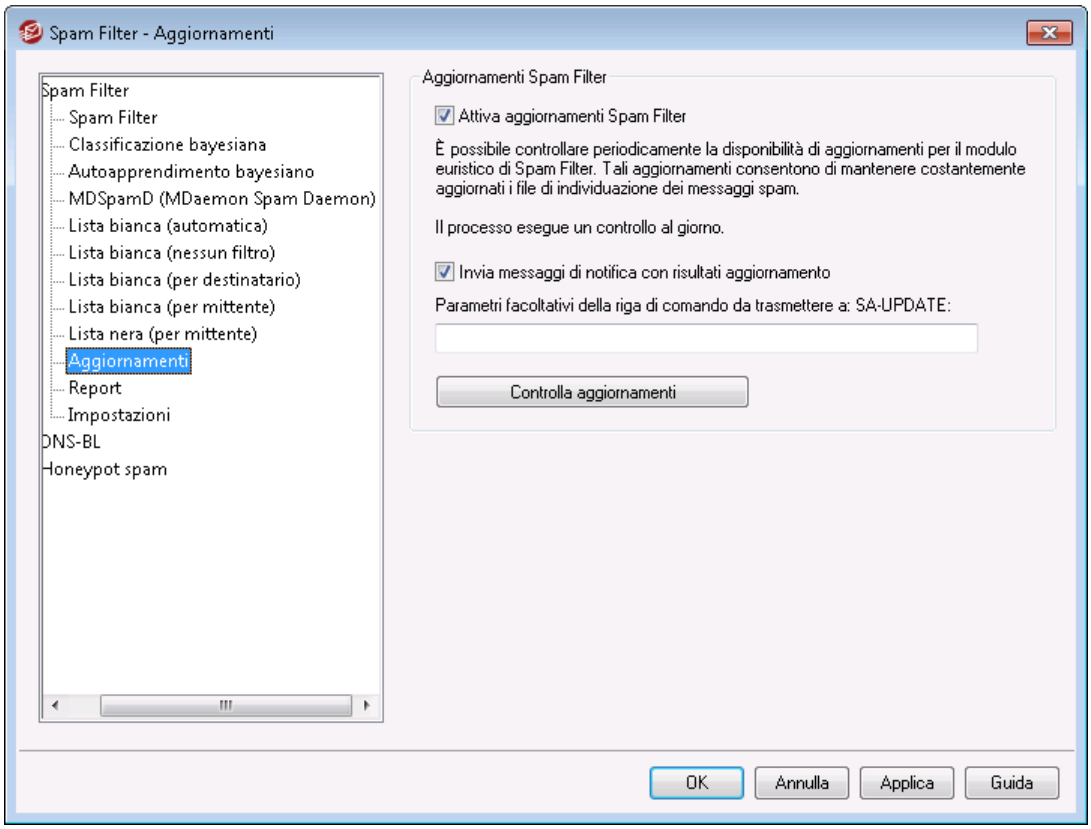


Il punteggio dei messaggi provenienti da questi indirizzi viene corretto in senso negativo.
Fare clic su **Avanzate** per aggiungere indirizzi a questa lista. I messaggi che provengono da indirizzi presenti in questa lista bloccati viene attribuito un punteggio di Spam Filter 692 aumentato della quantità specificata nella schermata Impostazioni Spam Filter 715, provocandone in genere la segnalazione come spam. Tuttavia,

l'inserimento di un indirizzo in questa lista non garantisce automaticamente che un messaggio proveniente da quell'indirizzo venga sempre considerato spam. Ad esempio, se un messaggio proviene da un mittente bloccato ma è indirizzato a un destinatario consentito, i modificatori del punteggio possono compensarsi a vicenda e configurare il messaggio in modo che abbia un punteggio finale inferiore alla soglia del punteggio di spam. Questo può accadere anche quando si è configurato un modificatore del punteggio della lista bloccati particolarmente basso.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 702.

4.6.1.10 Aggiornamenti



Aggiornamenti Spam Filter

Attiva aggiornamenti Spam Filter
Selezionare questa casella di controllo se si desidera che Spam Filter venga aggiornato automaticamente. MDaemon controllerà una volta al giorno la disponibilità

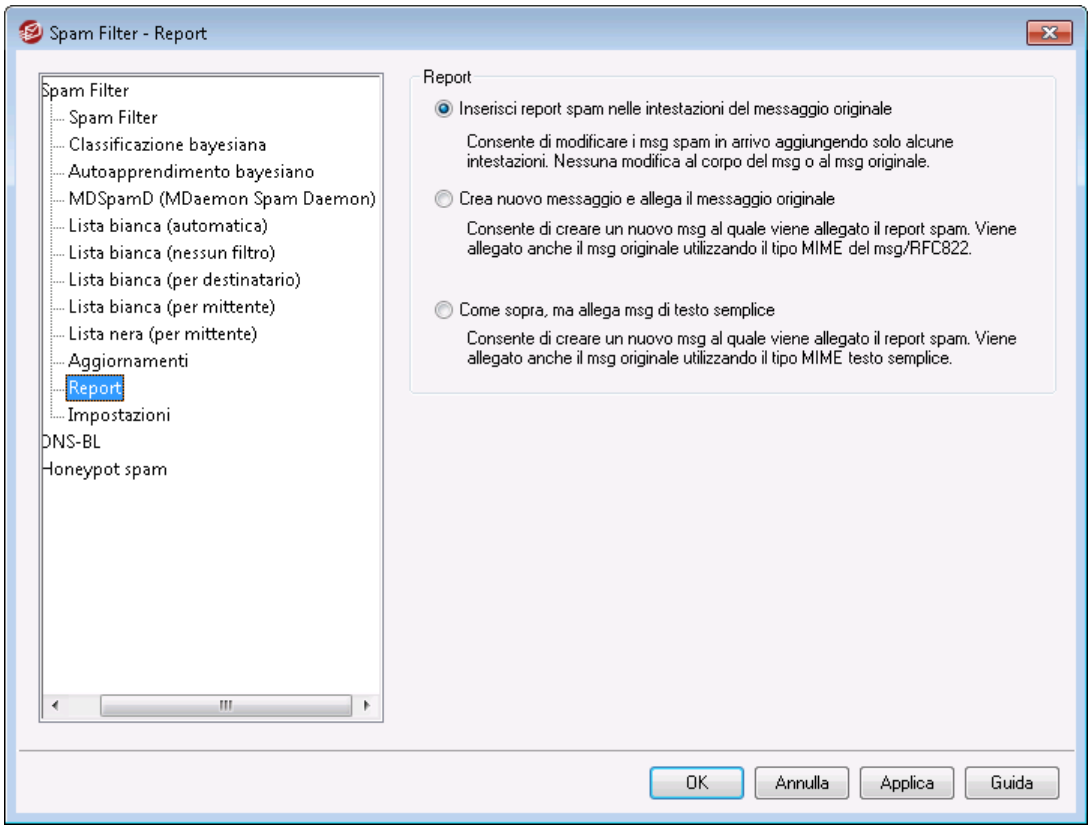
di aggiornamenti del modulo euristico di Spam Filter e, se tali aggiornamenti sono disponibili, li scaricherà e li installerà automaticamente.

Invia messaggi di notifica con risultati aggiornamento
Utilizzare questa opzione se si desidera inviare agli amministratori ad ogni aggiornamento di Spam Filter un messaggio e-mail contenente i risultati dell'aggiornamento. Questa opzione è uguale all'opzione "*Invia notifica di aggiornamento Spam Filter agli amministratori*" disponibile in: Filtro contenuti » Notifiche.

Opzioni facoltative della riga di comando da passare a SA-UPDATE
Utilizzare questa opzione avanzata se si desidera passare eventuali opzioni della riga di comando a SA-UPDATE.

Controlla aggiornamenti
Fare clic su questo pulsante per verificare in modo immediato se è disponibile un aggiornamento delle regole Spam Filter.

4.6.1.11 Report



Le opzioni di reportistica di Spam Filter non sono disponibili quando MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. La reportistica di Spam Filter verrà controllata dalle impostazioni di un altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon 702.

Report

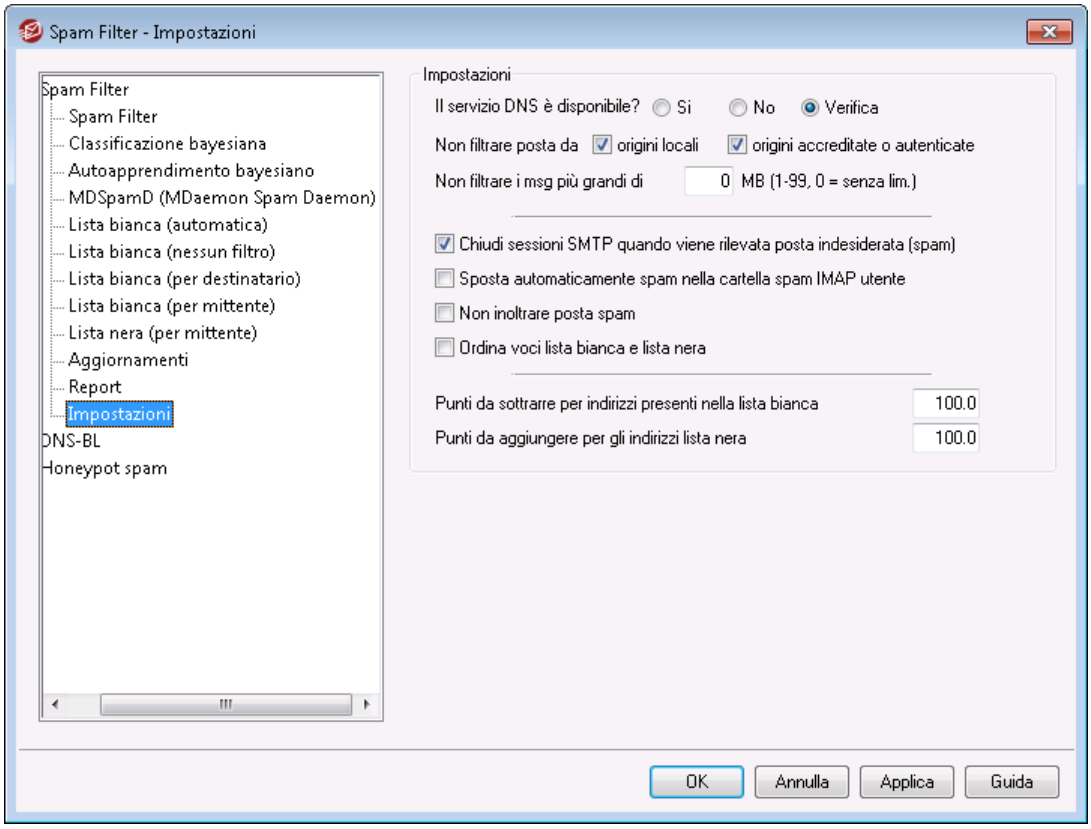
Inserisci report spam nelle intestazioni del messaggio originale
Questa è l'impostazione predefinita. Scegliere questa opzione se si desidera che Spam Filter inserisca un report di spam in ciascuna intestazione dei messaggi spam. Quanto segue è un esempio di report di spam di base:

```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
  * 3.0 -- Message has been marked by MDaemon's DNS-BL
  *  2.9 -- BODY: Impotence cure
  *  2.2 -- BODY: Talks about exercise with an exclamation!
  *  0.5 -- BODY: Message is 80% to 90% HTML
  *  0.1 -- BODY: HTML included in message
  *  1.6 -- BODY: HTML message is a saved web page
  *  2.0 -- Date: is 96 hours or more before Received: date
---- End of Spam Filter results
```

Crea nuovo messaggio e allega il messaggio originale
Scegliere questa opzione se si desidera che la posta spam generi un nuovo messaggio e-mail contenente un report di spam. Il messaggio spam originale viene incluso come file allegato.

Come sopra, ma allega msg di testo semplice
Come l'opzione precedente, questa genera un report di spam sotto forma di nuovo messaggio e include il messaggio spam originale come file allegato. La differenza consiste nell'allegare il messaggio originale con il tipo MIME text/plain. Dal momento che la posta spam contiene a volte codice HTML, differente per ciascun messaggio e può potenzialmente rivelare allo "spammer" l'indirizzo IP e l'indirizzo e-mail di chi apre il messaggio, questo metodo consente di evitare che ciò avvenga convertendo il codice HTML in semplice testo.

4.6.1.12 Impostazioni



Impostazioni

Il servizio DNS è disponibile?
Queste opzioni consentono di scegliere se utilizzare o meno il servizio DNS per Spam Filter durante l'elaborazione dei messaggi. È possibile scegliere una delle opzioni seguenti:

Sì - Il servizio DNS è disponibile. Di conseguenza, verranno utilizzate le funzioni SURBL/RBL e le altre regole che richiedono una connessione DNS.

No - Il servizio DNS non è disponibile. Non verranno utilizzate le regole di Spam Filter che richiedono una connessione DNS.

Verifica - Consente di verificare la disponibilità del servizio DNS che, se presente, verrà utilizzato. Questa è l'impostazione predefinita.

Non filtrare posta da...

origini locali
Selezionare questa casella di controllo se si desidera escludere dal filtro spam i messaggi inviati da utenti e domini locali.

origini accreditate o autenticate
Attivare questa opzione se si desidera escludere dal filtro spam i messaggi inviati da domini accreditati o autenticati.

Non filtrare i messaggi di dimensioni maggiori di [XX] MB (1-99, 0 = nessun limite)
Solitamente i messaggi spam sono di dimensioni abbastanza ridotte poiché l'obiettivo comune dei cosiddetti "spammer" è quello di consegnare il maggior numero di messaggi nel minor tempo possibile. Se si desidera esentare i messaggi di dimensioni maggiori di un determinato numero di MB, specificare qui le dimensioni (in MB). Utilizzare "0" per non impostare alcun limite di dimensione dei messaggi per il filtro spam.

Chiudere le sessioni SMTP quando viene rilevato un messaggio spam
Questa opzione è abilitata per impostazione predefinita e determina la chiusura di una sessione SMTP qualora l'analisi in linea rilevi un messaggio spam.

Sposta automaticamente spam nella cartella spam IMAP utente
Selezionare questa opzione se si desidera che MDaemon sposti automaticamente i messaggi riconosciuti come posta indesiderata da Spam Filter nella cartella IMAP "Spam" IMAP relativa all'utente, se questa esiste. In questo modo viene creata automaticamente una cartella per ogni nuovo account utente.

Facendo clic su questa opzione è possibile scegliere se generare o meno questa cartella per tutti gli account utente già esistenti. Se si sceglie "Sì" viene creata una cartella per tutti gli utenti, mentre se si sceglie "No" viene creata una cartella solo quando si aggiunge un nuovo utente. Tutte le cartelle degli utenti già esistenti non subiscono alcuna variazione o modifica.

Non inoltrare spam
Selezionare questa casella di controllo se si desidera consentire l'inoltro di messaggi spam.

Ordina voci liste consentiti e bloccati
Utilizzare questa opzione per mantenere le voci delle liste consentiti e bloccati di Spam Filter in sequenza ordinata. **Nota:** se si sono aggiunti commenti al file (righe che iniziano con #), l'abilitazione di questa opzione comporterà lo spostamento di queste righe all'inizio del file. Questa funzione è disabilitata per impostazione predefinita. Se si attiva l'opzione, l'ordinamento avverrà alla successiva modifica del file della lista consentiti o della lista bloccati.

Le opzioni rimanenti di questa schermata non sono disponibili se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Per ulteriori informazioni, vedere la schermata Spam Daemon 702.

Una corrispondenza rilevata nell'elenco consentiti sottrae questi punti dal punteggio spam
Se si inserisce un indirizzo nelle schermate Lista consentiti (per destinatario) 709 o Lista consentiti (per mittente) 710 di Spam Filter, questo non garantisce automaticamente che un messaggio inviato o ricevuto dall'indirizzo non venga considerato spam. Per tali indirizzi, invece, verrà semplicemente sottratto dal

punteggio spam il valore specificato in questo controllo. Ad esempio, se la soglia del punteggio spam è impostata su 5,0 e il valore della lista consentiti è impostato su 100 e arriva un messaggio di spam particolarmente eccessivo che ottiene un punteggio di 105,0 o superiore prima che il valore della lista consentiti venga sottratto, il punteggio spam finale del messaggio sarà di almeno 5,0 e il messaggio verrà quindi considerato spam. Questa è tuttavia un'eventualità molto improbabile, poiché è raro che lo spam abbia un valore così alto, a meno che non contenga qualche altro elemento con un punteggio eccezionalmente alto, ad esempio un indirizzo incluso nella lista bloccati. Ovviamente, se si imposta un valore da sottrarre della lista consentiti molto più basso, il fenomeno si verificherà più di frequente.

Se si desidera che i messaggi indirizzati ad alcuni destinatari vengano completamente esclusi da Spam Filter, includere gli indirizzi dei destinatari nell'elenco che si trova nella Lista consentiti (nessun filtro) 708 nella schermata.È inoltre possibile escludere i messaggi dalla definizione del punteggio di Spam Filter in base al mittente utilizzando le opzioni della schermata Lista consentiti (automatica) 705.

Una corrispondenza rilevata nell'elenco bloccati aggiunge questi punti al punteggio spam
Il valore viene aggiunto al punteggio spam dei messaggi provenienti dagli indirizzi riportati nella schermata Lista bloccati (per mittente) 711. Come accade con la lista consentiti descritta in precedenza, l'inserimento di un indirizzo nella lista bloccati di Spam Filter non garantisce automaticamente che un messaggio proveniente da quell'indirizzo venga considerato spam. Al contrario, il valore indicato in questo campo viene aggiunto al punteggio di spam del messaggio e utilizzato quindi per determinare se un messaggio debba essere considerato spam.

4.6.2 Liste bloccati DNS (DNS-BL)

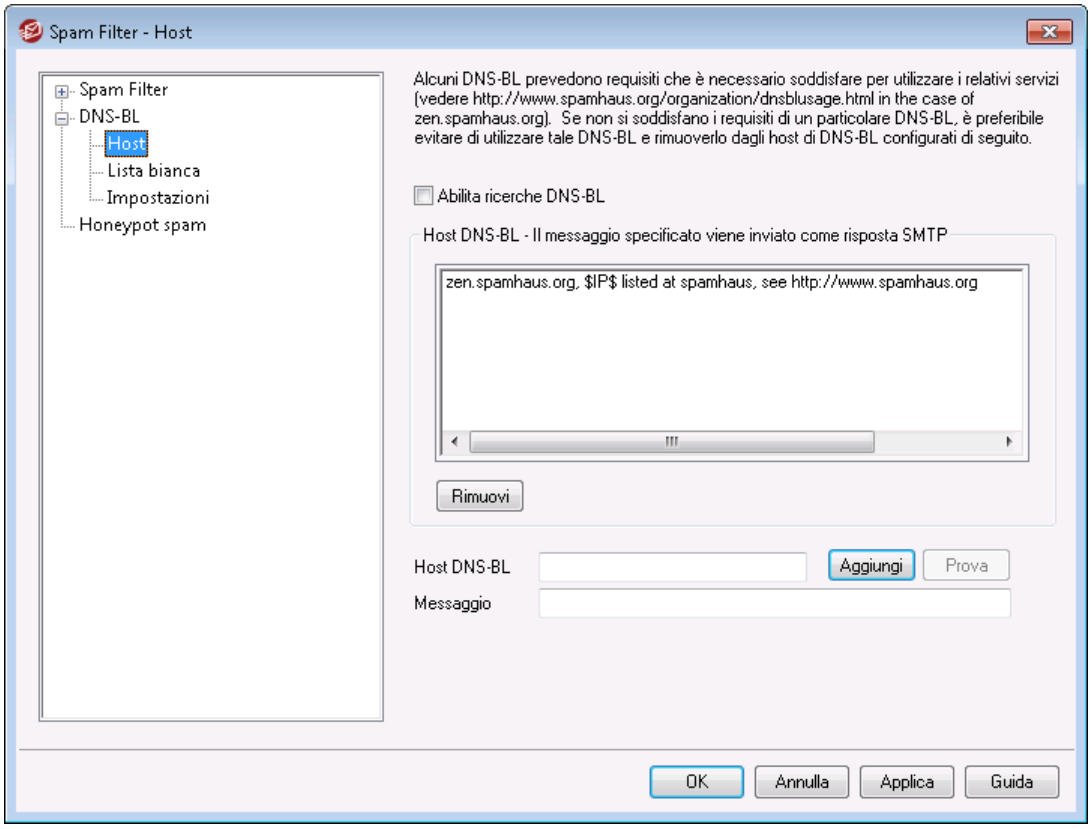
Le liste bloccati DNS (DNS-BL) si possono utilizzare per evitare che i messaggi e-mail di spam raggiungano gli utenti. Questa funzionalità di sicurezza consente di specificare diversi servizi DNS di liste bloccati (che gestiscono gli elenchi dei server noti per l'invio di spam) che verranno controllati ogni volta che qualcuno tenta di inviare un messaggio al server. Se l'IP di connessione è stato incluso negli elenchi di uno di questi servizi, i messaggi saranno rifiutati o contrassegnati in base alle impostazioni del servizio configurate nella schermata Impostazioni 720.

DNS La Lista bloccati include una Lista consentiti per designare gli indirizzi IP che si desidera escludere dalle query DNS-BL. Prima di attivare il DNS-BL, è necessario accertarsi che l'intervallo di indirizzi IP locali sia presente nella Lista consentiti per evitare che vengano eseguite ricerche su tali indirizzi. "`127.0.0.1`" è già escluso e non è necessario aggiungerlo alle eccezioni.

Per ulteriori informazioni, vedere:

Host DNS-BL 718
Impostazioni DNS-BL 720
Lista consentiti DNS-BL 719

4.6.2.1 Host



Host DNS-BL

Abilita ricerche DNS-BL
Attivare questa opzione se si desidera controllare la posta in arrivo a fronte delle Liste bloccati DNS. Durante la ricerca DNS-BL dell'indirizzo IP mittente, MDaemon interroga ciascuno degli host presenti nell'elenco. Se un host risponde alla query con un risultato positivo, MDaemon può contrassegnare il messaggio o rifiutarlo, a seconda delle opzioni attivate nella schermata Impostazioni DNS-BL 720.

Rimuovi
Selezionare una voce dall'elenco dei servizi DNS-BL, quindi premere questo pulsante per rimuoverla dall'elenco.

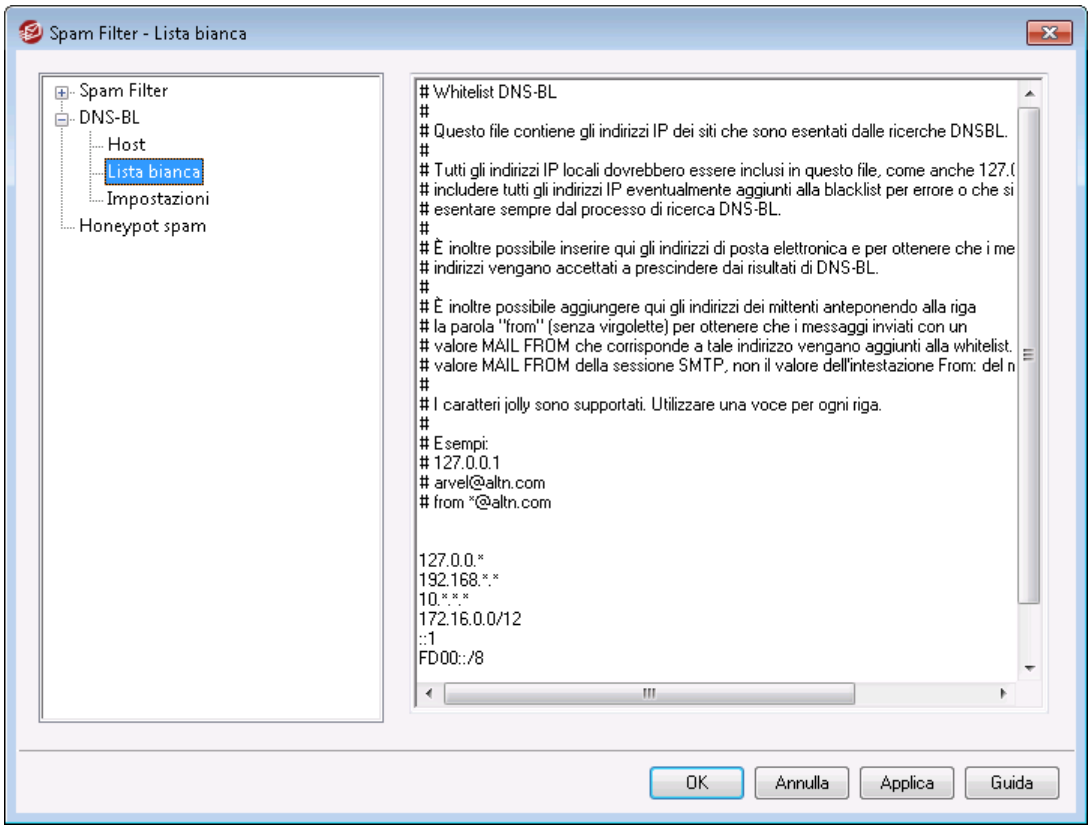
Host DNS-BL
Se si desidera aggiungere un nuovo host a cui inoltrare le query per gli indirizzi IP inclusi nelle liste bloccati, immetterlo qui.

Verifica
Immettere un host nell'opzione *Host DNS-BL* e fare clic su questo pulsante per eseguire un test cercando l'indirizzo 127.0.0.2.

Messaggio
Questo è il messaggio che può essere inviato durante la sessione SMTP quando un indirizzo IP è stato incluso nell'host DNS-BL corrispondente sopra riportato. Questo messaggio corrisponde all'opzione*...e rispondi con "Messaggio" invece che con "utente sconosciuto"* disponibile nella schermata Impostazioni DNS-BL 720.

Aggiungi
Una volta immesso l'host e il messaggio da restituire, fare clic su questo pulsante per aggiungere la voce all'elenco degli host DNS-BL.

4.6.2.2 Lista consentiti

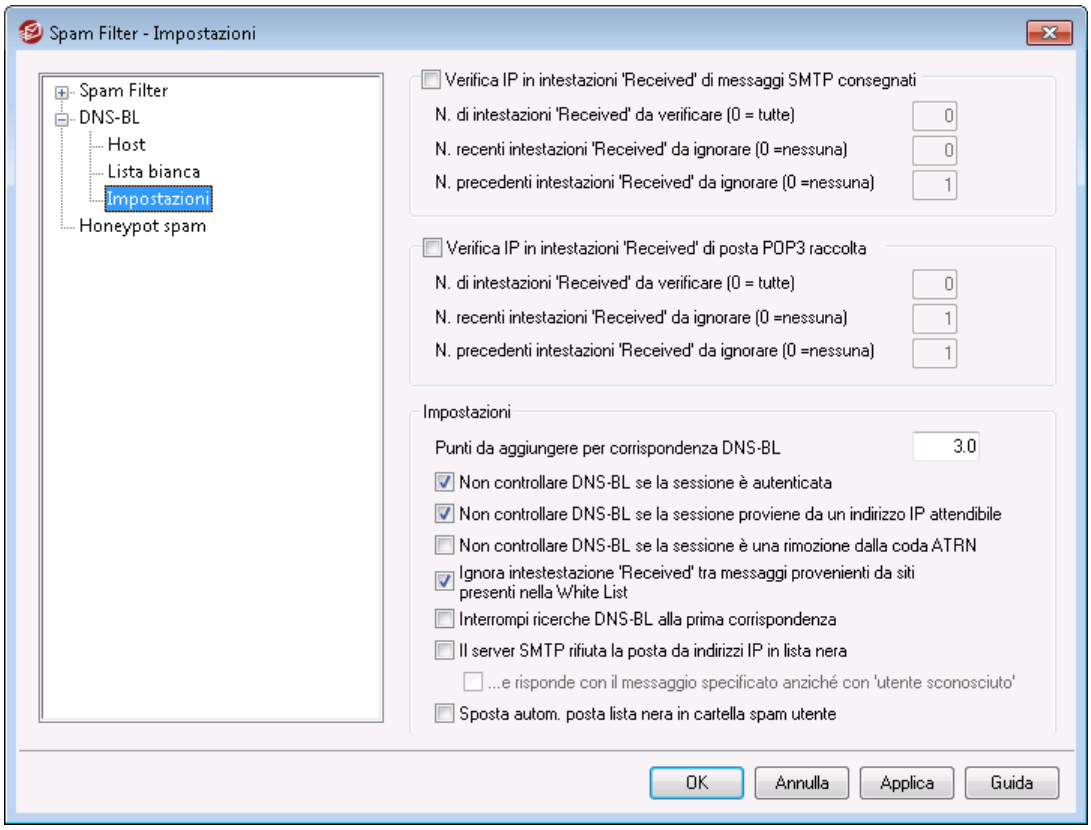


Utilizzare questa schermata per designare gli indirizzi IP che saranno esentati da query della lista bloccati DNS. È opportuno includere sempre l'indirizzo IP locale per impedire che il servizio DNS-BL effettui ricerche sui messaggi originati da utenti e domini locali, ossia `127.0.0.*`, `192.168.*.*` e così via. È inoltre possibile includere indirizzi e-mail nella lista. Quando un messaggio è indirizzato a uno di tali indirizzi, il messaggio verrà

accettato indipendentemente dai risultati della ricerca DNS-BL. Infine, è possibile escludere mittenti specifici dai risultati della ricerca DNS-BL immettendo "da *mittente@esempio.com*" nella lista. Questo indirizzo deve corrispondere al valore "MAIL FROM" della sessione SMTP, non all'intestazione "From:" dei messaggi.

Inserire una voce per ogni riga. I caratteri jolly sono accettati.

4.6.2.3 Impostazioni



Verifica IP in intestazioni 'Received' di messaggi SMTP consegnati
Fare clic su questa opzione se si desidera che La Lista bloccati DNS controlli l'indirizzo IP riportato nell'intestazione "`Received`" dei messaggi ricevuti via SMTP.

N. di intestazioni 'Received' da verificare (0 = tutte)
Specifica il numero di intestazioni "`Received`" da sottoporre alla verifica delle DNS-BL, a partire dal messaggio più recente. Con il valore "0", vengono verificate tutte le intestazioni "`Received`".

N. recenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che la funzione DNS-BL ignori le intestazioni `Received` più recenti durante la verifica dei messaggi SMTP, utilizzare questa opzione.

N. precedenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che le intestazioni "Received" meno recenti vengano ignorate durante la verifica dei messaggi SMTP, utilizzare questa opzione.

Verifica IP in intestazioni 'Received' di posta POP3 raccolta
Se questa opzione è abilitata, la funzione DNS-BL verifica l'indirizzo IP inserito nell'intestazione "Received" dei messaggi raccolti tramite DomainPOP e MultiPOP.

N. di intestazioni 'Received' da verificare (0 = tutte)
Specificare il numero di intestazioni "Received" da sottoporre alla verifica DNS-BL, a partire dal messaggio più recente. Con il valore "0", vengono verificate tutte le intestazioni "Received".

N. recenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che la funzione DNS-BL ignori le intestazioni Received più recenti durante la verifica dei messaggi DomainPOP e MultiPOP, utilizzare questa opzione. Poiché risulta spesso necessario ignorare l'intestazione Received più recente della posta POP3 raccolta, ad esempio DomainPOP, per impostazione predefinita a questa opzione è assegnato il valore "1".

N. precedenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che le intestazioni "Received" meno recenti vengano ignorate durante la verifica dei messaggi DomainPOP e MultiPOP, utilizzare questa opzione.

Impostazioni

Punti da aggiungere per corrispondenza DNS-BL
Usare questa opzione per specificare un valore da aggiungere al punteggio di spam[692] del messaggio in presenza di una corrispondenza delle liste DNS-BL. A volte un messaggio non viene considerato spam in base al controllo euristico di Spam Filter perché raggiunge un punteggio insufficiente, mentre le ricerche DNS-BL sono in grado di classificarlo come probabile spam. Pertanto l'aggiunta di questo valore al punteggio di spam consente di ridurre il numero di messaggi spam che potrebbero altrimenti sfuggire al rilevamento. Per impostazione predefinita una corrispondenza DNS-BL aggiunge 3.0 punti al punteggio di spam.

Non controllare DNS-BL se la sessione è...

autenticata
Fare clic su questa casella di controllo per escludere dalla ricerca delle DNS-BL le sessioni autenticate mediante il comando AUTH.

da un indirizzo IP attendibile
Fare clic su questa casella di controllo per escludere dalla ricerca delle DNS-BL gli indirizzi elencati nella schermata Host accreditati[526].

una rimozione dalla coda ATRN
Attivare questa opzione se non si desidera eseguire ricerche DNS-BL sulla posta raccolta nelle sessioni di rimozione dalla coda ATRN. Questa impostazione è disattivata per impostazione predefinita ma è possibile attivarla se ad esempio l'host intelligente sta già eseguendo i controlli DNS-BL sulla posta memorizzata.

Ignora intestazioni "Received" in messaggi da IP nella lista consentiti
Quando si attiva questa opzione, DNS-BL non controllerà le intestazioni "Received" dei messaggi provenienti dagli indirizzi IP riportati nella Lista consentiti DNS-BL 719.

Interrompi ricerche DNS-BL alla prima corrispondenza
Nelle intestazioni di ciascun messaggio elaborato dai servizi DNS-BL sono spesso presenti più host e anche i servizi DNS-BL interrogati sono numerosi. Per impostazione predefinita, queste ricerche interrogano tutti i servizi disponibili al fine di individuare tutti gli host presenti nel messaggio, senza tener conto del numero di corrispondenze trovate. Fare clic su questa opzione se si desidera che le ricerche DNS-BL relative a un messaggio vengano interrotte appena viene trovata una corrispondenza.

Il server SMTP deve rifiutare i messaggi provenienti da IP della lista bloccati
Per impostazione predefinita questa casella è deselezionata, quindi i messaggi che provengono da indirizzi IP inseriti nella lista bloccati non saranno rifiutati durante la sessione SMTP, ma conterranno un'intestazione X-MDDNSBL-Result. Sarà poi sufficiente utilizzare la funzione Filtro contenuti per trovare i messaggi con tale intestazione e destinarli di conseguenza. È inoltre possibile utilizzare l'opzione "*Filtra automaticamente i messaggi da lista bloccati nella cartella spam dell'utente*" riportata in basso per filtrare automaticamente i messaggi nella cartella spam di ciascun utente. Selezionare questa casella di controllo se si desidera che MDaemon rifiuti i messaggi ricevuti da indirizzi IP inseriti nella lista bloccati invece di contrassegnarli.

Poiché alcuni indirizzi IP potrebbero essere stati inseriti nella lista bloccati per errore, è necessario prestare attenzione prima di scegliere di rifiutare i messaggi piuttosto che limitarsi a segnalarli. Si noti inoltre che, oltre a contrassegnare un messaggio, è possibile modificarne il punteggio spam sulla base dei risultati DNS-BL mediante l'opzione *Punti da aggiungere per corrispondenza DNS-BL* situata in Spam Filter 692.

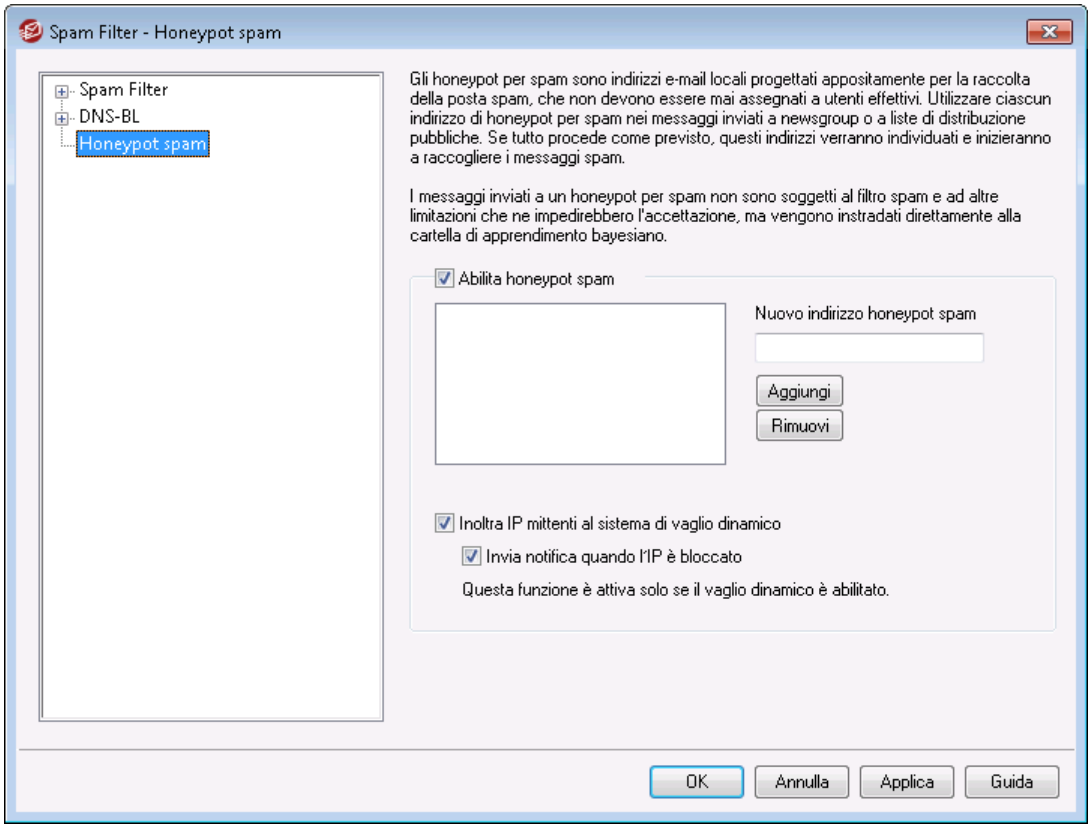
...e risponde con il messaggio specificato anziché con 'utente sconosciuto'
Fare clic su questa opzione se si desidera assegnare un messaggio specifico all'Host DNS-BL 718 da passare durante la sessione SMTP ogni volta che un indirizzo IP risulta essere riportato nella lista bloccati. In caso contrario, viene trasmesso il messaggio "user unknown". Questa opzione è disponibile solo se si è scelto di utilizzare l'opzione "*Il server SMTP deve rifiutare i messaggi provenienti da IP della lista bloccati*" sopra riportata.

Filtra automaticamente i messaggi da lista bloccati nella cartella spam dell'utente
Fare clic su questa opzione per generare una cartella IMAP "Junk E-mail" per tutti i futuri account utente aggiunti a MDaemon. In questo caso, MDaemon genera automaticamente per ogni utente anche un filtro di posta che ricerca l'intestazione X-MDDNSBL-Result, quindi sposta i messaggi contenenti questa intestazione nella cartella spam dell'utente. Facendo clic su questa opzione MDaemon richiede se si desidera o meno generare la cartella e la regola di filtro per tutti gli account utente già esistenti. Vedere *Generazione automatica della cartella Spam per ogni account*.

Generazione automatica della cartella Spam per ogni account

MDaemon è in grado di creare automaticamente una cartella di posta IMAP "Posta indesiderata" per ogni account e di generare un filtro di posta per spostare i messaggi in tale cartella ogni volta che viene individuata l'intestazione `X-MDDNSBL-Result`. Ogni volta che si fa clic su *Filtra automaticamente i messaggi da lista bloccati nella cartella spam dell'utente*, viene offerta l'opzione di creare la cartella e il relativo filtro per tutti gli account. Per creare le cartelle e le regole, è sufficiente scegliere "sì" nella finestra di dialogo di conferma. Sebbene non sia inattaccabile, questo è un metodo agevole e generalmente affidabile per consentire agli utenti di identificare rapidamente i messaggi di posta elettronica indesiderati e di evitare che si confondano con quelli accettati. Sarà sufficiente esaminare occasionalmente il contenuto della cartella Spam solo per assicurarsi che non vi siano finiti inavvertitamente messaggi importanti, cosa che talvolta può accadere. Durante la creazione automatica delle cartelle e delle regole di filtro, se a un account è già associata una regola per il controllo dell'esistenza dell'intestazione `X-MDDNSBL-Result`, per tale account non viene intrapresa alcuna azione e non viene creata alcuna regola. Se si desidera assegnare alla cartella IMAP un nome diverso da "Junk E-mail", modificare l'impostazione predefinita dell'opzione *Nome predefinito cartella spam* situata nella schermata Sistema[501] di Impostazioni » Preferenze.

4.6.3 Honeypot spam



Con Honeypot spam (situato in Sicurezza » Spam Filter » Honeypot spam) si intendono indirizzi di e-mail locali, appositamente definiti per la raccolta della posta spam. Gli honeypot (trappole) spam non sono account o alias di indirizzi validi utilizzati per l'invio o la ricezione di posta normale. Possono essere utilizzati per inviare messaggi a newsgroup, a liste di distribuzione pubbliche o ad altre liste frequentate dagli spammer al fine di raccogliere indirizzi e-mail. In questo caso, se tutto procede come previsto, gli indirizzi honeypot spam verranno individuati dagli spammer e a essi verranno inviati messaggi spam. È inoltre possibile estrarre indirizzi di honeypot spam dai messaggi spam ricevuti e diretti a indirizzi locali non validi. Poiché gli honeypot non vengono utilizzati per la ricezione di posta normale, tutti i messaggi a loro indirizzati vengono sempre instradati direttamente alla cartella di apprendimento bayesiano 696 per le successive elaborazioni. È inoltre possibile aggiungere gli indirizzi IP dei server mittenti al sistema di vaglio dinamico 575, impedendo così le connessioni provenienti da tali indirizzi per un periodo di tempo specificato. Queste caratteristiche consentono di aumentare la probabilità di identificare e bloccare i messaggi spam in futuro.

Honeypot spam

Questo elenco include tutti gli indirizzi definiti come honeypot spam.

Abilita honeypot spam
L'opzione è abilitata per impostazione predefinita. Deselezionare questa casella per disattivare questa funzione per honeypot spam.

Nuovo indirizzo honeypot spam
Per aggiungere un honeypot spam, immettere l'indirizzo e fare clic su *Aggiungi*.

Rimuovi
Per rimuovere un honeypot spam, selezionare l'indirizzo desiderato e fare clic su Rimuovi.

Inoltra IP mittenti al sistema di vaglio dinamico
Selezionare questa casella di controllo se si desidera inoltrare al sistema di vaglio dinamico 575 tutti gli IP dai quali vengono inviati i messaggi honeypot spam. Per utilizzare questa funzionalità è necessario abilitare nel server la funzione di vaglio dinamico, disponibile in Sicurezza » Impostazioni sicurezza » Vaglio » Vaglio dinamico.

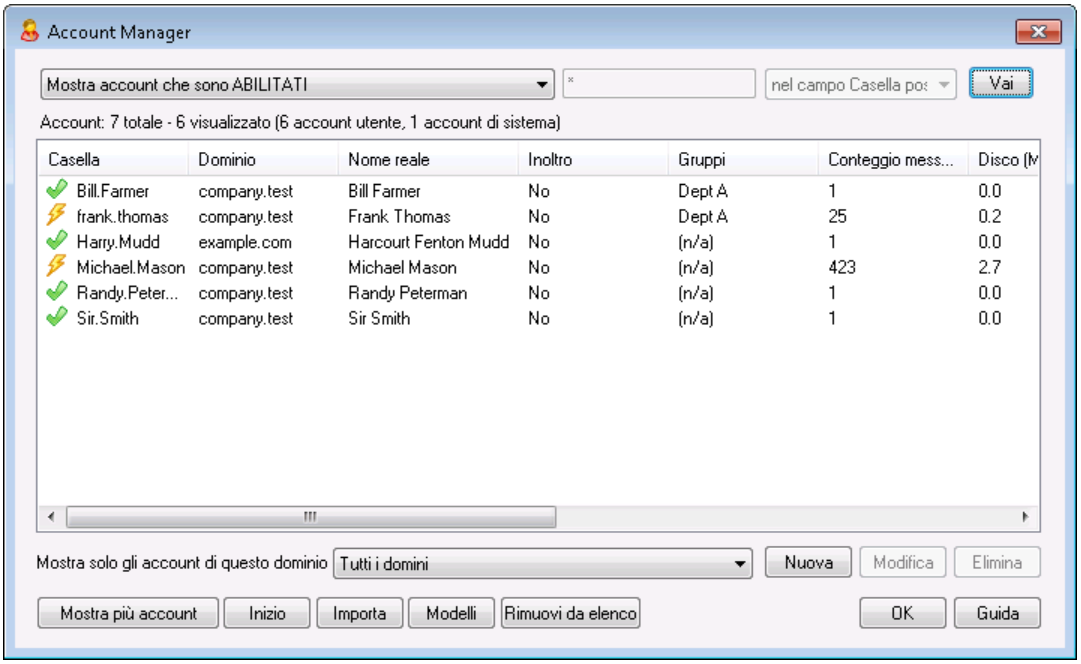
Invia notifica quando l'IP è bloccato
Per impostazione predefinita, quando un indirizzo IP presentato viene bloccato dal sistema di vaglio dinamico, vengono utilizzate le opzioni *Resoconti blocco indirizzo IP* 631 di Vaglio dinamico per notificare tale azione all'utente. Deselezionare questa casella di controllo se non si desidera ricevere notifiche quando un indirizzo IP viene bloccato a causa di segnalazioni Honeypot spam.

Sezione V

5 Menu Account

5.1 Account Manager

Per gestire al meglio la selezione, l'aggiunta, l'eliminazione o la modifica degli account, MDaemon offre lo strumento Account Manager. Questa finestra di dialogo fornisce l'accesso alle informazioni sugli account e può essere utilizzata per ordinarli in base alla casella postale, al dominio, al nome reale o alla cartella di posta. Account Manager è disponibile in: Account » Account Manager



Gestione degli account

Nella parte superiore dell'elenco degli account vengono visualizzate due statistiche relative all'elenco. Il primo dato indica il numero totale di account utente di MDaemon attualmente esistenti nel sistema. Il secondo dato rappresenta il numero degli account attualmente visualizzati nell'elenco. Gli account visualizzati dipendono dalla selezione effettuata nell'opzione *Mostra solo gli account di questo dominio* che si trova sotto l'elenco. Se è stata selezionata l'opzione "Tutti i domini", nell'elenco vengono visualizzati tutti gli account di MDaemon. Nella parte superiore della finestra di dialogo è presente un'opzione di ricerca che consente di definire esattamente gli account da visualizzare, non solo in base al dominio al quale appartengono.

Ciascuna voce dell'elenco contiene un'icona dello stato dell'account (vedere di seguito), la casella postale, il dominio a cui appartiene, il "nome reale" del proprietario dell'account, gli eventuali gruppi di cui fa parte l'account, il conteggio dei messaggi, lo spazio occupato su disco (in MB), l'ora dell'ultimo accesso all'account e la cartella di posta in cui vengono memorizzati i messaggi dell'account. L'elenco può essere organizzato in ordine crescente o decrescente in base a qualsiasi colonna. Fare clic su un'intestazione di colonna per applicare all'elenco l'ordine ascendente in base a tale colonna. Fare di nuovo clic sulla colonna per applicare l'ordine discendente.

Per impostazione predefinita, l'elenco visualizza solo 500 account per volta. Per visualizzare più account dal dominio attualmente selezionato (o da tutti i domini, se si seleziona la relativa opzione) è necessario fare clic sul pulsante *Mostra più account* per visualizzare i 500 successivi. Per visualizzare più di 500 account per volta, aprire il file `MDaemon.ini` e modificare la chiave `MaxAccountManagerEntries=500` immettendo il valore desiderato.

Icone di stato dell'account

L'account è un amministratore globale o di dominio.

Account con accesso completo. Sono abilitati sia gli accessi POP che IMAP.

Account con accesso limitato. POP, IMAP o entrambi sono disattivati.

L'account è bloccato. MDaemon accetta la posta per l'account, ma l'utente non può inviare o controllare la posta.

Account disabilitato. È disabilitato qualsiasi accesso all'account.

Nuovo
Per creare un nuovo account, fare clic su questo pulsante e aprire Account Editor 729 .

Modifica
Selezionare un account nell'elenco, quindi fare clic su questo pulsante per aprirlo in Account Editor 729. È inoltre possibile fare doppio clic sull'account per aprirlo.

Elimina
Per eliminare un account, selezionarlo e fare clic su questo pulsante. Verrà chiesto di confermare l'operazione.

Mostra solo gli account di questo dominio
Per visualizzare tutti gli account di MDaemon, selezionare "Tutti i domini" nella casella di riepilogo a discesa. Scegliere un dominio specifico per visualizzare solo gli account relativi.

Mostra più account
L'elenco visualizza solo 500 account alla volta. Se il dominio selezionato contiene più di 500 account, fare clic su questo pulsante per visualizzare i 500 account

successivi. Vedere la nota precedente per istruzioni su come incrementare il numero massimo di account visualizzabili.

Superiore
Fare clic su questo pulsante per spostarsi rapidamente all'inizio dell'elenco.

Importa
Fare clic su questo pulsante per importare gli account da un file di testo delimitato da virgole. Con questo pulsante si ottiene lo stesso risultato che si otterrebbe con la selezione di menu Account » Importazione » Importa account da file di testo delimitato da virgole.

Modelli
Fare clic su questo pulsante per aprire la finestra di dialogo Gruppi e modelli 796, da cui è possibile gestire le impostazioni predefinite per i nuovi account 807 e controllare l'appartenenza al gruppo di account.

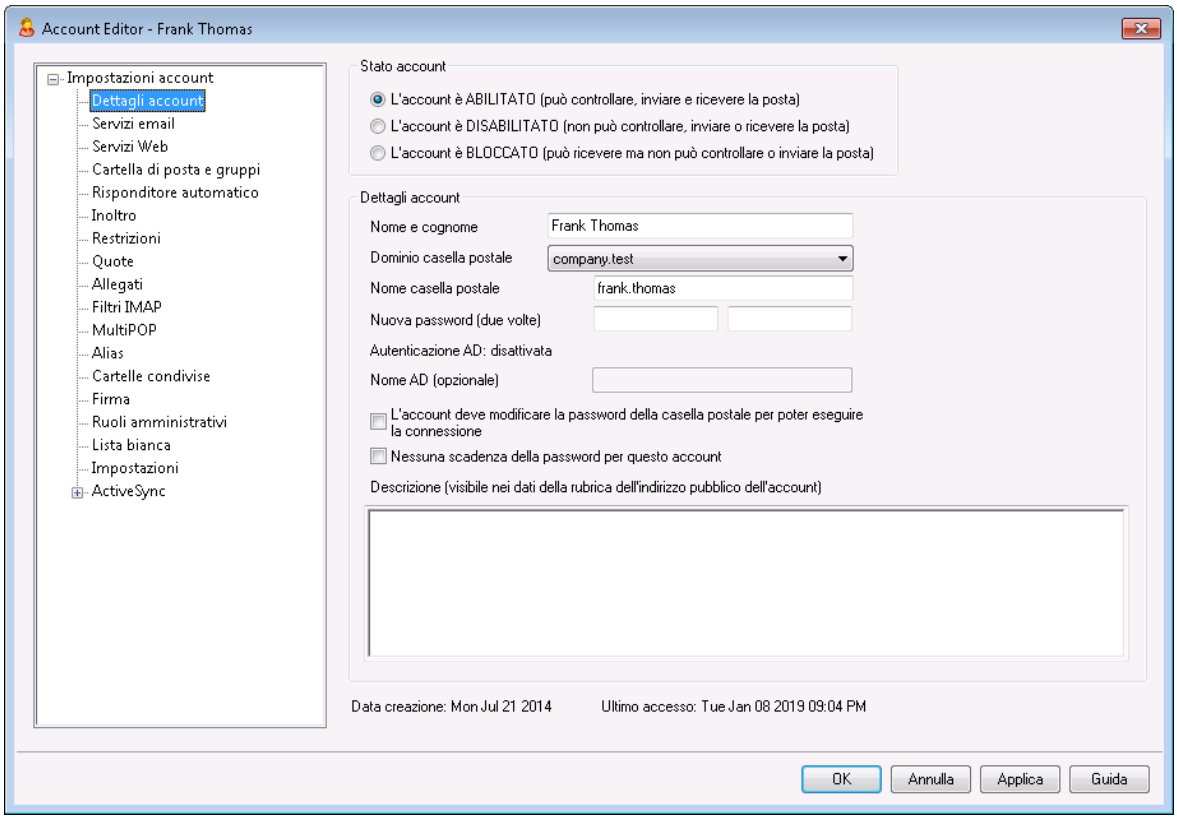
Rimuovi da elenco
Selezionare uno o più account, quindi fare clic su questo pulsante per annullarne le iscrizioni dalle Liste di distribuzione 281 ospitate sul server. Viene aperta una finestra che chiede di confermare la rimozione degli indirizzi dalle liste.

Vedere:

Account Editor 729
Modello Nuovi account 807

5.1.1 Account Editor

5.1.1.1 Dettagli account



Stato dell'account

L'account è ABILITATO (può controllare, inviare e ricevere la posta)
Questa è l'opzione predefinita; l'account può controllare, inviare e ricevere i messaggi e-mail.

L'account è DISABILITATO (non può controllare, inviare e ricevere la posta)
Selezionare questa opzione per disabilitare tutti gli accessi all'account. L'utente non sarà in grado in alcun modo di accedere all'account e MDaemon non ne accetterà la posta. Non sarà eliminato e continuerà a essere incluso nel numero di account utilizzati nell'limite di account della propria licenza, ma MDaemon si comporterà come se l'account non esistesse, con un'unica eccezione: sarà ancora possibile accedere a tutte le cartelle dell'account condivise con altri utenti, in base alle autorizzazioni ACL 319 della cartella.

L'account è BLOCCATO (può ricevere ma non può controllare o inviare la posta)
Selezionare questa opzione per consentire all'account di ricevere i messaggi in arrivo, ma impedire all'account di controllare o inviare i messaggi. Questa opzione è utile, ad esempio, quando si sospetta un hijack dell'account. Il blocco dell'account impedisce all'utente malintenzionato di accedere ai messaggi o di utilizzare l'account per inviare i messaggi, ma l'utente sarà comunque in grado di ricevere i messaggi e-mail in arrivo.

Dettagli account

Nome e cognome
Inserire in questo campo il nome e il cognome dell'utente. Quando si crea un nuovo account, molti dei campi delle varie schermate di Account Editor, ad esempio *Nome casella postale* e*Cartella di posta*, vengono compilati automaticamente al momento dell'inserimento del nome e del cognome dell'utente e quando si seleziona *Dominio casella postale*. È possibile, tuttavia, modificare uno di questi valori predefiniti. Il campo relativo al nome e al cognome non può contenere caratteri "! " o "|".

Dominio casella postale
Utilizzare questa casella di riepilogo a discesa per selezionare il dominio a cui si desidera assegnare l'account e che verrà utilizzato nel relativo indirizzo e-mail. Per impostazione predefinita, nell'elenco a discesa viene visualizzato il dominio predefinito 185 di MDaemon.

Nome casella postale
Indica la parte dell'indirizzo e-mail dell'account che distingue l'account da altri account del dominio. L'indirizzo e-mail completo (ad es. [*Nome casella postale*] @[*Dominio casella postale*]) è usato come identificativo univoco per l'account e come credenziale di accesso per POP3, IMAP, Webmail e così via. Gli indirizzi di posta elettronica non possono contenere spazi né i caratteri "! " o "|". Non utilizzare "@" in questa opzione. Utilizzare, ad esempio, "franco.tommaso" non "franco.tommaso@".

Nuova password (due volte)
Per modificare la password dell'account, digitarne una nuova qui, una volta in ogni casella. Questa è la password che l'account utilizzerà per la connessione a MDaemon per inviare o ricevere messaggi e-mail via POP3 o IMAP, per l'autenticazione durante il processo SMTP o durante l'uso di Webmail, Remote Administration, or MDaemon Connector. Entrambe queste caselle saranno evidenziate in rosso se le password non corrispondono o se violano le delle limitazioni imposte alle password 870. In caso contrario, saranno di colore verde.

Se si utilizza Autenticazione Active Directory 882 per questo account, è necessario immettere due barre retroverse seguite dal dominio Windows al quale appartiene l'utente, invece di inserire una password (ad esempio, `\\ALTN` invece di `123Password`). Sotto i campi della password è riportato un breve messaggio che indica se l'autenticazione AD è attivata o disattivata per l'account.

L'account deve avere una password, anche se non si desidera consentire l'accesso POP3/IMAP all'account di posta. Oltre che per la verifica della sessione di posta, i valori Indirizzo e-mail e *Password casella postale* vengono utilizzati per consentire la configurazione remota dell'account e il recupero remoto dei file. Se si desidera impedire l'accesso POP/IMAP, utilizzare le opzioni della schermata Servizi di posta 733. Se si desidera impedire tutte le modalità di accesso, utilizzare l'opzione *L'account è DISABILITATO* o *L'account è BLOCCATO*.

Nome AD (opzionale)
Utilizzare questa impostazione per specificare un nome account Active Directory opzionale per l'accesso all'account.

L'account deve modificare la password della casella postale per poter eseguire la connessione
Selezionare questa casella di controllo se si desidera che l'utente debba modificare la *Password casella postale* prima di poter accedere a POP, IMAP, SMTP, Webmail o Remote Administration. L'utente può connettersi a Webmail o a Remote Administration ma gli verrà richiesto di modificare la password prima di procedere. Si noti, comunque, che perché gli utenti possano modificare le password via Webmail o Remote Administration, devono prima ottenere l'autorizzazione di accesso Web "*...modifica password*" nella schermata Servizi Web 735. Una volta modificata la password, questa opzione viene disattivata.

Poiché la modifica della password potrebbe non essere semplice o possibile per alcuni utenti, prestare attenzione prima di attivare questa opzione.

Nessuna scadenza della password per questo account
Selezionare questa casella di controllo per escludere l'account dall'opzione di scadenza della password impostata nella finestra di dialogo Password 870.

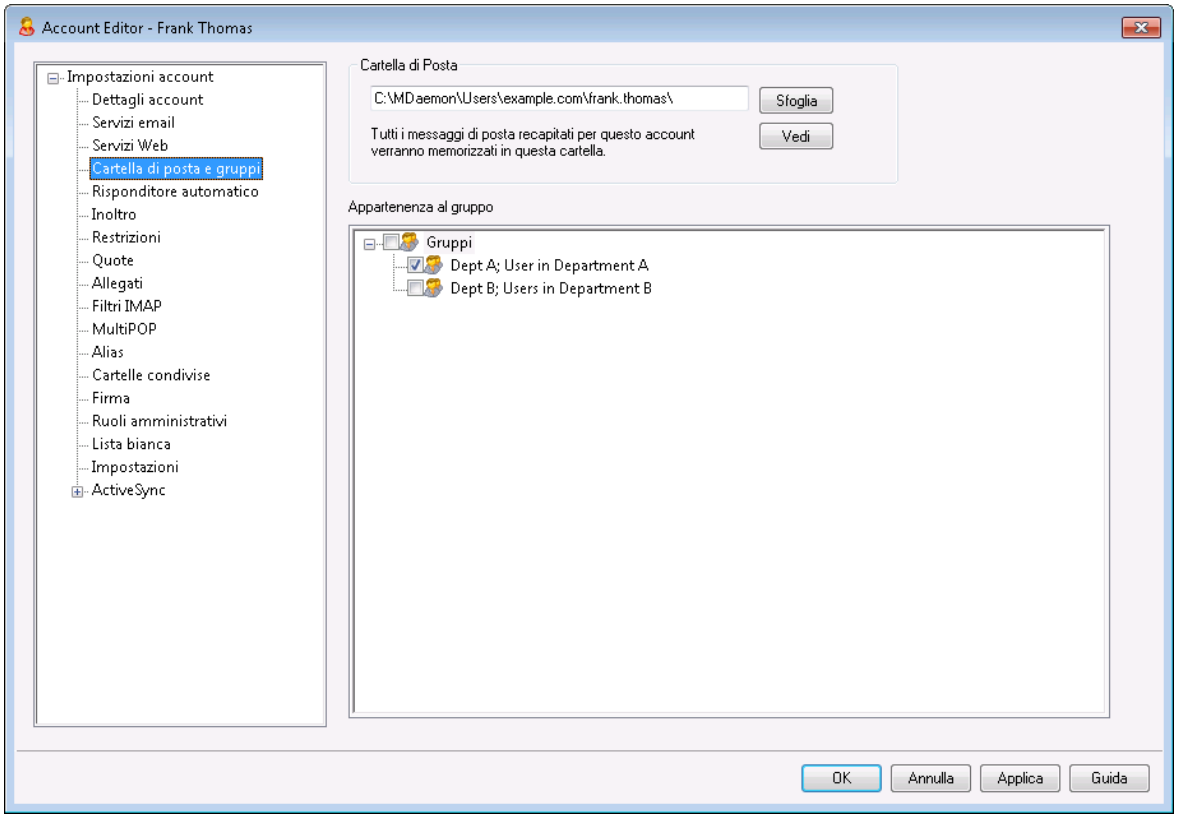
Descrizione
Utilizzare quest'area per aggiungere una descrizione pubblica dell'account.

Questa descrizione è inclusa nel record dei contatti pubblici dell'account e può essere visualizzata da altri. Non includere informazioni private o riservate in questo campo. Per commenti o note private relativi all'account, utilizzare lo spazio disponibile nella schermata Ruoli amministratore 773.

Vedere:

Autenticazione AD 882
Password 870
Account Editor » Servizi Web 735

5.1.1.2 Cartella di posta e gruppi



Cartella di posta

Immettere il nome della cartella nella quale si desidera memorizzare i messaggi e-mail relativi all'account. La posizione predefinita della cartella in fase di creazione di un nuovo account dipende dalla *Cartella di posta* specificata nel modello Nuovi account 808.

Visualizza
Fare clic su questo pulsante per aprire Gestione code/statistiche 900 nella *Cartella di posta* dell'utente.

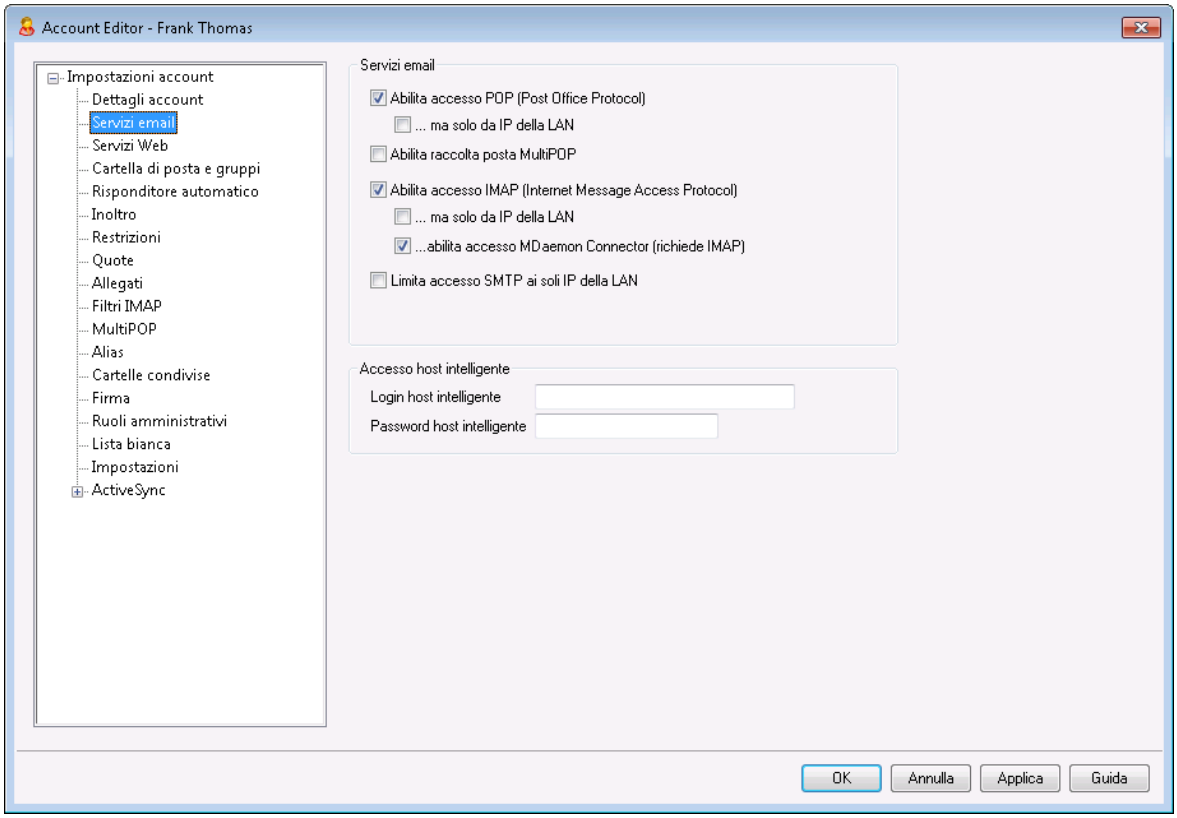
Appartenenza al gruppo

Questa casella consente di aggiungere l'account a uno o più Gruppi 796. Selezionare la casella accanto a ciascun gruppo a cui si desidera che l'account si unisca.

Vedere:

Modello Nuovi account 808
Gruppi 796

5.1.1.3 Servizi di posta



Le opzioni in questa schermata specificano i servizi di posta che l'account è autorizzato a utilizzare: POP, IMAP, MultiPOP e MDaemon Connector. L'accesso alle e-mail mediante Webmail può essere controllato dalla schermata Servizi Web 735. La schermata contiene inoltre le opzioni per specificare le credenziali facoltative dell'account per Accesso host intelligente.

Servizi di posta

Abilita accesso POP (Post Office Protocol)
Quando questa casella è selezionata, è possibile accedere alla posta dell'account mediante Post Office Protocol (POP). Questo protocollo è supportato da tutti i software client di posta elettronica.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che l'account sia accessibile tramite POP solo quando l'utente si connette da un indirizzo IP LAN 620.

Abilita raccolta posta MultiPOP
Selezionare questa casella di controllo se si desidera che l'account utilizzi MultiPOP 754. MultiPOP consente all'utente di raccogliere la posta da altri account di posta elettronica, gestiti su altri server di posta.

Abilita accesso IMAP (Internet Message Access Protocol)
Quando questa casella è selezionata, è possibile accedere alla posta dell'account mediante Internet Message Access Protocol (IMAP). Il protocollo IMAP è più versatile del protocollo POP3, in quanto consente di gestire la posta elettronica dal server e di accedervi mediante più client. Questo protocollo è supportato dalla maggior parte dei client di posta elettronica.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che l'account sia accessibile tramite IMAP solo quando l'utente si connette da un indirizzo IP LAN 620.

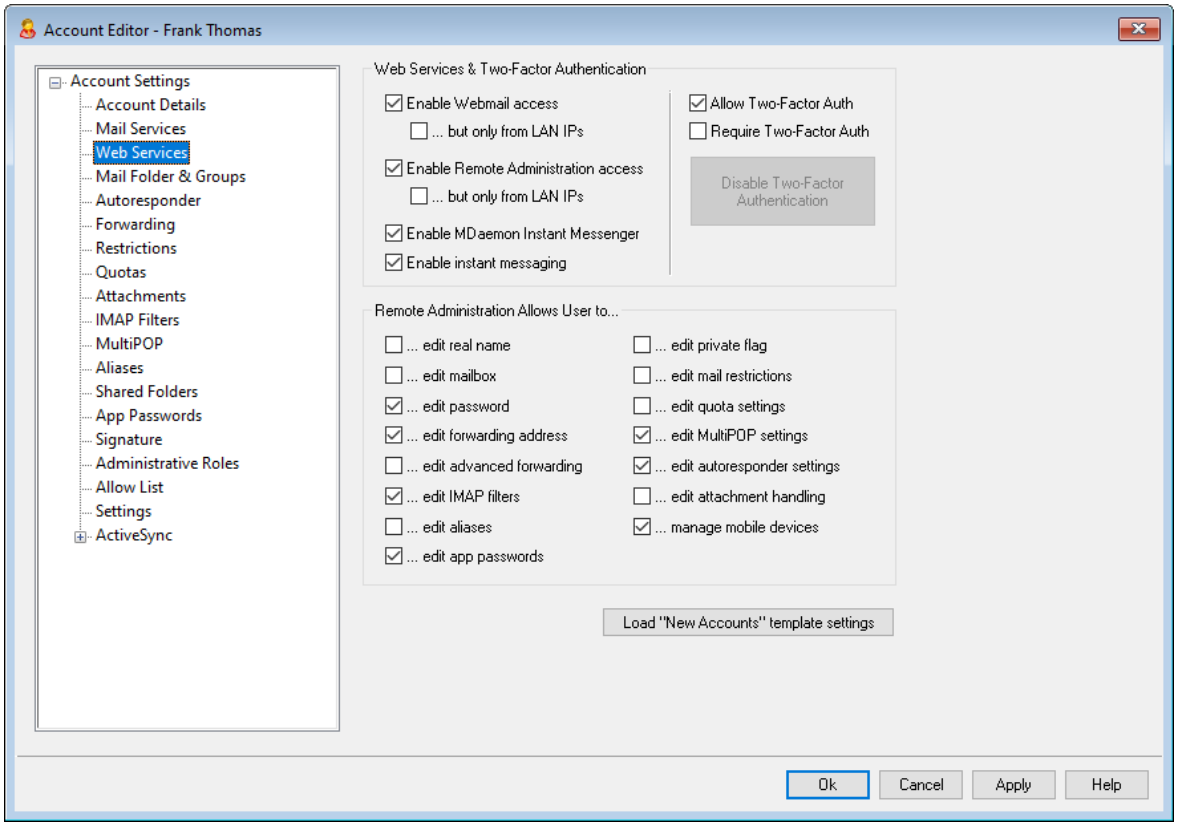
...abilita accesso MDaemon Connector (richiede IMAP)
Fare clic su questa opzione per consentire ai titolari dell'account di utilizzare MDaemon Connector 395. **Nota:** questa opzione sarà disponibile solo quando sul server è attivato il supporto di MDaemon Connector.

Limita accesso SMTP ai soli IP della LAN
Selezionare questa casella di controllo se si desidera limitare accesso SMTP ai soli IP della LAN. Questo impedirà agli account di inviare messaggi a meno che non siano connessi alla rete. Se l'account tenta di inviare la posta da un indirizzo IP esterno, la connessione verrà rifiutata e chiusa.

Accesso host intelligente

Password/login host intelligente
Se è abilitata l'opzione *Consenti autenticazione in base ad account* della schermata Consegna 97 situata in Impostazioni » Impostazioni servere per questo account si desidera utilizzare l'autenticazione in base all'account anziché le credenziali indicate nella schermata, è necessario specificare le credenziali facoltative dell'account per l'host intelligente. Se non si desidera utilizzare l'autenticazione in base all'account, lasciare vuote queste opzioni.

5.1.1.4 Servizi Web



Servizio Web

Abilita accesso Webmail
Selezionare questa casella di controllo se si desidera autorizzare gli account ad accedere al server Webmail 325, che consente di accedere ai messaggi e-mail, ai calendari e ad altre funzioni mediante un browser Web.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che l'account acceda a Webmail solo quando la connessione viene eseguita da un indirizzo IP LAN 620.

Abilita accesso amministrazione Web
Selezionare questa casella per autorizzare gli utenti alla modifica delle impostazioni dell'account mediante Remote Administration 359. Gli utenti potranno modificare solo le impostazioni specificate successivamente.

Se si abilita questa funzione e se il server Remote Administration è attivo, è possibile accedere a Remote Administration inserendo nel browser il dominio di MDaemon desiderato e la porta assegnata a Remote Administration 361 (ad es. `http://esempio.com:1000`). Dapprima viene visualizzata una schermata di registrazione, quindi la schermata delle impostazioni che si è autorizzati a modificare. È sufficiente modificare le impostazioni desiderate e fare clic sul pulsante *Salva modifiche*. Quindi, uscire e chiudere il browser. Se si dispone dell'accesso a Webmail è

possibile accedere a Remote Administration anche dal menu Opzioni avanzate di Webmail.

Se l'utente è un amministratore globale o un amministratore di dominio, privilegio indicato nella schermata Ruoli amministrativi 773 di Account Editor, dopo l'accesso a Remote Administration verrà visualizzata una schermata diversa.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che l'account acceda a Remote Administration solo quando la connessione viene eseguita da un indirizzo IP LAN 620.

Abilita MDaemon Instant Messenger
Fare clic su questa casella per abilitare il supporto di MDIM 326 per questo account.

Abilita messaggistica istantanea
Quando il supporto di MDIM è abilitato per l'account, fare clic su questa opzione se si desidera anche abilitare il supporto per il sistema di messaggistica istantanea di MDIM. Quando si deseleziona questa casella, è possibile accedere alle altre funzioni di MDIM, ma non alla messaggistica istantanea.

Autenticazione a due fattori

MDaemon supporta l'autenticazione a due fattori (2FA) per gli utenti che accedono all'interfaccia Web di Webmail o Remote Administration di MDaemon. Gli account che accedono a Webmail via HTTPS possono attivare l'autenticazione a due fattori per l'account nella schermata **Opzioni » Sicurezza** di Webmail. Da quel momento l'utente quando accede a Webmail o Remote Administration dovrà immettere un codice di verifica. Il codice viene fornito all'accesso da una app di autenticazione installata nel dispositivo mobile o tablet dell'utente. Questa funzione è progettata per i client che supportano Google Authenticator. Vedere il file della Guida in linea di Webmail per ulteriori informazioni sull'impostazione della 2FA per un account.

Consenti autenticazione a due fattori
Per impostazione predefinita, i nuovi account 814 sono autorizzati a impostare e utilizzare la funzionalità di autenticazione a due fattori (2FA) di Webmail. Se non si desidera consentire all'account di utilizzare la 2FA, deselezionare questa casella di controllo.

Richiedi autenticazione a due fattori
Attivare questa opzione per forzare l'uso dell'autenticazione a due fattori (2FA) da parte dell'account all'accesso di Webmail. Se non è stata ancora configurata la 2FA per l'account, al successivo accesso dell'account in Webmail l'utente verrà reindirizzato a una pagina di configurazione. Vedere il file della Guida in linea di Webmail per ulteriori informazioni sull'impostazione della 2FA per un account.

Disabilita l'autenticazione a due fattori
Fare clic su questo pulsante se si desidera disabilitare l'autenticazione a due fattori dell'account. Questa operazione può essere necessaria se, ad esempio, l'utente smarrisce il proprio dispositivo e non può accedere in altro modo ai dati di autenticazione.

Remote Administration consente agli utenti di...

...modifica nome reale
Abilitando questa funzione, l'utente può modificare l'impostazione *Nome e cognome* 729.

...modifica casella postale
Se si abilita questa funzione, l'utente è autorizzato a modificare l'impostazione *Nome casella postale* 729 dell'account.

Poiché il *Nome casella postale* fa parte dell'indirizzo e-mail dell'account e rappresenta l'identificativo univoco e il valore dell'ID utente utilizzato per l'account, la modifica di questa opzione determina la modifica dell'effettivo indirizzo e-mail dell'utente. Ciò può determinare il rifiuto, l'eliminazione o comunque la perdita dei futuri messaggi diretti al precedente indirizzo.

...modifica password
Selezionare questa casella di controllo per consentire all'utente di modificare la *Password casella postale* dell'account. Per ulteriori informazioni sui requisiti delle password, vedere: Password 870.

...modifica indirizzo inoltro
Quando questa funzione è abilitata, l'utente è in grado di modificare le impostazioni dell'indirizzo di inoltro 742.

...modifica inoltro avanzato
Quando si attiva questa funzionalità, l'utente può modificare le *impostazioni di inoltro avanzate* 742.

...modificare i filtri IMAP
Questa opzione consente all'utente di creare e gestire i propri filtri IMAP 751.

...modifica alias
Selezionare questa opzione per consentire ai titolari dell'account di utilizzare Remote Administration per modificare gli Alias 756 associati al proprio account.

...modificare le password di applicazione
Per impostazione predefinita, gli utenti possono modificare le proprie password di applicazione 766. Se si desidera impedire all'utente di modificarle, deselezionare questa casella di controllo.

...modificare il flag privato
Questa opzione consente di decidere se l'utente è autorizzato o meno a utilizzare Remote Administration per modificare l'opzione "*Account nascosto da elenchi*

"Everyone", calendari condivisi e VRFY" disponibile nella schermata Impostazioni[776] dell'editor degli account.

...modifica restrizioni di posta
Questa casella di controllo consente di autorizzare l'account alla modifica delle limitazioni relative alla posta in entrata e in uscita, situate nella schermata Restrizioni[744].

...modifica impostazioni di quota
Con questa casella di controllo è possibile consentire all'account la modifica delle impostazioni relative alla Quota[746].

...modifica impostazioni MultiPOP
Selezionare questa casella di controllo se si desidera concedere all'account l'autorizzazione ad aggiungere nuove voci MultiPOP[754] e attivare/disattivare la raccolta MultiPOP per tali voci in MDRA[359]. Quando questa opzione e l'opzione *Attiva MultiPOP*[754] sono entrambe attivate, la pagina Cassette postali sarà disponibile in Webmail[325] e consentirà all'utente di gestire le opzioni della cassetta postale MultiPOP. Infine, l'opzione globale per attivare/disattivare il server MultiPOP è disponibile in: Impostazioni » Impostazioni server » MultiPOP[146].

...modifica impostazioni risposta automatica
Selezionare questa casella di controllo per consentire all'utente di aggiungere, modificare o eliminare le Risposte automatiche[739] per il proprio account.

...modifica gestione allegati
Se si seleziona questa casella, l'utente ha la possibilità di modificare le opzioni di gestione degli allegati dell'account nella schermata Allegati[749].

...gestisce dispositivo mobile
Selezionare questa opzione per consentire al proprietario dell'account di utilizzare Remote Administration per la gestione delle impostazioni specifiche per i dispositivi, ad esempio per i dispositivi ActiveSync.

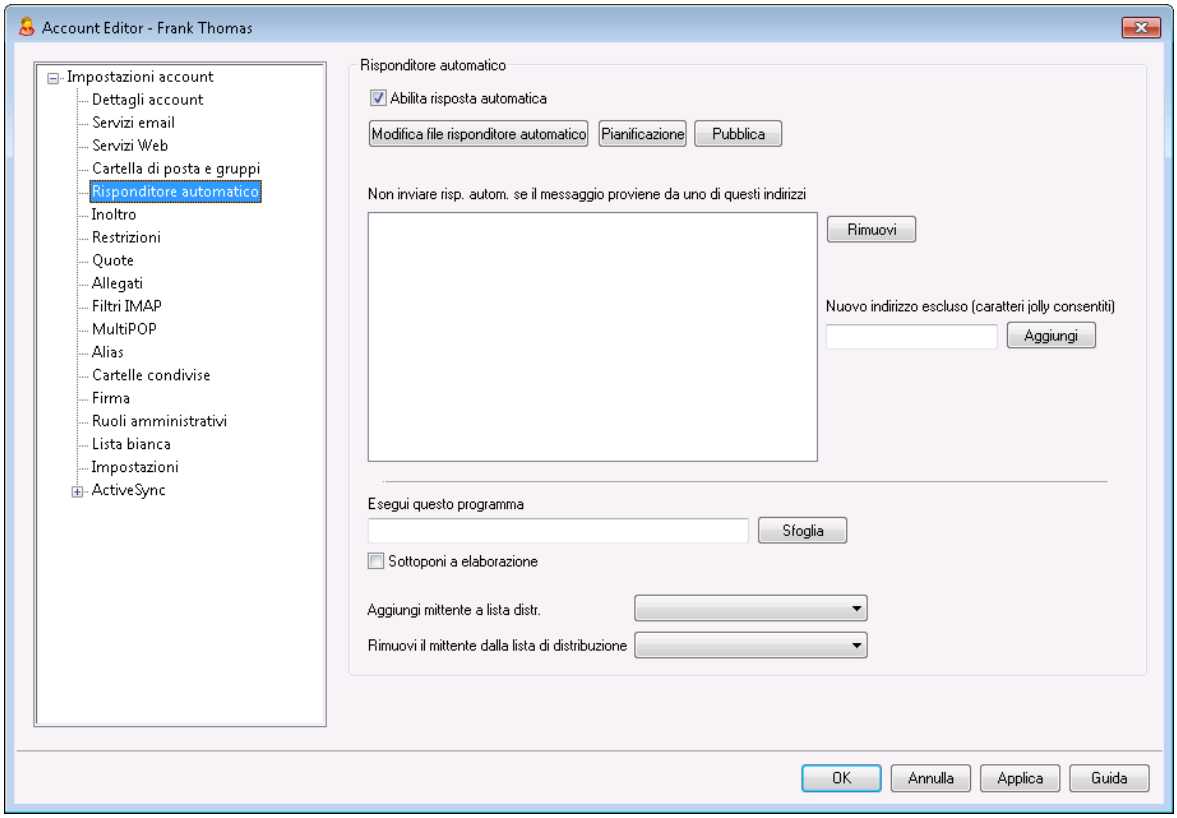
Carica impostazioni modello "Nuovi account"

Questo pulsante consente di riportare le impostazioni della schermata ai valori predefiniti indicati nella schermata Servizi Web[814] del modello *Nuovi account*.

Vedere:

Webmail[325]
Remote Administration[359]
Gestione account » Servizi Web[814]

5.1.1.5 Risposta automatica



Le risposte automatiche sono strumenti utili che consentono, in base ai messaggi e-mail in arrivo, di attivare eventi specifici quali l'esecuzione di un programma, l'inserimento di un mittente in una lista di distribuzione, l'invio di una risposta con un messaggio generato automaticamente e altro ancora. L'utilizzo più comune delle risposte automatiche consiste nella risposta automatica ai messaggi in entrata con un messaggio definito dall'utente con il quale viene comunicato che il destinatario è in vacanza, non è disponibile, risponderà appena possibile e così via. Gli utenti di MDaemon con accesso Web 735 a Webmail 325 o Remote Administration 359 possono utilizzare le opzioni disponibili per comporre propri messaggi di risposta automatica e pianificare le relative date di utilizzo. Infine, i messaggi di risposta automatica sono basati sul contenuto del file `OOF.mrk` che si trova nella cartella radice `\data\` di ciascun utente. Questo file supporta un elevato numero di macro, che possono essere utilizzate per la generazione dinamica di molta parte del contenuto dei messaggi, il che rende le risposte automatiche piuttosto versatili.

Gli eventi di risposta automatica vengono utilizzati quando il messaggio di attivazione proviene da un'origine remota. Tuttavia, per i messaggi che provengono dallo stesso dominio dell'utente, le risposte automatiche si attivano solo se si seleziona l'opzione *Risposte automatiche attivate da mail dallo stesso dominio*, disponibile nella schermata Risposte automatiche » Impostazioni 856. Questa schermata consente

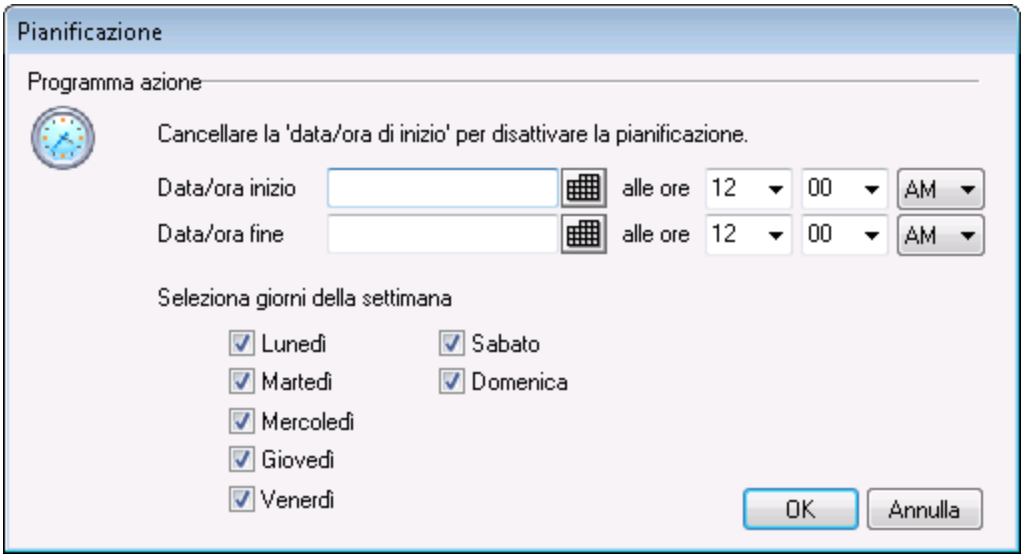
inoltre di utilizzare un'opzione per limitare i messaggi di risposta automatica a una risposta al giorno per ogni mittente.

Risposta automatica

Abilita risposta automatica
Selezionare questa casella di controllo per attivare una risposta automatica per l'account. Per ulteriori informazioni sulle risposte automatiche, vedere: Risposte automatiche 852.

Modifica file risposta automatica
Fare clic su questo pulsante per modificare il file di risposte automatiche dell'account. Il file è nel file `oof.mrk` che si trova nella cartella `\data\` dell'account.

Pianificazione
Fare clic su questo pulsante per aprire la finestra di dialogo Pianificazione, che consente di impostare la data e l'ora di inizio e di fine dell'intervallo temporale e i giorni della settimana in cui deve essere attiva la funzione di risposta automatica. Se si desidera che la risposta automatica sia sempre attiva, lasciare vuoti i campi.



Pubblica
Fare clic su questo pulsante se si desidera copiare il file di risposta automatica dell'account e le impostazioni su uno o più altri account. Selezionare gli account sui quali si desidera copiare la risposta automatica e fare clic su **OK**.

Non inviare risp. autom. se il messaggio proviene da uno di questi indirizzi
In questo campo è possibile elencare gli indirizzi che si desidera escludere dall'invio della risposta automatica.

Può accadere che i messaggi di risposta automatica vengano inviati a un indirizzo che utilizza a sua volta lo stesso meccanismo. In questo caso, viene a crearsi un effetto "ping-pong" per cui i messaggi vengono continuamente scambiati tra i due server. Per evitare tale problema è possibile inserire l'indirizzo in questo campo. Nella schermata Risposte automatiche » Impostazioni 856 è disponibile un'opzione che consente di limitare i messaggi di risposta automatica a non più di uno al giorno per ogni mittente.

Rimuovi
Fare clic su questo pulsante per eliminare le voci selezionate dall'elenco degli indirizzi esclusi.

Nuovo indir. escluso (car. jolly consentiti)
Se si desidera aggiungere un indirizzo all'elenco degli indirizzi esclusi, inserirlo in questo campo e fare clic sul pulsante *Aggiungi*.

Esecuzione di un programma

Esegui programma
Questo campo consente di specificare il percorso e il nome del file in un programma da eseguire all'arrivo della posta in questo account. Accertarsi che tale programma termini in modo corretto e possa essere eseguito senza supervisione. È possibile inserire eventuali parametri della riga di comando subito dopo il percorso del file eseguibile.

Sottoponi a elaborazione
Se si seleziona questa opzione, il nome del messaggio di attivazione verrà passato al processo specificato nel campo *Esegui questo programma* come primo parametro disponibile della riga di comando. Se si imposta la risposta automatica per un account che inoltra la posta a un'altra posizione **senza** conservarne copia locale nella propria casella postale (vedere Inoltro 742), questa funzione viene disabilitata.

Per impostazione predefinita, MDaemon inserisce il nome del file di messaggio come ultimo parametro della riga di comando. Per ignorare questo comportamento, utilizzare la macro `$MESSAGE$`. Inserire la macro al posto del nome file del messaggio. Ciò consente di aumentare la flessibilità della funzione, in quanto sarà possibile utilizzare righe di comando complesse come la seguente: `logmail /e /j /message=$MESSAGE$ /q`.

Liste di distribuzione

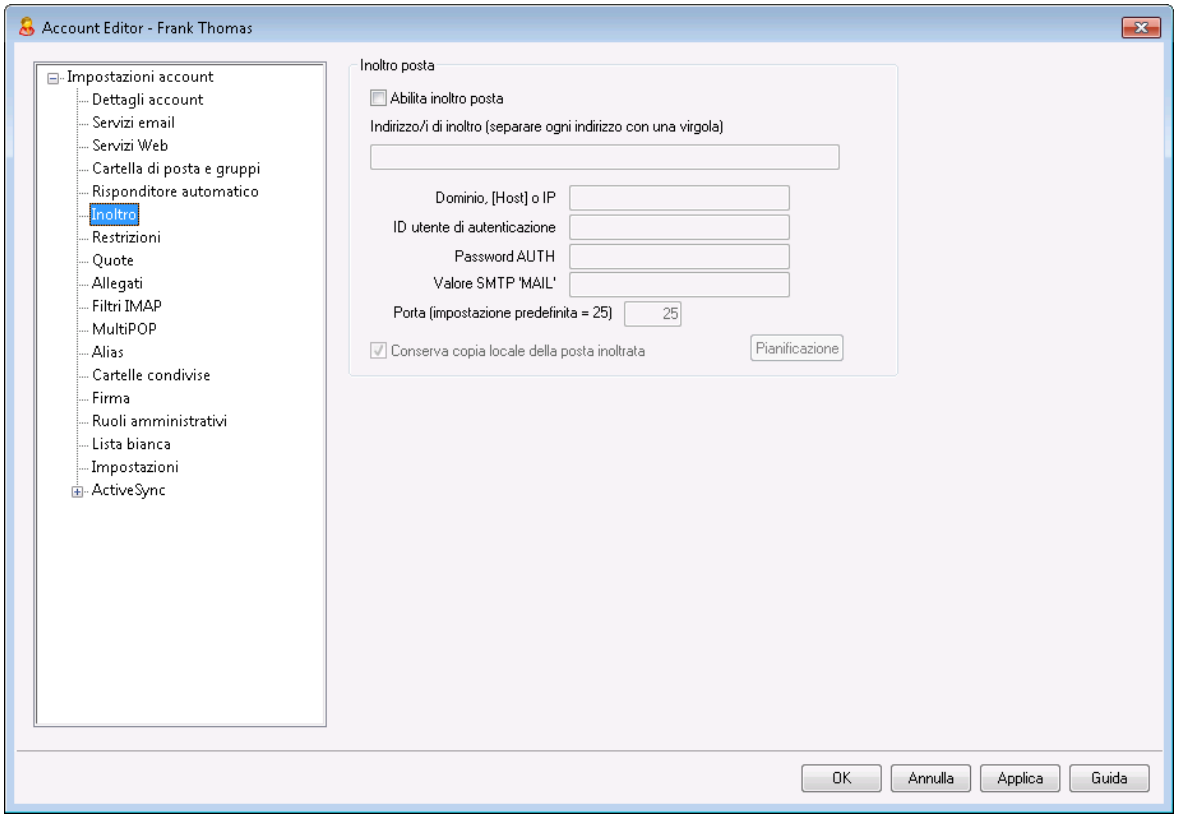
Aggiungi mittente a lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in entrata diventa automaticamente un membro di tale lista. Questa funzione è molto utile per la creazione automatica delle liste.

Rimuovi mittente da lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in arrivo viene automaticamente rimosso dalla lista specificata.

Vedere:

Risposte automatiche » Account 852
Risposte automatiche » Elenco esenzioni 855
Risposte automatiche » Impostazioni 856
Creazione di messaggi di risposta automatica 857

5.1.1.6 Inoltro



Inoltro posta

Abilita inoltro posta
Se si abilita questa casella, i messaggi in entrata dell'account vengono inoltrati agli indirizzi indicati nell'opzione *Indirizzo/i di inoltro*. Gli utenti di MDaemon con accesso Web 735 a Webmail 325 o a Remote Administration 359 possono utilizzare le opzioni disponibili per impostare le opzioni di inoltro autonomamente invece di chiedere a un amministratore di farlo.

Indirizzo/i di inoltro (separare ogni indirizzo con una virgola)
Questo campo consente di indicare gli indirizzi e-mail ai quali inoltrare copie dei messaggi in entrata, man mano che questi pervengono all'account. Una copia di ogni nuovo messaggio in arrivo al server viene generata e inoltrata automaticamente all'indirizzo specificato in questo campo, purché sia stata selezionata l'opzione *Abilita inoltro posta*. Per specificare più indirizzi, utilizzare la virgola come separatore.

Dominio, [Host] o IP
Per instradare i messaggi inoltrati attraverso un altro server, ad esempio i server MX di un determinato dominio, specificare in questo campo il dominio o l'indirizzo IP. Se si desidera instradare i messaggi a un host specifico, racchiudere il valore tra parentesi (ad es. `[host1.example.com]`).

Accesso/Password AUTH
Immettere le eventuali credenziali di accesso/password necessarie per il server a cui si desidera inoltrare la posta dell'utente.

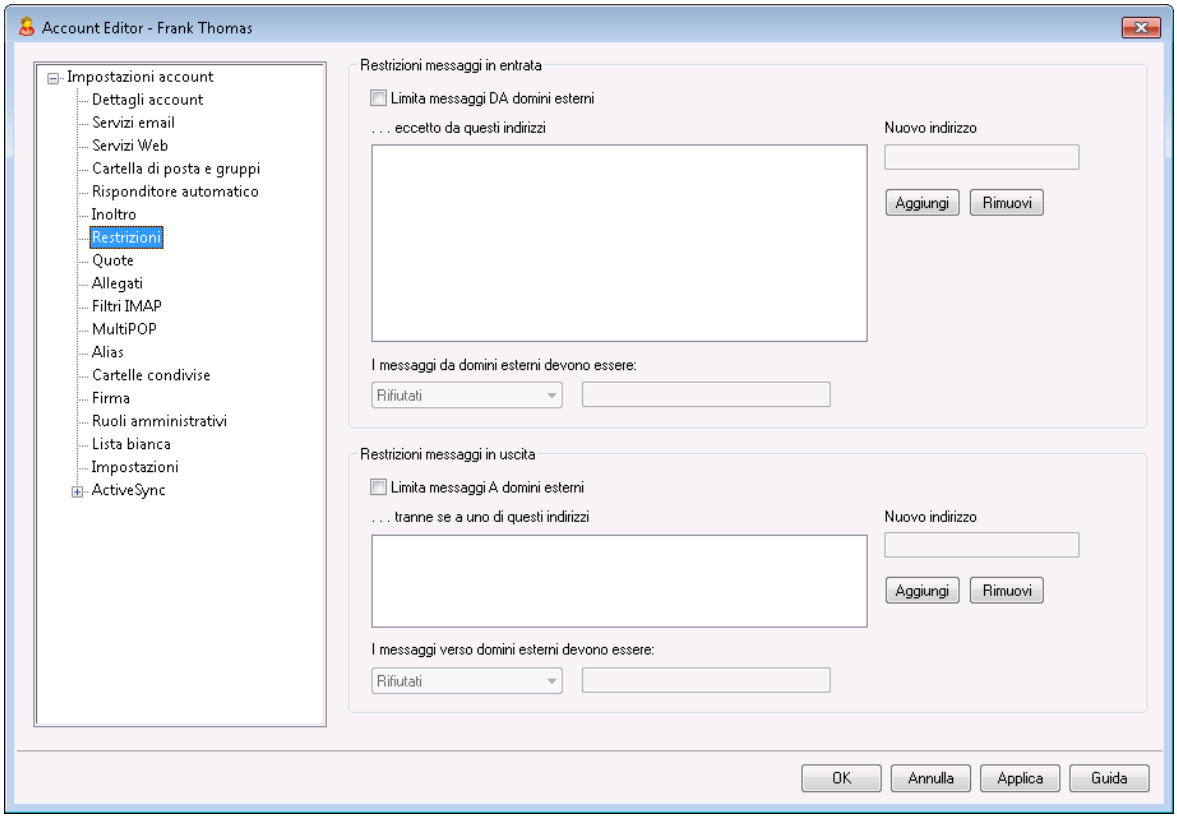
Valore SMTP 'MAIL'
Se si specifica un indirizzo in questa casella, nell'istruzione "`MAIL From`" inviata durante la sessione SMTP con l'host di destinazione verrà utilizzato tale indirizzo invece del mittente effettivo del messaggio. Se si desidera un'istruzione SMTP "`MAIL From`" vuota ("`MAIL FROM <>`") inserire la stringa "[trash]".

Porta (valore predefinito = 25)
MDaemon invierà i messaggi inoltrati mediante la porta TCP specificata in questa casella. Il valore predefinito della porta SMTP è 25.

Conserva copia locale della posta inoltrata
Per impostazione predefinita, una copia di ogni messaggio inoltrato viene consegnata normalmente alla casella postale dell'utente locale. Se si deseleziona questa casella, non viene conservata alcuna copia locale.

Pianificazione
Fare clic su questo pulsante per creare una pianificazione relativa a quando la posta dell'account verrà inoltrata. È possibile impostare una data e un'ora di inizio, una data e un'ora di fine e specificare i giorni della settimana in cui la posta verrà inoltrata.

5.1.1.7 Restrizioni



Le opzioni di questa schermata consentono di definire se l'account potrà o meno inviare o ricevere messaggi e-mail indirizzati o provenienti da domini non locali.

Restrizioni messaggi in entrata

Limita messaggi DA domini esterni
Selezionare questa casella di controllo per impedire all'account di ricevere messaggi e-mail provenienti da domini non locali.

...eccetto da questi indirizzi
Agli indirizzi specificati in quest'area non vengono applicate le restrizioni per i messaggi in entrata. I caratteri jolly sono accettati. Se si specifica "*@altn.com" come eccezione, vengono accettati tutti i messaggi in arrivo provenienti da qualsiasi indirizzo di altn.com.

Nuovo indirizzo
Se si desidera aggiungere un'eccezione di indirizzo all'elenco Restrizioni messaggi in entrata, immetterla qui e fare quindi clic sul pulsante *Aggiungi*.

Aggiungi
Una volta immesso un indirizzo nel campo *Nuovo indirizzo*, fare clic su questo pulsante per aggiungere l'indirizzo all'elenco delle eccezioni.

Rimuovi
Se si desidera rimuovere un indirizzo dall'elenco delle restrizioni, selezionarlo e fare clic su questo pulsante.

I messaggi da domini esterni devono essere:
Le opzioni di questa casella di riepilogo a discesa specificano il comportamento di MDaemon per i messaggi destinati all'account ma provenienti da un dominio non locale . È possibile scegliere una delle opzioni seguenti:

Rifiutati - I messaggi con restrizioni vengono rifiutati da MDaemon.

Restituiti al mittente - I messaggi provenienti da domini con restrizioni vengono restituiti al mittente.

Inviati al postmaster - I messaggi con restrizioni vengono accettati ma recapitati al postmaster invece che all'account.

Inviati a... - I messaggi con restrizioni vengono accettati, ma vengono consegnati all'indirizzo specificato nella casella di testo sulla destra.

Restrizioni messaggi in uscita

Limita messaggi A domini esterni
Selezionare questa casella di controllo per impedire all'account di inviare messaggi e-mail a domini non locali.

...eccetto da questi indirizzi
Agli indirizzi specificati in quest'area non vengono applicate le restrizioni per i messaggi in uscita. I caratteri jolly sono accettati. Se si specifica "*@altn.com" come eccezione, vengono accettati tutti i messaggi in uscita indirizzati a qualsiasi indirizzo di altn.com.

Nuovo indirizzo
Se si desidera aggiungere un'eccezione di indirizzo all'elenco Restrizioni messaggi in uscita, immetterla qui e fare quindi clic sul pulsante *Aggiungi*.

Aggiungi
Una volta immesso un indirizzo nel campo *Nuovo indirizzo*, fare clic su questo pulsante per aggiungere l'indirizzo all'elenco delle eccezioni.

Rimuovi
Se si desidera rimuovere un indirizzo dall'elenco delle restrizioni, selezionarlo e fare clic su questo pulsante.

I messaggi verso domini esterni devono essere:
Le opzioni di questa casella di riepilogo a discesa specificano il comportamento di MDaemon per i messaggi provenienti dall'account ma indirizzati a un dominio non locale . È possibile scegliere una delle opzioni seguenti:

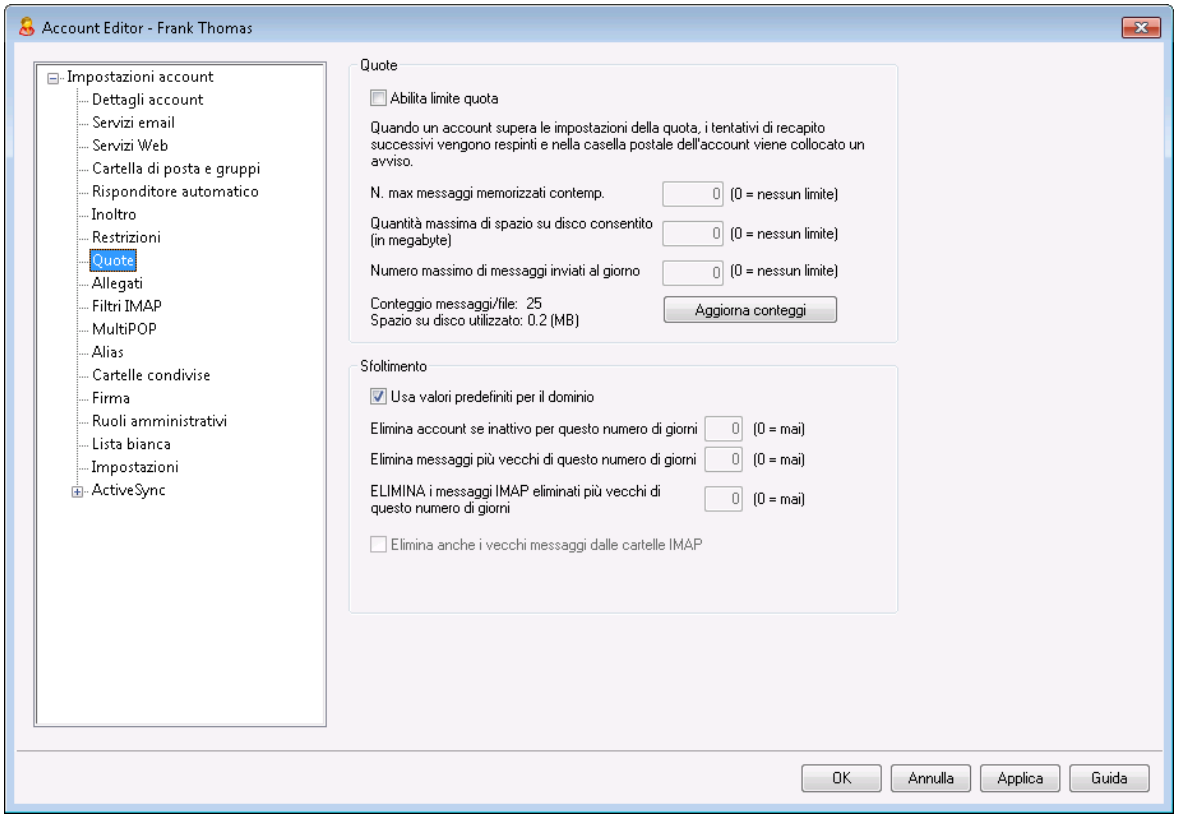
Rifiutati - I messaggi con restrizioni vengono rifiutati da MDaemon.

Restituiti al mittente - I messaggi indirizzati a domini con restrizioni vengono restituiti al mittente.

Inviati al postmaster - I messaggi con restrizioni vengono accettati ma consegnati al postmaster invece che al destinatario designato.

Inviati a... - I messaggi con restrizioni vengono accettati, ma vengono consegnati all'indirizzo specificato nella casella di testo sulla destra.

5.1.1.8 Quote



Quote

Abilita limite quota
Selezionare questa casella per specificare il numero massimo di messaggi che l'account può memorizzare, per impostare la quantità massima di spazio su disco utilizzabile dall'account (inclusi gli allegati dei file della cartella Documenti dell'account) o per definire il numero massimo di messaggi che l'account può inviare al giorno tramite SMTP. Se si tenta di consegnare una quantità di posta superiore ai limiti stabiliti per i messaggi e per lo spazio su disco, il messaggio viene respinto e nella casella postale dell'utente viene collocato un avviso appropriato. Se una raccolta MultiPOP 754 supera il massimo consentito per l'account viene emesso un avviso simile e le voci MultiPOP dell'account vengono disattivate automaticamente, ma non rimosse dal database.

Utilizzare l'opzione *Invia un'e-mail all'utente se viene raggiunta questa percentuale della quota* di "Account » Impostazioni account » Quote 825" affinché venga inviato un messaggio di avviso quando un account si avvicina ai limiti di quota. Quando un account supera il valore percentuale indicato per il limite *Numero massimo di messaggi memorizzati contemporaneamente* o *Massimo spazio su disco consentito*, a mezzanotte riceve un messaggio di avviso. Nel messaggio verranno inclusi il numero di messaggi memorizzati, la dimensione della casella postale, la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato.

Numero massimo di messaggi memorizzati contemporaneamente
Questa opzione consente di specificare il numero massimo dei messaggi che l'account può memorizzare. Il valore "0" indica che il numero di messaggi consentito è illimitato.

Massimo spazio su disco consentito (in megabyte)
Questa opzione consente di indicare la quantità massima di spazio su disco utilizzabile dall'account, inclusi i file allegati che è possibile memorizzare nella cartella Documenti dell'account. Il valore "0" indica che la quantità di spazio su disco consentita è illimitata.

Numero massimo di messaggi inviati al giorno
Questa opzione consente di specificare il numero massimo di messaggi che l'account può inviare al giorno tramite SMTP. Se l'account raggiunge questo limite, i nuovi messaggi inviati dall'account vengono rifiutati fino a quando il contatore non viene azzerato a mezzanotte. Specificare "0" nell'opzione se non si desidera limitare il numero di messaggi che l'account può inviare.

Aggiorna conteggi
Fare clic su questo pulsante per aggiornare le statistiche relative a *Conteggio messaggi/file* e *Spazio su disco utilizzato* visualizzate a sinistra.

Sfoltimento

Le opzioni di questa sezione consentono di specificare quando o se l'account verrà eliminato da MDaemon nel caso diventi inattivo. Consentono inoltre di indicare se i vecchi messaggi dell'account debbano essere eliminati dopo un determinato periodo di tempo. Ogni giorno a mezzanotte, MDaemon rimuove tutti i messaggi che hanno superato i limiti di tempo specificati o elimina completamente l'account, se questo ha raggiunto il limite di inattività.

Usa valori predefiniti per il dominio
Le impostazioni di sfoltimento predefinite sono specifiche dei domini e sono situate nella schermata Impostazioni 216 di Domain Manager. Per sovrascrivere le impostazioni predefinite di dominio per l'account, disabilitare questa casella di controllo e impostare i valori desiderati per le opzioni descritte di seguito.

Elimina account se inattivo per il seguente numero di giorni (0 = mai)
Specificare il numero di giorni per cui si desidera che l'account rimanga inattivo prima di essere eliminato. Con il valore "0", un account non viene mai eliminato per inattività.

Elimina messaggi più vecchi del seguente numero di giorni (0 = mai)
Indica il numero di giorni per cui un determinato messaggio può rimanere nella casella postale dell'account prima di essere eliminato automaticamente. Il valore "0" indica che, anche se di vecchia data, i messaggi non vengono mai eliminati.
Nota: L'impostazione di questa opzione non si applica ai messaggi contenuti nelle cartelle IMAP a meno che non si abiliti anche l'opzione "*Elimina anche i vecchi messaggi dalle cartelle IMAP*" di seguito.

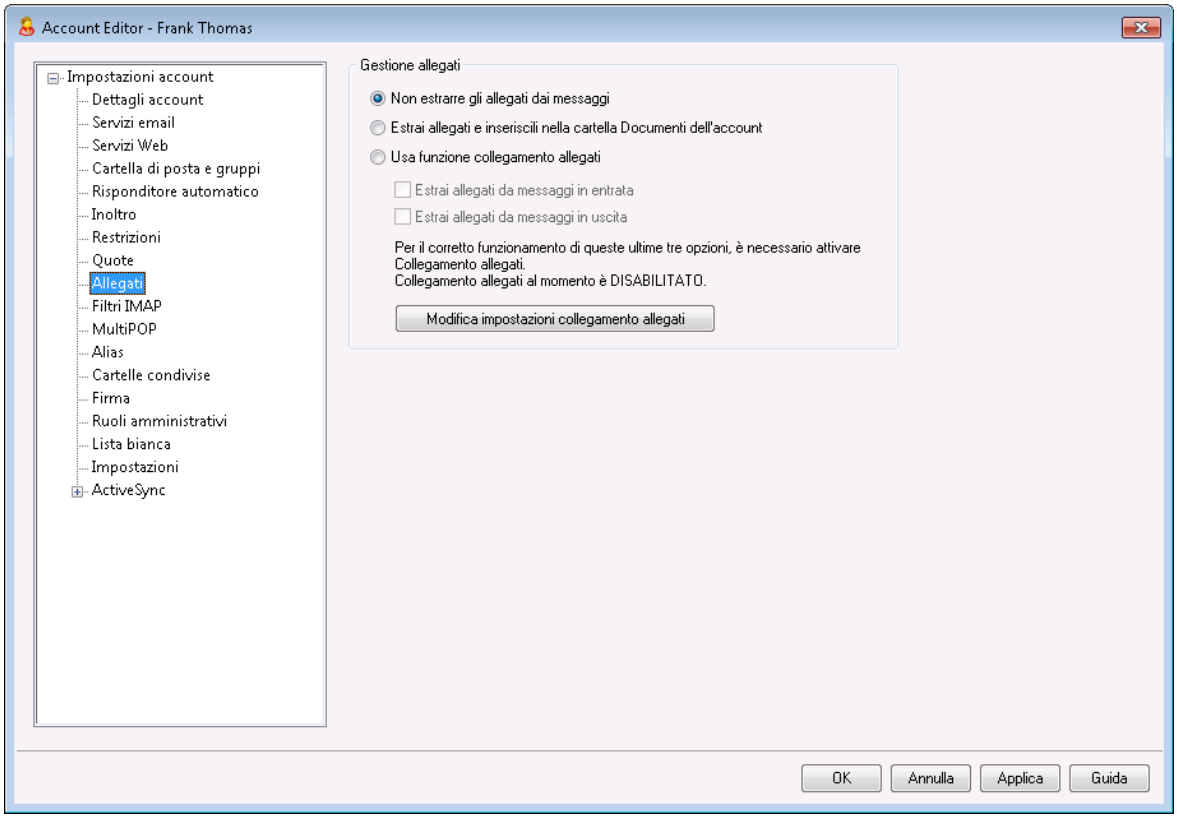
Elimina messaggi IMAP cestinati più vecchi del seguente numero di giorni (0 = mai)
Utilizzare questo comando per specificare il numero di giorni per cui si desidera che i messaggi IMAP contrassegnati per l'eliminazione rimangano nelle cartelle dell'utente. I messaggi contrassegnati per l'eliminazione da un numero di giorni superiore a questo valore vengono eliminati. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Elimina anche i vecchi messaggi dalle cartelle IMAP
Selezionare questa casella di controllo se si desidera applicare l'opzione "*Elimina i messaggi più vecchi del seguente numero di giorni*" anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i normali messaggi contenuti nelle cartelle IMAP non vengono eliminati in base al periodo di permanenza nelle cartelle in questione.

Vedere:

Gestione account » Quote 825
Impostazioni account » Quote 875

5.1.1.9 Allegati



Gestione allegati

Questa schermata viene utilizzata per verificare se MDaemon estrarrà gli allegati dai messaggi e-mail di questo account. È possibile utilizzare Gestione modelli 828 per specificare le impostazioni predefinite per queste opzioni.

Non estrarre gli allegati dai messaggi
Con questa opzione, gli allegati non vengono estratti dai messaggi dell'account. I messaggi con allegati vengono gestiti normalmente e gli allegati rimangono invariati.

Estrai allegati e inseriscili nella cartella Documenti dell'account
Se impostata, questa opzione indica a MDaemon di estrarre automaticamente tutti gli eventuali file incorporati MIME Base64 allegati ai messaggi di posta in arrivo dell'account. I file estratti vengono rimossi dal messaggio in arrivo, decodificati e collocati nella cartella Documenti dell'account. Quindi, nel corpo del messaggio viene inserita una nota, con l'elenco dei nomi dei file estratti. Questa opzione non offre un collegamento agli allegati memorizzati, ma gli utenti possono utilizzare Webmail 325 per accedere alla cartella Documenti.

Usa funzione collegamento allegati
Selezionare questa opzione per utilizzare la funzione Collegamento allegati per i messaggi in entrata o in uscita con allegati.

Se questa opzione è selezionata, ma la funzione Collegamento allegati della finestra di dialogo Collegamento allegati[373] è disabilitata, gli allegati non vengono estratti.

Estrai allegati da messaggi in entrata
Quando questa opzione è attivata, gli allegati vengono estratti dai messaggi in arrivo dell'account e memorizzati nella posizione indicata nella finestra di dialogo Collegamento allegati[373]. I collegamenti URL vengono quindi inseriti nel corpo del messaggio, dove è possibile selezionarli per scaricare i file. Per motivi di sicurezza, i collegamenti URL non contengono i percorsi diretti ai file. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura dei GUID è memorizzata nel file `AttachmentLinking.dat`. L'opzione è abilitata per impostazione predefinita.

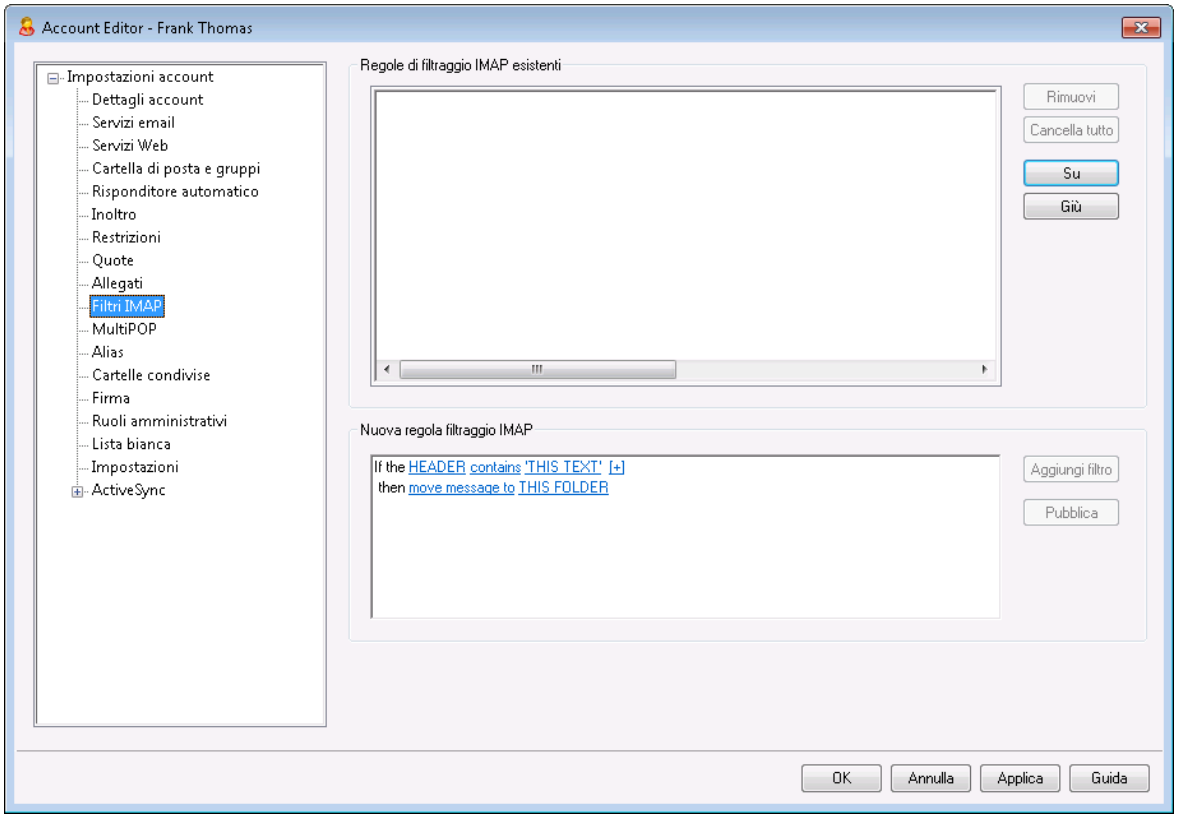
Estrai allegati da messaggi in uscita
Selezionare questa casella per utilizzare la funzione Collegamento allegati per estrarre gli allegati anche dai messaggi in uscita dell'account. Quando l'account invia un messaggio e-mail, Collegamento allegati estrae il file, lo archivia e lo sostituisce con un URL utilizzabile per scaricare il file.

Modifica impostazioni Collegamento allegati
Questo pulsante consente di aprire la finestra di dialogo Collegamento allegati[373].

Vedere:

Collegamento allegati[732]
Gestione modelli » Allegati[828]

5.1.1.10 Filtri IMAP



Gli utenti IMAP e Webmail[325] possono utilizzare i filtri per instradare automaticamente la posta in cartelle specifiche. Analogamente ai filtri di contenuto[659], le intestazioni di ciascun messaggio in entrata dell'account vengono esaminate e confrontate con i filtri definiti per l'account. Quando un messaggio indirizzato al titolare dell'account corrisponde a uno dei filtri, MDaemon lo sposta nella cartella specificata dal filtro in questione, elimina il messaggio o lo reindirizza o lo inoltra all'indirizzo e-mail selezionato. Questo metodo è molto più efficace, sia per il client sia per il server, rispetto al filtro dei messaggi del client e, poiché alcuni client di posta non supportano le regole o il filtro dei messaggi locali, i filtri IMAP consentono di sopperire a tale mancanza.

Gli amministratori possono creare i filtri mediante la schermata Filtri IMAP di Account Editor o utilizzando Remote Administration[359]. Tuttavia è anche possibile concedere agli utenti l'autorizzazione per creare e gestire autonomamente i filtri in Webmail or Remote Administration. Queste autorizzazioni vengono impostate nella schermata Servizi Web[735].

Regole filtro IMAP esistenti

In questa casella viene visualizzato l'elenco di tutte le regole di filtro create per l'account dell'utente. I filtri vengono elaborati nell'ordine in cui sono elencati fino al rilevamento di una corrispondenza. Di conseguenza, quando un messaggio corrisponde a uno dei filtri, viene spostato nella cartella specificata nel filtro stesso e l'elaborazione dei filtri per tale messaggio viene terminata. Utilizzare i pulsanti *Su* e *Giù* per spostare i filtri all'interno dell'elenco.

Rimuovi
Selezionare un filtro, quindi fare clic su *Rimuovi* per eliminarlo dall'elenco.

Cancella tutto
Fare clic su questo pulsante per eliminare tutti i filtri dell'utente.

Su
Selezionare un filtro, quindi scegliere questo pulsante per spostarlo più in alto all'interno dell'elenco.

Giù
Selezionare un filtro, quindi scegliere questo pulsante per spostarlo più in basso all'interno dell'elenco.

Nuova regola filtro IMAP

Utilizzare i collegamenti in quest'area per creare una nuova regola di filtro. Quando la regola è completa, fare clic su **Aggiungi filtro** per aggiungerla alle *regole di filtraggio IMAP esistenti*.

Condizioni filtro

Fare clic sui collegamenti nella prima sezione della regola di filtraggio per impostare le condizioni del filtro. Quando un messaggio corrisponde alle condizioni del filtro, viene eseguita l'azione di filtro.

INTESTAZIONE
Fare clic su "**HEADER"** per scegliere l'intestazione o un altro componente del messaggio che si desidera esaminare come parte della regola di filtro. È possibile scegliere: **TO**, **CC**, **FROM**, **SUBJECT**, **SENDER**, **LIST-ID**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE**, **MESSAGE BODY** o **Altro...** Se si sceglie "Altro..." verrà visualizzata una casella Condizione filtro che consente di specificare il nome di un'intestazione non presente in elenco. Se si fa clic su MESSAGE SIZE, i collegamenti "contiene" e "QUESTO TESTO" saranno sostituiti da "è maggiore di" e "0 KB" rispettivamente.

contiene/è maggiore di
Fare clic su "**contiene**" o su **è maggiore di** per scegliere che tipo di condizione impostare quando viene esaminata l'intestazione. Ad esempio, l'intestazione esiste o non esiste, contiene o non contiene un determinato testo, inizia o termina con un determinato testo e così via. È possibile scegliere una delle seguenti condizioni: **inizia con**, **finisce con**, **è uguale a**, **non è uguale a**, **contiene**, **non contiene**, **esiste**, **non esiste**, **è maggiore di** o **è minore di**. Le opzioni "è maggiore di" ed "è minore di" sono disponibili solo quando il collegamento INTESTAZIONE è impostato su "MESSAGE SIZE".

QUESTO TESTO/0 KB
Immettere il testo da cercare durante la scansione dell'intestazione selezionata per il filtro. Quando l'opzione INTESTAZIONE è impostata su MESSAGE SIZE, il collegamento riporterà "0 KB" e nella finestra di dialogo Condizione filtro sarà visualizzata una casella "Dimensione messaggio in KB."

[+] [x] and
Fare clic su **[+]** se si desidera impostare due o più condizioni per la regola di filtro. In questo modo verrà aggiunta un'altra riga contenente i componenti "INTESTAZIONE", "contiene" e "QUESTO TESTO" per espandere il filtro. Durante la verifica di un messaggio rispetto a una regola di filtro con più condizioni, per impostazione predefinita il messaggio deve soddisfare ciascuna delle condizioni perché corrisponda alla regola. Fare clic su "**and**" e quindi selezionare "**or**" se si desidera che il messaggio corrisponda alla regola quando soddisfa una delle condizioni. Quando una regola di filtro ha più righe, è possibile fare clic su **[x]** vicino a qualsiasi riga che si desidera eliminare.

Azioni filtro

Fare clic sui collegamenti nella sezione inferiore della regola di filtraggio per indicare le azioni da intraprendere quando un messaggio soddisfa le condizioni del filtro.

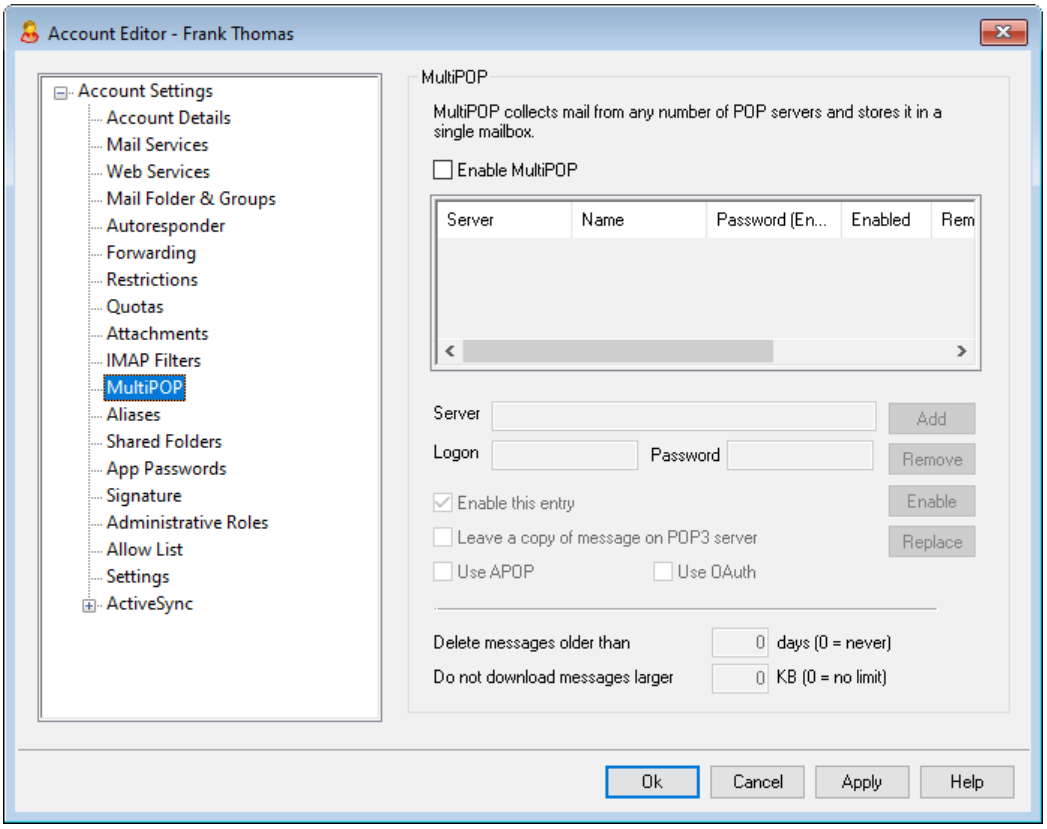
sposta messaggio in
Fare clic su "**sposta messaggio in**" per specificare l'azione del filtro. È possibile scegliere: **sposta messaggio in**, **elimina messaggio**, **reindirizza messaggio a** o **inoltra messaggio a**.

QUESTA CARTELLA/E-MAIL
Se si è selezionata l'azione "sposta messaggio in", fare clic su **QUESTA CARTELLA** per indicare in quale cartella deve essere spostato il messaggio. Se si sceglie di reindirizzare o inoltrare il messaggio, fare clic su **E-MAIL** e specificare l'indirizzo e-mail del destinatario. Per i messaggi reindirizzati non vengono apportate modifiche all'intestazione o al corpo del messaggio. Le uniche modifiche apportate interessano il destinatario della busta SMTP. Per i messaggi inoltrati, viene creato e inviato un nuovo messaggio con l'intestazione Subject e il contenuto del messaggio originale.

Aggiungi Filtro
Quando si è completata la creazione del nuovo filtro, fare clic su questo pulsante per aggiungerlo alle *Regole di filtraggio IMAP esistenti*.

Pubblica
Dopo aver creato una regola, fare clic su **Pubblica** se si desidera copiare la regola su ogni account utente del dominio dell'account. Verrà chiesto di confermare la decisione di copiare la regola sugli altri account.

5.1.1.11 MultiPOP



La funzione MultiPOP consente di creare un numero illimitato di combinazioni host/utente/password POP3 per la raccolta di messaggi di posta provenienti da più origini. Si tratta di uno strumento utile per gli utenti che dispongono di account di posta su più server ma preferiscono raccogliere tutta la posta in un'unica postazione. Prima di essere collocata nella casella postale dell'utente, la posta MultiPOP raccolta viene inserita nella coda di posta per l'elaborazione, analogamente a tutti i messaggi per cui sono stati applicati la risposta automatica e i filtri di contenuto. Le opzioni di pianificazione della funzione MultiPOP sono disponibili in: Impostazioni » Pianificazione eventi » Pianificazione della posta » Raccolta MultiPOP 391.

Abilita MultiPOP
Abilitare questa casella per consentire l'elaborazione MultiPOP per l'account. Se si desidera consentire all'utente di modificare le proprie impostazioni MultiPOP in MDRA 359, selezionare l'opzione "*...modificare le opzioni MultiPOP*" nella pagina Servizi Web 735 dell'account. Quando questa opzione e l'opzione dei servizi web sono entrambe attivate, la pagina Cassette postali sarà disponibile in Webmail 325 e consentirà all'utente di gestire le opzioni della cassetta postale MultiPOP. L'opzione globale per attivare/disattivare il server MultiPOP è disponibile in: Impostazioni » Impostazioni server » MultiPOP 146. Se l'opzione è disattivata, non è possibile utilizzare MultiPOP, anche quando l'opzione per l'account è attivata.

Creazione o modifica di una voce MultiPOP

Server
Immettere il server POP3 da cui si desidera raccogliere la posta. Se il server richiede la connessione a una porta specifica diversa dalle porte POP3 standard, aggiungere ":`[porta]`" al nome del server. Ad esempio, "`mail.esempio.com:1000`". Quando si raccoglie la posta da Gmail o da Microsoft (Office) 365, utilizzare "`pop.gmail.com:995`" o "`outlook.office365.com:995`", rispettivamente.

ID utente
Inserire il nome o l'ID utente POP3 associato all'account di posta del server specificato precedentemente.

Password
Immettere la password POP3 o APOP con cui accedere all'account di posta sul server specificato.

Usa APOP
Selezionare questa casella di controllo affinché la voce MultiPOP utilizzi il metodo di autenticazione APOP quando viene ritirata la posta dall'host corrispondente.

Utilizzo di OAuth
Scegliere questo metodo di autenticazione quando si raccoglie la posta da Gmail o Office365. Per ulteriori informazioni, vedere le istruzioni su MultiPOP OAuth 2.0 146 nella pagina Impostazioni server » MultiPOP. **Nota:** anche l'opzione "*...modificare le impostazioni MultiPOP*" nella pagina Servizi Web 735 dell'account deve essere attivata per consentire l'utilizzo di utilizzare OAuth con Gmail o Office 365, poiché l'utente deve accedere a Webmail e passare alla pagina **Cassette postali** per autenticare la voce della cassetta postale Gmail o Office 365.

Lascia copia del messaggio sul server POP3
Selezionare questa casella di controllo per lasciare sul server una copia dei messaggi raccolti. Questa funzione è particolarmente utile se si prevede di ritirare in un secondo momento gli stessi messaggi da una postazione diversa. Se si desidera escludere questa opzione per tutti gli utenti, in modo che i messaggi vengano sempre eliminati dal server POP dopo essere stati scaricati su MDaemon, attivare l'opzione "*MultiPOP elimina sempre le mail da tutti i server dopo la raccolta*" in Impostazioni » Impostazioni server » MultiPOP 146.

Aggiungi
Dopo aver inserito tutte le informazioni relative alla nuova voce MultiPOP, per aggiungerla all'elenco fare clic su questo pulsante.

Rimuovi
Per eliminare una delle voci MultiPOP, selezionarla e fare clic su questo pulsante.

Abilita/disabilita
Facendo clic su questo pulsante, si attivano/disattivano le voci MultiPOP selezionate, consentendo di indicare a MDaemon di raccogliere la posta relativa a questa voce o di ignorarla quando esegue l'elaborazione MultiPOP.

Sostituisci
Per modificare una voce, selezionarla nell'elenco, apportare le modifiche desiderate e fare clic sul pulsante per salvare le modifiche alla voce.

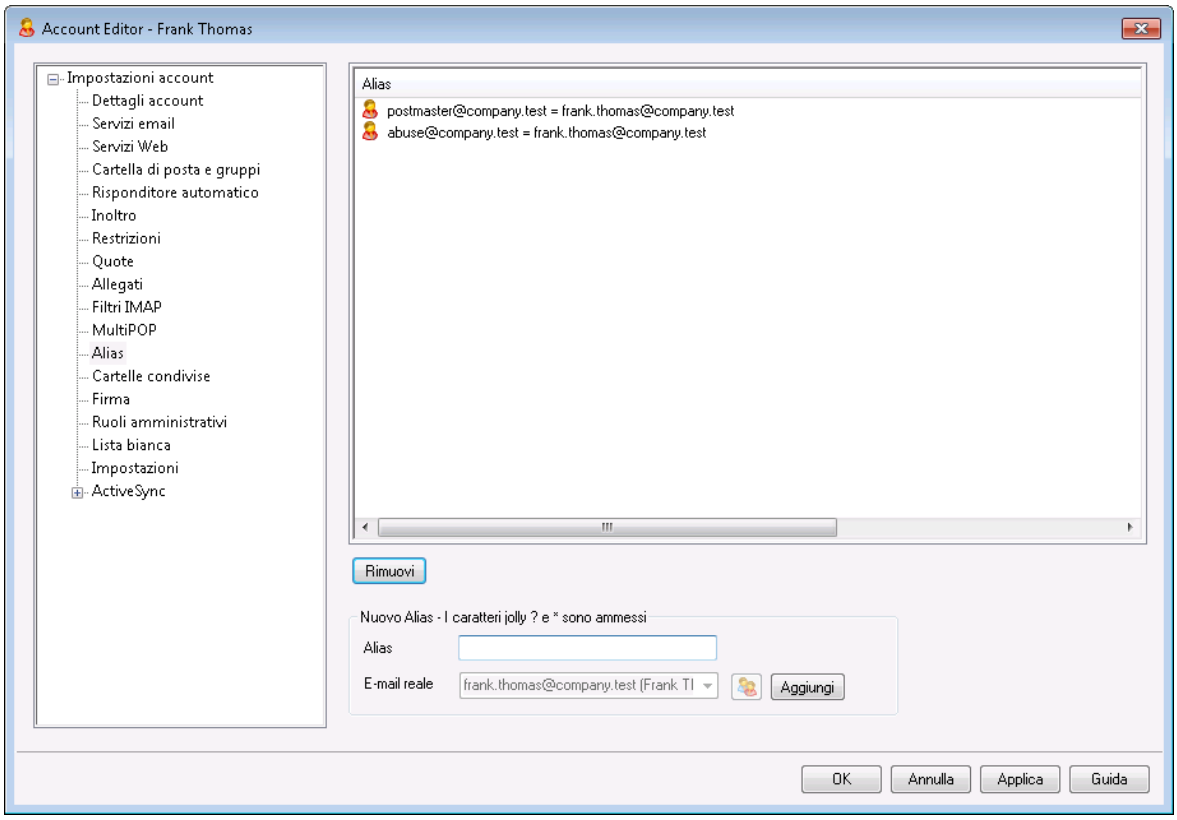
Elimina messaggi più vecchi di XX giorni (0 = mai)
Specificare il numero di giorni per cui si desidera conservare i messaggi nell'host MultiPOP prima di eliminarli. Inserire "0" se non si desidera eliminare alcun messaggio.

Non scaricare messaggi più grandi di [XX] KB (0 = senza lim.)
Immettere un valore in questo campo per limitare la dimensione dei messaggi da scaricare.

Vedere:

Impostazioni server » MultiPOP 146
Pianificazione della raccolta MultiPOP 391

5.1.1.12 Alias



Nella schermata sono elencati tutti gli alias[847] degli indirizzi associati con l'account ed è possibile effettuare aggiunte o rimozioni.

Rimozione di un alias

Per rimuovere un alias dall'account, selezionarlo nell'elenco e fare clic su **Rimuovi**.

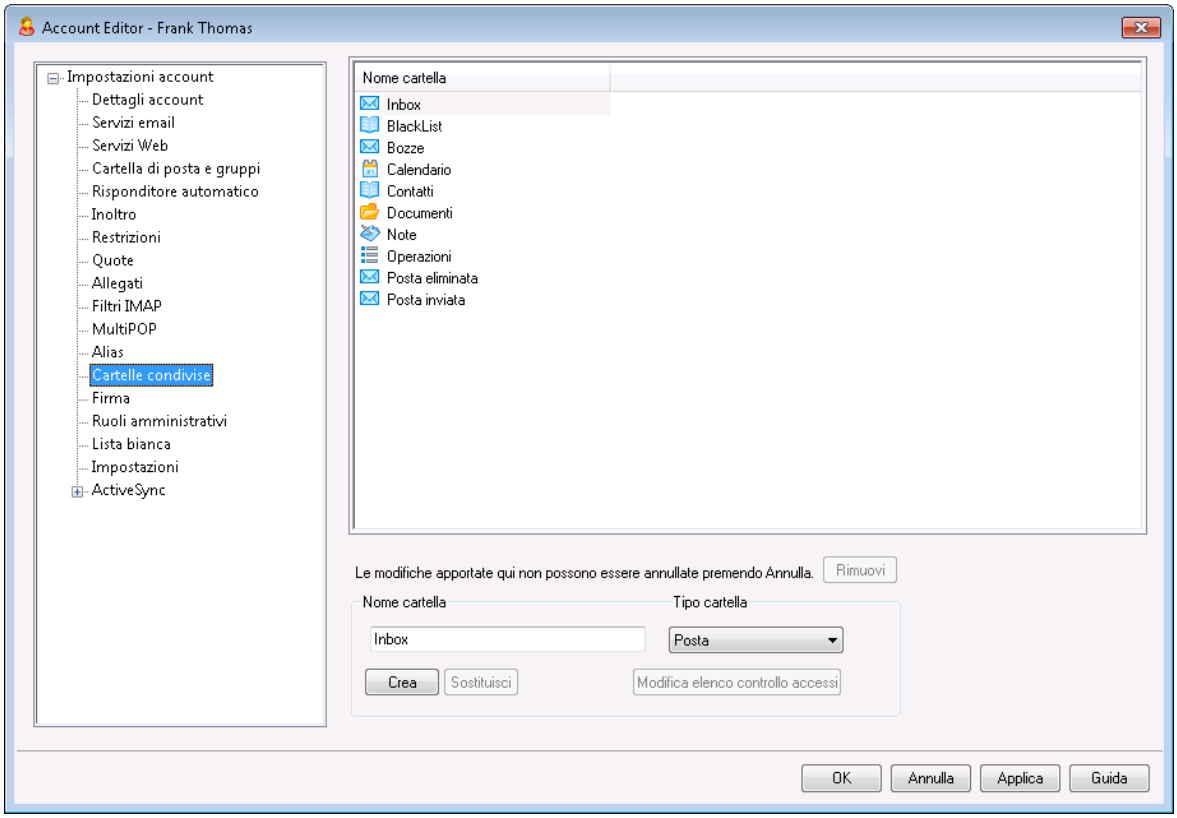
Aggiunta di un alias

Per aggiungere un nuovo alias all'account, digitare nella casella *Alias* l'indirizzo che si desidera associare con l'account e fare clic su **Aggiungi**. Sono consentiti i caratteri jolly "?" e "*" che rappresentano, rispettivamente, singoli caratteri e singole parole.

Vedere:

Impostazioni account » Alias[847]

5.1.1.13 Cartelle condivise



Questa schermata è disponibile solo se è stata selezionata l'opzione *Abilita cartelle pubbliche* della schermata Cartelle

> pubbliche e condivise[122], disponibile in Impostazioni » Impostazioni server » Cartelle pubbliche e condivise. Le cartelle pubbliche si possono gestire da Gestione cartelle pubbliche[317].

La sezione superiore consente di visualizzare tutte le cartelle IMAP dell'utente e può essere utilizzata per condividere l'accesso alle cartelle con altri utenti o Gruppi[796] di MDaemon. Quando l'account viene creato per la prima volta, l'area conterrà solo la cartella Posta in arrivo finché non si utilizzano le opzioni *Nome cartella* e *Crea* o le opzioni disponibili in Filtri IMAP[751] per aggiungervi una cartella. Nelle sottocartelle presenti in questo elenco, i nomi della cartella e della sottocartella sono separati dal carattere barra "/".

Rimuovi
Per rimuovere dall'elenco una cartella IMAP condivisa, selezionarla e fare clic sul pulsante *Rimuovi*.

Nome cartella
Per aggiungere una nuova cartella all'elenco, immetterne il nome in questo campo e fare clic su *Crea*. Se si desidera che la nuova cartella sia una sottocartella di una di quelle in elenco, fare precedere al nome della nuova cartella il nome di quella principale e il carattere barra ("/"). Ad esempio, se la cartella principale è "Cartella personale", il nome della nuova sottocartella è "Cartella personale/Nuova cartella personale". Se non si desidera che la nuova cartella sia una sottocartella, assegnare il nome "Nuova cartella personale" senza il prefisso.

Tipo cartella
Utilizzare questo elenco a discesa per scegliere il tipo di cartella da creare: Posta, Calendario, Contatti e così via.

Crea
Una volta specificato il nome di una cartella, fare clic su questo pulsante per aggiungere la cartella all'elenco.

Sostituisci
Per modificare una delle cartelle condivise, selezionare la voce e apportare le modifiche desiderate, quindi fare clic su *Sostituisci.*.

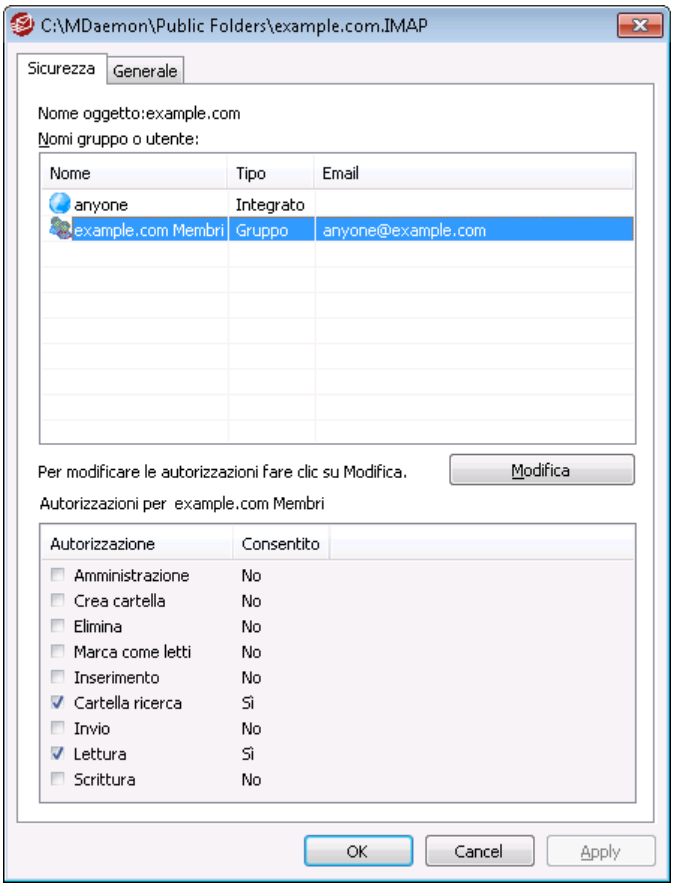
Modifica elenco controllo accessi
Selezionare una cartella e fare clic su questo pulsante per aprire la finestra di dialogo Elenco controllo accessi[319] per la cartella. Utilizzare la finestra di dialogo Elenco controllo accessi per specificare gli utenti o i gruppi a cui sarà consentito accedere alla cartella, nonché le rispettive autorizzazioni.

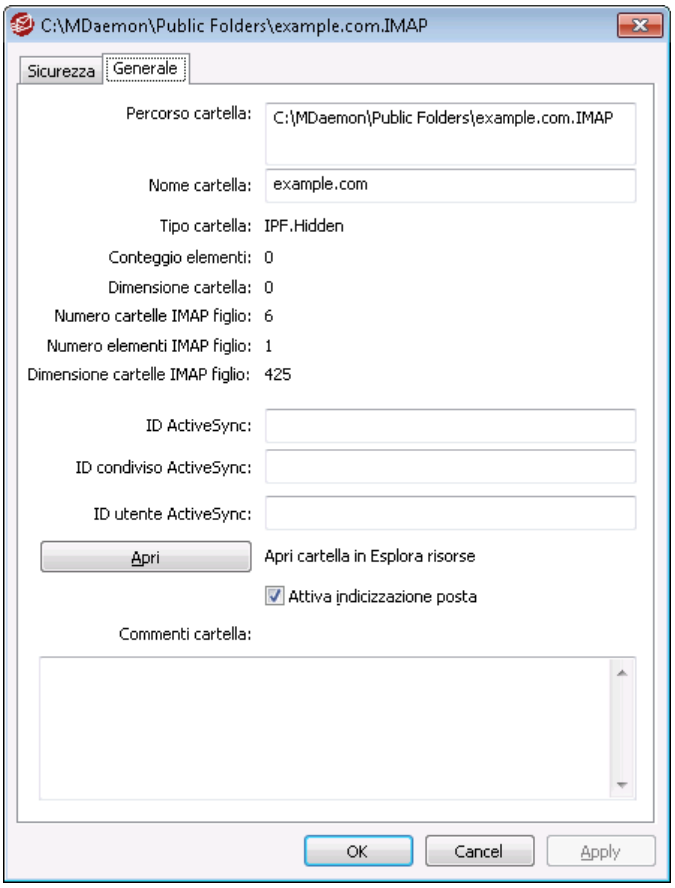
Vedere:

Elenco controllo accessi[319]
Gestione cartelle pubbliche[317]

5.1.1.13.1 Elenco controllo accessi

L'Elenco controllo accessi (ACL) viene utilizzato per impostare le autorizzazioni di accesso di utenti o gruppi alle cartelle pubbliche e condivise[120]. È possibile accedervi mediante il pulsante *Modifica ACL* in Gestione cartelle pubbliche[317] o mediante il pulsante *Modifica elenco controllo accessi* nella schermata Cartelle condivise[757] di Account Editor.





Sicurezza

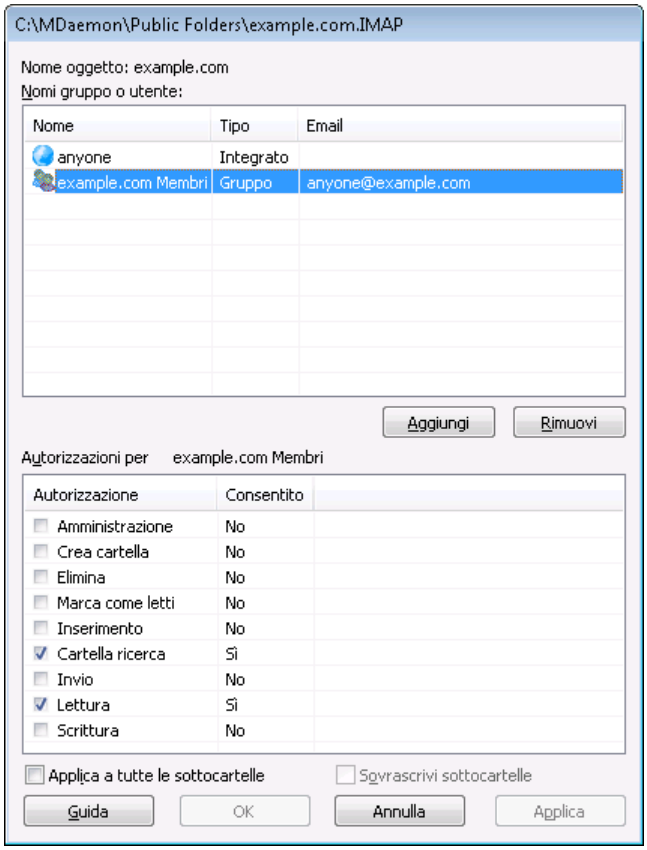
Questa scheda consente di visualizzare l'elenco di gruppi o utenti associati alla cartella e le autorizzazioni di accesso specifiche concesse a ciascuno di essi. Selezionare un gruppo o un utente nell'elenco per visualizzare le relative autorizzazioni 322 ed esaminarle nella finestra Autorizzazioni riportata di seguito. Per modificare le autorizzazioni, fare clic su **Modifica** 321.

Generale

Questa scheda consente di visualizzare le proprietà delle cartelle, come percorso, nome, tipo, dimensioni e così via.

Editor ACL

Fare clic su **Modifica** nella scheda Sicurezza dell'ACL per aprire l'Editor ACL per la modifica delle autorizzazioni di accesso.



Nome oggetto
Nome dell'oggetto o della cartella alla quale si applicano le autorizzazioni per l'ACL.

Nomi gruppo o utente
Sono i gruppi o gli utenti ai quali possono essere state concesse autorizzazioni di accesso di specifici livelli. Selezionare un gruppo o un utente per visualizzare le relative autorizzazioni nella finestra *Autorizzazioni per <gruppo o utente>* riportata di seguito. Selezionare la casella situata accanto alle autorizzazioni di accesso che si desidera concedere all'utente o al gruppo.

Aggiungi
Per concedere le autorizzazioni di accesso a un gruppo o un utente non presente nell'elenco, fare clic su **Aggiungi**.

Rimuovi
Per rimuovere un gruppo o un utente, selezionare la voce nell'elenco riportato sopra e fare clic su **Rimuovi**.

Autorizzazioni per <gruppo o utente>
Selezionare la casella situata accanto alle autorizzazioni di accesso che si desidera concedere all'utente o al gruppo selezionato sopra.

È possibile concedere le autorizzazioni di controllo dell'accesso seguenti:

Amministrazione - L'utente è in grado di amministrare l'ACL (Access Control List) relativo alla cartella.

Creazione - L'utente è in grado di creare delle sottocartelle della cartella.

Eliminazione - L'utente è in grado di eliminare elementi dalla cartella.

Contrassegno come letto - L'utente è in grado di modificare lo stato letto/non letto dei messaggi presenti nella cartella.

Inserimento - L'utente è in grado di allegare e copiare i messaggi nella cartella.

Ricerca cartella - L'utente è in grado di visualizzare la cartella nel proprio elenco personale di cartelle IMAP.

Invio - L'utente è in grado di inviare la posta direttamente alla cartella, se quest'ultima lo consente.

Lettura - L'utente è in grado di aprire la cartella e visualizzarne il contenuto.

Scrittura - L'utente è in grado di modificare i flag applicati ai messaggi della cartella.

Applica a tutte le sottocartelle
Selezionare questa casella per applicare le autorizzazioni di controllo accessi della cartella a tutte le sottocartelle in essa contenute. In questo modo si aggiungeranno le autorizzazioni dell'utente o del gruppo alle sottocartelle, sostituendole in caso di eventuali conflitti. Non si elimineranno tuttavia altre autorizzazioni di utenti o gruppi che hanno attualmente accesso a tali cartelle.

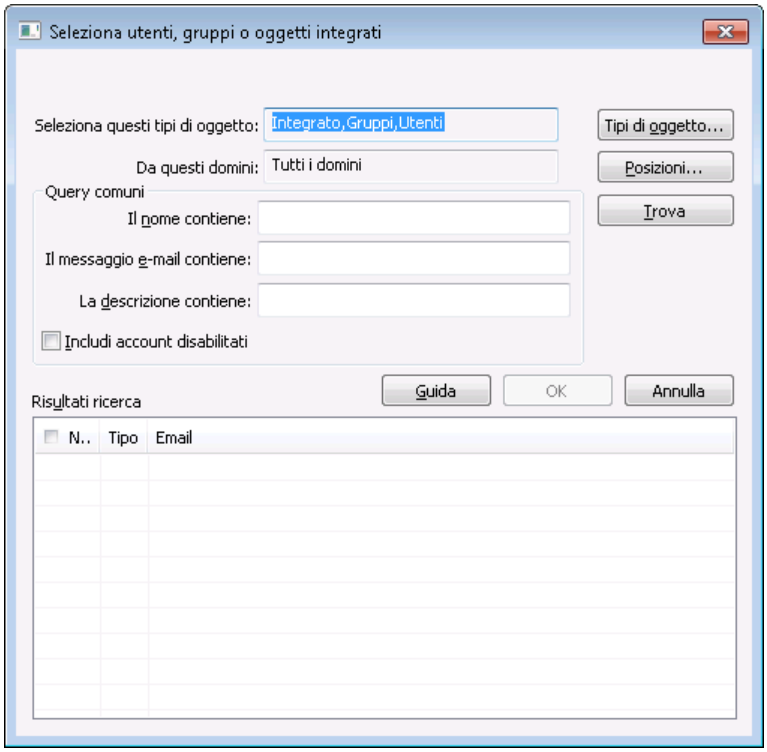
Esempio:

La cartella principale concede determinate autorizzazioni all'`Utente_A` e all'`Utente_B`. La sottocartella concede autorizzazioni all'`Utente_B` e all'`Utente_C`. Questa opzione consente di aggiungere le autorizzazioni dell'`Utente_A` alla sottocartella, sostituire le autorizzazioni dell'`Utente_B` della sottocartella con quelle della cartella principale e lasciare inalterate le autorizzazioni dell'`Utente_C`. Pertanto la sottocartella disporrà delle autorizzazioni per l'`Utente_A`, l'`Utente_B` e l'`Utente_C`.

Sovrascrivi sottocartelle
Selezionare questa casella se si desidera sostituire tutte le autorizzazioni di accesso della sottocartella con le autorizzazioni di accesso della cartella principale. Le autorizzazioni della sottocartella saranno quindi identiche a quelle della cartella principale.

Aggiunta di un gruppo o di un utente

Fare clic su **Aggiungi** nell'Editor ACL se si desidera aggiungere un altro utente o un altro gruppo all'elenco controllo accessi. Viene quindi aperta la schermata Aggiunta gruppo o utente che è possibile utilizzare per cercare e aggiungere utenti e gruppi.



Selezionare questi tipi di oggetti
Fare clic su **Tipi di oggetto...** per selezionare i tipi di oggetto all'interno dei quali si desidera cercare i gruppi o gli utenti da aggiungere. È possibile selezionare: Integrati, Gruppi e Utenti.

Da queste posizioni
Fare clic su **Posizioni...** per selezionare i domini nei quali si desidera cercare. È possibile selezionare tutti i domini MDaemon o domini specifici.

Interrogazioni comuni
Utilizzare le opzioni presenti in questa sezione per restringere la ricerca specificando in tutto o in parte nome dell'utente, indirizzo e-mail o i contenuti della Descrizione[729] dell'account. Lasciare vuoti questi campi se si desidera che i risultati della ricerca contengano tutti i gruppi e gli utenti corrispondenti ai Tipi di oggetto e alle Posizioni specificati sopra.

Includi account disabilitati
Selezionare questa casella di controllo se si desidera includere gli account disabilitati[729] nella ricerca.

Trova
Dopo aver specificato tutti i criteri di ricerca, fare clic su **Trova** per eseguire la ricerca.

Risultati ricerca
Dopo aver eseguito la ricerca, selezionare gli utenti o i gruppi desiderati nei Risultati della ricerca e fare clic su **OK** per aggiungerli all'ACL.

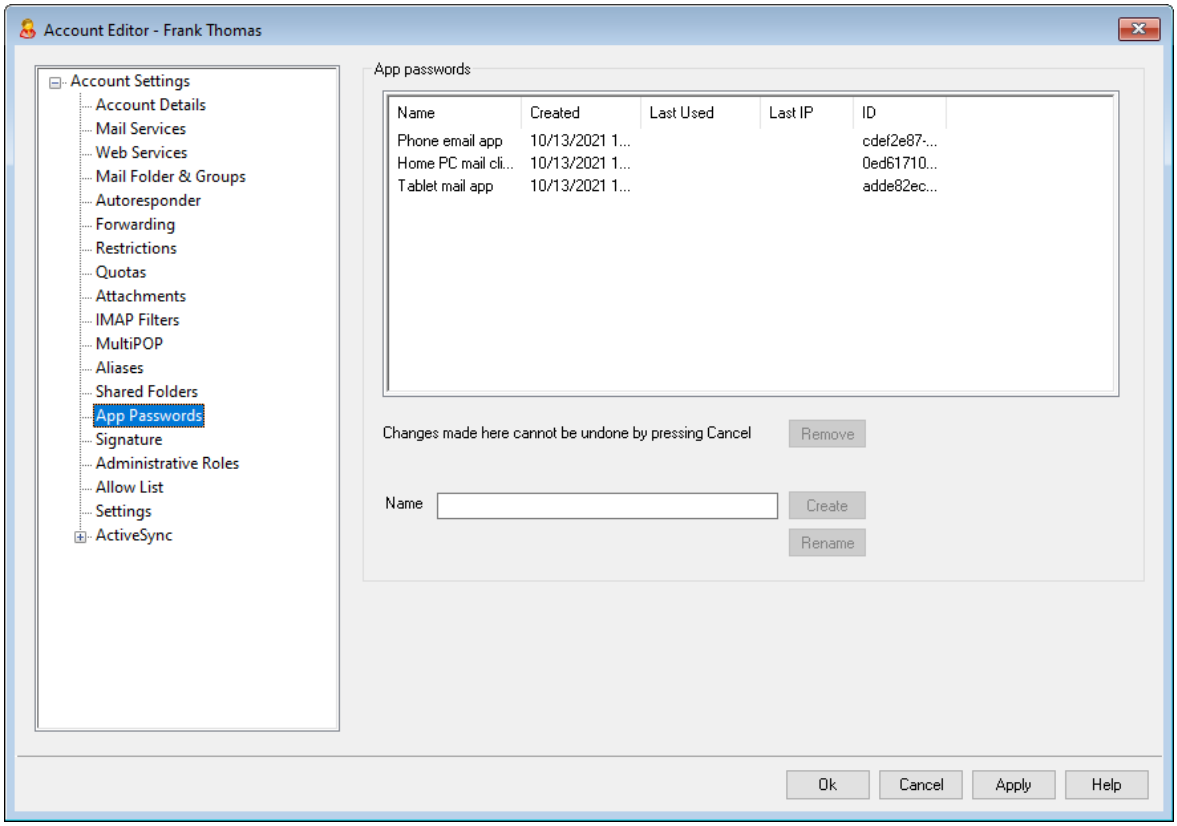
I diritti di accesso vengono controllati mediante le funzioni di supporto ACL (Access Control List) di MDaemon. Queste funzioni sono un'estensione del protocollo Internet Message Access Protocol (IMAP4) che consente di creare un elenco di accesso per ogni cartella di messaggi IMAP disponibile, accordando diritti di accesso a tali cartelle anche agli altri utenti che dispongono di un account sullo stesso server di posta. Se il client e-mail in uso non supporta ACL, è comunque possibile impostare le autorizzazioni mediante i comandi di questa finestra di dialogo.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo http://www.rfc-editor.org/rfc/rfc2086.txt.

Vedere:

Gestione cartelle pubbliche 317
Panoramica sulle cartelle pubbliche 120
Cartelle pubbliche e condivise 122
Account Editor » Cartelle condivise 757
Lista distribuzione » Cartelle pubbliche 306

5.1.1.14 Password di applicazione



Password di applicazione

Le password di applicazione sono password molto sicure, generate in modo casuale, da utilizzare nei client e nelle applicazioni di posta elettronica, per contribuire a rendere più sicure le applicazioni di posta elettronica che non possono essere protette da autenticazione a due fattori 735 (2FA). La 2FA è un metodo sicuro che gli utenti possono utilizzare per accedere a Webmail o a MDaemon Remote Administration (MDRA), ma un'applicazione di posta elettronica non può utilizzarla, poiché deve essere in grado di accedere alla posta elettronica in background senza che l'utente debba inserire un codice dall'applicazione di autenticazione. Le funzionalità delle password di applicazione consente di creare password solide e sicure da utilizzare nelle applicazioni, mantenendo la password dell'account protetta da 2FA. Le password di applicazione si possono utilizzare solo nelle applicazioni di posta elettronica, non è possibile utilizzarle per accedere a Webmail o MDRA. Ne consegue che, anche se una password di applicazione venisse in qualche modo compromessa, l'utente non autorizzato non sarebbe comunque in grado di accedere all'account dell'utente legittimo e modificare la password o altre impostazioni, mentre l'utente legittimo sarà comunque in grado di accedere all'account con la password dell'account e la 2FA per eliminare la password dell'applicazione compromessa e crearne una nuova, se necessario.

Se non si desidera consentire a un utente di utilizzare la funzionalità delle password di applicazione, è possibile disattivare l'opzione *...modificare password di applicazione* 735 nella pagina Servizi Web dell'utente. Se si desidera disattivare il

supporto per le password di applicazione per tutti gli utenti, utilizzare l'opzione *Attiva password applicazione* 870 nella pagina Password.

Requisiti e raccomandazioni per la password di applicazione

- Per creare le password di applicazione, è necessario che la 2FA sia attivata per l'account (anche se si può eliminare questo requisito 870 se necessario).
- Le password di applicazione si possono utilizzare solo nelle applicazioni di posta elettronica, non è possibile utilizzarle per accedere a Webmail o MDRA.
- Ogni password di applicazione viene visualizzata solo una volta, al momento della creazione. Non sarà possibile recuperarla in un secondo momento, quindi gli utenti devono essere pronti a immettere la password nella propria applicazione quando questa viene creata.
- Gli utenti devono utilizzare una password di applicazione diversa per ogni applicazione di posta elettronica e devono revocare (eliminare) la password ogni volta che smettono di utilizzare un'applicazione o quando il dispositivo viene smarrito o rubato.
- Per ogni password di applicazione viene specificato il momento della creazione, quando è stata utilizzata per l'ultima volta e l'indirizzo IP da cui è stato effettuato l'ultimo accesso all'e-mail dell'account. Se un utente rileva qualcosa di sospetto nei dati relativi all'ultimo utilizzo o all'ultimo IP, deve revocare la password e crearne una nuova per la propria applicazione.
- Quando si cambia la password di un account, tutte le password di applicazione vengono eliminate automaticamente: l'utente non può continuare a usare le password di applicazione precedenti.

Creazione e utilizzo delle password di applicazione

In genere gli utenti creano e gestiscono le proprie password di applicazione dall'interno di Webmail seguendo la procedura descritta di seguito (queste informazioni sono riportate nel file di guida di Webmail). Prima di iniziare, l'utente deve avere l'applicazione o il client di posta elettronica pronto per l'immissione della password, perché la password di applicazione verrà visualizzata una sola volta durante la creazione.

1. Preparare l'applicazione o il client di posta elettronica per l'immissione della password di applicazione.
2. Accedere a Webmail e fare clic su **Opzioni » Sicurezza**.
3. Immettere la password dell'account in **Password corrente**.
4. Fare clic su **Nuova password di applicazione**.
5. Immettere il nome dell'applicazione che utilizzerà questa password (ad esempio, "Applicazione e-mail telefono") e fare clic su **OK**.
6. Copiare/incollare o immettere manualmente la password visualizzata nell'applicazione e-mail oppure incollarla in un file di testo o prenderne nota, se necessario. Se si copia la password per utilizzarla in seguito, eliminare la copia dopo l'immissione nel client di posta elettronica. Al termine, fare clic su **OK**.

Se per qualche motivo si rivela necessario creare o eliminare una password di applicazione per uno degli utenti, è possibile utilizzare le opzioni presenti in questa

pagina. Proprio come in Webmail, la password di applicazione verrà visualizzata una sola volta al momento della creazione, quindi deve essere immessa immediatamente nell'applicazione o copiata e fornita all'utente in un secondo momento.

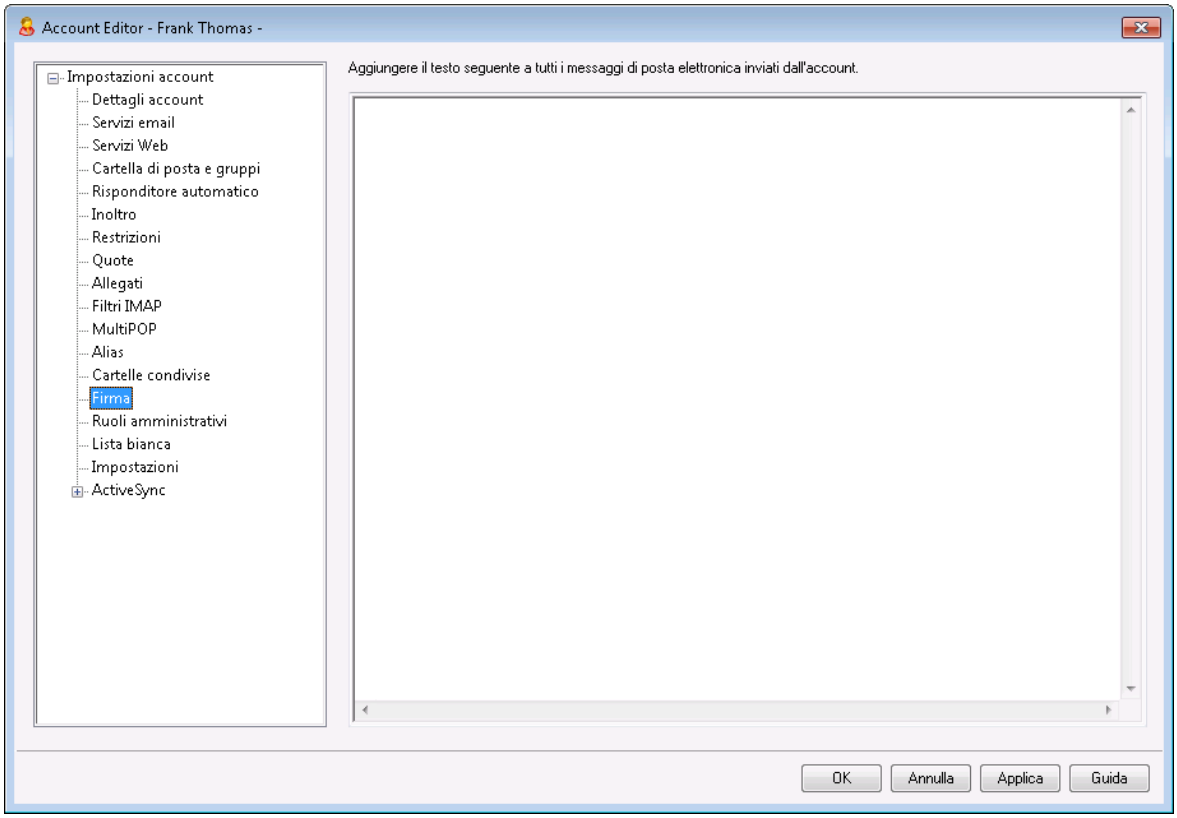
Nella pagina di impostazioni di Account Editor 776 è disponibile un'opzione per gli account: "*Richiedi la password di applicazione per l'accesso a SMTP, IMAP, ActiveSync, ecc.*".

La richiesta di password di applicazione può aiutare a proteggere le password degli account da attacchi a dizionario e a forza bruta via SMTP, IMAP, ecc. La sicurezza è garantita dal fatto che, ove mai con un attacco di questo tipo si riuscisse a indovinare la password reale di un account, questa non funzionerebbe senza che l'aggressore possa accorgersene, perché MDaemon accetta solo una password di applicazione corretta. Inoltre, se gli account in MDaemon utilizzano l'autenticazione con Active Directory 835 e Active Directory blocca un account dopo un certo numero di tentativi non riusciti, questa opzione può aiutare a prevenire il blocco degli account, poiché MDaemon verifica solo le password di applicazione e non tenta l'autenticazione con Active Directory.

Vedere:

Password 870
Account Editor » Impostazioni 776

5.1.1.15 Firma



Firma dell'account

Utilizzare questa schermata per indicare una firma che verrà aggiunta alla fine di ogni messaggio e-mail inviato dall'account. Questa firma viene aggiunta a tutte le altre firme o ai piè di pagina aggiunti da altre opzioni, come l'opzione di firma disponibile in Webmail e in altri client di posta, le opzioni di firma Predefinita 136 e Dominio 206 e i piè di pagina delle liste di distribuzione 304. Le firme di dominio/predefinite e i piè di pagina delle liste di distribuzione vengono sempre aggiunti successivamente alle firme dell'account.

Gli utenti che accedono a Webmail o a Remote Administration 359 possono modificare le proprie firme in tali applicazioni.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. `Ad esempio, $CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e `$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**
ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**
Numeri di telefono e fax	

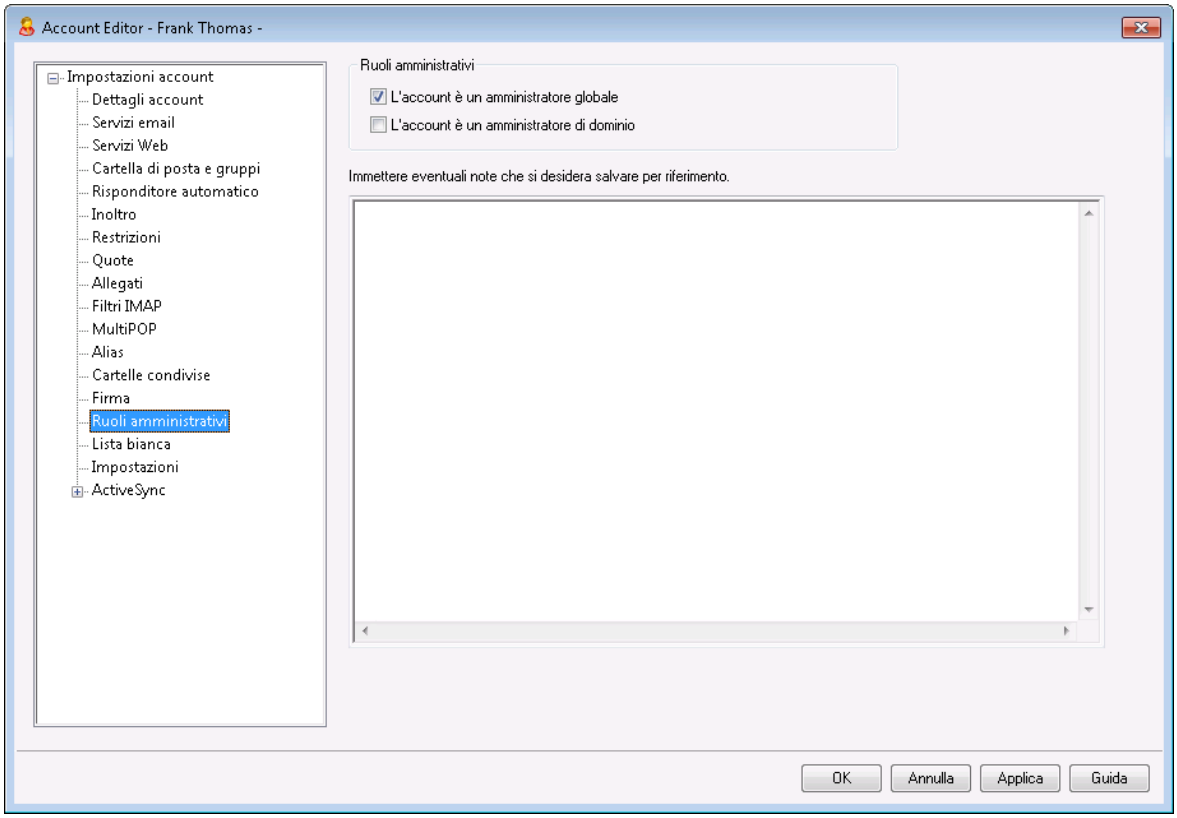
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**
Mansione lavorativa	**$CONTACTBUSINESSTITLE$**

Ufficio	$CONTACTBUSINESSOFFICE$
Reparto dell'azienda	$CONTACTBUSINESSDEPARTMENT$
Responsabile dell'azienda	$CONTACTBUSINESSMANAGER$
Assistente in azienda	$CONTACTBUSINESSASSISTANT$
Telefono assistente in azienda	$CONTACTBUSINESSASSISTANTPHONE$
Telefono principale dell'azienda	$CONTACTBUSINESSMAINPHONE$
Telefono al lavoro	$CONTACTBUSINESSPHONE$
Telefono al lavoro 2	$CONTACTBUSINESSPHONE2$
Telefono IP al lavoro	$CONTACTBUSINESSIPPHONE$
Fax di lavoro	$CONTACTBUSINESSFAX$
Cercapersone in azienda	$CONTACTBUSINESSPAGER$
Radiotelefono in azienda	$CONTACTBUSINESSRADIO$
Indirizzo di lavoro	$CONTACTBUSINESSADDRESS$
Città di lavoro	$CONTACTBUSINESSCITY$
Provincia di lavoro	$CONTACTBUSINESSSTATE$
CAP di lavoro	$CONTACTBUSINESSZIPCODE$
Paese di lavoro	$CONTACTBUSINESSCOUNTRY$
Indirizzo Web aziendale	$CONTACTBUSINESSWEBADDRESS$
Altro	
Coniuge	$CONTACTSPOUSE$
Figli	$CONTACTCHILDREN$
Categorie	$CONTACTCATEGORIES$
Commento	$CONTACTCOMMENT$

Vedere:

Firme predefinite 136
Firma di dominio 206
Piè di pagina delle liste di distribuzione 304

5.1.1.16 Ruoli amministrativi



Ruoli amministrativi

L'account è un amministratore globale
Selezionare questa casella di controllo per concedere all'utente accesso al server come amministratore. Agli amministratori globali sono associate le caratteristiche riportate di seguito.

- Accesso completo alla configurazione del server, a tutti gli utenti e a tutti i domini via Remote Administration.
- Accesso agli utenti di tutti i domini di MDaemon come compagni di conversazione di messaggistica istantanea.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche se di sola lettura.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche non si è iscritti.

L'utente avrà inoltre accesso a tutti i file e le opzioni di MDaemon. Per ulteriori informazioni sulle opzioni di amministrazione nell'interfaccia Web di Remote Administration, vedere Remote Administration 359.

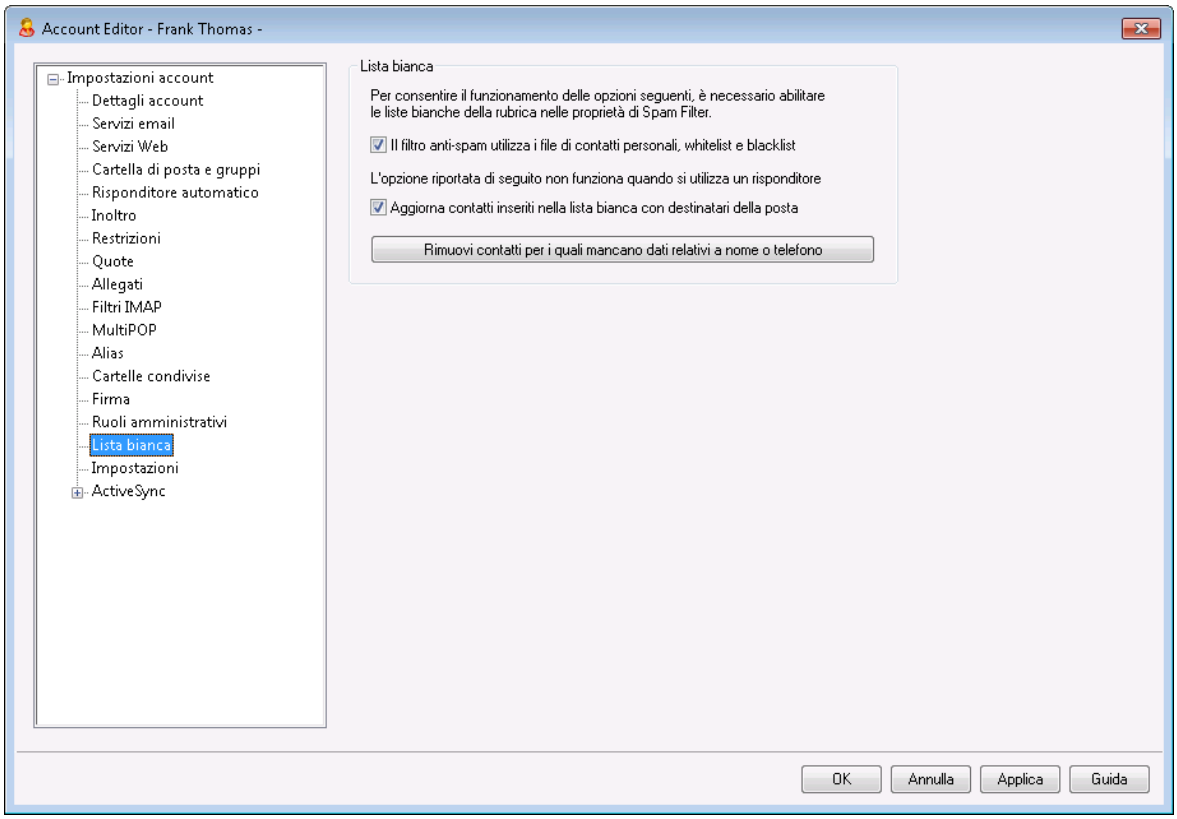
L'account è un amministratore di dominio
Selezionare questa casella di controllo per designare l'utente come amministratore di dominio. Gli amministratori di dominio hanno privilegi simili a quelli degli amministratori

globali, con l'unica differenza che l'accesso a livello amministrativo è limitato a questo dominio e alle autorizzazioni concesse nella pagina Servizi Web 735.

Per consentire a questo account di amministrare un altro dominio, impostare le autorizzazioni all'interno dell'interfaccia Web di Remote Administration 359, nella pagina Domain Manager » Amministratori.

Immettere eventuali note che si desidera salvare per riferimento.
Utilizzare questo spazio per immettere eventuali note o altre informazioni che si desidera salvare per riferimento in relazione a questo account. A differenza del campo *Descrizione* nella schermata Dettagli account 729, questa nota non sarà sincronizzata con i contatti pubblici o associata a qualsiasi campo in Active Directory.

5.1.1.17 Lista consentiti



Lista consentiti

Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati.
In Spam Filter la schermata Lista consentiti (automatica) 705 contiene un'opzione globale che si può utilizzare per fare in modo che il filtro antispam consenta automaticamente la ricezione di un messaggio quando il mittente di tale messaggio viene trovato nei contatti personali del destinatario locale o nella cartella dei mittenti autorizzati. Inoltre, il filtro bloccherà automaticamente i messaggi i cui mittenti vengono trovati nella cartella dei mittenti bloccati dell'utente. Se si è abilitata l'opzione globale di Spam Filter, ma non si desidera applicarla a questo account,

deselezionare la casella di controllo per ignorare l'impostazione globale. Se l'opzione globale è disattivata, questa opzione non sarà disponibile.

Aggiungi automaticamente i destinatari di posta ai mittenti consentiti
Fare clic su questa opzione per la cartella dei mittenti consentitidell'account ogni volta che questo invia un messaggio a un indirizzo e-mail non locale. Se utilizzata insieme all'opzione precedente, *Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati*, consente di ridurre drasticamente il numero di falsi positivi di Spam Filter. L'opzione *Aggiungi automaticamente i destinatari di posta ai mittenti consentiti* disponibile nella schermata Lista consentiti (automatica) 705 deve essere attivata prima di utilizzare questa funzione.

questa opzione è disabilitata se l'account utilizza la funziona di risposta automatica.

Rimuovi contatti per i quali mancano dati relativi a nome o telefono
Questo pulsante consente di rimuovere dalla cartella Contatti predefinita dell'account tutti i contatti che contengono solo l'indirizzo di posta elettronica. I contatti privi del nome o dei dati telefonici vengono rimossi. L'opzione ha lo scopo principale di aiutare chi utilizzava l'opzione di MDaemon per la gestione delle liste dei consentiti precedente alla versione 11 a eliminare i contatti che erano stati aggiunti solo come risultato della funzione della lista consentiti. Nelle versioni precedenti di MDaemon gli indirizzi venivano aggiunti ai contatti principali invece che a una lista consentiti dedicata. Ciò può comportare un account con molte voci nella cartella dei contatti che sarebbe preferibile non avere.

È consigliabile utilizzare questa opzione con grande cautela, perché i contatti contenenti solo l'indirizzo di posta elettronica potrebbero essere legittimi.

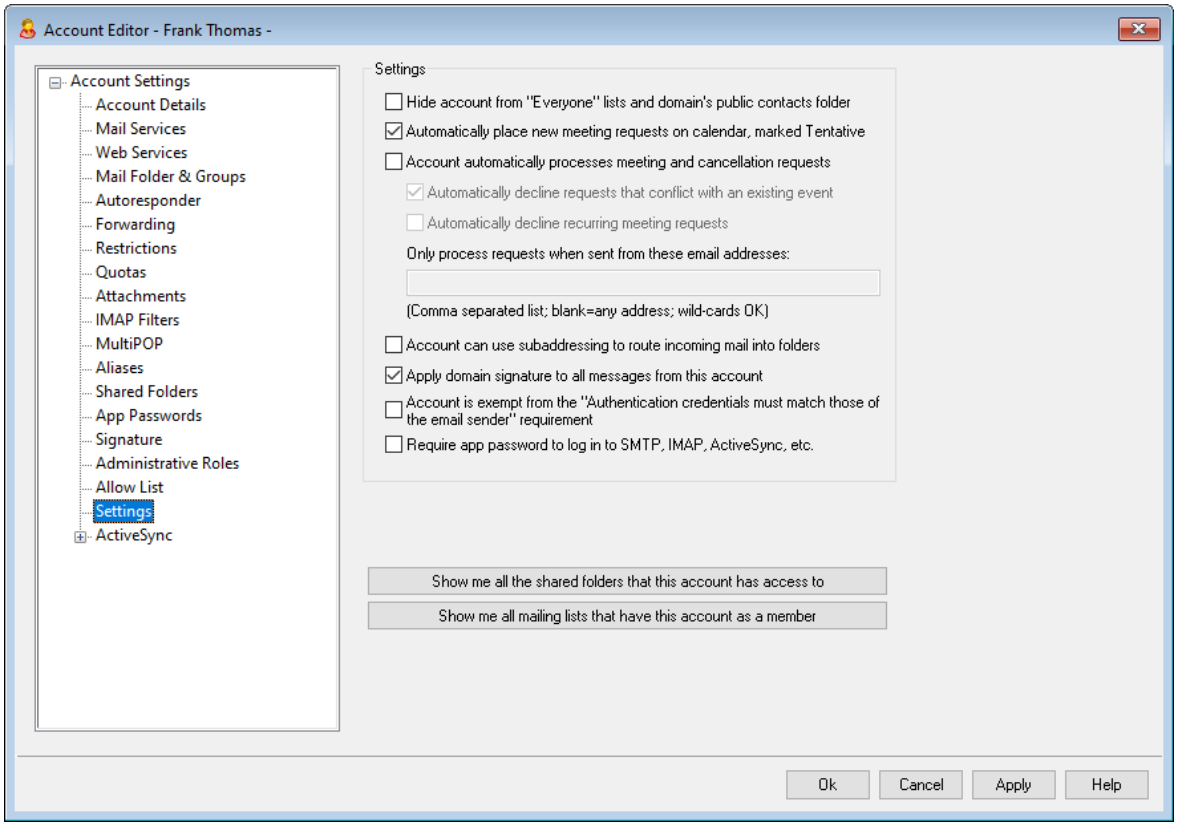
Impostazione dei valori predefiniti per nuovi account e gruppi

Le opzioni di questa schermata corrispondono a quelle presenti nella schermata Proprietà modello » Lista consentiti 831 , che si può utilizzare per impostare i valori predefiniti per i nuovi account 807 e valori per gli account che appartengono a determinati gruppi 796.

Vedere:

Lista consentiti (automatica) 705
Gestione account 806
Proprietà modello » Lista consentiti 831

5.1.1.18 Impostazioni



Impostazioni

Nascondi account da elenchi "Everyone" e da cartella contatti pubblica del dominio
MDaemon può creare e gestire automaticamente liste di distribuzione "Everyone@" e "MasterEveryone@"278, che è possibile utilizzare per inviare un messaggio rispettivamente a tutti gli utenti di un dominio e a tutti gli utenti di MDaemon. Per impostazione predefinita questi elenchi includono tutti gli account di ciascun dominio, ma è possibile selezionare questa casella se si desidera nascondere l'account da questi elenchi: i messaggi inviati a tali elenchi non saranno inviati all'account. L'account verrà rimosso dalla cartella pubblica dei contatti del dominio.

Inserire automaticamente in calendario nuove richieste di riunione, contrassegnate come Tentativo
Per impostazione predefinita quando un account riceve una nuova richiesta di riunione, tale riunione viene inserita nel calendario dell'utente e contrassegnata come *Tentativo*.

L'account elabora automaticamente le richieste di riunione e gli annullamenti
Selezionare questa casella di controllo se si desidera abilitare l'elaborazione automatica delle richieste di riunione, delle modifiche e degli annullamenti per l'account. Se viene ricevuto un messaggio che contiene una richiesta di riunione, il calendario dell'account viene aggiornato automaticamente. Per impostazione predefinita, l'opzione è disabilitata per tutti gli account.

Rifiuta automaticamente richieste in conflitto con un evento esistente
Se per l'account è abilitata l'elaborazione automatica delle richieste di riunione e degli annullamenti, per impostazione predefinita, le richieste di riunione vengono rifiutate automaticamente se in conflitto con un evento esistente. Deselezionare questa casella di controllo per creare l'evento in conflitto.

Rifiuta automaticamente richieste di riunioni ricorrenti
Fare clic su questa casella se per questo account è abilitata l'elaborazione automatica delle richieste di riunione e degli annullamenti, ma si desidera rifiutare tali richieste se sono relative a riunioni ricorrenti.

Elabora le richieste solo se inviate da questi indirizzi e-mail
Per elaborare automaticamente le richieste solo per alcuni indirizzi e-mail, riportare qui tali indirizzi. Separare gli indirizzi con una virgola. È consentito l'uso dei caratteri jolly negli indirizzi (ad esempio, *@esempio.com). Se si lascia vuota questa casella, sarà consentito qualsiasi indirizzo.

L'account può utilizzare il subaddressing per instradare la posta in entrata nelle cartelle
Selezionare questa casella di controllo se si desidera consentire il subaddressing 778 per l'account.

Applica firma dominio a tutti i messaggi da questo account
Quando esiste una firma dominio 206 per il dominio a cui appartiene l'account, questa opzione consente di aggiungerla a tutti i messaggi di posta elettronica inviati dall'account. L'opzione è abilitata per impostazione predefinita.

L'account è esente dal requisito "Le credenziali di autenticazione devono corrispondere a quelle del mittente"
Utilizzare questa opzione per escludere l'account dall'opzione globale "*Le credenziali di autenticazione devono corrispondere a quelle del mittente*" della schermata Autenticazione SMTP 531. L'opzione è disabilitata per impostazione predefinita.

Richiedi la password di applicazione per l'accesso a SMTP, IMAP, ActiveSync, ecc.
Selezionare questa casella se si desidera richiedere che l'account utilizzi obbligatoriamente le password di applicazione 766 nei client di e-mail, per accedere a SMTP, IMAP, ActiveSync o ad altri protocolli dei servizi di posta. La normale password 870 dell'account, tuttavia, dovrà essere ancora utilizzata per accedere a Webmail o Remote Admin.

La richiesta di password di applicazione può aiutare a proteggere le password degli account da attacchi a dizionario e a forza bruta via SMTP, IMAP, ecc. La sicurezza è garantita dal fatto che, ove mai con un attacco di questo tipo si riuscisse a indovinare la password reale di un account, questa non funzionerebbe senza che l'aggressore possa accorgersene, perché MDaemon accetta solo una password di applicazione corretta. Inoltre, se gli account in MDaemon utilizzano l'autenticazione con Active Directory 835 e si è configurato Active Directory in modo da bloccare un account dopo un certo numero di tentativi non riusciti, questa opzione può aiutare a prevenire il blocco degli account, poiché MDaemon verifica solo le password di applicazione e non tenta l'autenticazione con Active Directory.

Mostra tutte le cartelle condivise a cui ha accesso questo account
Fare clic su questo pulsante per visualizzare tutte le cartelle condivise alle quali l'account ha accesso.

Mostra tutte le liste di distribuzione di cui è membro l'account
Questo pulsante consente di aprire l'elenco di tutte le liste di distribuzione[275] cui l'account appartiene.

Subaddressing

Il subaddressing è una tecnica che consente di includere il nome di una cartella nella parte relativa alla casella postale di un indirizzo e-mail. Utilizzando questa tecnica, i messaggi destinati alla combinazione *casella postale+nome cartella* vengono instradati automaticamente alla cartella dell'account inclusa nell'indirizzo, senza che sia necessario creare regole di filtro a tale scopo.

Ad esempio, se `roberto.rossi@esempio.com` ha una cartella IMAP denominata "`materiale`", la posta in arrivo all'indirizzo "`roberto.rossi+materiale@esempio.com`" verrà instradata automaticamente a tale cartella. Per specificare sottocartelle è possibile separare i nomi della cartella e della sottocartella con un carattere aggiuntivo "+", mentre per sostituire eventuali spazi presenti nei nomi delle cartelle è necessario utilizzare il carattere di sottolineatura. In base all'esempio precedente, se nella cartella "`materiale`" di Roberto è presente una sottocartella denominata "`materiale vecchio`," i messaggi inviati a "`roberto.rossi+materiale+materiale_vecchio@esempio.com`" verranno instradati automaticamente alla cartella di posta "`\materiale\materiale vecchio\`" di Roberto.

Poiché il subaddressing prevede l'utilizzo del carattere "+", non è possibile utilizzare questa tecnica con le caselle postali il cui nome contiene "+". Nell'esempio precedente, se l'indirizzo effettivo fosse "`roberto+rossi@esempio.com`", anziché "`roberto.rossi@esempio.com`", la funzionalità di subaddressing non potrebbe essere utilizzata. Inoltre, non è possibile utilizzare un alias di indirizzo con questa tecnica. È possibile, tuttavia, creare un alias che fa riferimento all'intero indirizzo con subaddressing. Di conseguenza, anche se "`alias+materiale@esempio.com`" non è consentito, è possibile utilizzare "`alias@esempio.com`" per indicare "`roberto.rossi+materiale@esempio.com`".

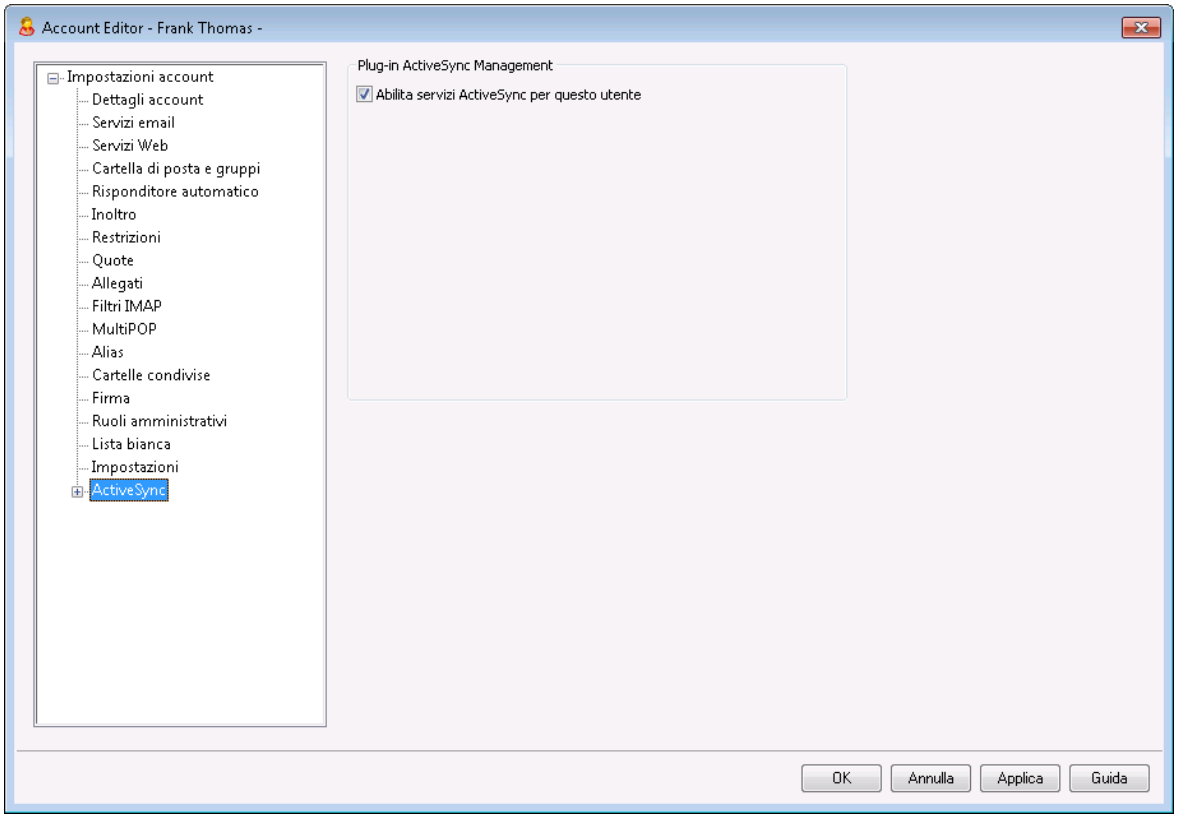
Per impedire l'uso improprio o fraudolento di questa funzionalità, la cartella IMAP inclusa nell'indirizzo con subaddressing **deve** essere valida. Se il subaddressing di un messaggio in arrivo fa riferimento a una cartella non esistente per l'account, l'indirizzo viene considerato come indirizzo di posta non esistente e gestito in base alle relative impostazioni definite in MDaemon. Ad esempio, se per `roberto.rossi@esempio.com` non esiste la cartella "`materiale`", ma viene ricevuto un messaggio indirizzato a "`roberto.rossi+materiale@esempio.com`", il messaggio viene considerato come indirizzato a un utente sconosciuto e, molto probabilmente, respinto.

Per impostazione predefinita, il subaddressing è disabilitato per tutti gli account. È possibile disattivare questa funzionalità a livello globale mediante l'opzione *Disabilita funzione subaddressing per tutti gli account* della schermata Varie[511] presente nella finestra di dialogo Preferenze. In questo caso, tale funzionalità viene disattivata per tutti gli account, indipendentemente dalle impostazioni dei singoli account.

Vedere:

Lista consentiti (automatica)[705]
Remote Administration[359]
Gestione account[806]
Password[870]

5.1.1.19 ActiveSync per MDaemon



Le schermate di ActiveSync per MDaemon nell'Account Editor sono utilizzate per attivare o disattivare ActiveSync per l'account, configurare impostazioni specifiche dell'account 780, assegnare un criterio predefinito 786 e gestire i client ActiveSync 787 dell'account.

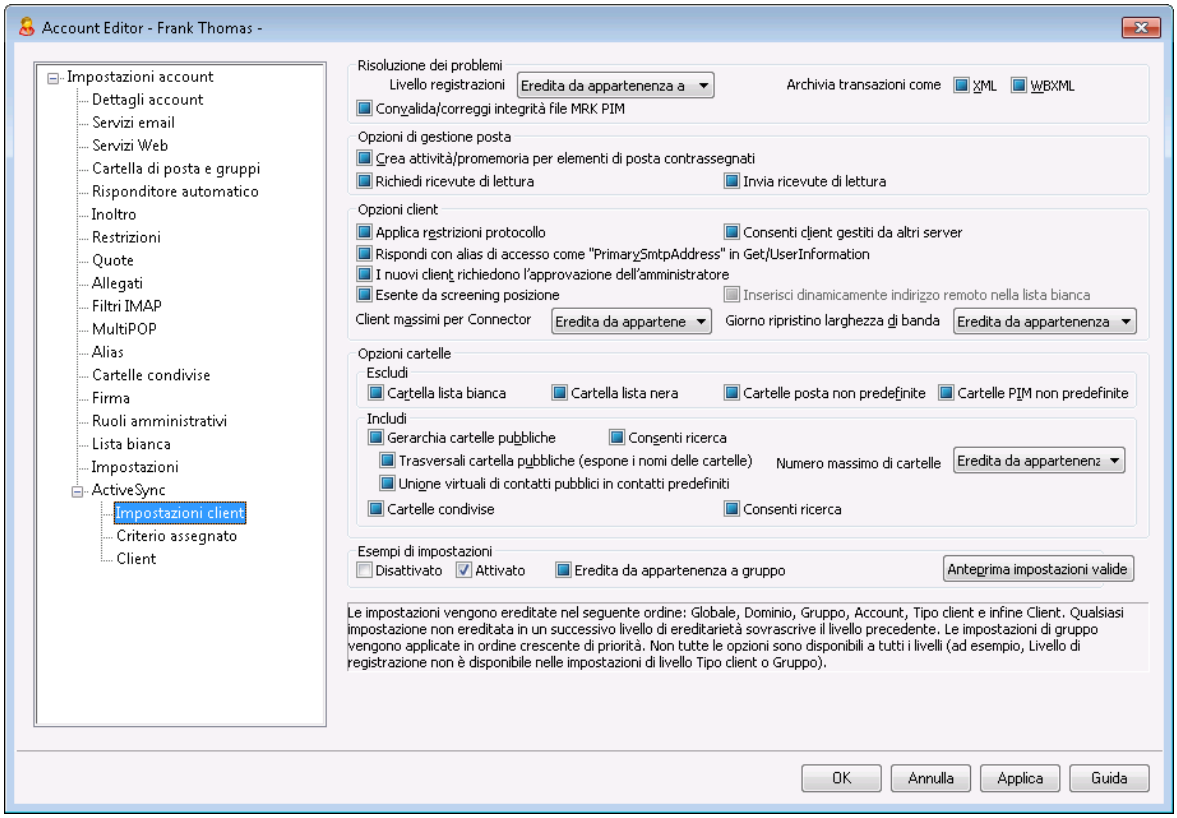
Attivazione/disattivazione di ActiveSync per l'account

Attivare questa opzione se si desidera consentire all'account di utilizzare un client ActiveSync per l'accesso alle e-mail e ai dati PIM.

Per ulteriori informazioni, vedere:

Account Editor » ActiveSync » Impostazioni client 780
Account Editor » ActiveSync » Criterio assegnato 786
Account Editor » ActiveSync » Client 787

5.1.1.19.1 Impostazioni client



Le opzioni di questa schermata sono utilizzate per controllare le impostazioni del client ActiveSync per i client associati all'account. Per impostazione predefinita ciascuna di queste opzioni è configurata per ereditare la relativa impostazione dal dominio corrispondente al quale appartiene l'account. La modifica di qualsiasi impostazione in questa schermata sovrascriverà l'impostazione del dominio 444 per questo account. È inoltre possibile utilizzare l'opzione *Impostazioni* della schermata Client 787 se si desidera sovrascrivere queste impostazioni a livello di account per client specifici.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug	È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei problemi.
Info	Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.
Avviso	Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.
Errore	Vengono registrati errori, errori critici ed eventi di avvio e di arresto.
Critico	Vengono registrati errori critici ed eventi di avvio e di arresto.
Nessuno	Vengono registrati solo gli eventi di avvio e di arresto.
Ereditarietà	Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per

il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per

impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se

richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

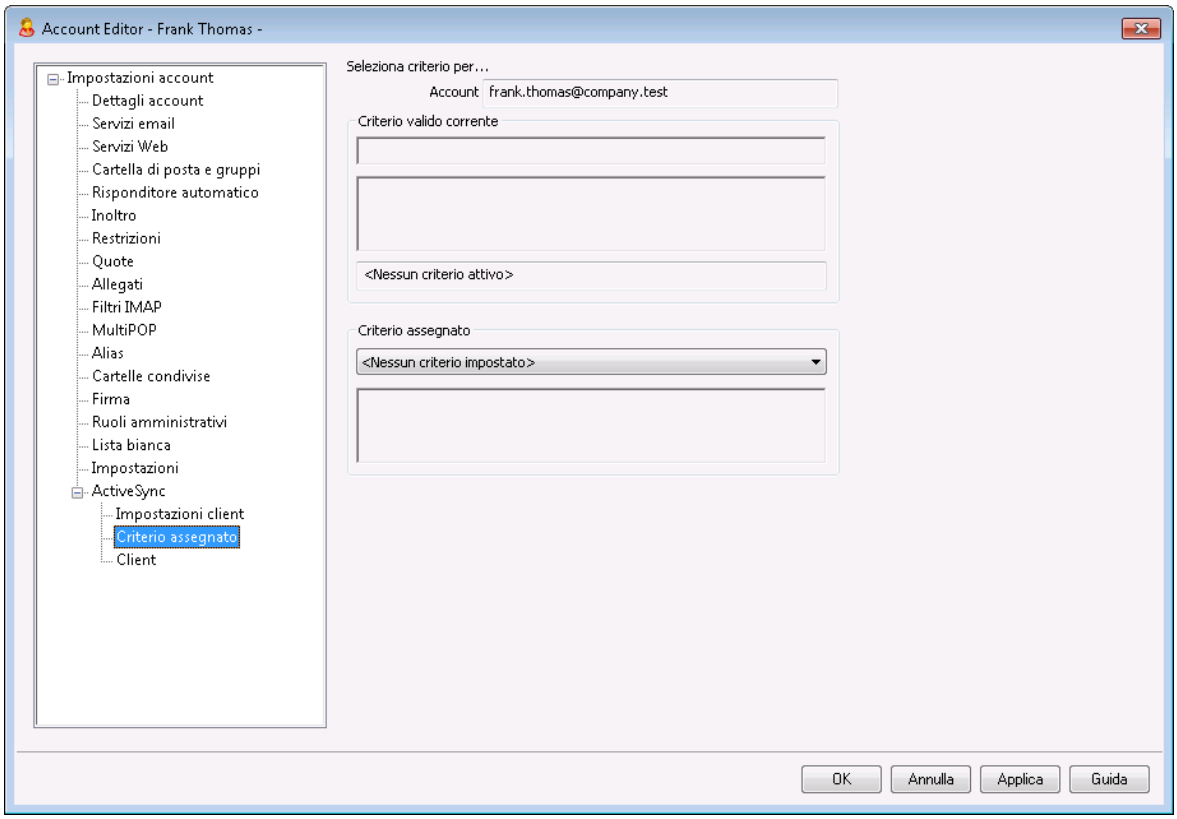
Anteprima impostazioni applicate

Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

ActiveSync » Domini 444
Account Editor » ActiveSync » Client 787

5.1.1.19.2 Criterio assegnato



Utilizzare questa schermata per indicare il criterio ActiveSync 452 predefinito che sarà utilizzato per qualsiasi client ActiveSync che si connette utilizzando questo account. Per impostazione predefinita l'impostazione di questo criterio viene ereditata dall'impostazione del criterio del dominio 236, ma è possibile modificarla qui per sovrascrivere tale impostazione per questo account. È inoltre possibile sovrascrivere l'impostazione specifica dell'account e assegnare criteri diversi a specifici client 787.

Assegnazione di un criterio ActiveSync

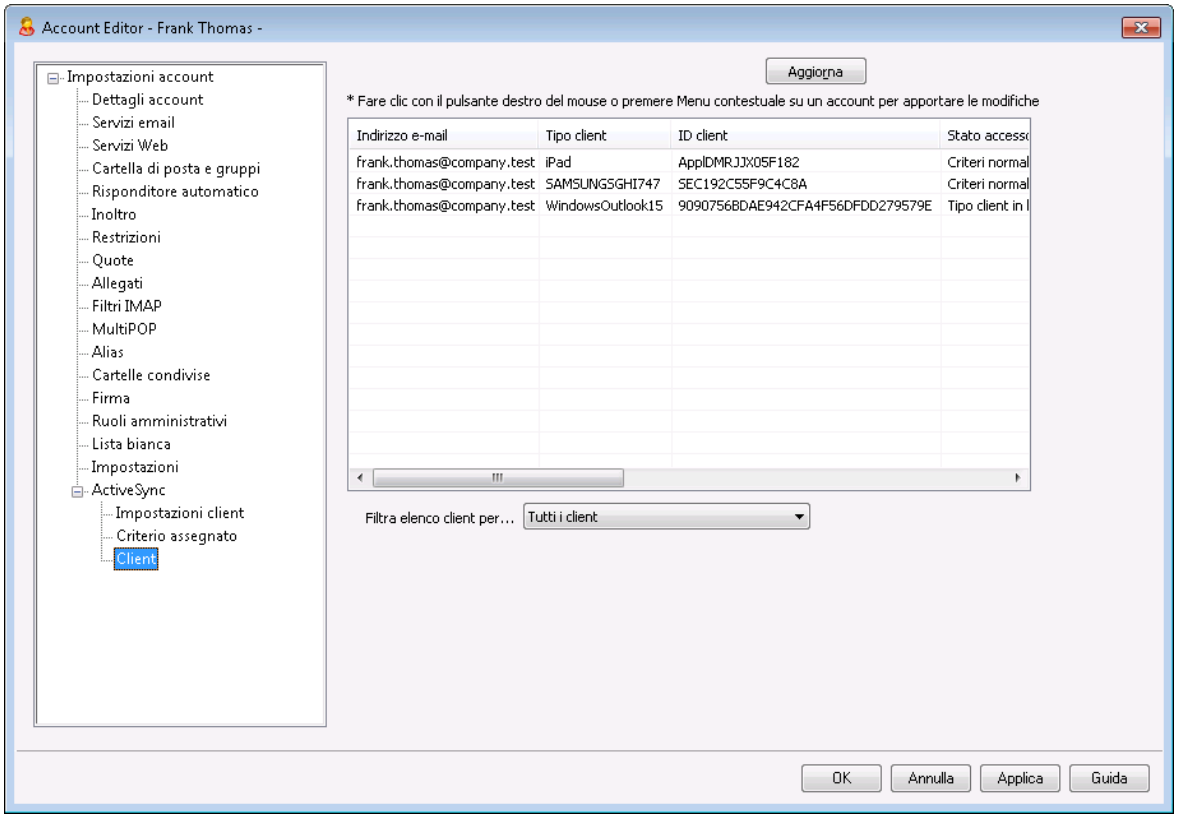
Per assegnare un criterio all'account, fare clic sull'elenco a discesa **Criterio da assegnare**, scegliere il criterio, quindi fare clic su **Ok** o **Applica**.

Non tutti i dispositivi ActiveSync riconoscono o applicano i criteri in modo coerente. Alcuni potrebbero ignorare del tutto i criteri o alcuni elementi dei criteri, mentre altri potrebbero richiedere un riavvio del dispositivo per rendere effettive le modifiche. Inoltre, quando si tenta di assegnare un nuovo criterio, il criterio viene applicato solo alla successiva connessione del dispositivo al server ActiveSync; non è possibile inviare i criteri ai dispositivi fino a quando questi ultimi non eseguono la connessione.

Per ulteriori informazioni, vedere:

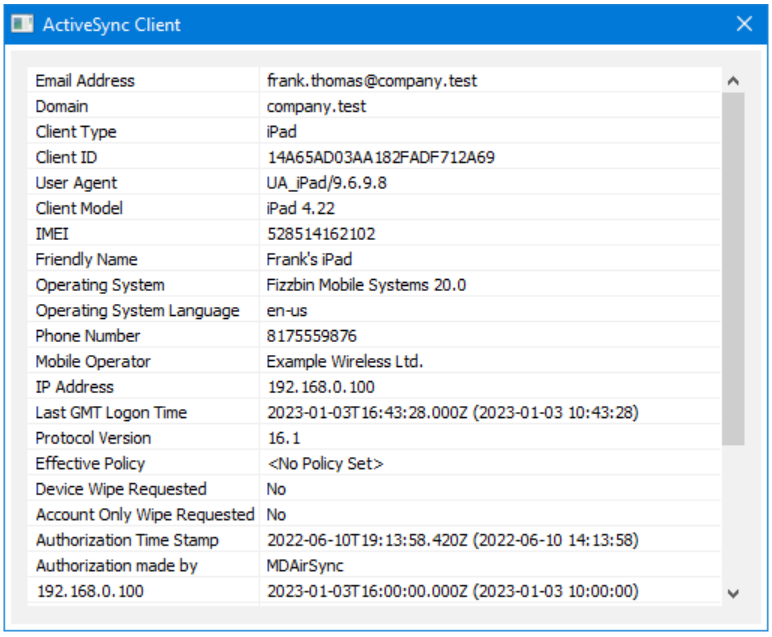
ActiveSync » Policy Manager 452
ActiveSync » Domini 444
Account Editor » ActiveSync » Client 787

5.1.1.19.3 Client



In questa schermata vengono visualizzate informazioni su tutti i client ActiveSync associati all'account dell'utente. Da questa posizione è possibile assegnare un criterio ActiveSync 786 a ciascun client, controllare diverse impostazioni del client, rimuovere client, cancellarne i dati da remoto e resettare le statistiche del client in MDaemon.

Dettagli client ActiveSync



Fare doppio clic su una voce oppure fare clic con il pulsante destro sulla voce e scegliere **Visualizza dettagli client** per visualizzare la finestra di dialogo Dettagli client. In questa schermata sono riportate informazioni relative al client, come Tipo client, ID client, ora di ultimo accesso e simili.

Impostazioni client

Fare clic con il pulsante destro su un client e scegliere **Personalizza impostazioni client** per gestire le impostazioni del client. Per impostazione predefinita queste impostazioni vengono ereditate da Tipo client, ma si possono modificare secondo necessità. Vedere Gestione delle impostazioni del client di un dispositivo 789 di seguito.

Assegnazione di un criterio ActiveSync

Per assegnare un Criterio 452 al dispositivo:

1. Fare clic con il pulsante destro su un dispositivo nell'elenco.
2. Fare clic su **Applica criterio**. Verrà aperta la finestra di dialogo Applicazione criterio.
3. Fare clic sull'elenco a discesa **Criterio da assegnare** e scegliere il criterio desiderato.
4. Fare clic su **OK**.

Statistiche

Fare clic con il pulsante destro su una voce, quindi su **Visualizza statistiche** per visualizzare la finestra di dialogo Statistiche client, che contiene alcune statistiche sull'uso del client.

Ripristina statistiche

Per azzerare le statistiche di un client, fare clic con il pulsante destro sul client, quindi su **Azzera statistiche**, infine su **OK** per confermare l'azione.

Rimozione di un client ActiveSync

Per rimuovere un client ActiveSync, fare clic con il pulsante destro sul client e scegliere **Elimina**, quindi selezionare **Sì**. In questo modo si rimuove il client dall'elenco e si eliminano tutte le informazioni di sincronizzazione a esso correlate in MDaemon. Ne consegue che, se in futuro l'account utilizzerà ActiveSync per la sincronizzazione dello stesso client, MDaemon tratterà tale client come se non fosse mai stato utilizzato prima sul server; sarà dunque necessario risincronizzare tutti i dati del client con MDaemon.

Cancellazione completa di un client ActiveSync

Quando un criterio 452 è stato applicato a un client ActiveSync selezionato e il client l'ha applicato e ha risposto, per tale client sarà disponibile un'opzione Cancellazione completa. Per effettuare una cancellazione completa, fare clic con il tasto destro del mouse sul client (o selezionarlo se si utilizza MDRA) e fare clic su **Cancellazione completa**. Al successivo collegamento del client, MDaemon imposterà il dispositivo in modo da eliminare tutti i dati o da ripristinare le impostazioni di fabbrica. In base al client, ciò potrebbe comportare la totale rimozione di tutti i dati, app scaricate incluse. Inoltre, finché esisterà la voce ActiveSync del client, MDaemon continuerà a inviare la richiesta di cancellazione ogni volta che il dispositivo si connetterà. Se a un certo punto si desidera eliminare il client, accertarsi di aggiungerlo prima alla Lista bloccati 437, in modo che non possa connettersi di nuovo in futuro. Infine, se un dispositivo eliminato viene recuperato e si desidera consentirgli di connettersi nuovamente, selezionare il dispositivo e fare clic su **Annulla azioni di cancellazione**. Sarà anche necessario rimuoverlo dalla Lista bloccati.

Cancellazione account di un client ActiveSync

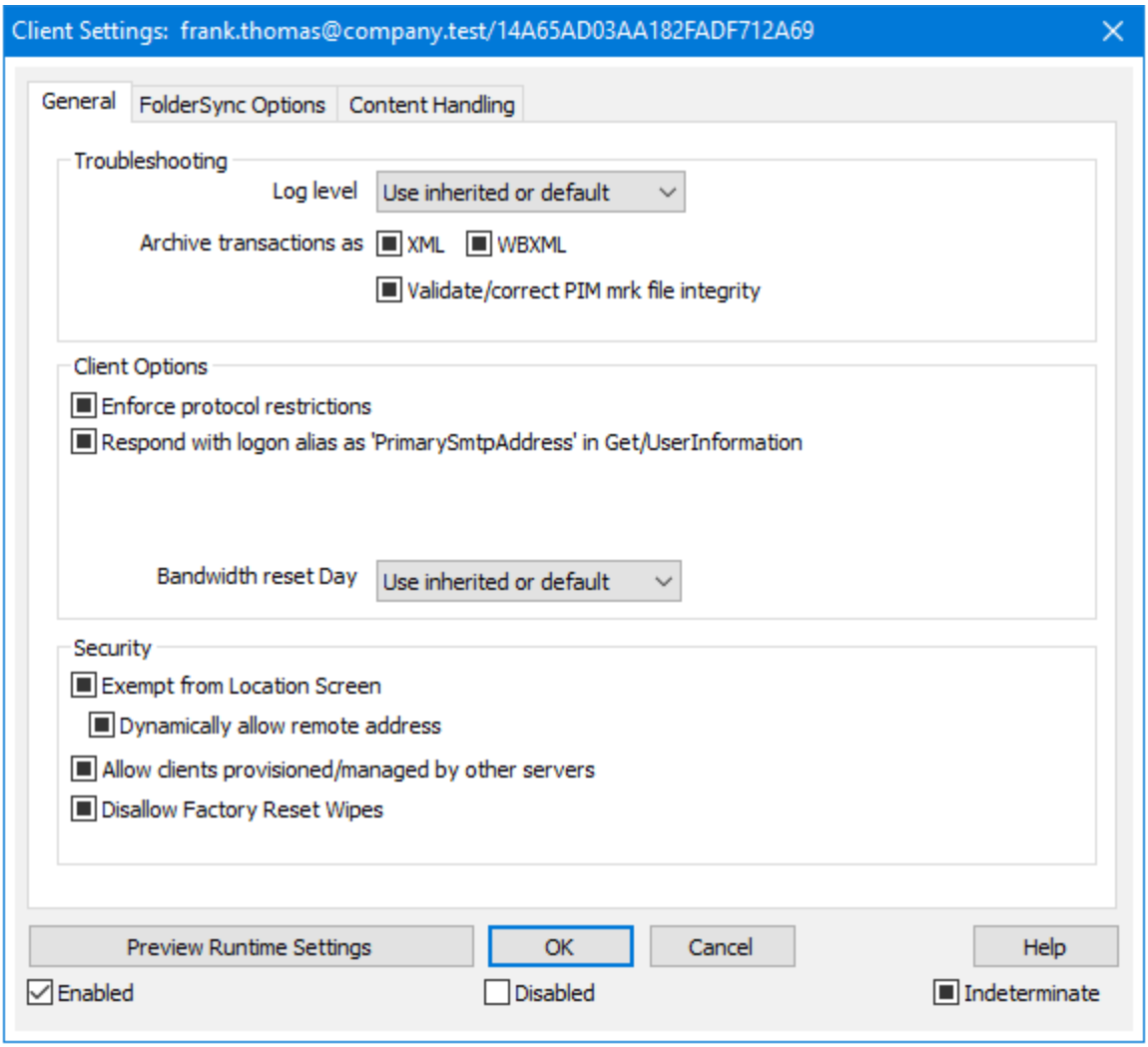
Per cancellare la posta dell'account e i dati PIM dal client o dal dispositivo, fare clic con il pulsante destro e scegliere **Cancella posta e PIM dell'account dal client**. L'opzione *Cancellazione account* è simile all'opzione *Cancellazione completa* descritta sopra, ma invece di eliminare tutti i dati, elimina solo i dati dell'account, come i messaggi di posta elettronica, le voci di calendario, i contatti e così via. Tutto il resto, come applicazioni, foto e musica, viene lasciato dove si trova.

Autorizzazione del client

Se l'opzione "*I nuovi client richiedono l'approvazione dell'amministratore*" nella schermata Impostazioni client ActiveSync 430 è attivata, selezionare un client e fare clic su Approva sincronizzazione client per autorizzarlo alla sincronizzazione con il server.

Gestione delle impostazioni del client di un dispositivo

La schermata Impostazioni client a livello di dispositivo consente di gestire le impostazioni per un dispositivo specifico.



Per impostazione predefinita, tutte le opzioni di questa schermata sono impostate su "Usa ereditate o predefinite", a significare che vengono impostate come l'opzione corrispondente disponibile nella schermata Tipi client Impostazioni client 486. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra. Al contrario, le modifiche apportate in questa schermata sovrascriveranno le impostazioni a livello di tipi di client per il dispositivo.

Generale

Risoluzione dei problemi

Livello di registrazione
ActiveSync per MDaemon prevede sei livelli di registrazione, in base alla quantità di dati registrati:

Debug È il livello di registrazione più esteso. Registra tutte le voci disponibili e viene in genere utilizzato solo per la diagnostica dei

problemi.

Info Registrazione di livello moderato. Registra le operazioni generali senza i dettagli. È il livello di registrazione predefinito.

Avviso Vengono registrati avvisi, errori, errori critici ed eventi di avvio e di arresto.

Errore Vengono registrati errori, errori critici ed eventi di avvio e di arresto.

Critico Vengono registrati errori critici ed eventi di avvio e di arresto.

Nessuno Vengono registrati solo gli eventi di avvio e di arresto.

Ereditarietà Per impostazione predefinita, l'impostazione del livello di registrazione viene ereditata dalla gerarchia Impostazioni client. Ne consegue che per i client le impostazioni vengono ereditate da Tipi client, Tipi client da Account, Account da Gruppi e così via. Le opzioni delle impostazioni client globali sono determinate dall'impostazione del livello di registrazione nella finestra di dialogo Diagnostica 440.

Archivia transazioni come [XML | WBXML]
Utilizzare le opzioni *Archivia XML...* e *WBXML* per salvare i dati corrispondenti, operazione che si può rivelare utile per il debug. Le opzioni globali sono disabilitate per impostazione predefinita.

Convalida/correggi integrità file contrassegno PIM
Questa opzione esegue un processo di convalida e correzione sui dati PIM del client per individuare problemi noti che potrebbero impedire la sincronizzazione corretta, ad esempio UID iCal duplicati o campi obbligatori vuoti. L'opzione globale è disabilitata per impostazione predefinita.

Opzioni client

Applica restrizioni protocollo
Abilitare questa opzione se si desidera impedire le connessioni dei client che tentano di utilizzare un protocollo diverso dalle *Versioni protocollo consentite* specificate per il client. Per impostazione predefinita questa opzione è disattivata, il che significa che le restrizioni protocollo non impediscono a un client di tentare di utilizzare un protocollo diverso, indicano solo al client quale protocollo utilizzare. Se un client tenta di utilizzare comunque un protocollo per il quale esiste una restrizione, MDaemon consentirà la connessione. Vedere: Restrizioni dei protocolli 442 per ulteriori informazioni.

Rispondi con alias di accesso come "PrimarySmtpAddress" in Get/UserInformation
Questo consente al servizio di restituire un alias/indirizzo secondario come indirizzo principale in risposta a una richiesta Impostazioni/Get/UserInformation. In questo

modo si risolve un problema causato da un aggiornamento successivo a iOS 9.x che ha modificato i client in modo che non siano in grado di inviare messaggi di posta utilizzando un alias. Se si utilizza questa opzione, si ottiene una risposta conforme non specifica a Impostazioni/Get/UserInformation.

I nuovi client richiedono l'approvazione dell'amministratore
Attivare questa opzione se si desidera richiedere ai nuovi client di ottenere l'autorizzazione di un amministratore prima di poter iniziare a sincronizzarsi con un account. L'elenco Client 470 contiene gli eventuali client in attesa di autorizzazione e l'amministratore può autorizzarli dalla medesima schermata. Questa impostazione è disattivata per impostazione predefinita.

Client per utente max
Per limitare il numero di dispositivi o client ActiveSync che è possibile associare a un account MDaemon, specificare il numero desiderato in questa opzione. L'opzione globale è impostata su "illimitato" in modo predefinito. Questa opzione è disponibile nella schermata di impostazioni client Globale, Dominio e Account, non nelle singole schermate Client.

Giorno di ripristino della larghezza di banda
Utilizzare questa opzione per reimpostare le statistiche di utilizzo della larghezza di banda relative ai dispositivi ActiveSync in un determinato giorno del mese. L'evento di ripristino avviene come parte del normale processo di manutenzione notturna e viene registrato nel registro di sistema come le altre routine di manutenzione. L' opzione globale è "0" (Mai) per impostazione predefinita, a significare che le statistiche di utilizzo non saranno mai reimpostate. Impostare le opzioni figlio su un giorno diverso se si desidera che il giorno delle reimpostazione coincida con la data di azzeramento dell'addebito operatore wireless di un utente o di un client.

Sicurezza

Esenta da screening posizione
Attivare questa opzione nella schermata di impostazione del client ActiveSync per consentire al dispositivo di bypassare lo Screening posizione 582. In tal modo si consente a un utente valido di continuare ad accedere al proprio account mediante ActiveSync quando, ad esempio, è in viaggio verso un'area altrimenti bloccata per i tentativi di autenticazione. Perché sia possibile esentarlo, il dispositivo si deve connettere e autenticare con ActiveSync entro il periodo di tempo configurato in Disattiva account dopo questo numero di giorni di inattività 427 disponibile nella schermata Regolazione.

Inserisci dinamicamente indirizzo remoto nella lista consentiti
Quando si esenta un dispositivo dallo Screening posizione, attivare questa opzione se si desidera anche inserire nella lista consentiti l'indirizzo IP remoto dal quale il dispositivo si sta connettendo. Questa operazione può essere utile per consentire ad altri client di connettersi dal medesimo indirizzo IP.

Client consentiti predisposti/gestiti da altri server
Per impostazione predefinita, quando il server ActiveSync invia dati/criteri di provisioning specifici a un client e questo riferisce di essere gestito anche da un altro server ActiveSync, al client viene comunque consentito di connettersi a

MDaemon. In questa circostanza, tuttavia, non è possibile garantire che vengano applicate le specifiche dei propri criteri nei casi in cui queste siano in conflitto con i criteri dell'altro server ActiveSync. In generale, in caso di conflitto i client utilizzano per impostazione predefinita l'opzione più restrittiva. Disattivare questa opzione se non si desidera consentire la connessione di questi client.

Impedisci cancellazioni da ripristino impostazioni di fabbrica
Se si imposta su Attivo/Sì, non sarà possibile la **Cancellazione completa** di un client ActiveSync. Se si desidera eseguire una cancellazione completa su un client da remoto, è necessario prima disattivare questa opzione. L'opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni, vedere: **Cancellazione completa di un client ActiveSync** 470 nella pagina Client.

Opzioni FolderSync

Opzioni FolderSync

Escludi

Cartella mittenti consentiti/bloccati
Per impostazione predefinita, le cartelle dei contatti dei mittenti consentiti e bloccati dell'utente non sono sincronizzate con i dispositivi. Vengono generalmente utilizzate solo da MDaemon per consentire il blocco automatico dello spam. Per questo motivo, non è necessario che queste cartelle vengano visualizzate sui dispositivi come contatti.

Cartelle di posta non predefinite
Per impostazione predefinita si possono sincronizzare con il dispositivo tutte le cartelle di posta create dall'utente e predefinite. Attivare questa opzione per consentire la sincronizzazione delle sole cartelle di posta predefinite, vale a dire Posta in entrata, Posta inviata, Posta eliminata, Bozze e così via. Le cartelle create dall'utente non verranno incluse. L'opzione è disabilitata per impostazione predefinita.

Cartelle PIM non predefinite
Per impostazione predefinita, vengono sincronizzate con il dispositivo tutte le cartelle PIM dell'utente (ovvero contatti, calendario, note, attività ecc.). Attivare questa opzione per consentire la sincronizzazione delle sole cartelle PIM predefinite. Se, ad esempio, si attiva questa opzione e l'utente ha più cartelle del calendario, verrà sincronizzata solo quella predefinita. L'opzione è disabilitata per impostazione predefinita.

Includi

Gerarchia cartelle pubbliche
Selezionare questa casella di controllo se si desidera che le cartelle pubbliche 317 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle pubbliche 317 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Trasversali cartella pubbliche (espone i nomi delle cartelle)
Per impostazione predefinita, perché un client possa sincronizzare/accedere a una sottocartella pubblica, l'account deve disporre delle autorizzazioni di ricerca 319 sia per la sottocartella (vale a dire, per la cartella figlio) che per tutte le cartelle pubbliche 317 padre ai livelli superiori. Se l'account non dispone delle autorizzazioni per visualizzare le cartelle padre, non potrà visualizzare nemmeno la cartella figlio, anche quando l'account è autorizzato a visualizzarla. Selezionare questa opzione per consentire al client di accedere a queste cartelle figlio. **Nota:** l'abilitazione di questa opzione comporta necessariamente l'esposizione al client dei nomi delle cartelle padre, cosa che può rappresentare un rischio per la sicurezza. L'opzione è disabilitata per impostazione predefinita.

Numero massimo di cartelle pubbliche
Questa opzione consente di impostare un limite al numero consentito di cartelle pubbliche sul dispositivo. Quando si imposta un limite, il server esegue un'iterazione nell'elenco di cartelle fino a raggiungere il limite, senza inviarne quindi altre al dispositivo. Non è possibile garantire un ordine specifico per l'elaborazione delle cartelle. L'impostazione predefinita non prevede alcun limite globale.

Cartelle condivise
Selezionare questa casella di controllo se si desidera che le cartelle condivise 122 a cui un utente ha accesso vengano incluse nell'elenco delle cartelle sui dispositivi ActiveSync. Per impostazione predefinita, questa opzione è abilitata.

Consenti ricerca
Consente al client di eseguire le ricerche nelle Cartelle condivise 757 a cui ha accesso. L'opzione è abilitata per impostazione predefinita.

Gestione contenuto

Opzioni di gestione contenuto

Creare attività/promemoria per gli elementi di posta quando contrassegnati dal client
Questa opzione consente a MDaemon di ricordare all'utente gli elementi contrassegnati, creando una voce di attività per ogni e-mail contrassegnata, se richiesto dal client. Per impostazione predefinita, l'opzione globale di questo controllo è selezionata.

Invia sempre aggiornamenti delle riunioni quando l'evento viene modificato
Alcuni client non inviano correttamente le e-mail di aggiornamento delle riunioni modificate. Questa opzione forza l'invio da parte del servizio ActiveSync di un aggiornamento della riunione quando un elemento della riunione viene modificato dall'organizzatore. L'opzione deve essere attivata solo per client 470 e tipi di client 486 che non riescono a inviare correttamente gli aggiornamenti delle riunioni, altrimenti si

otterrà l'invio di duplicati di tali aggiornamenti. Di conseguenza, questa opzione è disponibile solo nelle pagine di impostazione di client e tipi di client.

Richiedi ricevute di lettura per tutti i messaggi inviati
Attivare questa opzione se si desidera che il server richieda una conferma di lettura per tutti i messaggi inviati da un client. È disabilitata per impostazione predefinita.

Invia le ricevute di lettura dal server quando i messaggi vengono contrassegnati come letti e quando sono richieste dai mittenti.
Attivare questa opzione se si desidera che il server supporti le richieste di conferma di lettura ed invii una ricevuta di lettura quando un messaggio viene contrassegnato come letto dal client. È disabilitata per impostazione predefinita.

Invia con l'alias specificato nell'indirizzo ReplyTo
Alcuni client potrebbero non consentire al mittente di inviare i messaggi utilizzando un alias. Questa funzionalità è stata aggiunta al protocollo Exchange ActiveSync (EAS) 442 16.x, ma alcuni client non supportano la versione 16.x. Ad esempio, Outlook per Windows utilizza solo EAS 14.0 e, sebbene consenta all'utente di specificare un indirizzo alternativo per l'invio, il messaggio generato non riflette correttamente le scelte dell'utente. Questa opzione consente di utilizzare il campo ReplyTo per l'invio del messaggio e-mail, a condizione che l'indirizzo ReplyTo sia un indirizzo di tipo alias valido 847 per l'utente. L'opzione globale è abilitata per impostazione predefinita.

Unione virtuale dei contatti pubblici con i contatti predefiniti
Abilitare questa opzione per unire i contatti pubblici con i contatti predefiniti dell'utente sul dispositivo. L'unione è solo virtuale, i contatti non vengono fisicamente copiati nella cartella dei contatti dell'utente. La funzione può rivelarsi utile sui client che non supportano le ricerche Global Address List (GAL). È disabilitata per impostazione predefinita.

Bloccare il mittente quando la posta viene spostata nella cartella Posta indesiderata
Se si attiva questa opzione, quando un cliente sposta un messaggio e-mail nella cartella Posta indesiderata dell'account, il servizio aggiunge l'indirizzo del mittente o del destinatario alla cartella Contatti mittenti bloccati.

Forza l'invio di risposte alle riunioni quando una richiesta di riunione viene accettata/rifiutata, ecc.
Se si attiva questa opzione, quando un client accetta, rifiuta o sceglie un'altra azione in risposta a una richiesta di riunione, il servizio invia una risposta all'organizzatore della riunione. Questo è per i client specifici che non inviano correttamente questi aggiornamenti.

Anteprima impostazioni applicate

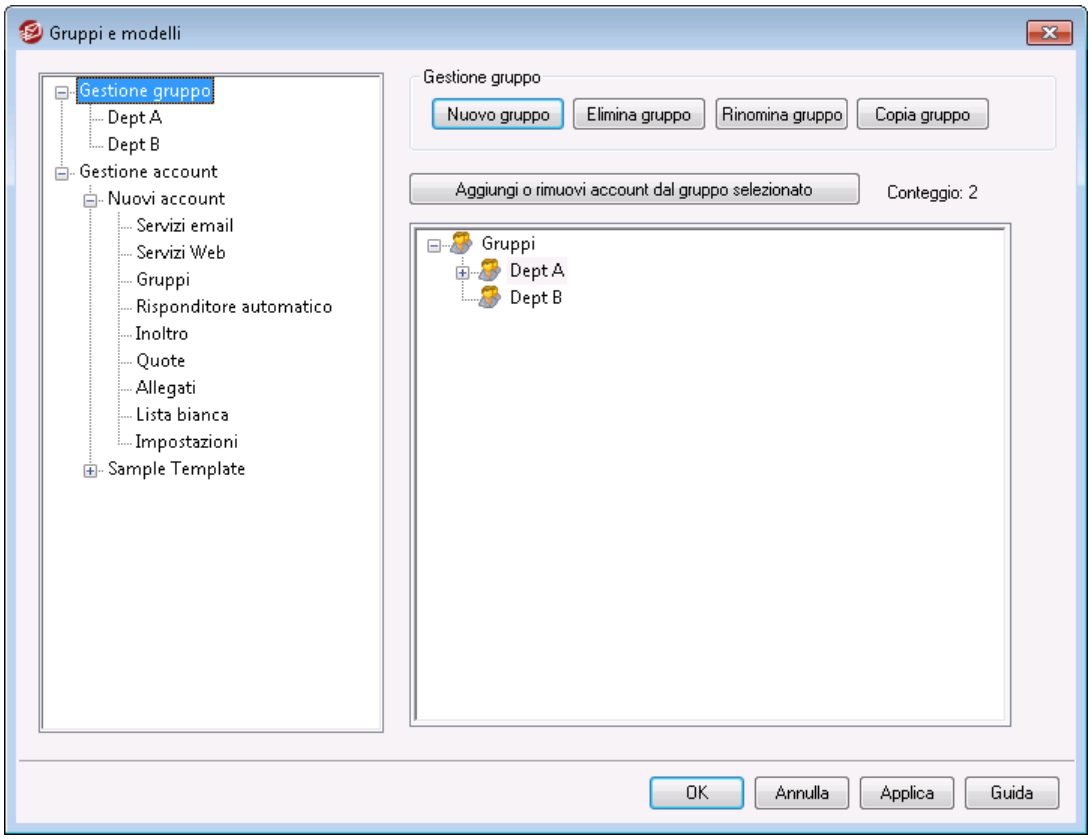
Questo pulsante è disponibile in tutte le schermate figlio Impostazioni client (ovvero domini 444, account 461 e client 470). Poiché le opzioni in tali schermate sono per impostazione predefinita configurate in modo da ereditare le relative impostazioni da una schermata padre, è possibile utilizzare questa funzionalità per vedere quali impostazioni vengono applicate alle schermate visualizzate.

Per ulteriori informazioni, vedere:

ActiveSync » Impostazioni client 430
ActiveSync » Domini 444
ActiveSync » Account 461

5.2 Gruppi e modelli

5.2.1 Gestione gruppo



Gestione gruppo (Account » Gruppi e modelli... » Gestione gruppo) viene utilizzato per creare gruppi di account e gestirli in base agli account di appartenenza. I gruppi rivestono diversi utilizzi e funzioni. Ad esempio, utilizzando la schermata Proprietà gruppo 798 è possibile assegnare un modello 806 di account a un gruppo, il che consente di controllare diverse impostazioni account per i membri del gruppo. È anche possibile controllare se i membri del gruppo hanno accesso o meno a MDaemon Instant Messenger 326 e alla messaggistica istantanea. Filtro contenuti supporta anche i gruppi, il che consente di creare condizioni per le regole 661 in base all'eventuale appartenenza del mittente o del destinatario di un messaggio a un determinato gruppo. Infine, per quanto riguarda le Cartelle condivise 120 è possibile assegnare a gruppi specifici i diritti ACL (Access Control List 319) in modo che tutti i membri di quel gruppo condividano tali diritti di accesso.

Per aggiungere account a un gruppo, selezionare il gruppo dall'elenco e fare clic sul pulsante "*Aggiungi o rimuovi account...*". È inoltre possibile aggiungere utenti a gruppi dalla schermata Cartella di posta e gruppi 732 di ciascun utente.

Gestione gruppo

Nuovo gruppo
Per creare un nuovo gruppo di account, fare clic su *Nuovo gruppo*, digitare un nome e una descrizione per il gruppo, quindi fare clic su *OK*. Il nuovo gruppo verrà visualizzato nell'elenco di gruppi sottostante e nel riquadro sinistro.

Elimina gruppo
Per eliminare un gruppo, selezionare il gruppo nell'elenco sottostante, fare clic su *Elimina gruppo*, quindi su *Sì* per confermare la decisione di eliminare il gruppo.

Rinomina gruppo
Per rinominare un gruppo, selezionarlo dall'elenco e fare clic su *Rinomina gruppo*. Digitare un nuovo nome per il gruppo e fare clic su *OK*.

Copia gruppo
Per creare un nuovo gruppo con impostazioni che corrispondono a un altro gruppo, selezionare un gruppo dall'elenco, fare clic su questo pulsante e specificare un nome per il nuovo gruppo.

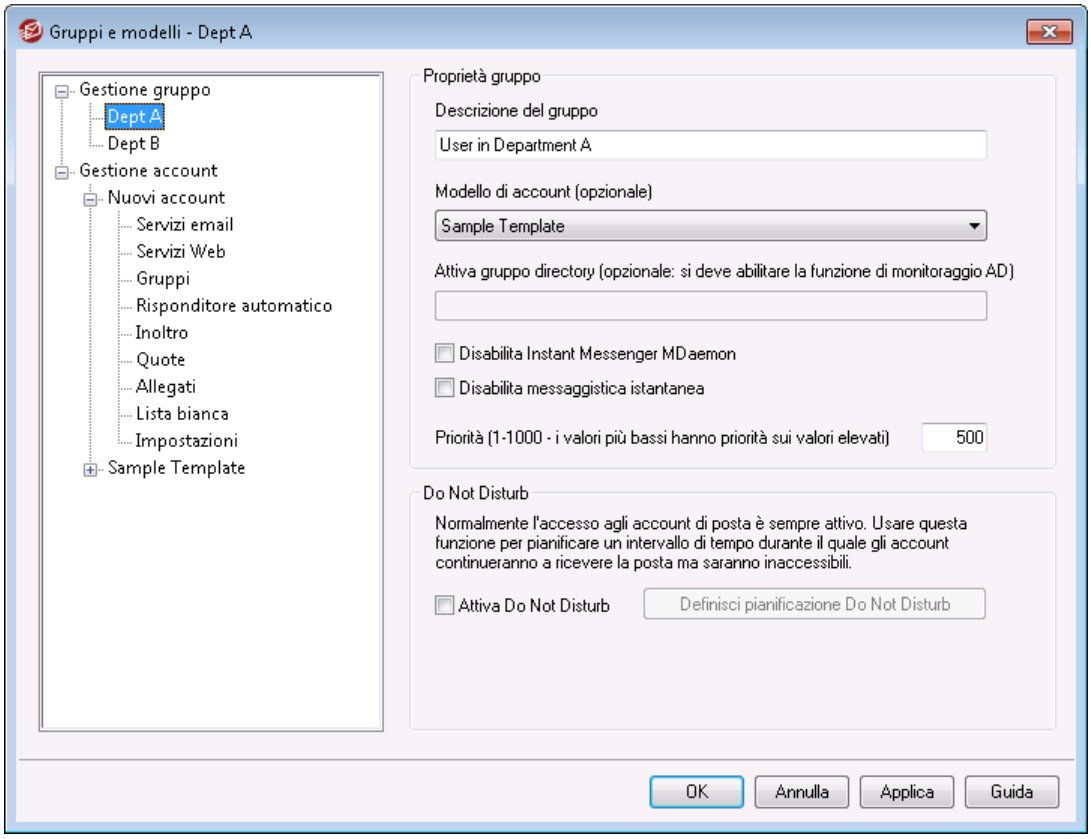
Aggiungi o rimuovi account dal gruppo selezionato

Per gestire l'appartenenza al gruppo, selezionarlo dall'elenco e fare clic su questo pulsante. Selezionare la casella di controllo accanto agli account che si desidera aggiungere al gruppo e deselezionare quella accanto ai membri da rimuovere. Fare clic su *OK*.

Vedere:

Cartella di posta e gruppi 732
Creazione di una nuova regola di Filtro contenuti 661
Cartelle condivise 120

5.2.1.1 Proprietà gruppo



Laschermata Proprietà gruppo (Account » Gruppi e modelli... » [nome del gruppo]) viene utilizzata per configurare le impostazioni di ciascun gruppo creato mediante Gestione gruppo 796. Per aprire Proprietà gruppo da Gestione gruppo, fare doppio clic sul gruppo da modificare o sul nome del gruppo nel riquadro sinistro. In questa schermata è possibile assegnare un Modello di account 806 a un gruppo, il che consente di controllare diverse impostazioni account per i membri del gruppo. È inoltre possibile collegare un gruppo a un gruppo di Active Directory, verificare se i membri dispongono o meno di accesso a MDaemon Instant Messenger (MDIM) 326 e alla messaggistica istantanea, quindi impostare un livello di priorità per il gruppo. Per controllare l'appartenenza a un gruppo, utilizzare Gestione gruppo e la schermata Cartella di posta e gruppi 732 in Account Editor.

Proprietà gruppo

Descrizione del gruppo
Inserire qui una descrizione del gruppo, come riferimento. Queste informazioni vengono generalmente immesse quando si crea il gruppo ma possono essere modificate in questa schermata in qualsiasi momento.

Modello di account (opzionale)
Se è stato creato un Modello di account 806 che si desidera utilizzare per controllare alcune delle impostazioni account per i membri del gruppo, utilizzare questo menu a discesa per selezionare il modello desiderato. Quando un modello di account è collegato a un gruppo, qualsiasi categoria di impostazioni account specificata in

Proprietà modello 808 verrà utilizzata per tutti gli account appartenenti al gruppo. Il modello verrà utilizzato per controllare le impostazioni anziché utilizzare le singole impostazioni dell'account in Account Editor. Se un account viene rimosso da un gruppo che stava controllando le relative impostazioni, queste ultime verranno ripristinate sui valori specificati dal Modello Nuovi account 807.

Se un account appartiene a più gruppi collegati a modelli diversi, tutti i modelli verranno utilizzati ovunque non siano presenti conflitti nelle proprietà del modello 808 specificate. Se più modelli vengono impostati per controllare le stesse proprietà, il primo modello elencato sarà quello che verrà utilizzato.

Gruppo Active Directory (opzionale - richiede il monitoraggio di AD)
Utilizzare questa opzione per collegare il gruppo a un gruppo Active Directory specifico. I membri del gruppo Active Directory vengono aggiunti automaticamente al gruppo di account, ma affinché l'operazione riesca, è necessario utilizzare la funzione Monitoraggio di Active Directory 841.

È possibile effettuare la mappatura di qualsiasi attributo Active Directory che si desidera utilizzare come meccanismo di attivazione per aggiungere gli account ai gruppi; tuttavia, l'attributo che verrà utilizzato con maggiore probabilità è l'attributo "`memberOf`". È possibile configurare questo attributo modificando `ActiveDS.dat` in Blocco note. Questa funzione è disabilitata per impostazione predefinita. Per abilitarla, modificare `ActiveDS.dat` e specificare l'attributo da utilizzare come meccanismo di attivazione per il gruppo in uso oppure rimuovere il commento dalla riga "`Groups=%memberOf%`" in `ActiveDS.dat` per utilizzarlo.

Disattiva MDaemon Instant Messenger
Selezionare questa casella di controllo se si desidera disattivare il supporto per MDIM per tutti i membri del gruppo.

> **Disabilita messaggistica istantanea**
> Selezionare questa casella di controllo se si desidera consentire il supporto per MDIM ma non la sua funzione di messaggistica istantanea.

Priorità (1-1000 - i valori più bassi hanno priorità sui valori elevati)
Utilizzare questa opzione per impostare un livello di priorità (1-1000) per i gruppi in uso affinché gli account possano essere membri di più gruppi ed evitare possibili conflitti tra impostazioni di gruppo. Ad esempio, quando un account è membro di più gruppi, ciascuno dei quali presenta un modello di account collegato che controlla le stesse impostazioni, verranno utilizzate le impostazioni per il gruppo con la prima priorità. In altre parole, un gruppo con un valore di priorità "1" starà al di sopra di un gruppo con valore "10". In assenza di conflitto, le impostazioni di ciascun gruppo vengono applicate collettivamente. In caso di collegamento, il primo gruppo trovato ha la priorità. Quando un account viene rimosso da un gruppo collegato a un modello di account, le impostazioni dell'account precedentemente controllate dal modello di account diventeranno le impostazioni dell'account specificate dal successivo gruppo di priorità. Se non è presente un altro gruppo che controlla tali impostazioni, queste ultime verranno ripristinate sui valori specificati dal Modello Nuovi account 807.

Crea la firma del cliente
Fare clic su questo pulsante se si desidera aggiungere una firma del cliente da utilizzare per i membri del gruppo. Vedi: Firma del cliente di gruppo 801

Non disturbare

Utilizzare la funzione Non disturbare per pianificare un periodo di tempo durante il quale un account non può inviare messaggi di e-mail o accettare l'acceso degli utenti a esso associati. L'accesso durante un periodo Non disturbare non è consentito e restituisce una risposta di errore appropriata alle richieste di accesso IMAP, POP, SMTP, ActiveSync e Webmail. MDaemon accetta la posta in arrivo per gli account in questo stato, ma tali account non possono comunque inviare messaggi o accettare l'acceso degli utenti di posta.

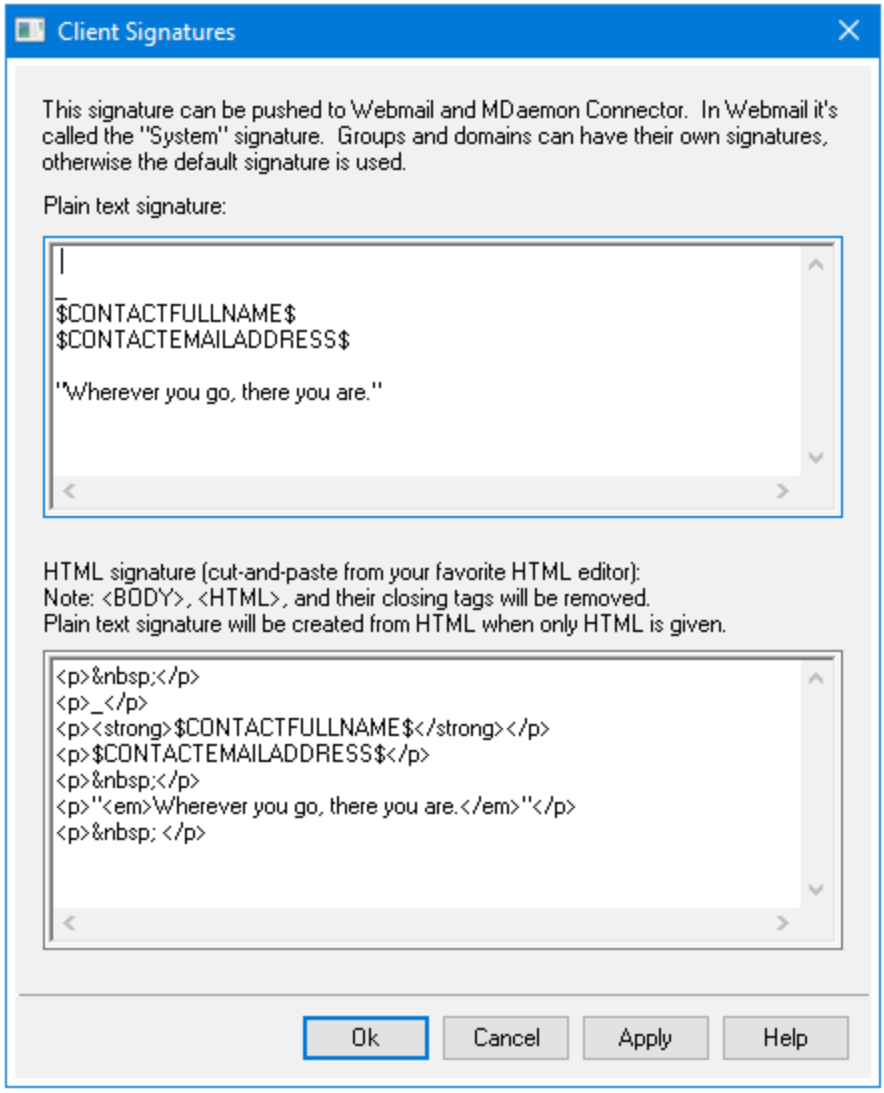
Per applicare l'opzione Non disturbare a uno o più account:

1. Fare clic su **Attiva non disturbare**.
2. Fare clic su **Definisci pianificazione Non disturbare**.
3. Impostare le date gli orari di inizio e fine, con i giorni della settimana in cui si intende attivare la funzione.
4. Fare clic su **OK**.
5. Utilizzare Gestione gruppo 796 per assegnare gli account a questo gruppo.

Vedere:

Gestione gruppo 796
Cartella di posta e gruppi 732
Gestione account 806
Proprietà modello 808

5.2.1.1.1 Firme client



Ora è possibile impostare una firma client per ogni gruppo. La firma client viene inviata via push ai membri che utilizzano Webmail[354] o MDaemon Connector[413]. Una firma client del gruppo sostituisce l'eventuale firma client del dominio[211], che a sua volta sostituisce la firma client predefinita[141]. Nell'interfaccia grafica di MDaemon passare ad Account | Gruppi e modelli per modificare un gruppo e impostare la firma client corrispondente. Per rimuovere una firma client, cancellare il testo nell'editor.

Firme in formato solo testo

Quest'area è destinata all'inserimento di una firma in formato solo testo. Per indicare una firma html corrispondente da utilizzare nella parte testo/html dei messaggi multipart, utilizzare l'area *Firma HTML*. Se una firma è inclusa in entrambe le posizioni, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non viene specificata alcuna firma html, in entrambe le parti viene utilizzata la firma in formato solo testo.

Firma HTML (copiare e incollare la firma dall'editor HTML desiderato)

Quest'area è destinata all'inserimento di una firma html da utilizzare nella parte testo/html dei messaggi multipart. Se una firma è inclusa qui e nell'area *Firme in formato solo testo*, MDaemon utilizza quella appropriata per ciascuna parte del messaggio multipart. Se non è specificata una firma in formato solo testo, verrà utilizzato il formato HTML per crearne una.

Per creare la firma html, digitare il codice HTML manualmente o tagliarlo e incollarlo direttamente dall'editor HTML desiderato. Per includere le immagini in linea nella firma HTML, è possibile utilizzare la macro `$ATTACH_INLINE:path_to_image_file$`.

Ad esempio,

```
<IMG border=0 hspace=0 alt="" align=baseline src="$ATTACH_INLINE:c:
  \images\mr_t_and_arnold.jpg$">
```

È inoltre possibile utilizzare diversi metodi per inserire immagini in linea nelle firme dall'interfaccia Web di MDaemon Remote Administration 359:

- Nella schermata Firme client in Remote Administration, fare clic sul pulsante "Immagine" della barra degli strumenti nell'editor HTML e selezionare la scheda di caricamento.
- Nella schermata Firme client in Remote Administration, fare clic sul pulsante "Aggiungi immagine" della barra degli strumenti nell'editor HTML.
- Trascinare un'immagine nella schermata Firme client dell'editor HTML con Chrome, FireFox, Safari o MSIE 10+
- Copiare e incollare un'immagine dagli Appunti nella schermata Firme client dell'editor HTML con Chrome, FireFox, MSIE 11+

I tag <body></body> e <html></html> non sono consentiti nelle firme e saranno rimossi se trovati.

Macro firme

Le firme di MDaemon supportano le macro per l'inserimento delle informazioni di contatto del mittente nella firma, estratte dal contatto del mittente disponibile nella cartella Contatti pubblici del suo dominio. Questo consente la personalizzazione delle firme predefinite e di dominio con le informazioni del mittente. Ad esempio, `$CONTACTFULLNAME$`, inserisce il nome completo del mittente e `$CONTACTEMAILADDRESS$` inserisce l'indirizzo di posta elettronica del mittente. Utilizzare Webmail, MDaemon Connector o ActiveSync per modificare i contatti pubblici. I campi vengono lasciati vuoti se non esistono i dati del mittente. Le macro disponibili sono riportate di seguito.

Gli utenti possono controllare il posizionamento delle firme di MDaemon nei messaggi utilizzando la macro `$SYSTEMSIGNATURE$` per inserire la firma predefinita/dominio e

`$ACCOUNTSIGNATURE$` per inserire la firma dell'account.

Selettore di firme	
$SYSTEMSIGNATURE$	Places the Default Signature 136 or Domain Signature 206 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 141 or Domain Client Signature 211 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 769 in the message.
Nomi e ID	
Nome completo	**$CONTACTFULLNAME$**
Nome	**$CONTACTFIRSTNAME$**
Secondo nome	**$CONTACTMIDDLENAME$,**
Cognome	**$CONTACTFIRSTNAME$**
Titolo	**$CONTACTTITLE$**
Suffisso	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Trascrizione fonetica nome	**$CONTACTYOMIFIRSTNAME$**
Trascrizione fonetica cognome	**$CONTACTYOMILASTNAME$**
Nome account	**$CONTACTACCOUNTNAME$**
ID cliente	**$CONTACTCUSTOMERID$**
ID governo	**$CONTACTGOVERNMENTID$**
Archivia come	**$CONTACTFILEAS$**
Indirizzi e-mail	
Indirizzo e-mail	**$CONTACTEMAILADDRESS$**
Indirizzo e-mail 2	**$CONTACTEMAILADDRESS2$**
Indirizzo e-mail 3	**$CONTACTEMAILADDRESS3$**
Numeri di telefono e fax	
Numero di cellulare	**$CONTACTHOMEMOBILE$**
Numero di cellulare 2	**$CONTACTMOBILE2$**

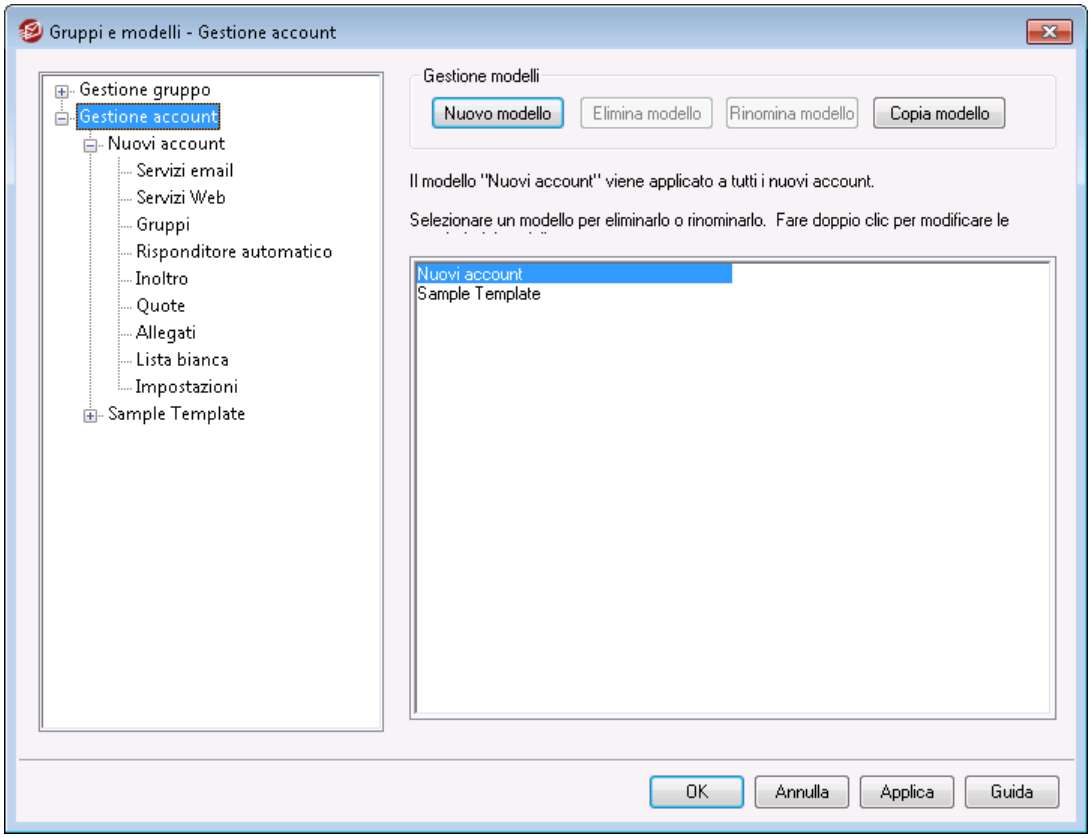
Telefono in macchina	**$CONTACTCARPHONENUMBER$**
Telefono di casa	**$CONTACTHOMEPHONE$**
Telefono di casa 2	**$CONTACTHOMEPHONE2$**
Fax di casa	**$CONTACTHOMEFAX$**
Altro telefono	**$CONTACTOTHERPHONE$**
Messaggistica istantanea e Web	
Indirizzo messaggistica istantanea	**$CONTACTIMADDRESS$**
Indirizzo messaggistica istantanea 2	**$CONTACTIMADDRESS2$**
Indirizzo messaggistica istantanea 3	**$CONTACTIMADDRESS3$**
Indirizzo MMS	**$CONTACTMMSADDRESS$**
Indirizzo web personale	**$CONTACTHOMEWEBADDRESS$**
Indirizzo	
Indirizzo di casa	**$CONTACTHOMEADDRESS$**
Città di residenza	**$CONTACTHOMECITY$**
Provincia di residenza	**$CONTACTHOMESTATE$**
CAP residenza	**$CONTACTHOMEZIPCODE$**
Paese di residenza	**$CONTACTHOMECOUNTRY$**
Altro indirizzo	**$CONTACTOTHERADDRESS$**
Altra città	**$CONTACTOTHERCITY$**
Altra provincia	**$CONTACTOTHERSTATE$**
Altro CAP	**$CONTACTOTHERZIPCODE$**
Altro Paese	**$CONTACTOTHERCOUNTRY$**
Relative al lavoro	
Nome dell'azienda	**$CONTACTBUSINESSCOMPANY$**
Nome fonetico dell'azienda	**$CONTACTYOMICOMPANYNAME$**
Mansione lavorativa	**$CONTACTBUSINESSTITLE$**
Ufficio	**$CONTACTBUSINESSOFFICE$**
Reparto dell'azienda	**$CONTACTBUSINESSDEPARTMENT$**

Responsabile dell'azienda	$CONTACTBUSINESSMANAGER$
Assistente in azienda	$CONTACTBUSINESSASSISTANT$
Telefono assistente in azienda	$CONTACTBUSINESSASSISTANTPHONE$
Telefono principale dell'azienda	$CONTACTBUSINESSMAINPHONE$
Telefono al lavoro	$CONTACTBUSINESSPHONE$
Telefono al lavoro 2	$CONTACTBUSINESSPHONE2$
Telefono IP al lavoro	$CONTACTBUSINESSIPPHONE$
Fax di lavoro	$CONTACTBUSINESSFAX$
Cercapersone in azienda	$CONTACTBUSINESSPAGER$
Radiotelefono in azienda	$CONTACTBUSINESSRADIO$
Indirizzo di lavoro	$CONTACTBUSINESSADDRESS$
Città di lavoro	$CONTACTBUSINESSCITY$
Provincia di lavoro	$CONTACTBUSINESSSTATE$
CAP di lavoro	$CONTACTBUSINESSZIPCODE$
Paese di lavoro	$CONTACTBUSINESSCOUNTRY$
Indirizzo Web aziendale	$CONTACTBUSINESSWEBADDRESS$
Altro	
Coniuge	$CONTACTSPOUSE$
Figli	$CONTACTCHILDREN$
Categorie	$CONTACTCATEGORIES$
Commento	$CONTACTCOMMENT$

Vedere:

Firme client predefinite 141
Firme predefinite 136
Domain Manager » Firme 206
Account Editor » Firma 769
Domain Manager » Impostazioni Webmail 198
Impostazioni client MC » Firma 413

5.2.2 Gestione account



Con il modello Gestione account (Account » Gruppi e modelli... » Gestione account) è possibile creare e gestire modelli di account, ovvero set denominati di impostazioni account che possono essere assegnate a Gruppi[796] specifici. Per ogni account appartenente a uno o più gruppi, le impostazioni degli account designate sono bloccate, in quanto vengono controllate solo dai modelli assegnati anziché da Account Editor. Le categorie di impostazioni degli account controllate da un modello sono specificate nella schermata delle proprietà[808] di ciascun modello, a cui è possibile accedere facendo doppio clic sul nome del modello nell'elenco riportato di seguito o facendo clic sul modello nel riquadro di sinistra.

Gestione modelli

Nuovo modello

Per creare un nuovo modello di account, fare clic su *Nuovo modello*, digitare un nome per il modello e fare clic su *OK*. Il nuovo modello viene visualizzato nell'elenco dei modelli riportato di seguito e nel riquadro di sinistra.

Elimina modello

Per eliminare un modello, selezionare il modello nell'elenco riportato di seguito, fare clic su *Elimina modello*, quindi fare clic su *Sì* per confermare l'eliminazione del modello.

Rinomina modello
Per rinominare un modello, selezionare il modello nell'elenco riportato di seguito, quindi fare clic su *Rinomina modello*. Digitare un nuovo nome del modello, quindi fare clic su *OK*.

Copia modello
Per creare un modello con impostazioni che corrispondono a un altro modello, selezionare un modello dall'elenco, fare clic su questo pulsante e specificare un nome per il nuovo modello.

Elenco modelli

L'elenco nella parte inferiore di Gestione account contiene tutti i modelli. Fare clic su un modello e utilizzare i pulsanti nella parte superiore della schermata per eliminarlo o rinominarlo. Fare doppio clic su un modello per aprire la schermata delle proprietà 808 corrispondente, da cui è possibile designare le categorie di impostazioni degli account che verranno controllate dal modello. È possibile accedere direttamente al modello desiderato e alle relative impostazioni account utilizzando i comandi disponibili nel riquadro di sinistra. Il modello *Nuovi account* è un modello speciale che viene sempre visualizzato per primo nell'elenco.

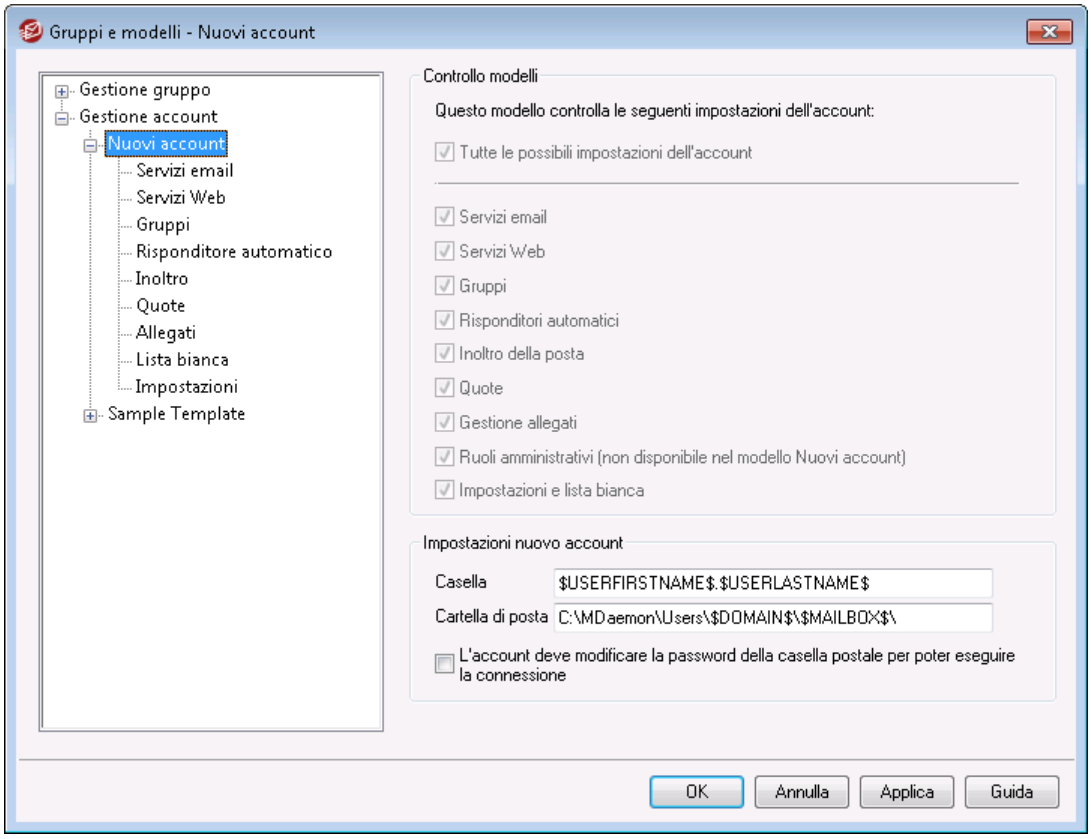
Modello Nuovi account

Il modello *Nuovi account* è un modello speciale che viene applicato a tutti i nuovi account in fase di creazione. Anziché bloccare e controllare determinate impostazioni degli account, analogamente agli altri modelli, il modello *Nuovi account* viene utilizzato semplicemente per specificare le impostazioni iniziali per i nuovi account. Queste impostazioni iniziali possono essere modificate normalmente utilizzando Account Editor per modificare i singoli account. Alcune impostazioni del modello, come le opzioni che si trovano nella schermata Ruoli amministrativi 830, non sono disponibili per il modello Nuovi account.

Vedere:

Proprietà modello 808
Gestione gruppo 796

5.2.2.1 Proprietà modello



Per accedere alla schermata delle proprietà di un modello, aprire Gestione account 806 e fare clic sul nome del modello nel riquadro di sinistra. Utilizzare la schermata delle proprietà di ciascun modello per specificare le categorie di impostazioni degli account che verranno controllate dal modello. Per ogni account appartenente a un Gruppo 796 che utilizza un modello di account, le schermate di Account Editor corrispondenti saranno bloccate, in quanto tali impostazioni verranno controllate dal modello. Se un account appartiene a più gruppi collegati a modelli diversi, tutti i modelli verranno utilizzati ovunque non siano presenti conflitti nelle proprietà del modello specificate. Se più modelli vengono impostati per controllare le stesse proprietà, il primo modello elencato sarà quello che verrà utilizzato.

Controllo modelli

Tutte le possibili impostazioni dell'account
Fare clic su questa casella di controllo se si desidera che il modello controlli tutte le impostazioni degli account disponibili per i Gruppi 796 che utilizzano il modello. Verranno utilizzate tutte le schermate del modello relative alle impostazioni degli account dei membri di ciascun gruppo anziché le schermate corrispondenti con lo stesso nome di Account Editor. Deselezionare questa casella di controllo se si desidera selezionare specifiche impostazioni degli account da controllare mediante le opzioni delle *Impostazioni account* riportate di seguito.

Impostazioni account
Questa sezione elenca tutte le categorie di impostazioni degli account che possono essere controllate dal modello per i gruppi che utilizzano il modello. Ogni opzione corrisponde alla schermata del modello con lo steso nome. Quando si seleziona un'opzione, vengono utilizzate le impostazioni della schermata del modello specificato anziché le impostazioni della schermata di Account Editor corrispondente per i membri dei gruppi associati.

Impostazioni nuovo account

Queste opzioni sono disponibili solo nel modello Nuovi account 807. Utilizzano numerose macro speciali 810 per la generazione automatica della cartella di memorizzazione della posta e della parte dell'indirizzo e-mail relativa alla casella postale per i nuovi account.

Casella
Utilizzare questo campo per controllare la parte relativa al *Nome casella postale* 729 predefinito dell'indirizzo e-mail che verrà generato per i nuovi account. Per un elenco delle macro utilizzabili in questa stringa di modello, vedere la sezione Macro dei modelli 810 riportata di seguito. Per questa opzione, il modello predefinito è "`$USERFIRSTNAMELC$.$USERLASTNAMELC$`". Pertanto, la creazione di un account per "Michele Masone" nel dominio esempio.com darà come risultato l'indirizzo "`michele.masone@esempio.com`".

Cartella di posta
Utilizzare questo campo per controllare la *Cartella di posta* 732 predefinita che verrà utilizzata per i nuovi account. La *cartella della posta* di ogni account rappresenta la posizione in cui vengono memorizzati i relativi messaggi e-mail nel server. Ad esempio, "`...\$DOMAIN$\$MAILBOX$\`" consente di creare il percorso "`...\esempio.com\michele.masone\`" per l'utente "michele.masone@esempio.com".

MDaemon supporta un sistema di base di hashing delle cartelle. In NTFS, ad esempio, mantenere numerose cartelle sotto la stessa radice può avere talvolta un effetto negativo sulle prestazioni. Se si dispone di un numero elevato di utenti e si desidera suddividere le cartelle degli utenti utilizzando un valore diverso dall'impostazione predefinita di `$DOMAIN$\$MAILBOX$\`, è possibile utilizzare la macro `$MAILBOXFIRSTCHARSn$` per eseguire questa operazione. In questa macro, il valore "`n`" è un numero compreso tra 1 e 10. La macro viene espansa ai primi "`n`" caratteri del nome della casella postale. Se si modifica il percorso predefinito della *Cartella di posta* seguendo un metodo simile a quello riportato di seguito, sarà possibile ottenere un sistema di hashing delle cartelle sufficientemente valido:

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\.
```

L'account deve modificare la password della casella postale per poter eseguire la connessione
Questa opzione controlla se il nuovo account deve modificare o meno la *Password casella postale* prima dell'accesso a POP, IMAP, SMTP, Webmail o Remote Administration. L'utente può connettersi a Webmail o a Remote Administration ma gli verrà richiesto di modificare la password prima di procedere. Tuttavia, affinché gli utenti possano modificare le password via Webmail o Remote Administration, devono prima ottenere l'autorizzazione di accesso Web "*...modifica password*" nella schermata Servizi Web 814. Dopo la modifica della password questa opzione verrà disattivata nella schermata Dettagli account 729 dell'account.

Poiché la modifica della password potrebbe non essere semplice o possibile per alcuni utenti, prestare attenzione prima di attivare questa opzione.

Macro dei modelli

Di seguito è riportato un elenco di riferimento rapido di tutte le macro disponibili per l'automazione della configurazione degli account.

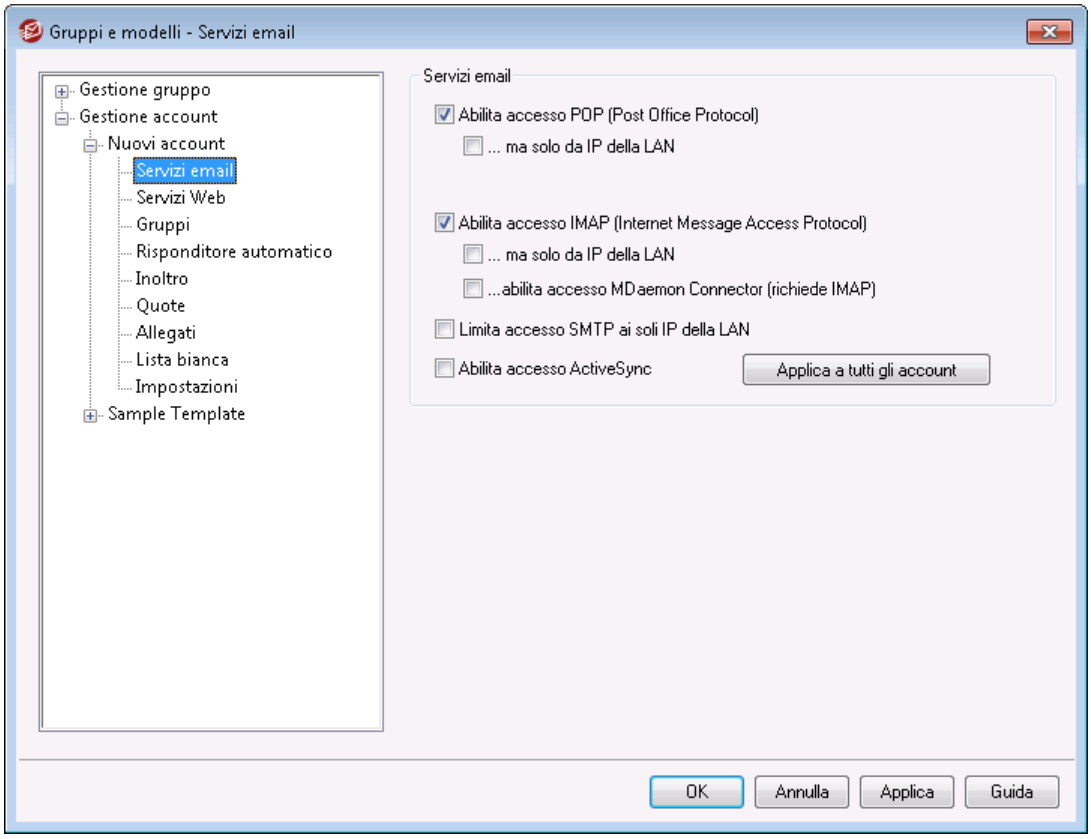
`$DOMAIN$`	Questa variabile viene sostituita dal nome di dominio selezionato per l'account.
`$DOMAINIP$`	Questa variabile viene sostituita dall'indirizzo IPv4 associato al dominio attualmente selezionato per l'account.
`$DOMAINIP6$`	Questa variabile viene sostituita dall'indirizzo IPv6 associato al dominio attualmente selezionato per l'account.
`$MACHINENAME$`	Questa macro restituisce il nome host del dominio predefinito, dalla schermata Nome host e IP di Manager dominio. La macro viene utilizzata per le nuove installazioni nello script contenente informazioni predefinite sugli account (NEWUSERHELP.DAT).
`$USERNAME$`	Questa variabile viene sostituita dal nome e cognome del titolare dell'account. Questo campo equivale a "$USERFIRSTNAME$ $USERLASTNAME$"
`$USERFIRSTNAME$`	Questa variabile viene sostituita dal nome del titolare dell'account.
`$USERFIRSTNAMELC$`	Questa variabile viene sostituita dal nome del titolare dell'account in lettere minuscole.

$USERLASTNAME$	Questa variabile viene sostituita dal cognome del titolare dell'account.
$USERLASTNAMELC$	Questa variabile viene sostituita dal cognome del titolare dell'account in lettere minuscole.
$USERFIRSTINITIAL$	Questa variabile viene sostituita dalla prima lettera del nome del titolare dell'account.
$USERFIRSTINITIALLC$	Questa variabile viene sostituita dalla prima lettera del nome del titolare dell'account in lettere minuscole.
$USERLASTINITIAL$	Questa variabile viene sostituita dalla prima lettera del cognome del titolare dell'account.
$USERLASTINITIALLC$	Questa variabile viene sostituita dalla prima lettera del cognome del titolare dell'account in lettere minuscole.
$MAILBOX$	Questa variabile viene sostituita dal nome della casella postale dell'account corrente. Il valore verrà utilizzato anche come valore del comando USER trasmesso durante le sessioni di posta POP3.
$MAILBOXFIRSTCHARSn$	Dove "n" è un numero compreso tra 1 e 10. La macro viene sostituita con i primi "n" caratteri del nome della casella postale.

Vedere:

Gestione account 806
Gestione gruppo 796

5.2.2.1.1 Servizi di posta



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Servizi di posta[733] di Account Editor. Quando è configurato per il controllo di questa schermata[808], il modello controlla le opzioni relative ai servizi di posta per qualsiasi account appartenente a un Gruppo[798] che utilizza il modello.

Servizi di posta

Abilita accesso POP (Post Office Protocol)
Quando questa casella è selezionata, è possibile accedere agli account con le impostazioni controllate da questo modello mediante Post Office Protocol (POP). Questo protocollo è supportato da tutti i software client di posta elettronica. Se non si desidera consentire l'accesso POP, deselezionare questa casella di controllo.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che gli account siano accessibili tramite POP solo quando l'utente si connette da un indirizzo IP LAN[620].

Abilita accesso IMAP (Internet Message Access Protocol)
Quando questa casella è selezionata, è possibile accedere agli account con le impostazioni controllate da questo modello mediante Internet Message Access Protocol (IMAP). Il protocollo IMAP è più versatile del protocollo POP, in quanto consente di gestire la posta elettronica dal server e di accedervi mediante più client. Questo protocollo è supportato dalla maggior parte dei client di posta elettronica.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che gli account siano accessibili tramite IMAP solo quando l'utente si connette da un indirizzo IP LAN 620.

...abilita accesso MDaemon Connector (richiede IMAP)
Questa opzione è disponibile solo nel modello Nuovi account. Fare clic su questa opzione per consentire ai titolari dell'account di utilizzare MDaemon Connector 395.
Nota: questa opzione sarà disponibile solo quando sul server è attivato il supporto di MDaemon Connector.

Limita accesso SMTP ai soli IP della LAN
Selezionare questa casella di controllo se si desidera limitare accesso SMTP ai soli IP della LAN. Questo impedirà agli account di inviare messaggi a meno che non siano connessi alla rete. Se l'account tenta di inviare la posta da un indirizzo IP esterno, la connessione verrà rifiutata e chiusa.

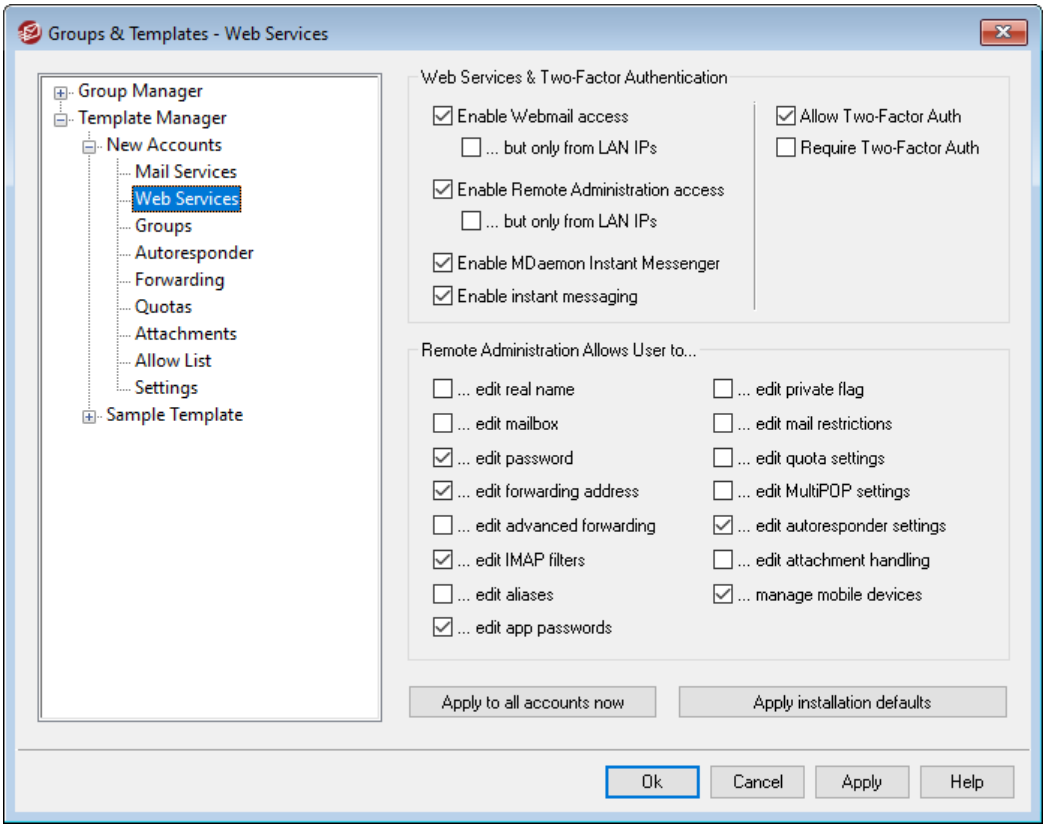
Abilita accesso ActiveSync
Questa opzione è disponibile solo nel modello Nuovi account. Selezionare questa casella per consentire ai nuovi account di utilizzare ActiveSync su un dispositivo mobile per sincronizzare e-mail, contatti, calendario e altri dati con MDaemon/Webmail. Questa impostazione corrisponde all'opzione*Abilita servizi ActiveSync per questo utente* disponibile nella schermata ActiveSync per MDaemon 779 di Acount Editor.

Applica a tutti gli account
Questa opzione è disponibile solo nel modello Nuovi account. Fare clic su questo pulsante per applicare immediatamente le impostazioni di questa schermata alle schermate Servizi di posta 733 e ActiveSync per MDaemon 779 di tutti gli account MDaemon esistenti.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Servizi di posta 733

5.2.2.1.2 Servizi Web



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Servizi Web[735] di Account Editor. Quando è configurato per il controllo di questa schermata[808], il modello controlla le opzioni relative ai servizi Web per qualsiasi account appartenente a un Gruppo[798] che utilizza il modello.

Servizi Web e Autenticazione a due fattori

Abilita accesso Webmail
Selezionare questa casella di controllo se si desidera autorizzare gli account controllati da questo modello ad accedere al server Webmail[325], che consente di accedere ai messaggi e-mail, ai calendari e ad altre funzioni mediante un browser Web.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che gli account associati accedano a Webmail solo quando la connessione viene eseguita da un indirizzo IP LAN[620].

Abilita accesso amministrazione Web
Selezionare questa casella se si desidera consentire agli account controllati da questo modello di modificare le proprie impostazioni mediante Remote Administration[359]. Gli account potranno modificare solo le impostazioni specificate successivamente.

Se si abilita questa funzione e se il server Remote Administration è attivo, è possibile accedere a Remote Administration inserendo nel browser il dominio di MDaemon desiderato e la porta assegnata a Remote Administration 361 (ad esempio, `http://esempio.com:1000`). Dapprima viene visualizzata una schermata di registrazione, quindi la schermata delle impostazioni che si è autorizzati a modificare. È sufficiente modificare le impostazioni desiderate e fare clic sul pulsante *Salva modifiche*. Quindi, uscire e chiudere il browser. Se si dispone dell'accesso a Webmail è possibile accedere a Remote Administration anche dal menu Opzioni avanzate di Webmail.

Se l'utente è un amministratore globale o un amministratore di dominio, privilegio indicato nella schermata Ruoli amministrativi 773 di Account Editor, dopo l'accesso a Remote Administration verrà visualizzata una schermata diversa.

...ma solo da indirizzi IP LAN
Selezionare questa casella se si desidera che l'account acceda a Remote Administration solo quando la connessione viene eseguita da un indirizzo IP LAN 620.

Abilita MDaemon Instant Messenger
Fare clic su questa casella per abilitare il supporto predefinito di MDIM 326 per i nuovi account. Questa opzione è disponibile solo nel modello Nuovi account 807. Un'opzione simile è disponibile in Proprietà gruppo 798 che può essere utilizzata per controllare l'accesso dei membri dei gruppi a MDIM.

Abilita messaggistica istantanea
Fare clic su questa casella per abilitare il supporto predefinito per il sistema di messaggistica istantanea di MDIM per i nuovi account. Questa opzione è disponibile solo nel modello Nuovi account 807. Un'opzione simile è disponibile in Proprietà gruppo 798 che può essere utilizzata per controllare l'accesso dei membri dei gruppi al sistema di messaggistica istantanea.

Autenticazione a due fattori

MDaemon supporta l'autenticazione a due fattori (2FA) per gli utenti che accedono all'interfaccia Web di Webmail o Remote Administration di MDaemon. Gli account che accedono a Webmail via HTTPS possono attivare l'autenticazione a due fattori per l'account nella schermata **Opzioni » Sicurezza** di Webmail. Da quel momento l'utente quando accede a Webmail o Remote Administration dovrà immettere un codice di verifica. Il codice viene fornito all'accesso da una app di autenticazione installata nel dispositivo mobile o tablet dell'utente. Questa funzione è progettata per i client che supportano Google Authenticator. Vedere il file della Guida in linea di Webmail per ulteriori informazioni sull'impostazione della 2FA per un account.

Consenti autenticazione a due fattori
Per impostazione predefinita i nuovi account possono impostare e utilizzare la funzione di autenticazione a due fattori di Webmail (2FA). Selezionare questa casella di controllo se non si desidera consentire la 2FA dei nuovi account per impostazione predefinita. Non è possibile controllare questa impostazione per account specifici nella pagina Servizi Web 735 per ciascun account.

Richiedi autenticazione a due fattori
Attivare questa opzione per forzare l'uso dell'autenticazione a due fattori (2FA) per tutti i nuovi account che accedono a Webmail o all'interfaccia Web di amministrazione remota di MDaemon. Quando la 2FA è obbligatoria, gli account che non sono stati ancora configurati per utilizzarla e tentano di accedere a Webmail vengono reindirizzati alla pagina di configurazione corrispondente. Vedere il file della Guida in linea di Webmail per ulteriori informazioni sull'impostazione della 2FA per un account.

Remote Administration consente agli utenti di...

...modificare il nome reale
Abilitando questa funzione, gli account associati a questo modello possono modificare l'impostazione *Nome e cognome* 729.

...modificare la casella postale
Abilitando questa funzione, gli utenti sono autorizzati a modificare l'impostazione *Nome casella postale* 729.

Poiché il *Nome casella postale* fa parte dell'indirizzo e-mail dell'account e rappresenta l'identificativo univoco e il valore dell'ID utente utilizzato per l'account, la modifica di questa opzione determina la modifica dell'effettivo indirizzo e-mail dell'utente. Ciò può determinare il rifiuto, l'eliminazione o comunque la perdita dei futuri messaggi diretti al precedente indirizzo.

...modificare la password
Selezionare questa casella di controllo per consentire agli account di modificare la *Password casella postale*. Per ulteriori informazioni sui requisiti delle password, vedere: Password 870.

...modificare l'indirizzo di inoltro
Quando questa funzione è abilitata, gli account associati al modello sono in grado di modificare le impostazioni dell'indirizzo di inoltro 742.

...modificare l'inoltro avanzato
Quando si attiva questa funzionalità, gli utenti vengono autorizzati a modificare le *impostazioni di inoltro avanzate* 742.

...modificare i filtri IMAP
Utilizzare questa opzione per consentire all'utente di creare e gestire i propri Filtri IMAP 751.

...modifica alias
Selezionare questa opzione per consentire ai titolari dell'account di utilizzare Remote Administration per modificare gli Alias 756 associati al proprio account.

...modificare le password di applicazione
Per impostazione predefinita, gli utenti possono modificare le proprie password di applicazione[766]. Se si desidera impedire all'utente di modificarle, deselezionare questa casella di controllo.

...modificare il flag privato
Questa opzione consente di decidere se ciascun utente è autorizzato o meno a utilizzare Remote Administration per modificare l'opzione "*Account nascosto da elenchi "Everyone", calendari condivisi e VRFY*" disponibile nella schermata Impostazioni[776] dell'editor degli account.

...modificare le restrizioni di posta
Questa casella di controllo consente di autorizzare l'account alla modifica delle limitazioni relative alla posta in entrata e in uscita, situate nella schermata Restrizioni[744].

...modificare le impostazioni di quota
Con questa casella di controllo è possibile consentire all'account la modifica delle impostazioni relative alla Quota[746].

...modificare le impostazioni MultiPOP
Selezionare questa casella di controllo per consentire all'account di aggiungere nuove voci MultiPOP[754] e di attivare/disattivare la raccolta di posta MultiPOP per tali voci.

...modificare le impostazioni di risposta automatica
Selezionare questa casella di controllo per consentire all'utente di aggiungere, modificare o eliminare le Risposte automatiche[739] per il proprio account.

...modifica gestione allegati
Se si seleziona questa casella, l'utente ha la possibilità di modificare le opzioni di gestione degli allegati dell'account nella schermata Allegati[749].

...gestisce dispositivo mobile
Selezionare questa opzione per consentire al proprietario dell'account di utilizzare Remote Administration per la gestione delle impostazioni specifiche per i dispositivi, ad esempio per i dispositivi ActiveSync.

Applica a tutti gli account

Questa opzione è disponibile solo nel modello Nuovi account[807]. Fare clic su questa opzione per applicare le impostazioni di questa schermata a tutti gli account di MDaemon esistenti che non sono specificamente controllati da un modello di account Servizi Web.

Applica valori predefiniti di installazione

Questa opzione è disponibile solo nel modello Nuovi account[807]. Fare clic su questa opzione per ripristinare i valori predefiniti di installazione del modello Nuovi account. Vengono modificate solo le impostazioni del modello. Gli account esistenti non verranno modificati.

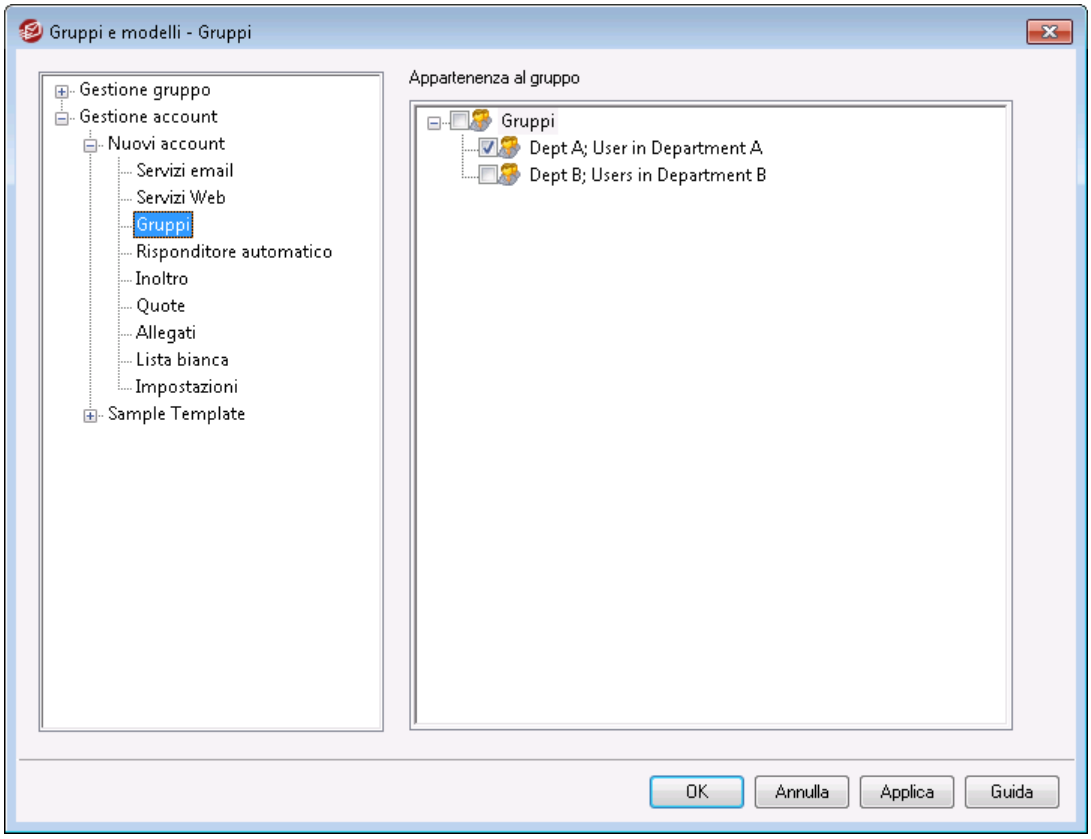
Carica impostazioni modello "Nuovi account"

Questa opzione è disponibile solo per i modelli personalizzati. Fare clic su questa opzione per impostare le opzioni di questa schermata sui valori predefiniti indicati nella schermata Servizi Web del modello Nuovi account 807.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Servizi Web 735

5.2.2.1.3 Gruppi



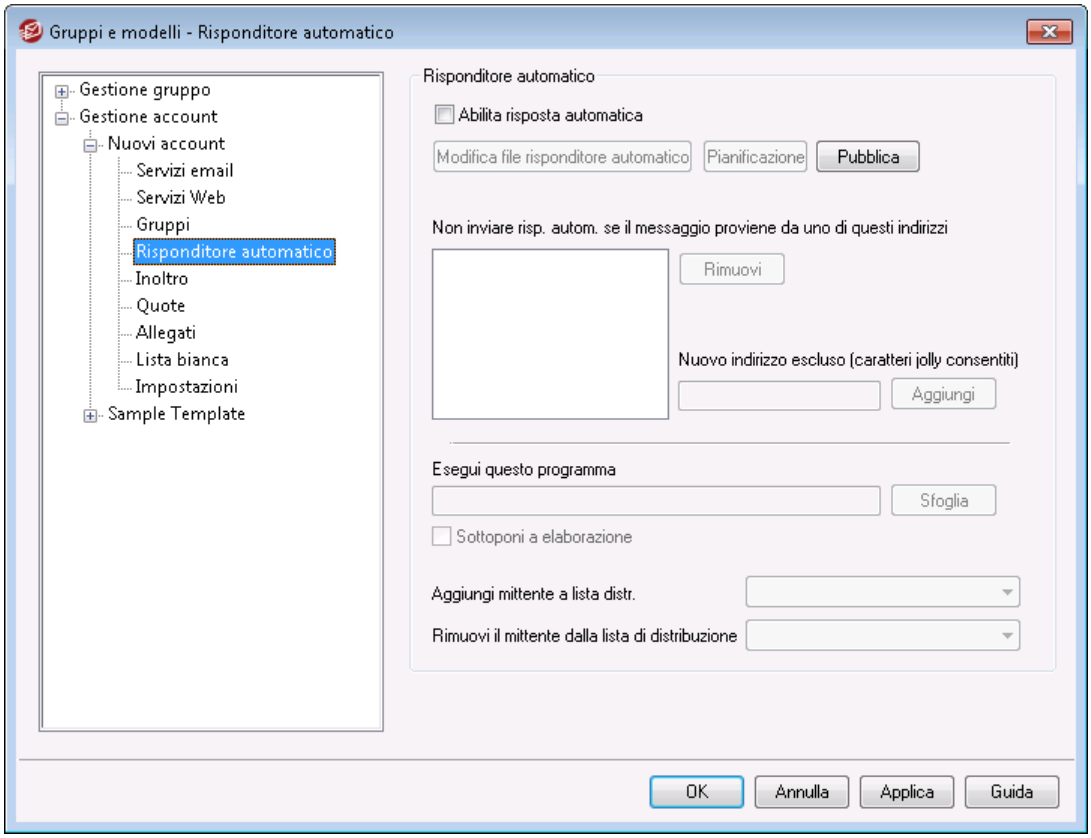
Appartenenza ai gruppi

Questa schermata è disponibile solo nel modello Nuovi account 807 e corrisponde alla sezione Appartenenza a gruppo della schermata Cartelle e gruppi di posta 732 di Account Editor. Quando si seleziona uno o più gruppi in questa schermata, i nuovi account vengono automaticamente aggiunti a tali gruppi.

Vedere:

Modello Nuovi account 807
Gestione gruppo 796
Proprietà gruppo 798

5.2.2.1.4 Risposta automatica



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Risposta automatica 739 di Account Editor. Quando è configurato per il controllo di questa schermata 808, il modello controlla le opzioni di risposta automatica per qualsiasi account appartenente a un Gruppo 798 che utilizza il modello.

Le risposte automatiche sono strumenti utili che consentono, in base ai messaggi e-mail in arrivo, di attivare eventi specifici quali l'esecuzione di un programma, l'inserimento di un mittente in una lista di distribuzione, l'invio di una risposta con un messaggio generato automaticamente e altro ancora. L'utilizzo più comune delle risposte automatiche consiste nella risposta automatica ai messaggi in entrata con un messaggio definito dall'utente con il quale viene comunicato che il destinatario è in vacanza, non è disponibile, risponderà appena possibile e così via. Gli utenti di MDaemon con Accesso Web 735 a Webmail 325 o Remote Administration 359 possono utilizzare le opzioni disponibili per comporre propri messaggi di risposta automatica e pianificare le relative date di utilizzo. Infine, i messaggi di risposta automatica sono basati sul contenuto del file `OOF.mrk` che si trova nella cartella radice `\data\` di

ciascun utente. Questo file supporta un elevato numero di macro, che possono essere utilizzate per la generazione dinamica di molta parte del contenuto dei messaggi, il che rende le risposte automatiche piuttosto versatili.

Gli eventi di risposta automatica vengono utilizzati quando il messaggio di attivazione proviene da un'origine remota. Tuttavia, per i messaggi che provengono dallo stesso dominio dell'utente, le risposte automatiche si attivano solo se si seleziona l'opzione *Risposte automatiche attivate da mail dallo stesso dominio*, disponibile nella schermata Risposte automatiche » Impostazioni 856. Questa schermata consente inoltre di utilizzare un'opzione per limitare i messaggi di risposta automatica a una risposta al giorno per ogni mittente.

Risposta automatica

Abilita risposta automatica

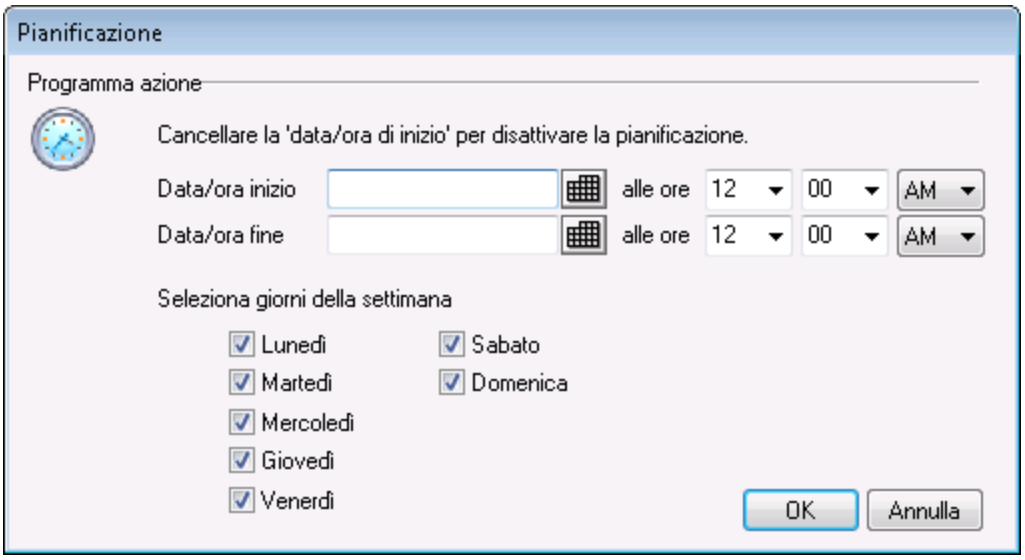
Attivare questo controllo per abilitare una risposta automatica per tutti i gruppi controllati da questo modello. Per ulteriori informazioni sulle risposte automatiche, vedere: Risposte automatiche 852.

Modifica file risposta automatica

Fare clic su questo pulsante per modificare il file di risposte automatiche che sarà utilizzato per gli utenti associati a questo modello.

Pianificazione

Fare clic su questo pulsante per aprire la finestra di dialogo Pianificazione, che consente di impostare la data e l'ora di inizio e di fine dell'intervallo temporale e i giorni della settimana in cui deve essere attiva la funzione di risposta automatica. Se si desidera che la risposta automatica sia sempre attiva, lasciare vuoti i campi.



Pubblica
Fare clic su questo pulsante se si desidera copiare il file di risposta automatica del modello e le impostazioni su uno o più altri account. Selezionare gli account sui quali si desidera copiare la risposta automatica e fare clic su **OK**.

Non inviare risp. autom. se il messaggio proviene da uno di questi indirizzi
In questo campo è possibile elencare gli indirizzi che si desidera escludere dall'invio della risposta automatica.

Può accadere che i messaggi di risposta automatica vengano inviati a un indirizzo che utilizza a sua volta lo stesso meccanismo. In questo caso, viene a crearsi un effetto "ping-pong" per cui i messaggi vengono continuamente scambiati tra i due server. Per evitare tale problema è possibile inserire l'indirizzo in questo campo. Nella schermata Risposte automatiche » Impostazioni 856 è disponibile un'opzione che consente di limitare i messaggi di risposta automatica a non più di uno al giorno per ogni mittente.

Rimuovi
Fare clic su questo pulsante per eliminare le voci selezionate dall'elenco degli indirizzi esclusi.

Nuovo indir. escluso (car. jolly consentiti)
Se si desidera aggiungere un indirizzo all'elenco degli indirizzi esclusi, inserirlo in questo campo e fare clic sul pulsante *Aggiungi*.

Esecuzione di un programma

Esegui programma
Questo campo consente di specificare il percorso e il nome del file in un programma da eseguire all'arrivo della posta per un membro del gruppo controllato da questo modello. Accertarsi che tale programma termini in modo corretto e possa essere eseguito senza supervisione. È possibile inserire eventuali parametri della riga di comando subito dopo il percorso del file eseguibile.

Sottoponi a elaborazione
Se si seleziona questa opzione, il nome del messaggio di attivazione verrà passato al processo specificato nel campo *Esegui questo programma* come primo parametro disponibile della riga di comando. Se si imposta la risposta automatica per un account che inoltra la posta a un'altra posizione **senza** conservarne copia locale nella propria casella postale (vedere Inoltro 742), questa funzione viene disabilitata.

Per impostazione predefinita, MDaemon inserisce il nome del file di messaggio come ultimo parametro della riga di comando. Per ignorare questo comportamento, utilizzare la macro `$MESSAGE$`. Inserire la macro al posto del nome file del messaggio. Ciò consente di aumentare la flessibilità della funzione, in quanto

> sarà possibile utilizzare righe di comando complesse come la seguente: `logmail /e /j /message=$MESSAGE$ /q`.

Liste di distribuzione

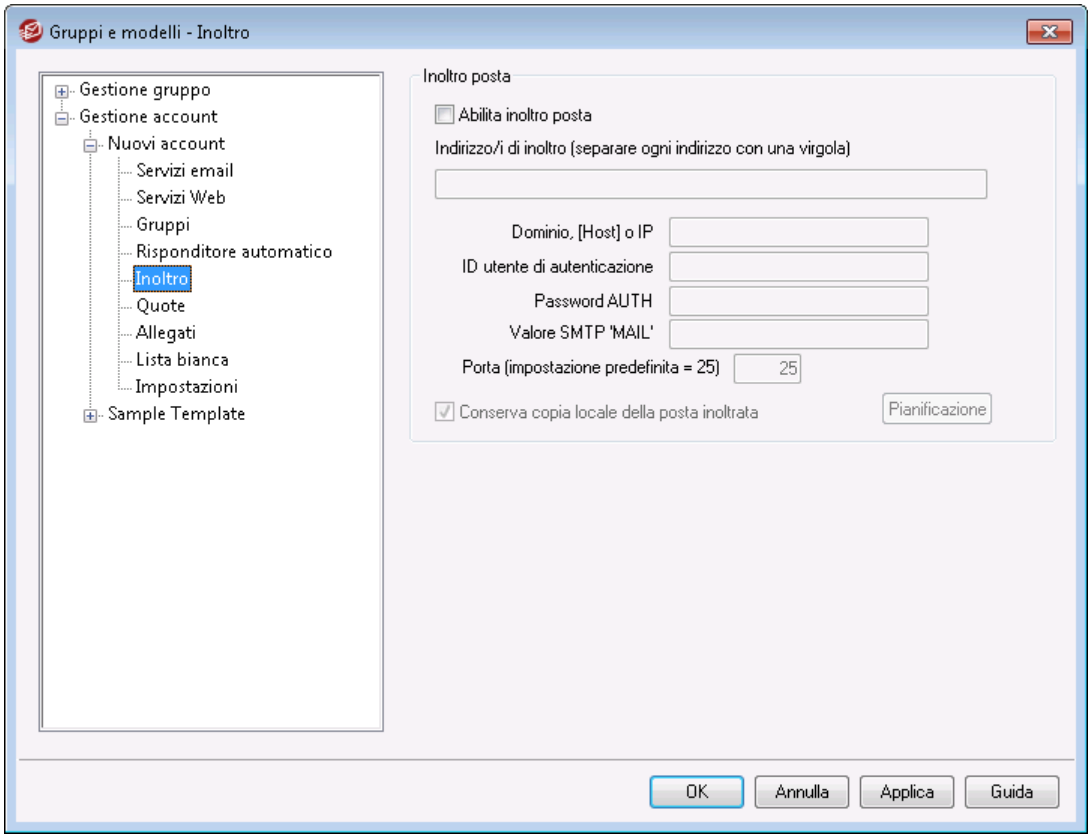
Aggiungi mittente a lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in entrata diventa automaticamente un membro di tale lista. Questa funzione è molto utile per la creazione automatica delle liste.

Rimuovi mittente da lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in arrivo viene automaticamente rimosso dalla lista specificata.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Risposta automatica 739

5.2.2.1.5 Inoltro



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Inoltro 742 di Account Editor. Quando è configurato per il controllo di questa schermata 808, il modello controlla le opzioni di inoltro per qualsiasi account appartenente a un Gruppo 798 che utilizza il modello.

Inoltro posta

Abilita inoltro posta
Se si abilita questa casella, i messaggi in entrata dell'account associato vengono inoltrati agli indirizzi indicati nell'opzione *Indirizzo/i di inoltro*. Gli utenti MDaemon con accesso Web 735 a Webmail 325 o Remote Administration 359 possono utilizzare le opzioni fornite per impostare le opzioni di inoltro autonomamente, anziché chiedere all'amministratore di eseguire l'operazione.

Indirizzo/i di inoltro (separare ogni indirizzo con una virgola)
Questo campo consente di indicare gli indirizzi e-mail ai quali inoltrare copie dei messaggi in entrata, man mano che questi pervengono all'account associato. Una copia di ogni nuovo messaggio in arrivo al server viene generata e inoltrata automaticamente all'indirizzo specificato in questo campo, purché sia stata selezionata l'opzione *Abilita inoltro posta*. Per specificare più indirizzi, utilizzare la virgola come separatore.

Dominio, [Host] o IP
Per instradare i messaggi inoltrati attraverso un altro server, ad esempio i server MX di un determinato dominio, specificare in questo campo il dominio o l'indirizzo IP. Per indirizzare i messaggi verso un host specifico, racchiudere il valore tra parentesi (ad esempio, `[host1.esempio.com]`).

Accesso/Password AUTH
Immettere le eventuali credenziali di accesso/password necessarie per il server a cui si desidera inoltrare la posta dell'utente associato.

Valore SMTP 'MAIL'
Se si specifica un indirizzo in questa casella, nell'istruzione "`MAIL From`" inviata durante la sessione SMTP con l'host di destinazione verrà utilizzato tale indirizzo invece del mittente effettivo del messaggio. Se si desidera un'istruzione SMTP "`MAIL From`" vuota ("`MAIL FROM <>`") inserire la stringa "[trash]".

Porta (valore predefinito = 25)
MDaemon invierà i messaggi inoltrati mediante la porta TCP specificata in questa casella. Il valore predefinito della porta SMTP è 25.

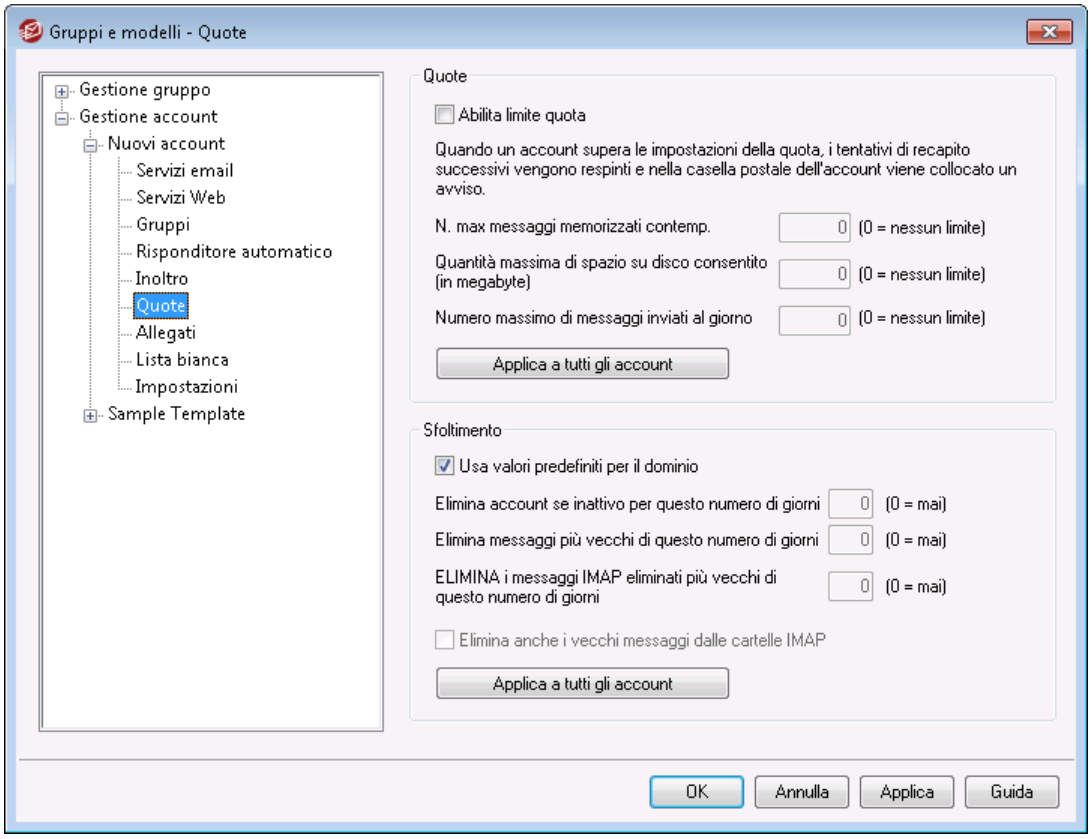
Conserva copia locale della posta inoltrata
Per impostazione predefinita, una copia di ogni messaggio inoltrato viene consegnata normalmente alla casella postale dell'utente locale. Se si deseleziona questa casella, non viene conservata alcuna copia locale.

Pianificazione
Fare clic su questo pulsante per creare una pianificazione relativa a quando la posta dell'account associato verrà inoltrata. È possibile impostare una data e un'ora di inizio, una data e un'ora di fine e specificare i giorni della settimana in cui la posta verrà inoltrata.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Inoltro 742

5.2.2.1.6 Quote



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Quote[746] di Account Editor. Quando è configurato per il controllo di questa schermata[808], il modello controlla le opzioni relative quote per qualsiasi account appartenente a un Gruppo[798] che utilizza il modello.

Quote

Abilita limite quota
Selezionare questa casella per specificare il numero massimo di messaggi che gli account controllati da questo modello possono memorizzare, per impostare la quantità massima di spazio su disco utilizzabile dagli account, inclusi gli allegati dei file della cartella Documenti di ogni account e per definire il numero massimo di messaggi che gli account possono inviare al giorno tramite SMTP. Se si tenta di consegnare una quantità di posta superiore ai limiti stabiliti per i messaggi e per lo spazio su disco, il messaggio viene respinto e nella casella postale dell'utente viene collocato un avviso appropriato. Se una raccolta MultiPOP[754] supera il massimo consentito per l'account viene emesso un avviso simile e le voci MultiPOP dell'account vengono disattivate automaticamente, ma non rimosse dal database.

Utilizzare l'opzione *Invia un'e-mail all'utente se viene raggiunta questa percentuale della quota* di"Account » Impostazioni account » Quote[825]" affinché venga inviato un messaggio di

avviso quando un account si avvicina ai limiti di quota. Quando un account supera il valore percentuale indicato per il limite *Numero massimo di messaggi memorizzati contemporaneamente* o *Massimo spazio su disco consentito*, a mezzanotte riceve un messaggio di avviso. Nel messaggio verranno inclusi il numero di messaggi memorizzati, la dimensione della casella postale, la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato.

Numero massimo di messaggi memorizzati contemporaneamente
Questa opzione consente di specificare il numero massimo dei messaggi che gli account possono memorizzare. Il valore "0" indica che il numero di messaggi consentito è illimitato.

Massimo spazio su disco consentito (in megabyte)
Questa opzione consente di indicare la quantità massima di spazio su disco utilizzabile dagli account, inclusi gli allegati di file che è possibile memorizzare nella cartella Documenti di ogni account. Il valore "0" indica che la quantità di spazio su disco consentita è illimitata.

Numero massimo di messaggi inviati al giorno
Questa opzione consente di specificare il numero massimo di messaggi che ogni account può inviare al giorno tramite SMTP. Se l'account raggiunge questo limite, i nuovi messaggi inviati dall'account vengono rifiutati fino a quando il contatore non viene azzerato a mezzanotte. Specificare "0" nell'opzione se non si desidera limitare il numero di messaggi che l'account può inviare.

Applica a tutti gli account

Fare clic su questo pulsante per applicare le impostazioni di questa schermata a tutti gli account di MDaemon esistenti per i quali le impostazioni relative alle quote non sono specificamente controllate da un modello di account. In tal modo, tutti gli account vengono reimpostati sui valori delle quote predefiniti. Questa opzione è disponibile solo nel modello Nuovi account 807.

Sfoltimento

Le opzioni di questa sezione consentono di specificare quando o se un account controllato da questo modello verrà eliminato nel caso diventi inattivo. Consentono inoltre di indicare se i vecchi messaggi dell'account debbano essere eliminati dopo un determinato periodo di tempo. Ogni giorno a mezzanotte, MDaemon rimuove tutti i messaggi che hanno superato i limiti di tempo specificati o elimina completamente l'account, se questo ha raggiunto il limite di inattività.

Usa valori predefiniti per il dominio
Le impostazioni di sfoltimento predefinite sono specifiche dei domini e sono situate nella schermata Impostazioni 216 di Domain Manager. Per sovrascrivere le impostazioni

predefinite di dominio per gli account controllati da questo modello, disabilitare la casella di controllo e impostare i valori desiderati per le opzioni descritte di seguito.

Elimina account se inattivo per il seguente numero di giorni (0 = mai)
Specificare il numero di giorni per cui si desidera che l'account rimanga inattivo prima di essere eliminato. Con il valore "0", un account non viene mai eliminato per inattività.

Elimina messaggi più vecchi del seguente numero di giorni (0 = mai)
Indica il numero di giorni per cui un determinato messaggio può rimanere nella casella postale dell'account prima di essere eliminato automaticamente. Il valore "0" indica che, anche se di vecchia data, i messaggi non vengono mai eliminati.
Nota: l'impostazione di questa opzione non si applica ai messaggi contenuti nelle cartelle IMAP a meno che non si abiliti anche l'opzione "*Elimina anche i vecchi messaggi dalle cartelle IMAP*" di seguito.

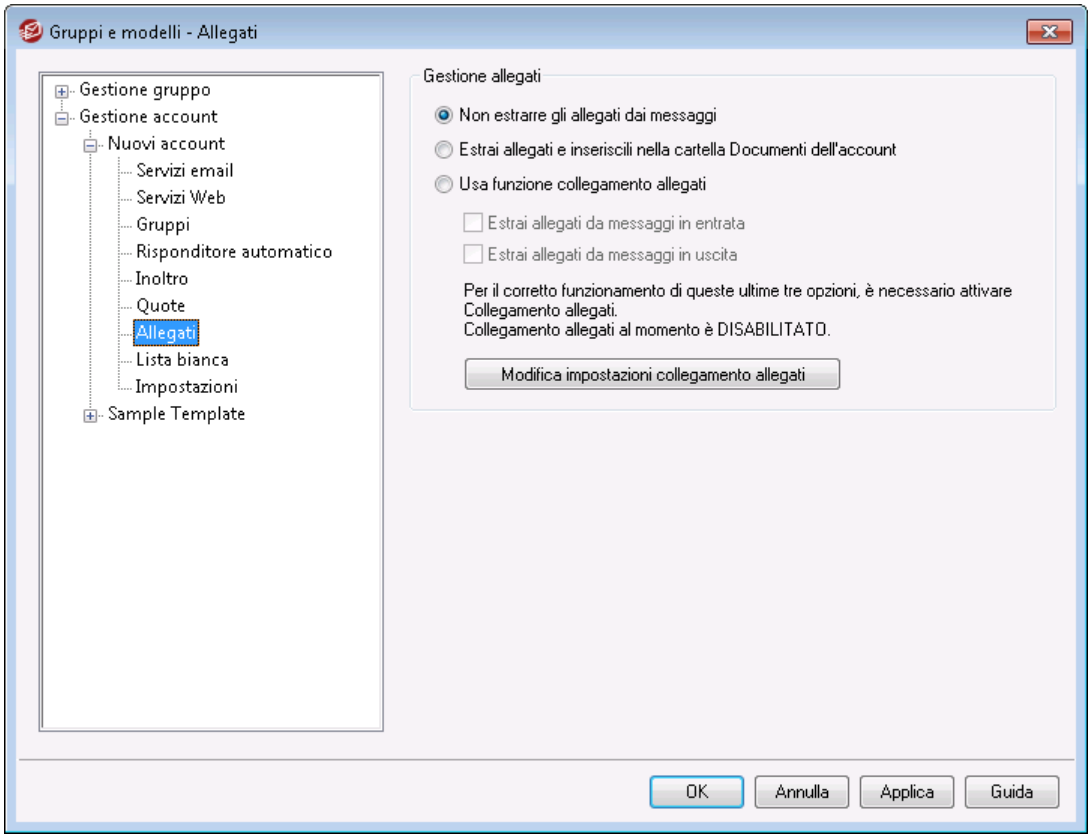
Elimina messaggi IMAP cestinati più vecchi del seguente numero di giorni (0 = mai)
Utilizzare questo comando per specificare il numero di giorni per cui si desidera che i messaggi IMAP contrassegnati per l'eliminazione rimangano nelle cartelle di un utente. I messaggi contrassegnati per l'eliminazione da un numero di giorni superiore a questo valore vengono eliminati. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Elimina anche i vecchi messaggi dalle cartelle IMAP
Selezionare questa casella di controllo se si desidera applicare l'opzione "*Elimina i messaggi più vecchi del seguente numero di giorni*" anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i normali messaggi contenuti nelle cartelle IMAP non vengono eliminati in base al periodo di permanenza nelle cartelle in questione.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Quote 746
Impostazioni account » Quote 875

5.2.2.1.7 Allegati



Le opzioni in questa schermata corrispondono alle opzioni disponibili nella schermata Allegati 749 di Account Editor. Quando è configurato per il controllo di questa schermata 808, il modello controlla le opzioni relative agli allegati per qualsiasi account appartenente a un Gruppo 798 che utilizza il modello.

Gestione allegati

Non estrarre gli allegati dai messaggi
Se si seleziona questa opzione, gli allegati non verranno estratti dai messaggi di un account controllato da modelli. I messaggi con allegati vengono gestiti normalmente e gli allegati rimangono invariati.

Estrai allegati e inseriscili nella cartella Documenti dell'account
Se impostata, questa opzione indica a MDaemon di estrarre automaticamente tutti gli eventuali file incorporati MIME Base64 allegati ai messaggi di posta in arrivo dell'account. I file estratti vengono rimossi dal messaggio in arrivo, decodificati e collocati nella cartella Documenti dell'account. Quindi, nel corpo del messaggio viene inserita una nota, con l'elenco dei nomi dei file estratti. Questa opzione non offre un collegamento agli allegati memorizzati, ma gli utenti possono utilizzare Webmail 325 per accedere alla cartella Documenti.

Usa funzione collegamento allegati
Selezionare questa opzione per utilizzare la funzione Collegamento allegati per i messaggi in entrata o in uscita con allegati.

Se questa opzione è selezionata, ma la funzione Collegamento allegati della finestra di dialogo Collegamento allegati 373 è disabilitata, gli allegati non vengono estratti.

Estrai allegati da messaggi in entrata
Quando questa opzione è attivata, gli allegati vengono estratti dai messaggi in arrivo dell'account e memorizzati nella posizione indicata nella finestra di dialogo Collegamento allegati 373. I collegamenti URL vengono quindi inseriti nel corpo del messaggio, dove è possibile selezionarli per scaricare i file. Per motivi di sicurezza, i collegamenti URL non contengono i percorsi diretti ai file. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura GUID è memorizzata nel file `AttachmentLinking.dat`.

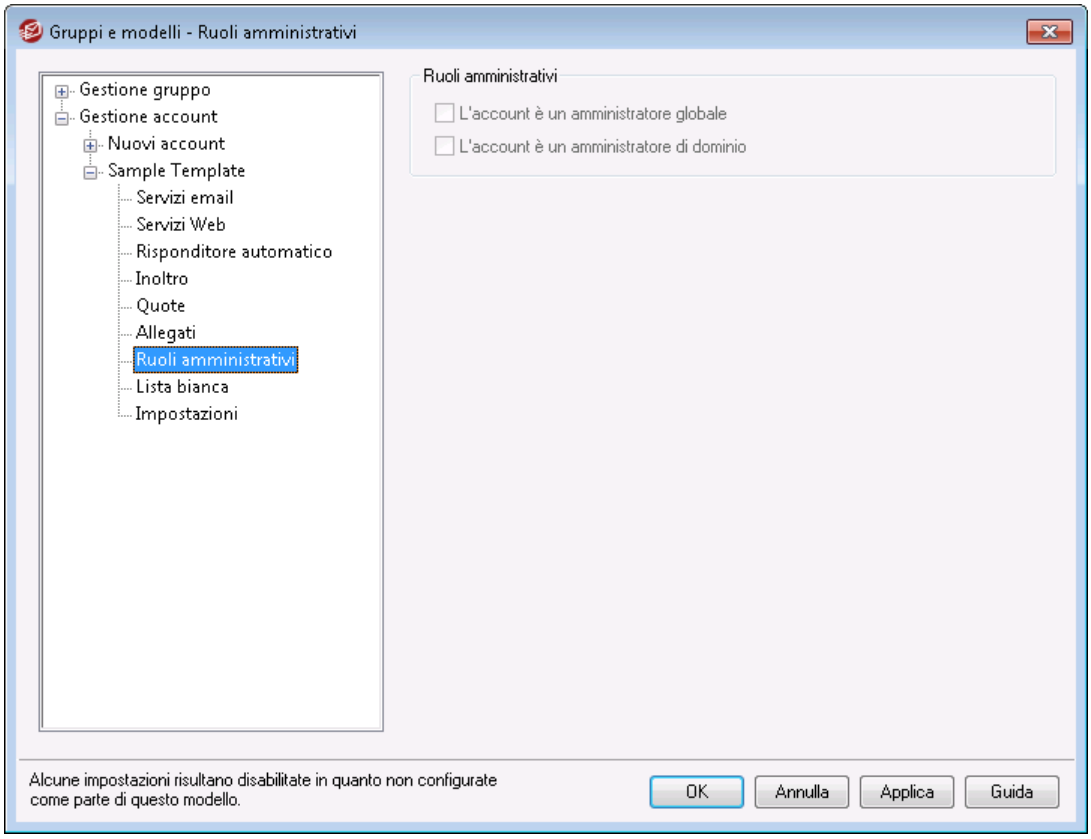
Estrai allegati da messaggi in uscita
Selezionare questa casella per utilizzare la funzione Collegamento allegati per estrarre gli allegati anche dai messaggi in uscita dell'account. Quando l'account invia un messaggio e-mail, Collegamento allegati estrae il file, lo archivia e lo sostituisce con un URL utilizzabile per scaricare il file.

Modifica impostazioni Collegamento allegati
Questo pulsante consente di aprire la finestra di dialogo Collegamento allegati 373.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Collegamento allegati 732
Account Editor » Allegati 749

5.2.2.1.8 Ruoli amministrativi



Ruoli amministrativi

L'account è un amministratore globale
Selezionare questa casella di controllo per concedere a questi utenti accesso al server come amministratore. Agli amministratori globali sono associate le caratteristiche riportate di seguito.

- Accesso completo alla configurazione del server, a tutti gli utenti e a tutti i domini tramite Remote Administration
- Accesso agli utenti di tutti i domini di MDaemon come compagni di conversazione di messaggistica istantanea.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche se di sola lettura.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche non si è iscritti.

L'utente avrà inoltre accesso a tutti i file e le opzioni di MDaemon. Per ulteriori informazioni sulle opzioni di amministrazione nell'interfaccia Web di Remote Administration, vedere Remote Administration 359.

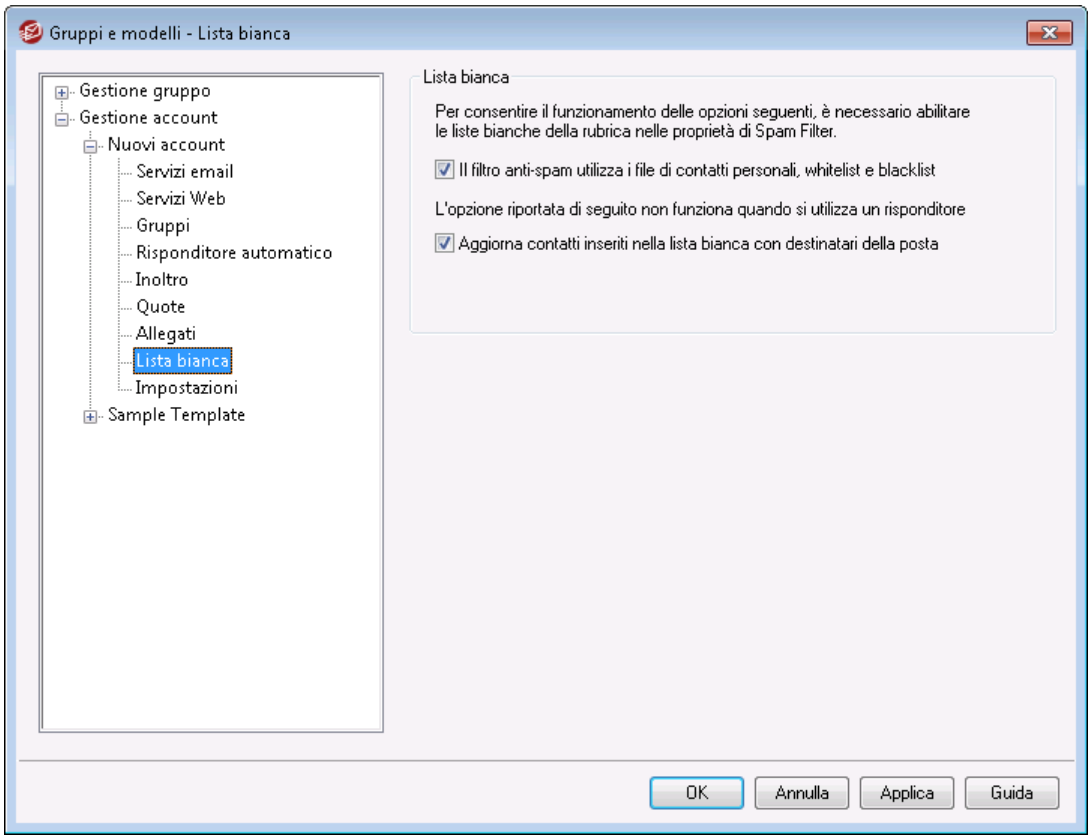
L'account è un amministratore di dominio
Selezionare questa casella di controllo per designare gli utenti come amministratori di dominio. Gli amministratori di dominio hanno privilegi simili a quelli degli amministratori globali, con l'unica differenza che l'accesso a livello amministrativo è limitato a questo dominio e alle autorizzazioni concesse nella pagina Servizi Web 735.

Questa schermata è disponibile solo nel modello Nuovi account 807. L'accesso come amministratore non può essere concesso automaticamente ai nuovi account. Per concedere l'accesso amministrativo a un account, associare l'account a un modello personalizzato che utilizza questa schermata per concedere l'accesso o designare manualmente l'account come amministratore dalla schermata Ruoli amministrativi 773 di Account Editor.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Ruoli amministrativi 773

5.2.2.1.9 Lista consentiti



Le opzioni in questa schermata del modello corrispondono alle impostazioni disponibili nella schermata Lista consentiti[774].Quando è configurato per il controllo di questa schermata[808], il modello controlla le la schermata Lista consentiti per verificare la presenza di eventuali account che appartengono a un Gruppo[798] che utilizza il modello.

Lista consentiti

Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati.
In Spam Filter la schermata Lista consentiti (automatica)[705] contiene un'opzione globale che si può utilizzare per fare in modo che il filtro antispam consenta automaticamente la ricezione di un messaggio quando il mittente di tale messaggio viene trovato nei contatti personali del destinatario locale o nella cartella dei mittenti autorizzati. Inoltre, il filtro bloccherà automaticamente i messaggi i cui mittenti vengono trovati nella cartella dei mittenti bloccati dell'utente. Se si è abilitata l'opzione globale di Spam Filter, ma non si desidera applicarla a questi account, deselezionare la casella di controllo per ignorare l'impostazione globale. Se l'opzione globale è disattivata, questa opzione non sarà disponibile.

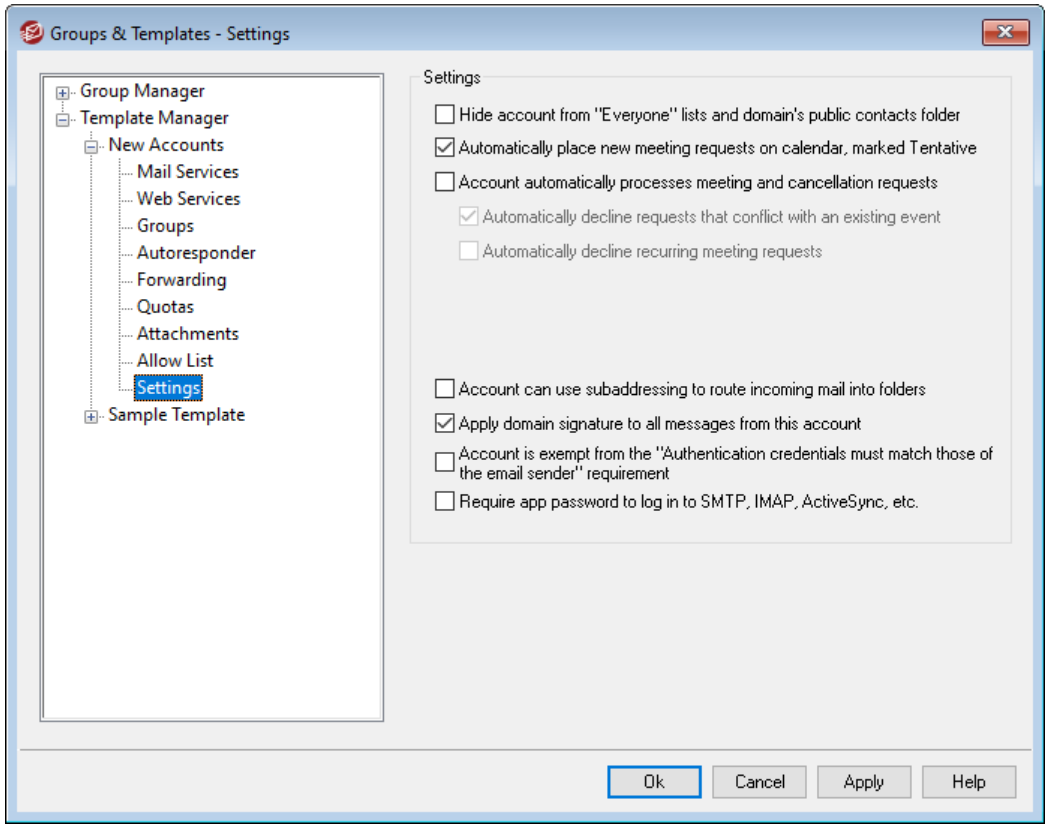
Aggiungi automaticamente i destinatari di posta ai mittenti consentiti
Fare clic su questa opzione se si desidera aggiornare la cartella dei mittenti consentiti di ciascun account ogni volta che viene inviato un messaggio a un indirizzo e-mail non locale. Se utilizzata insieme all'opzione precedente, *Spam Filter utilizza i contatti personali, i mittenti consentiti e i mittenti bloccati*, consente di ridurre drasticamente il numero di falsi positivi di Spam Filter. L'opzione *Aggiungi automaticamente i destinatari di posta ai mittenti consentiti* disponibile nella schermata Lista consentiti (automatica)[705] deve essere attivata prima di utilizzare questa funzione.

questa opzione è disabilitata se l'account utilizza la funziona di risposta automatica.

Vedere:

Proprietà modello[808]
Proprietà gruppo[798]
Modello Nuovi account[807]
Account Editor » Lista consentiti[774]

5.2.2.1.10 Impostazioni



Le opzioni in questo modello corrispondono alle impostazioni disponibili nella schermata Impostazioni 776 di Account Editor. Quando si imposta su controlla questa schermata 808, il modello controlla la schermata Impostazioni per verificare la presenza di eventuali account che appartengono a un Gruppo 798 che utilizza il modello.

Impostazioni

Account nascosto da elenchi "Everyone", calendari condivisi e VRFY
MDaemon crea e gestisce automaticamente una lista di distribuzione "everyone@" per ogni dominio, utilizzabile per inviare un messaggio contemporaneamente a tutti i membri della lista. In base all'impostazione predefinita, quando crea questa lista di distribuzione MDaemon include tutti gli account. La casella consente di escludere dalla lista gli account controllati da questo modello. In tal modo, gli account vengono esclusi anche dai calendari condivisi e dai risultati VRFY 94.

Inserire automaticamente in calendario nuove richieste di riunione, contrassegnate come Tentativo
Per impostazione predefinita quando un account riceve una nuova richiesta di riunione, tale riunione viene inserita nel calendario dell'utente e contrassegnata come *Tentativo*. Deselezionare questa casella di controllo se non si desidera che questa sia l'impostazione predefinita per i nuovi account.

L'account elabora automaticamente le richieste di riunione e gli annullamenti
Selezionare questa casella di controllo se si desidera abilitare l'elaborazione automatica delle richieste di riunione, delle modifiche e degli annullamenti per ogni account. Se un account riceve un messaggio che contiene una richiesta di riunione, il calendario dell'account viene aggiornato automaticamente. Per impostazione predefinita, l'opzione è disabilitata per tutti gli account.

Rifiuta automaticamente richieste in conflitto con un evento esistente
Se è abilitata l'elaborazione automatica delle richieste di riunione e degli annullamenti, per impostazione predefinita, le richieste di riunione vengono rifiutate automaticamente se in conflitto con un evento esistente. Deselezionare questa casella di controllo se si desidera creare l'evento in conflitto.

Rifiuta automaticamente richieste di riunioni ricorrenti
Fare clic su questa casella se è abilitata l'elaborazione automatica delle richieste di riunione e degli annullamenti, ma si desidera rifiutare tali richieste se sono relative a riunioni ricorrenti.

L'account può utilizzare il subaddressing per instradare la posta in entrata nelle cartelle
Selezionare questa casella di controllo se si desidera consentire il subaddressing 778 per gli account.

Applica firma dominio a tutti i messaggi da questo account
Quando esiste una firma dominio 206 per il dominio a cui appartengono gli account controllati da questo modello, l'opzione consente di aggiungerla a tutti i messaggi di posta elettronica inviati da tali account.

L'account è esente dal requisito "Le credenziali di autenticazione devono corrispondere a quelle del mittente"
Utilizzare questa opzione per escludere gli account controllati da questo modello dall'opzione globale "*Le credenziali di autenticazione devono corrispondere a quelle del mittente*" della schermata Autenticazione SMTP 531.

Richiedi la password di applicazione per l'accesso a SMTP, IMAP, ActiveSync, ecc.
Selezionare questa casella se si desidera richiedere che gli account che utilizzano questo modello utilizzino obbligatoriamente le password di applicazione 766 nei client di e-mail, per accedere a SMTP, IMAP, ActiveSync o ad altri protocolli dei servizi di posta. La normale password 870 dell'account, tuttavia, dovrà essere ancora utilizzata per accedere a Webmail o Remote Admin.

La richiesta di password di applicazione può aiutare a proteggere le password degli account da attacchi a dizionario e a forza bruta via SMTP, IMAP, ecc. La sicurezza è garantita dal fatto che, ove mai con un attacco di questo tipo si riuscisse a indovinare la password reale di un account, questa non funzionerebbe senza che l'aggressore possa accorgersene, perché MDaemon accetta solo una password di applicazione corretta. Inoltre, se gli account in MDaemon utilizzano l'autenticazione con Active Directory e Active Directory blocca un account dopo un certo numero di tentativi non riusciti, questa opzione può aiutare a prevenire il blocco degli account, poiché MDaemon verifica solo le password di applicazione e non tenta l'autenticazione con Active Directory.

Vedere:

Proprietà modello 808
Proprietà gruppo 798
Modello Nuovi account 807
Account Editor » Impostazioni 776

5.3 Impostazioni account

5.3.1 Active Directory

Le opzioni relative ad Active Directory, disponibili in Account » Impostazioni account » Active Directory, consentono di configurare il monitoraggio di Active Directory al fine di creare, modificare, eliminare e disattivare automaticamente gli account MDaemon quando in Active Directory vengono modificati gli account associati. È inoltre possibile impostarle in modo da conservare tutti i record dei contatti pubblici aggiornati con le informazioni più recenti memorizzate in Active Directory. I campi comuni, come l'indirizzo postale di un account, i numeri di telefono, le informazioni sui contatti commerciali e così via, possono essere inseriti nei record dei contatti pubblici e questi dati verranno aggiornati dopo ogni modifica in Active Directory.

Creazione degli account

Quando si imposta il monitoraggio di Active Directory, MDaemon esegue a intervalli prestabiliti interrogazioni relative alle modifiche e crea un nuovo account utente in MDaemon ogni qualvolta viene rilevata l'aggiunta di un nuovo account Active Directory. Tale nuovo account utente di MDaemon verrà creato utilizzando il nome completo, l'ID utente, la casella postale, la descrizione e lo stato attivo/inattivo riscontrato in Active Directory.

Per impostazione predefinita, i nuovi account MDaemon creati in seguito a un monitoraggio di Active Directory vengono aggiunti al dominio predefinito di MDaemon. In alternativa, è possibile scegliere di aggiungere questi account al dominio individuato in base all'attributo di Active Directory "`UserPrincipalName`" relativo all'account. Utilizzando questa opzione, se un account richiede un dominio non ancora esistente in MDaemon, viene creato automaticamente un nuovo dominio 185.

In alternativa è possibile configurare un *filtro di ricerca* 838 per monitorare un gruppo in Active Directory, di modo che quando si aggiunge un utente a un gruppo o un gruppo a un utente, l'utente verrà creato in MDaemon, e quando si rimuove un utente da un gruppo l'account verrà disattivato (non eliminato) in MDaemon.

Eliminazione degli account

MDaemon può essere configurato in modo da eseguire una delle operazioni specificate di seguito quando viene eliminato un account da Active Directory: non fare nulla, eliminare l'account MDaemon associato, disattivare l'account MDaemon associato o bloccare l'account MDaemon associato (ad esempio, l'account è ancora in grado di ricevere posta, ma l'utente non può riceverla o accedervi).

Aggiornamento degli account

Quando MDaemon rileva modifiche apportate agli account di Active Directory, eseguirà automaticamente un aggiornamento delle proprietà associate nel corrispondente account di MDaemon.

Sincronizzazione di MDaemon con la Active Directory

L'opzione "*Esegui scansione completa di AD*" consente di eseguire l'interrogazione del database di Active Directory e di creare o modificare, se necessario, gli account utente di MDaemon. Quando viene individuato un account di Active Directory che corrisponde ad un account MDaemon già esistente, i due account vengono collegati in modo che qualunque modifica futura dell'account Active Directory venga automaticamente apportata all'account MDaemon.

Autenticazione Active Directory

Gli account creati dalla funzionalità di Active Directory di MDaemon saranno configurati per impostazione predefinita per l'autenticazione tramite Active Directory (AD). Con l'autenticazione AD, non è necessario che MDaemon memorizzi la password dell'account all'interno del database utenti. Il titolare dell'account utilizzerà le proprie credenziali Windows (ID utente e password) e MDaemon le trasferirà a Windows per l'autenticazione dell'account associato.

Per utilizzare l'autenticazione AD con Active Directory, è necessario che nel campo incluso in Monitoraggio 841 venga indicato un nome di dominio di Windows che corrisponde al dominio utilizzato da MDaemon al momento dell'autenticazione degli account. Nella maggior parte dei casi, MDaemon individua il nome di dominio Windows e compila automaticamente il campo. Tuttavia, è possibile utilizzare un dominio alternativo in questa opzione se si desidera, oppure è possibile utilizzare "`NT_ANY`" se si desidera consentire l'autenticazione su tutti i domini Windows invece di limitarla a un dominio specifico. Se questa opzione viene lasciata vuota, MDaemon non utilizzerà l'autenticazione AD alla creazione di nuovi account, ma genererà una password casuale da modificare manualmente prima che agli utenti sia consentito l'accesso ai relativi account di posta.

Monitoraggio permanente

Il monitoraggio di Active Directory viene eseguito anche quando MDaemon è inattivo. Tutte le modifiche apportate in Active Directory vengono registrate ed elaborate al riavvio di MDaemon.

Sicurezza dei file di Active Directory

È importante notare che le funzionalità Active Directory di MDaemon non modificano i file di schema di Active Directory. Il monitoraggio viene effettuato in modo unidirezionale da Active Directory a MDaemon. .

Modello Active Directory

Quando MDaemon aggiunge o apporta modifiche agli account in base al monitoraggio e alla scansione di Active Directory, utilizzerà un modello Active Directory ("`MDaemon/app/ActiveDS.dat`") per collegare specifici nomi di attributi di Active Directory ai campi degli account in MDaemon. Ad esempio, per impostazione predefinita, MDaemon associa l'attributo "`cn`" di Active Directory al campo "`FullName`" di MDaemon.

Questi collegamenti, comunque, non sono codificati rigidamente. Se lo si desidera, è possibile aprire il modello con Blocco note e modificare qualunque corrispondenza predefinita tra i campi. Ad esempio, è possibile utilizzare "`FullName=%givenName% %sn%`" per sostituire la seguente impostazione predefinita: "FullName=%cn%". Per ulteriori informazioni, consultare il file `ActiveDS.dat`.

Aggiornamento delle rubriche pubbliche

È possibile utilizzare la funzione di monitoraggio di Active Directory per eseguire l'interrogazione periodica di Active Directory per mantenere aggiornati tutti i record dei contatti pubblici in MDaemon con le informazioni più recenti. I campi comuni, come l'indirizzo postale di un account, i numeri di telefono, le informazioni sui contatti commerciali e così via, verranno inseriti nel record dei contatti pubblici corrispondente e questi dati verranno aggiornati ogni volta che vengono modificati in Active Directory. Per attivare questa funzione, utilizzare l'opzione "*Controllo di Active Directory e aggiornamento rubriche pubbliche*", disponibile in: Active Directory » Monitoraggio 841.

È possibile monitorare molti campi relativi ai record dei contatti con questa funzione. Per un elenco completo dei campi relativi ai record dei contatti pubblici che possono essere mappati agli attributi di Active Directory, vedere il file `ActiveDS.dat`. Il file contiene diversi nuovi modelli di mappatura che consentono di specificare uno o più attributi Active Directory da inserire in uno specifico campo di record di contatti, ad esempio `%fullName%` per il campo relativo al nome completo, `%streetAddress%` per l'indirizzo postale e così via.

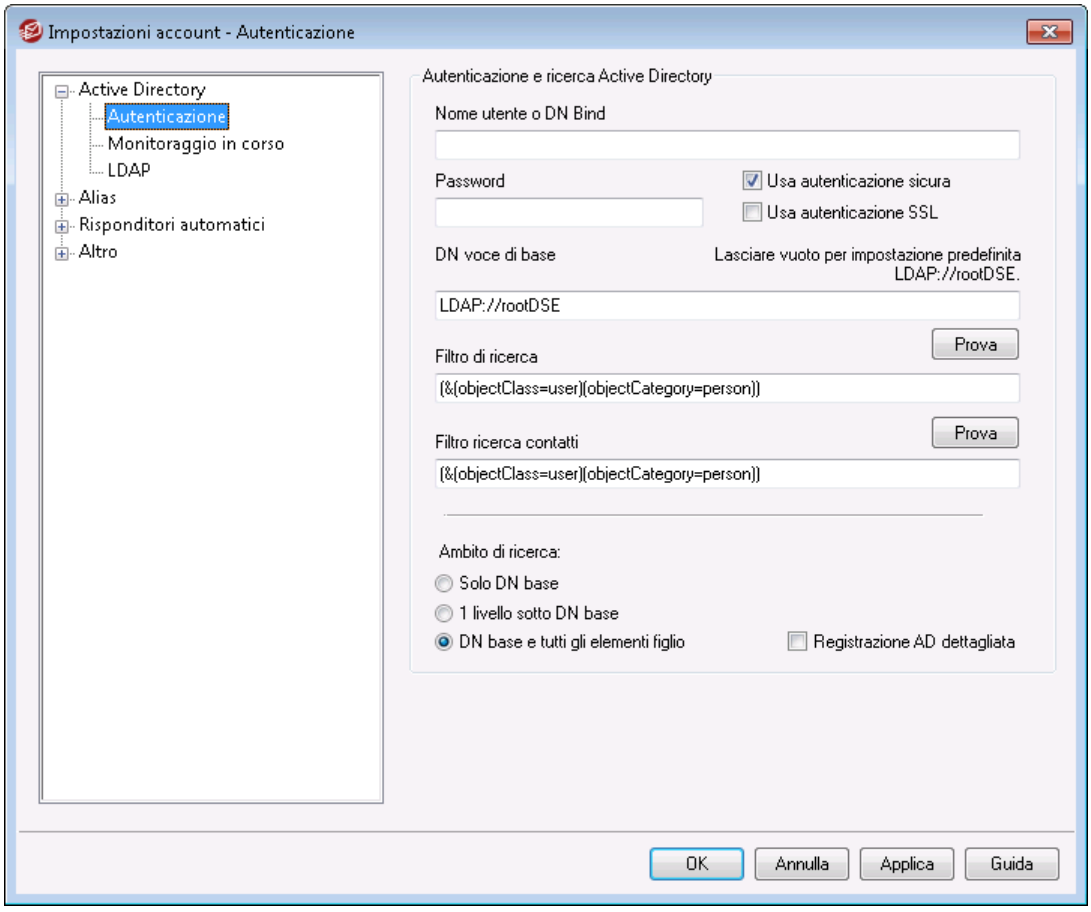
Per determinare il record dei contatti da aggiornare, MDaemon deve trovare una corrispondenza tra l'indirizzo di posta elettronica di un account e un attributo all'interno di Active Directory. Se non trova questa corrispondenza, non esegue alcuna operazione. Per impostazione predefinita, MDaemon tenta di creare un indirizzo di posta elettronica utilizzando i dati derivati dall'attributo mappato al modello di casella postale (vedere `ActiveDS.dat`) a cui MDaemon aggiungerà internamente il nome del dominio predefinito 185, analogamente a quanto avviene durante la creazione e l'eliminazione degli account in base ai dati di Active Directory. Tuttavia, è possibile rimuovere i commenti dal modello "abMappingEmail" all'interno del file `ActiveDS.dat` e associarlo all'attributo Active Directory desiderato, ad esempio `%mail%`. Tuttavia, il valore di questo attributo deve contenere un indirizzo e-mail che verrà riconosciuto come account utente locale valido.

Questa funzione consente di creare "al volo" i record dei contatti non ancora esistenti e di aggiornare i record dei contatti esistenti. Sovrascrive inoltre tutte le modifiche apportate all'esterno di Active Directory. I campi dei record dei contatti non mappati vengono lasciati inalterati; pertanto, tutti i dati esistenti che in genere non vengono influenzati da questo processo non verranno modificati né andranno persi. Infine, per gli account MDaemon impostati come nascosti 776 non vengono creati o aggiornati i record dei contatti.

Per ulteriori informazioni, vedere:

Active Directory » Monitoraggio 841
Active Directory » Autenticazione 838

5.3.1.1 Autenticazione



Per consentire l'utilizzo di tutte le funzionalità relative all'accesso ad Active Directory potrebbe essere necessario impostare autorizzazioni speciali.

Autenticazione e ricerca Active Directory

Nome utente o DN associato
ID utente dell'account Windows o il DN che MDaemon utilizzerà per l'associazione ad Active Directory mediante LDAP. Per l'associazione, Active Directory consente l'uso di un account Windows o di un UPN.

Quando si utilizza un DN invece di un ID utente Windows per questa opzione, è necessario disattivare/deselezionare l'opzione "*Usa autenticazione sicura*" riportata di seguito.

Password
Password corrispondente al DN o all'ID utente Windows indicato nell'opzione *DN associato*.

Usa autenticazione sicura
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione sicura durante l'esecuzione di ricerche in Active Directory. Non è possibile utilizzare questa opzione se nell'opzione *DN associato* indicata in precedenza viene specificato un DN anziché un ID utente Windows.

Usa autenticazione SSL
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione SSL durante l'esecuzione di ricerche in Active Directory.

L'utilizzo di questa opzione richiede la presenza di un server e di un'infrastruttura SSL nella rete Windows e in Active Directory. Se non si è certi dell'impostazione della rete o per ulteriori informazioni sulla possibilità di attivare questa opzione, rivolgersi al proprio reparto IT.

Ricerca in Active Directory

DN voce di base
Rappresenta il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la ricerca degli account e delle modifiche apportate all'interno di Active Directory. Per impostazione predefinita, MDaemon esegue la ricerca a partire dal Root DSE, che consiste nella voce di livello più alto nella gerarchia della Active Directory. L'indicazione di un punto iniziale più accurato e prossimo alla posizione dell'account nella struttura Active Directory può ridurre il tempo necessario per la ricerca degli account e delle modifiche apportate all'account. Lasciando vuoto questo campo, verrà ripristinata l'impostazione predefinita `LDAP://rootDSE`.

Filtro di ricerca
Rappresenta il filtro di ricerca LDAP utilizzato quando si esegue il monitoraggio o la ricerca di account e delle relative modifiche in Active Directory. Utilizzare questo

filtro per localizzare in modo più accurato gli account utente da includere nel monitoraggio di Active Directory.

È anche possibile configurare un filtro di ricerca per monitorare un gruppo in Active Directory, di modo che quando si aggiunge un utente a un gruppo o un gruppo a un utente, l'utente verrà creato in MDaemon, e quando si rimuove un utente da un gruppo l'account verrà disattivato (non eliminato) in MDaemon. Ad esempio, un filtro di ricerca corretto per un gruppo denominato "MyGroup" potrebbe essere:

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

Sostituire le parti 'ou=' e 'dc=' con qualcosa di appropriato alla propria rete.

Filtro ricerca contatti
Utilizzare questa opzione per specificare un filtro di ricerca separato per le ricerche dei contatti. Se in questo campo si utilizza lo stesso testo usato nell'opzione *Filtro di ricerca* indicata sopra, verrà utilizzata una sola query per aggiornare tutti i dati. Quando i filtri di ricerca sono diversi, sono necessarie due query separate.

Test
Usare i pulsanti *Test* per testare le impostazioni del filtro di ricerca.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche Active Directory.

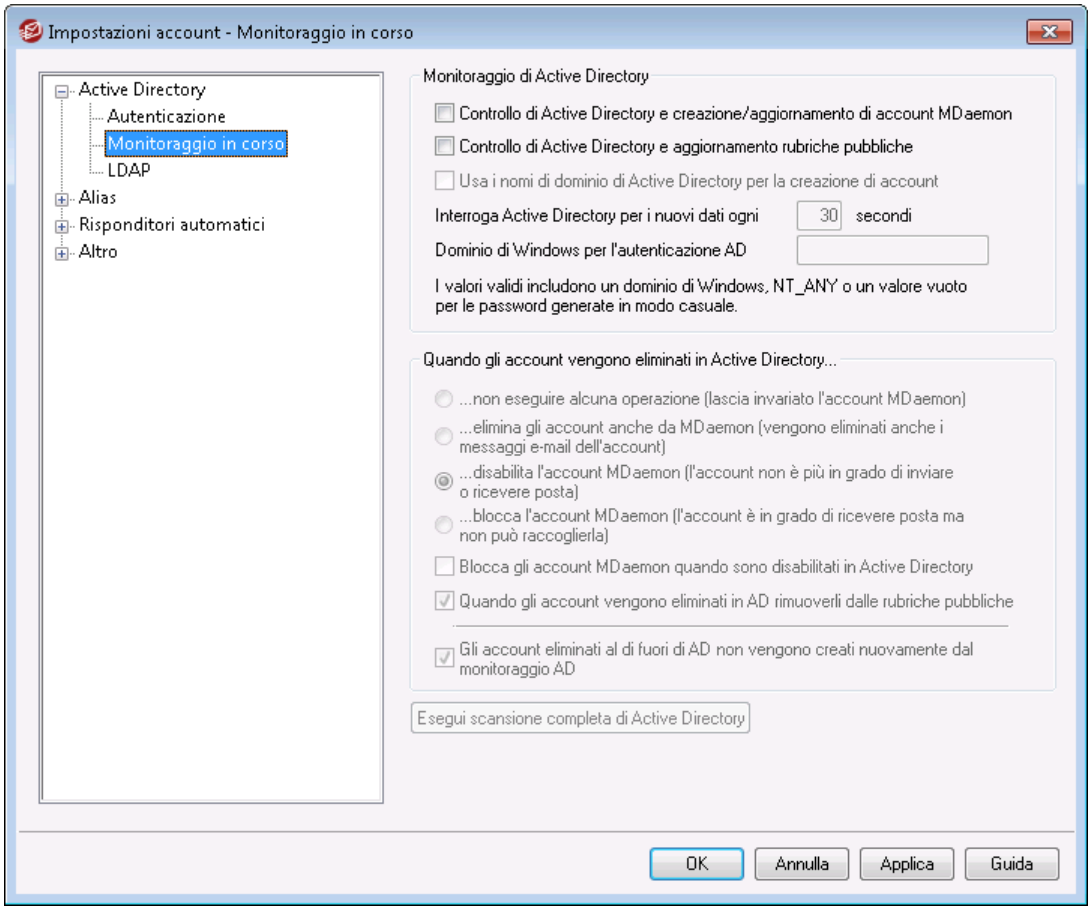
Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca nella struttura DIT di Active Directory ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT. È l'opzione selezionata per impostazione predefinita che consente, se combinata con l'impostazione relativa alla directory principale DSE indicata in precedenza, di eseguire la ricerca nell'intera struttura DIT sottostante alla directory principale DSE.

Registrazione AD dettagliata
Per impostazione predefinita, MDaemon utilizzerà la registrazione dettagliata per gli eventi di Active Directory. Deselezionare questa casella di controllo se si desidera utilizzare una modalità di registrazione Active Directory meno dettagliata.

5.3.1.2 Monitoraggio



Monitoraggio di Active Directory

Controllo di Active Directory e creazione/aggiornamento di account MDaemon
Fare clic su questa opzione per attivare il monitoraggio di Active Directory, in modo da creare e aggiornare gli account MDaemon durante l'aggiornamento di Active Directory.

Controllo di Active Directory e aggiornamento rubriche pubbliche
Attivare questa opzione se si desidera utilizzare Active Directory per mantenere aggiornati tutti i record dei contatti pubblici con le informazioni più recenti memorizzate in Active Directory. I campi comuni, come l'indirizzo postale di un account, i numeri di telefono, le informazioni sui contatti commerciali e così via, verranno inseriti nel record dei contatti pubblici corrispondente e questi dati verranno aggiornati ogni volta che vengono modificati in Active Directory. Numerosi campi relativi ai record dei contatti verranno monitorati con questo metodo. Per un elenco completo dei campi relativi ai record dei contatti pubblici che possono essere mappati agli attributi di Active Directory, vedere il file `ActiveDS.dat`. Vedere: Aggiornamento delle rubriche pubbliche 837 per ulteriori informazioni.

Usa i nomi di dominio di Active Directory per la creazione di account
Utilizzare questa opzione per aggiungere i nuovi account creati a seguito del monitoraggio di Active Directory al dominio specificato nell'attributo "`UserPrincipalName`" di Active Directory relativo all'account. Utilizzando questa opzione, se un account richiede un dominio non ancora esistente in MDaemon, viene creato automaticamente un nuovo dominio 185. Deselezionare/disattivare questa opzione se si desidera aggiungere tutti i nuovi account al dominio predefinito 185 di MDaemon.

Interroga Active Directory per i nuovi dati ogni XX secondi
Rappresenta l'intervallo di tempo trascorso il quale MDaemon esegue un nuovo monitoraggio di Active Directory al fine di individuare eventuali modifiche.

Dominio Windows per autenticazione AD
Specificare un nome di dominio Windows se si desidera utilizzare Autenticazione Active Directory per gli account creati dal monitoraggio di Active Directory. Se questo campo viene lasciato vuoto, ai nuovi account verranno assegnate password casuali che dovranno essere modificate manualmente per rendere accessibili gli account.

Quando gli account vengono eliminati in Active Directory...
Quando un account Active Directory associato a un account MDaemon viene eliminato, MDaemon esegue una determinata operazione, a seconda dell'opzione selezionata.

...non eseguire alcuna operazione
Scegliere questa opzione se non si desidera che MDaemon apporti modifiche all'account MDaemon quando l'account associato viene eliminato da Active Directory.

... elimina gli account anche da MDaemon
Scegliendo questa opzione, l'account MDaemon sarà eliminato insieme all'account associato di Active Directory.

In questo caso, l'account MDaemon associato verrà rimosso completamente. Saranno eliminati anche i messaggi dell'account, le cartelle, le rubriche, i calendari e così via.

...disabilita l'account MDaemon
Se si seleziona questa opzione, quando un account viene eliminato in Active Directory il corrispondente account MDaemon viene disabilitato. In tal caso, l'account MDaemon continua a esistere sul server, ma non è possibile utilizzarlo per inviare o per ricevere la posta, né accedere all'account stesso.

...blocca l'account MDaemon
Selezionando questa opzione, è ancora possibile accettare la posta in entrata dell'account, ma questa risulta "bloccata" e non è possibile quindi accedervi. In altre parole, la posta in arrivo indirizzata all'account non viene rifiutata o

eliminata da MDaemon, ma il proprietario dell'account non è in grado di accedervi o di raccoglierla finché l'account rimane bloccato.

Blocca gli account MDaemon quando sono disabilitati in Active Directory
Per impostazione predefinita, se un account viene disabilitato in Active Directory, viene disabilitato anche l'account MDaemon associato. In questo modo, l'account risulta inaccessibile e i messaggi indirizzati all'account non vengono accettati né consegnati da MDaemon. Tuttavia, se si desidera che l'account MDaemon associato venga bloccato anziché disabilitato, attivare questa opzione. MDaemon continuerà ad accettare i messaggi destinati agli account bloccati, ma gli utenti non potranno accedere a tali account per raccogliere o per inviare la posta.

Quando gli account vengono eliminati in AD rimuoverli dalle rubriche pubbliche
Per impostazione predefinita, i contatti della cartella Pubblica vengono eliminati quando l'account associato viene eliminato da Active Directory. Tuttavia, i contatti vengono eliminati solo se creati in origine dalla funzione di integrazione di Active Directory 837. Disattivare questa opzione se non si desidera eliminare i contatti quando gli account associati vengono eliminati in Active Directory.

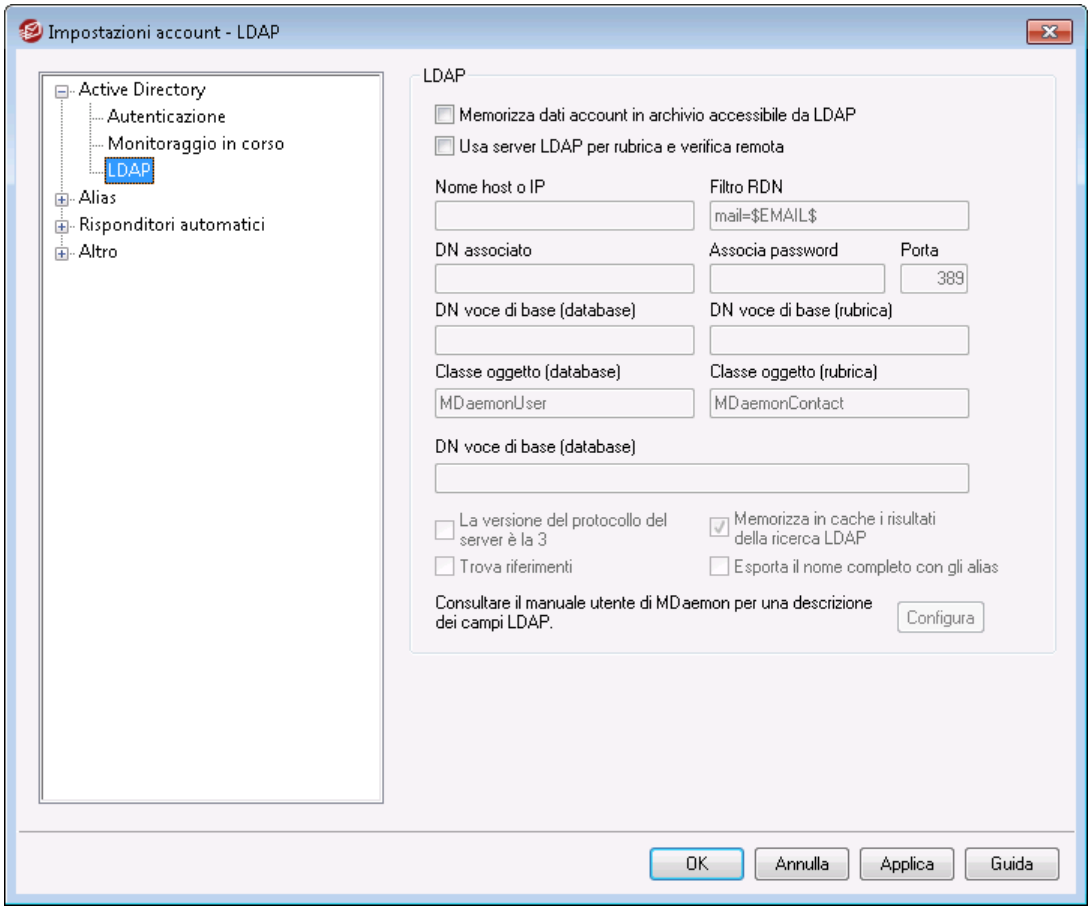
Gli account eliminati al di fuori di AD non vengono creati nuovamente dal monitoraggio AD
Quando si elimina un account MDaemon al di fuori di Active Directory (ad esempio, eliminandolo manualmente usando l'interfaccia di MDaemon), per impostazione predefinita l'account non verrà creato nuovamente dalla funzione di monitoraggio di Active Directory. Disattivare questa opzione se si desidera che questi account vengano creati nuovamente.

Esegui scansione completa di Active Directory
Fare clic su questo pulsante per consentire a MDaemon di interrogare il database di Active Directory e, se necessario, creare, modificare o eliminare gli account. Quando viene individuato un account di Active Directory che corrisponde ad un account MDaemon già esistente, i due account vengono collegati.

Vedere:

Active Directory 835
Active Directory » Autenticazione 838

5.3.1.3 LDAP



Daemon offre il supporto per il protocollo LDAP (Lightweight Directory Access Protocol). Fare clic su "Account » Impostazioni account » LDAP" per accedere alla schermata LDAP utilizzata per configurare MDaemon per mantenere aggiornato il server LDAP su tutti gli account utente. MDaemon è in grado di mantenere aggiornato il database degli utenti LDAP comunicando con il server LDAP a ogni aggiunta o rimozione di un account. In questo modo, gli utenti che utilizzano un client di posta che supporta il protocollo LDAP hanno la possibilità di condividere una rubrica globale contenente i contatti di tutti gli utenti di MDaemon e qualsiasi altro contatto desiderato.

È inoltre possibile utilizzare il server LDAP come database utenti di MDaemon 863 al posto del sistema `USERLIST.DAT` locale o di un database compatibile con ODBC. Questo metodo di aggiornamento delle informazioni utente può risultare utile se si dispone di più server MDaemon in siti diversi che utilizzano un database utenti condiviso: ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale.

LDAP

Memorizza dati account in un archivio accessibile da LDAP
Selezionare questa casella di controllo se si desidera che MDaemon utilizzi il server LDAP come database utenti anziché ODBC o il file `USERLIST.DAT` locale. Questo metodo di aggiornamento delle informazioni utente può risultare utile se si dispone di

più server MDaemon in siti diversi che utilizzano un database utenti condiviso: ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale.

Usa server LDAP per rubrica e verifica remota
Se questa opzione è abilitata, è possibile mantenere aggiornati i nomi, gli indirizzi e-mail e gli alias degli utenti del server LDAP sebbene si sia scelto di aggiornare il database account con ODBC o con il metodo predefinito `USERLIST.DAT`. Di conseguenza, è possibile mantenere aggiornato il server LDAP e utilizzarlo come rubrica globale per i client e-mail che offrono il supporto per le rubriche LDAP.

In tal modo, sarà possibile mantenere un database contenente le caselle di posta, gli alias e le liste di distribuzione che i server di backup remoti possono interrogare per la verifica remota delle informazioni relative all'indirizzo. Per ulteriori informazioni, consultare la successiva sezione *DN della voce di base (verifica remota)*.

Proprietà del server LDAP

Nome host o IP
Immettere in questo campo il nome dell'host o l'indirizzo IP del server LDAP.

Filtro RDN
Questo comando viene utilizzato per generare il nome specifico relativo (o RDN, Relative Distinguished Name) a ciascuna voce LDAP dell'utente. Il nome specifico relativo (RDN, Relative Distinguished Name) è la porzione all'estrema sinistra del nome specifico (DN) di ogni voce: poiché per tutte le voci presenti a uno stesso livello (ossia quelle che hanno in comune un livello immediatamente superiore) è necessario un RDN unico, è consigliabile utilizzare l'indirizzo e-mail di ogni utente come RDN in modo da eliminare possibili conflitti. Se come valore dell'attributo specificato in questo comando viene usata la macro $EMAIL$, ossia `mail=$EMAIL$`, l'attributo viene sostituito dall'indirizzo e-mail dell'utente al momento della creazione della voce LDAP. Il DN dell'utente è costituito dalla componente RDN cui viene aggiunto il valore del campo *DN della voce di base*.

DN associato
Immettere il DN della voce a cui è stato concesso di accedere come amministratore al server LDAP in modo che MDaemon possa aggiungere e modificare le voci relative ai propri utenti. Questo è il DN che viene usato per l'autenticazione nel procedimento di associazione.

Associa password
Nell'autenticazione, questa password viene trasmessa al server LDAP insieme al valore *Associa DN*.

Porta
Specificare la porta monitorata dal server LDAP. Si tratta della porta alla quale MDaemon invia le informazioni sull'account.

DN voce di base (database)
Immettere la voce di base (o DN root) da usare in tutte le voci relative agli utenti di MDaemon quando come database utenti si utilizza il server LDAP anziché il file

USERLIST.DAT. Per creare il DN dell'utente, il DN della voce di base viene combinato con l'RDN (vedere la precedente sezione *Filtro RDN*).

DN voce di base (rubrica)
Quando si riproducono le informazioni sull'account in una rubrica di database LDAP, immettere la voce di base (o DN root) da utilizzare in tutte le voci relative agli utenti di MDaemon. Per creare il DN dell'utente, il DN della voce di base viene combinato con l'RDN (vedere la precedente sezione *Filtro RDN*).

Classe oggetto (database)
Specificare la classe dell'oggetto a cui deve appartenere ciascuna voce del database utenti dell'utente di MDaemon. In ciascuna voce, al valore presente in questo campo è associato l'attributo objectclass=.

Classe oggetto (rubrica)
Specificare la classe dell'oggetto a cui deve appartenere ciascuna voce di indirizzo LDAP dell'utente di MDaemon. In ciascuna voce, al valore presente in questo campo è associato l'attributo objectclass=.

DN voce di base (database)
Un problema diffuso con i gateway di dominio e con i server di backup consiste nel non disporre generalmente di un sistema in grado di stabilire la validità del destinatario del messaggio in entrata. Ad esempio, se al server di backup di esempio.com arriva un messaggio per utente1@esempio.com il server di backup non ha modo di accertare se esista effettivamente una casella postale, un alias o una lista di distribuzione associata a "utente1". pertanto non può fare altro che accettare tutti i messaggi. MDaemon dispone di un sistema che consente di verificare gli indirizzi risolvendo, così, questo problema. Specificando un DN della voce di base, utilizzato per tutte le caselle postali, gli alias e le liste di distribuzione, il server LDAP è in grado di mantenere aggiornate tutte queste informazioni. In questo modo, ogni volta che arriva un messaggio al dominio, è sufficiente che il server di backup interroghi il server LDAP e verifichi la validità dell'indirizzo del destinatario. In caso negativo il messaggio viene respinto.

La versione del protocollo del server è la 3
Fare clic su questa casella di controllo se si desidera che MDaemon utilizzi la versione 3 del protocollo LDAP con il server.

Trova riferimenti
A volte un server non dispone dell'oggetto richiesto ma può avere un riferimento incrociato alla relativa posizione a cui può fare riferimento il client. Se si desidera che MDaemon segua questi riferimenti, attivare questa opzione. È disabilitata per impostazione predefinita.

Memorizza in cache i risultati della ricerca LDAP
Per impostazione predefinita MDaemon memorizza nella cache i risultati della ricerca LDAP. Disattivare questa opzione se non si desidera memorizzarli nella cache.

Esporta il nome completo con gli alias
I non alias esportati in una rubrica LDAP inseriscono il nome completo dell'account nel campo CN. Gli alias, tuttavia, hanno l'indirizzo e-mail effettivo (non alias) dell'account in questo campo. Selezionare questa casella di controllo se si desidera inserire invece il nome completo dell'account (se lo si conosce) in questo campo. L'opzione è disabilitata per impostazione predefinita.

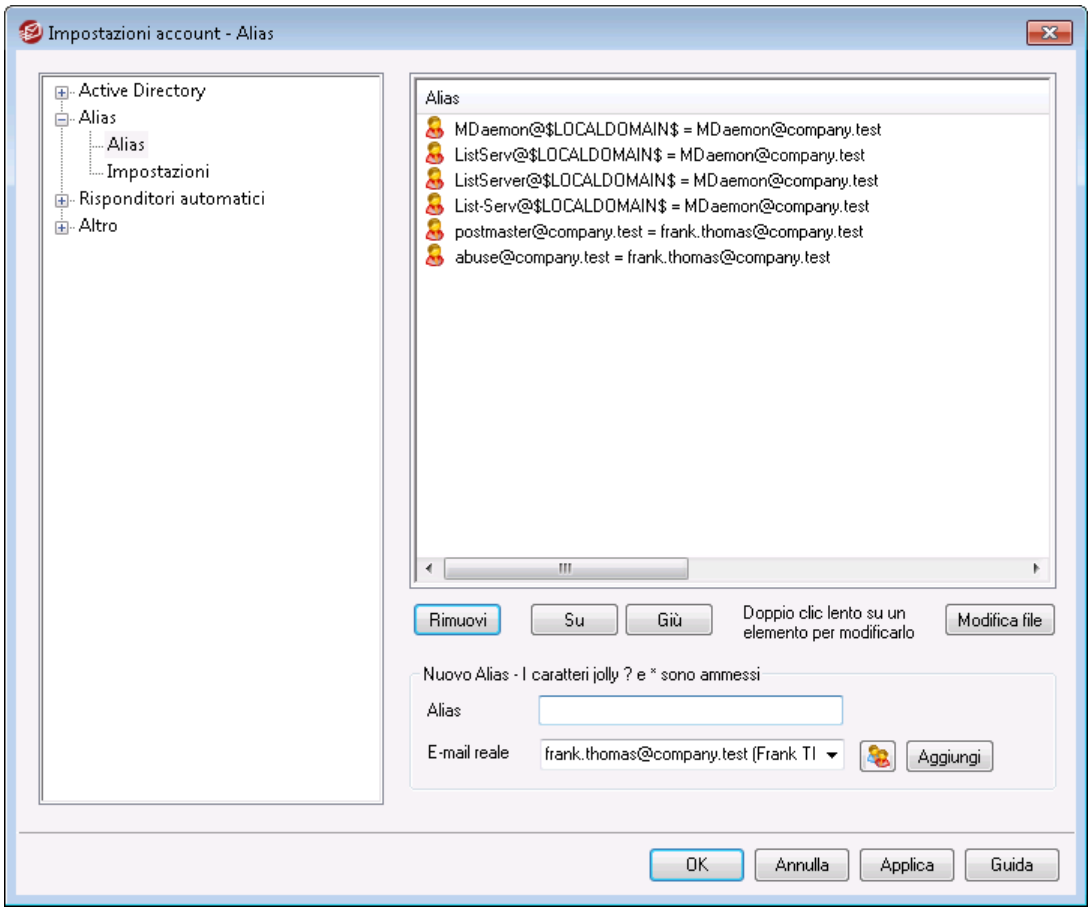
Configura
Fare clic su questo pulsante per aprire il file di configurazione `LDAP.dat` in un editor di testo, utilizzato per specificare i nomi degli attributi LDAP che corrispondono a ciascun campo degli account di MDaemon.

Vedere:

Opzioni del database account 863

5.3.2 Alias

5.3.2.1 Alias



Le funzionalità per gli alias consentono di creare nomi di caselle postali alternativi per i propri account o liste di distribuzione, utili se si desidera che più nomi di caselle postali vengano risolti in un singolo account o lista utente. In assenza di alias è necessario creare account utente distinti per ogni indirizzo e, quindi, inoltrare i messaggi o utilizzare complesse regole filtro da associare agli altri account.

Se, ad esempio, `utente1@esempio.com` gestisce tutte le richieste di fatturazione del proprio dominio, ma si desidera comunicare a tutti di inviarle a `fatturazione@esempio.com`, è possibile creare un alias affinché i messaggi indirizzati a `fatturazione@esempio.com` pervengano effettivamente a `utente1@esempio.com`. In alternativa, se si ospitano più domini e si desidera che tutti i messaggi indirizzati al postmaster, indipendentemente dal dominio, pervengano a `utente1@esempio.com`, è possibile associare all'indirizzo un alias con un carattere jolly, ossia `Postmaster@*`.

Alias correnti

In questa finestra sono inclusi tutti gli alias creati.

Rimuovi

Questo pulsante consente di rimuovere una voce selezionata dall'elenco *Alias correnti*.

Su

Gli alias vengono elaborati in base alla posizione all'interno dell'elenco. È possibile spostare un alias in una posizione superiore selezionandolo e facendo clic su questo pulsante.

Giù

Gli alias vengono elaborati in base alla posizione all'interno dell'elenco. È possibile spostare un alias in una posizione inferiore selezionandolo e facendo clic su questo pulsante.

Modifica file

Fare clic su questo pulsante per aprire il file `alias.dat` in un editor di testo per la ricerca o la modifica manuale. Dopo aver apportato le modifiche desiderate, chiudere l'editor di testo e MDaemon ricaricherà il file.

Alias

Inserire l'indirizzo email che si desidera come alias dell'*E-mail reale* indicato in precedenza. Sono consentiti i caratteri jolly "`?`" e "`*`" ed è possibile utilizzare "`@$LOCALDOMAIN$`" nell'alias come carattere jolly che corrisponde solo ai propri domini locali. Ad esempio: "`utente1@esempio.*`", "`*@$LOCALDOMAIN$`" e "`utente1@$LOCALDOMAIN$`" sono tutti alias ugualmente validi.

E-mail reale

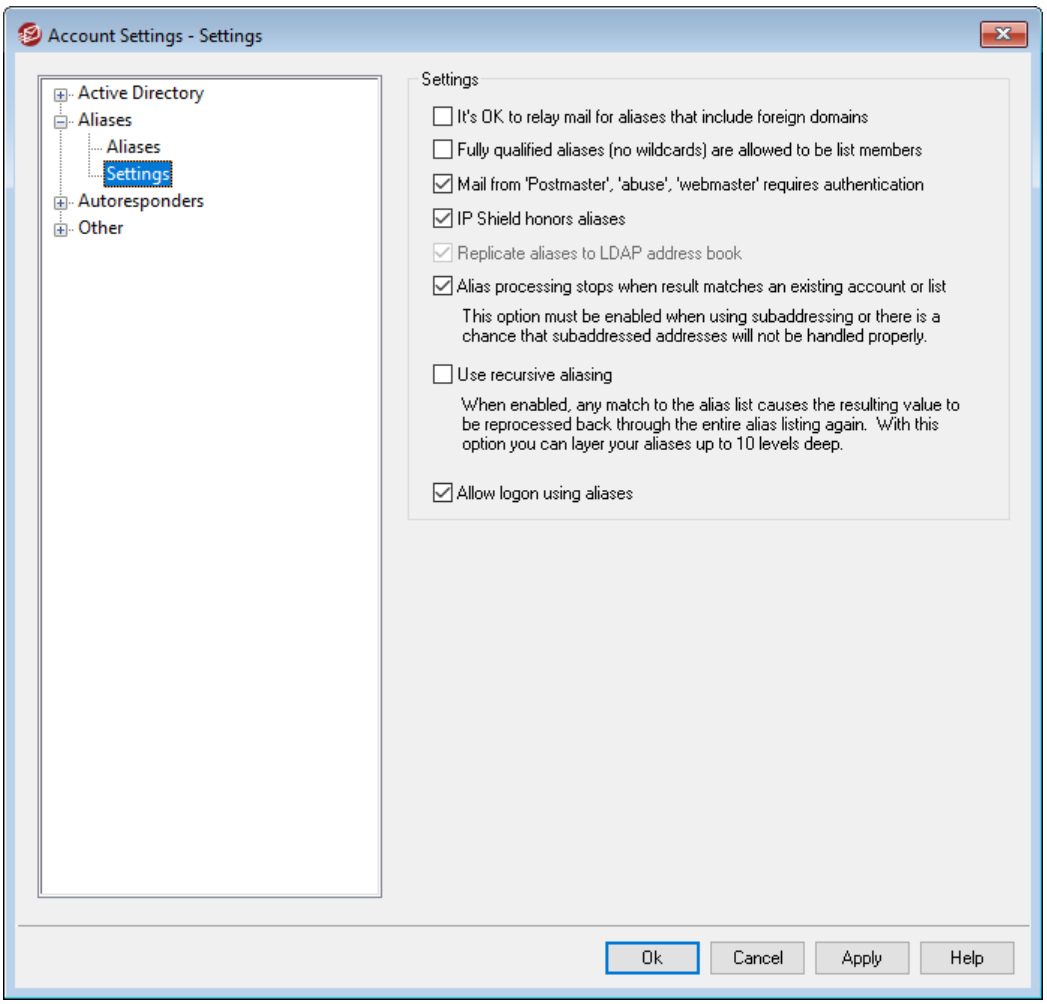
Selezionare un account dall'elenco a discesa, utilizzare l'icona Account per individuare un account oppure digitare un nuovo indirizzo e-mail o una nuova lista di distribuzione. Si tratta dell'indirizzo e-mail che riceve effettivamente i messaggi indirizzati a un alias corrispondente.

Aggiungi
Per aggiungere l'alias all'elenco, fare clic sul pulsante *Aggiungi*. I valori di *Alias* e *E-mail reale* vengono combinati e inseriti nella finestra *Alias correnti*.

Vedere:

Alias » Impostazioni 849
Account Editor » Alias 756

5.3.2.2 Impostazioni



Impostazioni

Consenti inoltro posta per gli alias di domini esterni
Abilitare questa casella di controllo per consentire a MDaemon di inoltrare la posta agli alias che comprendono domini non locali. Questa opzione ha la precedenza sull'opzione *Non consentire inoltro messaggi* di Controllo inoltro 519 relativa agli alias interessati.

Consenti alias completi (senza caratteri jolly) nelle liste di distribuzione
Selezionare questa casella di controllo per includere gli alias nelle liste di distribuzione di MDaemon. Se l'opzione è deselezionata, solo gli account reali potranno far parte di una lista di distribuzione. **Nota:** gli alias contenenti caratteri jolly non possono essere inclusi in una lista, anche se questa opzione è abilitata.

Le mail provenienti da 'postmaster', 'abuse' e 'webmaster' richiedono l'autenticazione
Abilitare questa opzione se si desidera che MDaemon richieda l'autenticazione dei messaggi che dichiarano di provenire dagli alias o dagli account "postmaster@...", "abuse@..." o "webmaster@..." prima di accettarli. Spammer e hacker sono a conoscenza della potenziale esistenza di tali indirizzi e possono, quindi, tentare di utilizzarli per inviare posta attraverso il sistema. Questa opzione consente di evitare questa eventualità. Per maggiore comodità questa opzione si trova anche nella schermata Autenticazione SMTP 531, disponibile in: `Sicurezza » Impostazioni sicurezza`. Qualsiasi modifica apportata in questa sede viene riportata anche nell'altra posizione.

Consenti alias per Scudo IP
Per impostazione predefinita, Scudo IP 528 accetta gli alias quando verifica i messaggi in entrata delle coppie dominio/IP valide. Con Scudo IP, l'alias viene convertito nell'account reale cui fa riferimento e, di conseguenza, viene accettato se il controllo ha esito positivo. Se questa opzione è disattivata, Scudo IP considera ogni alias come indirizzo indipendente dall'account che rappresenta. Di conseguenza, se l'indirizzo IP di un alias viola il controllo, il messaggio viene rifiutato. Questa opzione è duplicata nella schermata Scudo IP. Pertanto, se si modifica tale impostazione in questa sede, la modifica si rifletterà anche in quella.

Replica alias nella rubrica LDAP
Selezionare questa casella di controllo se si desidera che gli alias vengano replicati nella rubrica LDAP. La replica degli alias è necessaria affinché la funzione di verifica LDAP remota funzioni in modo affidabile. Tuttavia, se non si utilizza tale funzione, la replica nella rubrica LDAP non è necessaria. Se non si utilizza la verifica remota, è possibile disabilitare la funzione per ridurre il tempo di elaborazione. Per ulteriori informazioni sulla verifica LDAP remota, vedere: LDAP 844.

Arresta elaborazione alias se il risultato corrisponde ad account o lista
Se si abilita questa opzione, l'elaborazione degli alias si arresta quando il destinatario del messaggio in entrata corrisponde a un account esistente o a una lista di distribuzione. Questa caratteristica fa riferimento in particolare agli alias che includono caratteri jolly. Se, ad esempio, un alias è impostato su "`*@esempio.com=utente1@esempio.com`", con questa opzione l'alias viene applicato solo agli indirizzi che non esistono effettivamente nel server in uso. Se si dispone anche dell'account "`utente2@esempio.com`", i messaggi indirizzati a utente2 vengono comunque recapitati all'utente perché l'alias non viene applicato a tali messaggi. Tuttavia, i messaggi indirizzati ad account inesistenti o a una lista verranno inviati a "`utente1@esempio.com`" perché a questi messaggi viene applicato l'alias che include i caratteri jolly. L'opzione è abilitata per impostazione predefinita.

Quando si utilizza la funzione di subaddressing 778, è necessario abilitare questa opzione per evitare i potenziali problemi insiti nella gestione dei messaggi di questo tipo.

Usa alias ricorsivi
Selezionare questa casella di controllo se si desidera elaborare gli alias in modo ricorsivo. Se viene rilevata una corrispondenza di alias, il valore risultante verrà rielaborato attraverso l'intero elenco di alias. È possibile nidificare gli alias fino a 10 livelli. È ad esempio possibile specificare un'impostazione simile alla seguente:

```
utente2@esempio.com = utente1@esempio.com
utente1@esempio.com = utente5@esempio.net
utente5@esempio.net = utente9@esempio.org
```

Dal punto di vista logico, questa impostazione equivale al singolo alias:

```
utente2@esempio.com = utente9esempio.org
```

Questi alias implicano inoltre che:

```
utente1@esempio.com = utente9esempio.org
```

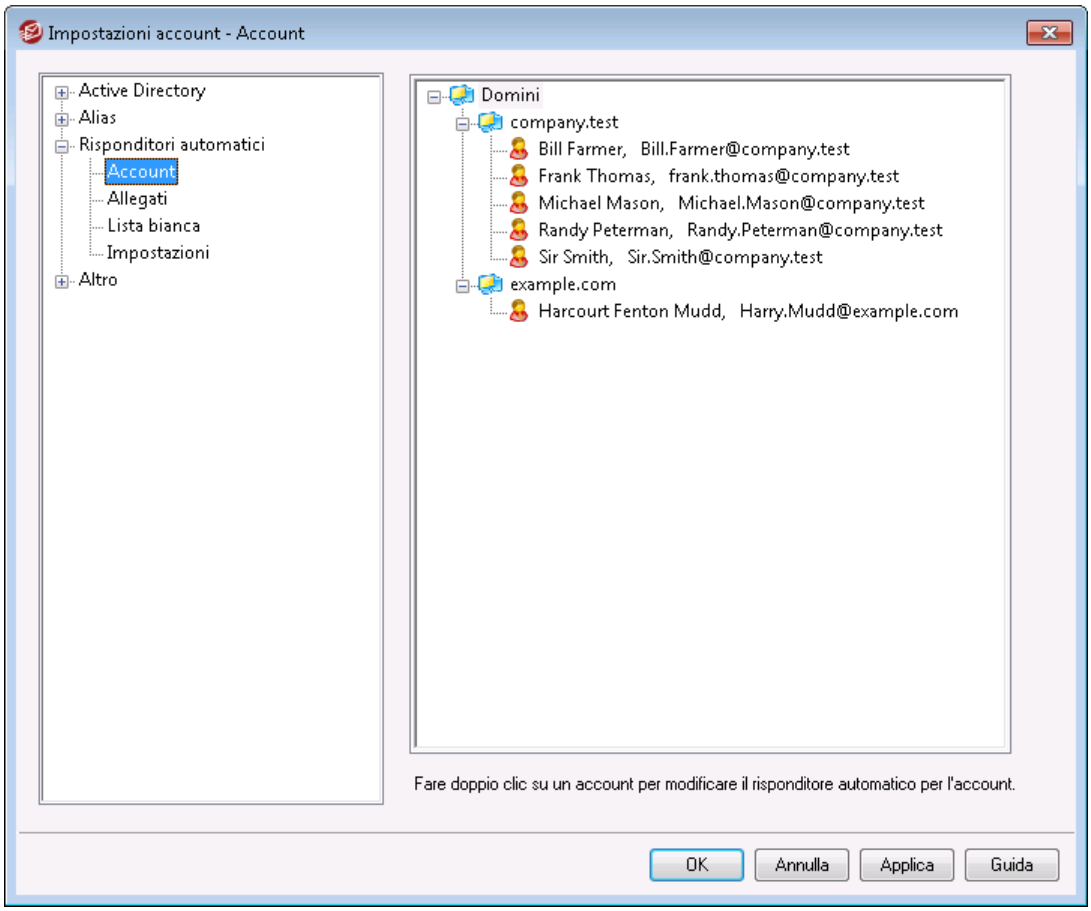
Consenti accesso con alias
Per impostazione predefinita, gli utenti sono autorizzati ad accedere ai propri account utilizzando uno dei propri alias 847 invece del nome effettivo della cassetta di posta. Se si desidera bloccare questa funzione, deselezionare la casella di controllo.

Vedere:

Alias 847

5.3.3 Risposte automatiche

5.3.3.1 Account



Le risposte automatiche sono strumenti utili che consentono, in base ai messaggi e-mail in arrivo, di attivare eventi specifici quali l'esecuzione di un programma, l'inserimento di un mittente in una lista di distribuzione, l'invio di una risposta con un messaggio generato automaticamente e altro ancora. L'utilizzo più comune delle risposte automatiche consiste nella risposta automatica ai messaggi in entrata con un messaggio definito dall'utente con il quale viene comunicato che il destinatario è in vacanza, non è disponibile, risponderà appena possibile e così via. Gli utenti di MDaemon con Accesso Web 735 a Webmail 325 o Remote Administration 359 possono utilizzare le opzioni disponibili per comporre propri messaggi di risposta automatica e pianificare le relative date di utilizzo. Infine, i messaggi di risposta automatica sono basati sul contenuto del file `OOF.mrk` che si trova nella cartella radice `\data\` di ciascun utente. Questo file supporta un elevato numero di macro, che possono essere utilizzate per la generazione dinamica di molta parte del contenuto dei messaggi, il che rende le risposte automatiche piuttosto versatili.

Gli eventi di risposta automatica vengono utilizzati quando il messaggio di attivazione proviene da un'origine remota. Tuttavia, per i messaggi che provengono dallo stesso dominio

dell'utente, le risposte automatiche si attivano solo se si seleziona l'opzione *Risposte automatiche attivate da mail dallo stesso dominio*, disponibile nella schermata Risposte automatiche » Impostazioni 856. Questa schermata consente inoltre di utilizzare un'opzione per limitare i messaggi di risposta automatica a una risposta al giorno per ogni mittente.

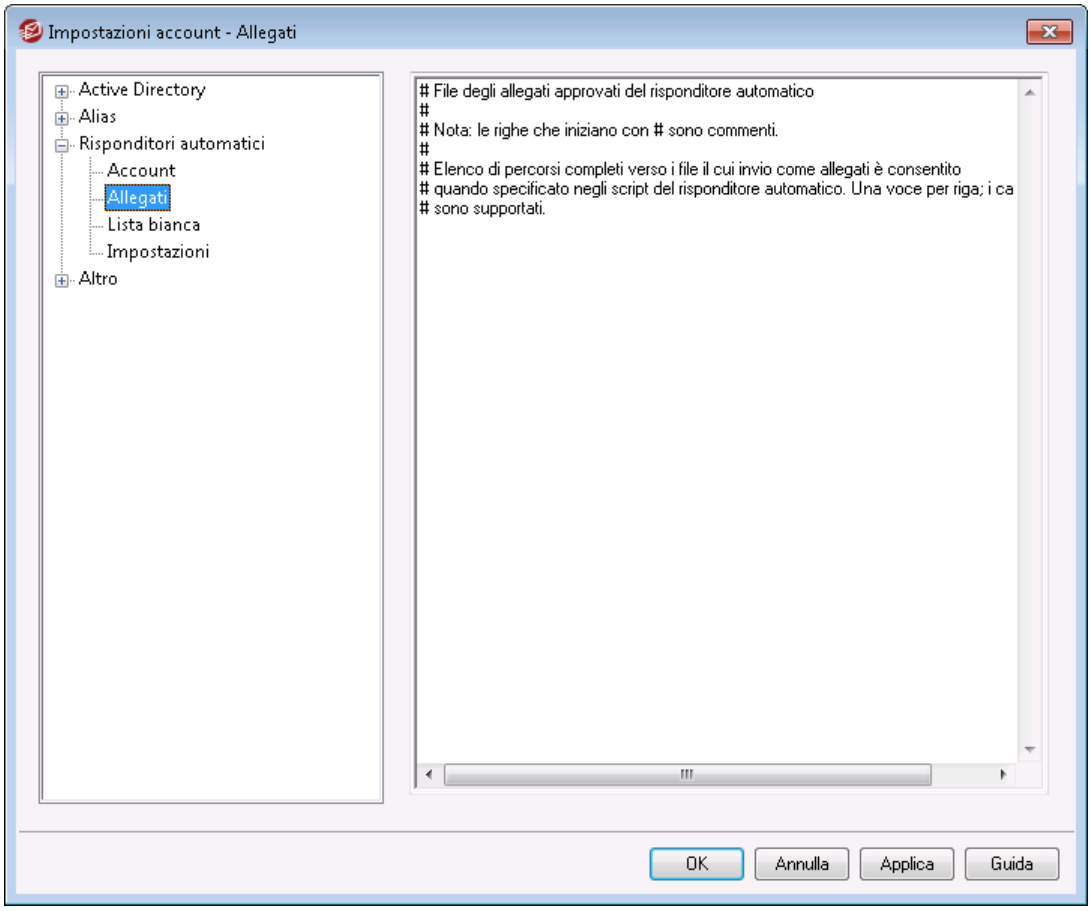
Elenco account

Quest'area include un elenco di tutte le caselle postali locali disponibili in grado di effettuare l'hosting delle risposte automatiche. Facendo doppio clic su un account verrà aperta la schermata Risposta automatica 739 corrispondente, in cui è possibile configurare le risposte automatiche relative all'account.

Vedere:

Risposte automatiche » Elenco esenzioni 855
Risposte automatiche » Impostazioni 856
Creazione di messaggi di risposta automatica 857
Account Editor » Risposte automatiche 739

5.3.3.2 Allegati

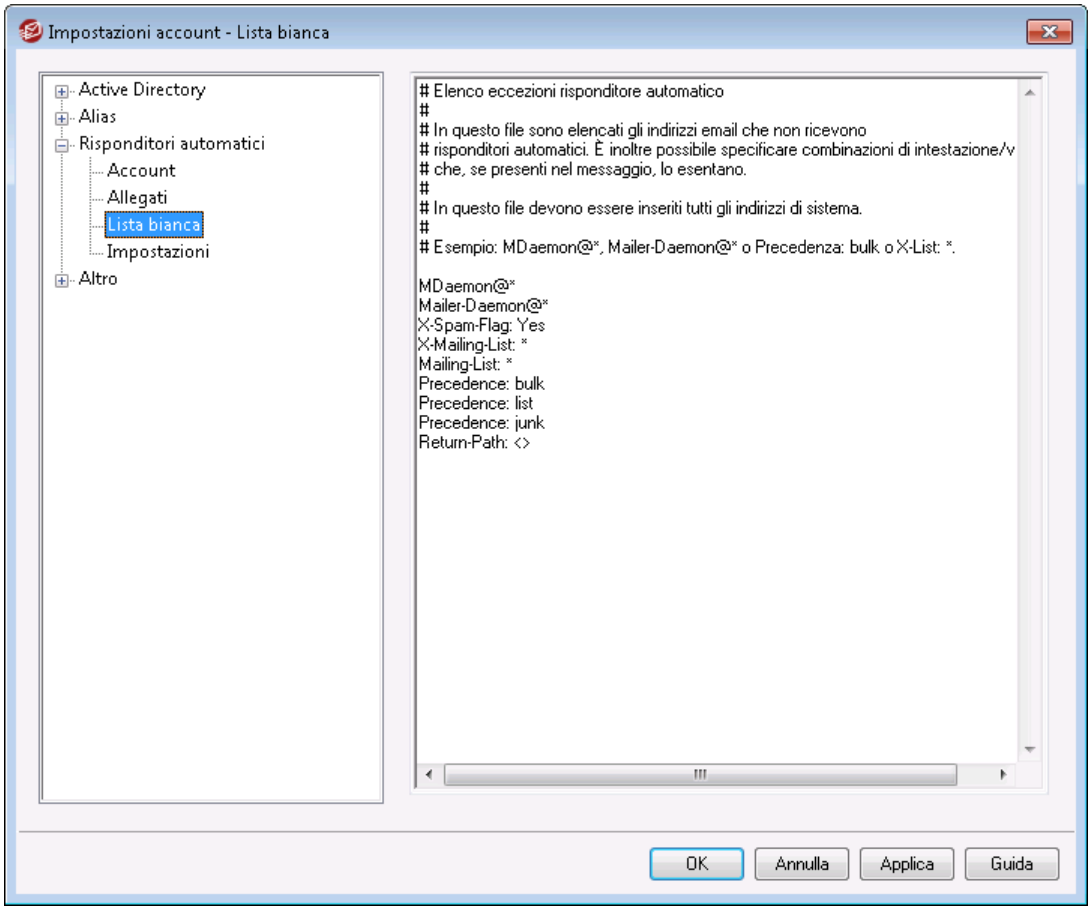


Specificare qui i percorsi completi verso i file per i quali si desidera autorizzare l'uso come allegati negli script del risponditore automatico 857. Nello script del risponditore automatico, utilizzare la macro di sostituzione **%SetAttachment%** per allegare il file.

Vedere:

Risposte automatiche » Account 852
Risposte automatiche » Elenco esenzioni 855
Risposte automatiche » Impostazioni 856
Creazione degli script di risposta automatica 857
Account Editor » Risposte automatiche 739

5.3.3.3 Elenco esenzioni



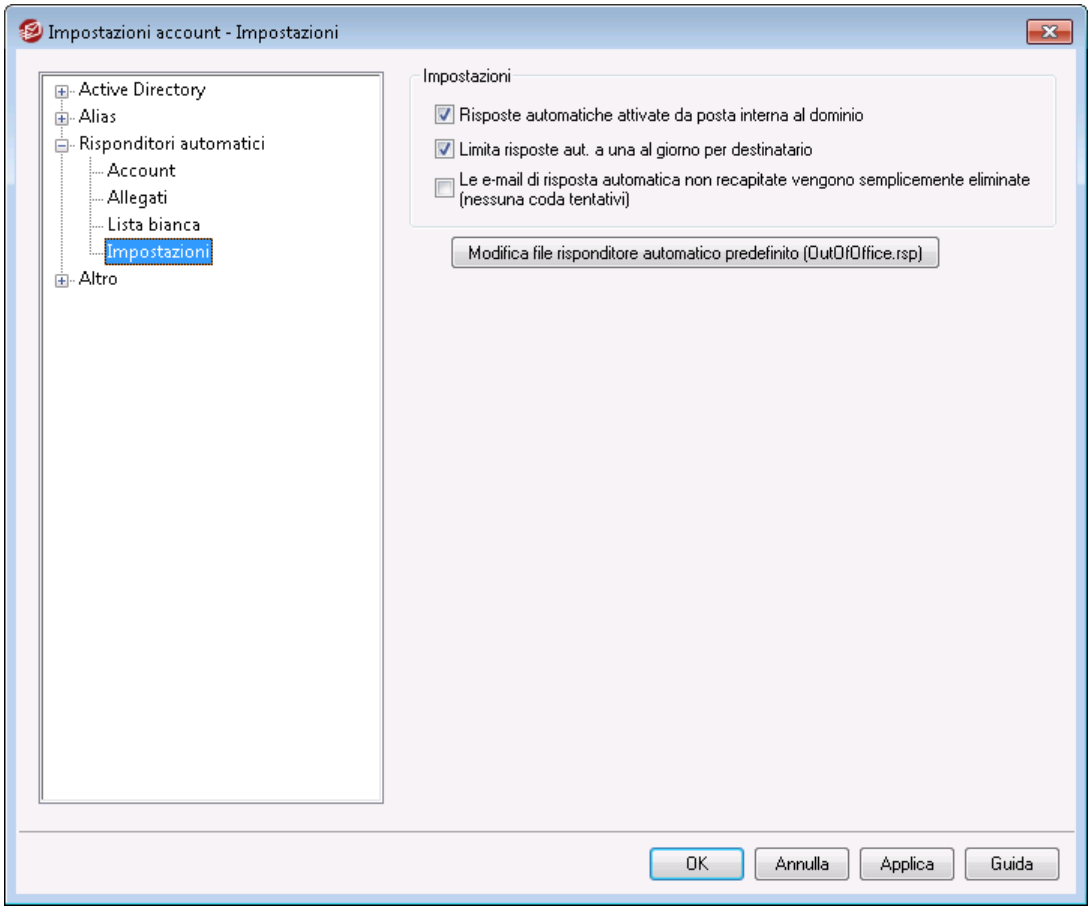
Utilizzare Risposte automatiche » Elenco esenzioni per configurare eccezioni globali per le risposte automatiche. I messaggi delle voci nell'elenco non riceveranno alcuna risposta automatica. Nell'elenco possono essere inclusi sia indirizzi e-mail sia coppie intestazione/valore. Immettere un indirizzo o una coppia intestazione/valore per riga. I caratteri jolly sono accettati.

Per evitare la ripetizione dei cicli di posta e altri problemi, è necessario elencare tutti gli indirizzi di sistema, ovvero mdaemon@*, mailer-daemon@* e così via.

Vedere:

Risposte automatiche » Account 852
Risposte automatiche » Impostazioni 856
Creazione degli script di risposta automatica 857
Account Editor » Risposte automatiche 739

5.3.3.4 Impostazioni



Impostazioni

Risposte automatiche attivate da posta interna al dominio
Per impostazione predefinita, le risposte automatiche vengono attivate sia in modalità locale che in modalità remota. Deselezionare questa casella di controllo se non si desidera attivare le risposte automatiche quando i messaggi ricevuti provengono dallo stesso dominio dell'utente.

Limita risposte aut. a una al giorno per destinatario
Per impostazione predefinita, le risposte automatiche generano un solo messaggio di risposta al giorno per un determinato indirizzo. In questo modo, si evita che il destinatario riceva lo stesso messaggio di risposta automatica più volte al giorno per ogni messaggio e-mail inviato. Per inviare una risposta automatica ad ogni messaggio ricevuto, anche se lo stesso mittente ne ha inviati più di uno al giorno, disabilitare questa casella.

Questa opzione consente di prevenire i loop che possono verificarsi quando il messaggio di risposta automatica viene inviato a un indirizzo per il quale siano state attivate le risposte automatiche. Per evitare che gli indirizzi continuino a

scambiarsi i messaggi di risposta automatica, con questa opzione viene inviato allo specifico indirizzo un solo messaggio al giorno.

Le e-mail di risposta automatica non recapitabili vengono eliminate (nessuna coda tentativi)
Attivare questa opzione se si desidera eliminare i messaggi di risposta automatica non recapitabili quando scadono dalla coda remota, invece di spostarli nel sistema di coda tentativi 888.

Modifica file risposta automatica predefinita (OutOfOffice.rsp)
È il file del messaggio di risposta automatica predefinito. Il contenuto di questo file verrà copiato nel file oof.mrk dell'account 739 se il file è mancante o è vuoto.

Vedere:

Risposte automatiche » Account 852
Risposte automatiche » Elenco esenzioni 855
Creazione degli script di risposta automatica 857
Account Editor » Risposte automatiche 739

5.3.3.5 Creazione di messaggi di risposta automatica

I file OOF.mrk sono file di testo semplice ASCII contenuti nella cartella radice `\data\` di ogni utente, che definiscono i messaggi restituiti come risultato di una funzione di risposta automatica. Quando viene attivato un messaggio di risposta dalla funzione di risposta automatica, il file viene elaborato ed esaminato alla ricerca di macro, che vengono quindi sostituite dai dati effettivi dal messaggio in arrivo che ha attivato la risposta. Le righe che iniziano con il carattere "#" vengono ignorate, perché utilizzate per i commenti. Di seguito sono riportati due messaggi di esempio 860.

Macro di risposta automatica

`$HEADERS$`	Questa macro viene sostituita da tutte le intestazioni dei messaggi in entrata. Il testo immediatamente precedente la macro viene duplicato all'inizio di ogni riga espansa.
`$HEADER:XX$`	Questa macro determina l'espansione nel messaggio del valore dell'intestazione specificata al posto di "`xx`". Ad esempio: se nel messaggio originale è presente "`TO: gianni@esempio.com`", la macro `$HEADER:TO$` verrà espansa in "`gianni@esempio.com`". Se nel messaggio originale è presente "`SUBJECT: Questo è`

l'oggetto", la macro $HEADER:SUBJECT$ verrà sostituita dal testo "Questo è l'oggetto".

$BODY$	Questa macro viene sostituita dall'intero corpo del messaggio. Nel tentativo di preservare i set caratteri di lingue diverse, MDaemon legge il corpo del messaggio come se si trattasse di dati binari anziché di testo semplice, consentendo una copia byte per byte del corpo del messaggio.
$BODY-AS-TEXT$	Analogamente alla macro $BODY$, anche questa viene sostituita dall'intero corpo del messaggio, ma viene letta come testo semplice anziché come dati binari. Il testo immediatamente precedente la macro viene duplicato all'inizio di ciascuna riga espansa. Pertanto, l'utilizzo della macro ">>$BODY-AS-TEXT$" in uno script collocherà nel messaggio generato ogni riga del messaggio originale, preceduta da ">>". È possibile aggiungere testo anche a destra della macro.
$SENDER$	Questa macro viene sostituita dall'indirizzo completo presente nell'intestazione "From:" del messaggio in entrata.
$SENDERMAILBOX$	Questa macro viene sostituita dalla casella postale del mittente. La casella postale è la porzione dell'indirizzo e-mail che si trova a sinistra del simbolo "@".
$SENDERDOMAIN$	Questa macro viene sostituita dal dominio del mittente. Si tratta della porzione dell'indirizzo e-mail che si trova a destra del simbolo "@".
$RECIPIENT$	Questa macro viene sostituita dall'indirizzo completo del destinatario del messaggio.
$RECIPIENTMAILBOX$	Questa macro viene sostituita dalla casella postale del destinatario del messaggio. La casella postale è la porzione dell'indirizzo e-mail che si trova a sinistra del simbolo "@".
$RECIPIENTDOMAIN$	Questa macro viene sostituita dal dominio del destinatario del messaggio. Il dominio è la porzione dell'indirizzo e-mail che si trova a destra del simbolo "@".
$SUBJECT$	Questa macro viene sostituita dal valore dell'intestazione "Subject:".

$MESSAGEID$	Questa macro viene sostituita dal valore dell'intestazione "Message-ID".
$CONTENTTYPE$	Questa macro viene sostituita dal valore dell'intestazione "Content-Type".
$PARTBOUNDARY$	Questa macro viene sostituita dal valore MIME "Part-Boundary" presente nell'intestazione "Content-Type" dei messaggi multipart.
$DATESTAMP$	Questa macro viene sostituita da una riga di indicatore data-ora nel formato specificato da RFC-2822.
$ACTUALTO$	Alcuni messaggi possono contenere un campo "ActualTo" che, generalmente, rappresenta la casella postale e l'host di destinazione immessi dall'utente originale prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$ACTUALFROM$	Alcuni messaggi possono contenere un campo "ActualFrom" che, in genere, rappresenta la casella postale e l'host di origine prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$REPLYTO$	Questa macro viene sostituita dal valore dell'intestazione "ReplyTo".
$PRODUCTID$	Questa macro viene sostituita dalla stringa relativa alle informazioni sulla versione di MDaemon.
AR_START	Restituisce la data/ora di inizio del risponditore automatico.
AR_END	Restituisce la data/ora di fine del risponditore automatico.

Macro per la sostituzione delle intestazioni

Le macro elencate di seguito controllano le intestazioni dei messaggi di risposta automatica.

%SetSender%
Esempio: %SetSender%=casellapostale@esempio.com
Solo nel caso dei messaggi di risposta automatica, questa macro reimposta il mittente del messaggio originale prima di creare le intestazioni del messaggio di

risposta automatica. Consente quindi di controllare l'intestazione `TO` del messaggio di risposta automatica. Se, ad esempio, il mittente del messaggio originale è "`utente2@dominio.org`" e la risposta automatica del destinatario ha utilizzato la macro `%SetSender%` per modificarlo in "`utente1@esempio.com`", l'intestazione `TO` del messaggio di risposta automatica verrà impostata su "`utente1@esempio.com`".

%SetRecipient%
Esempio: `%SetRecipient%=casellapostale@esempio.com`
Solo nel caso dei messaggi di risposta automatica, questa macro reimposta il destinatario del messaggio originale prima di creare le intestazioni del messaggio di risposta automatica. Consente quindi di controllare l'intestazione `FROM` del messaggio di risposta automatica. Se, ad esempio, il destinatario del messaggio originale è "`michele@esempio.com`" e la funzione di risposta automatica dell'account di Michele ha utilizzato la macro `%SetRecipient%` per modificarlo in "`michele.masone@esempio.com`", l'intestazione `FROM` del messaggio di risposta automatica verrà impostata su "`michele.masone@esempio.com`".

%SetReplyTo%
`Esempio: %SetReplyTo%=casellapostale@esempio.com`
Controlla il valore dell'intestazione `ReplyTo` del messaggio di risposta automatica.

%SetSubject%
`Esempio: %SetSubject%=Testo dell'oggetto`
Sostituisce il valore dell'oggetto del messaggio originale.

%SetMessageId%
`Esempio: %SetMessageId%=Stringa ID`
Modifica la stringa ID del messaggio.

%SetPartBoundary%
`Esempio: %SetPartBoundary%=Stringa Boundary`
Modifica il valore part-boundary.

%SetContentType%
`Esempio: %SetContentType%=Tipo MIME`
Modifica il tipo di contenuto del messaggio nel valore dichiarato.

%SetAttachment%
Esempio: `%SetAttachment%=filespec`
Impone a MDaemon di allegare il file specificato al messaggio di risposta automatica appena generato. Solo i file specificati nella schermata Allegati[854] possono essere allegati alle risposte automatiche.

Esempi di messaggi di risposta automatica

Un esempio di file oof.mrk di messaggio di risposta automatica che utilizza diverse macro di risposta automatica:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
```

```
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$
```

È inoltre possibile utilizzare alcune macro sostitutive delle intestazioni per espandere lo script e controllare le intestazioni generate quando il messaggio di risposta automatica viene reinviato a `$SENDER$`:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\foto\mie_vacanze.jpg
```

Utilizzando questo script, viene aggiunto"`RE: `" all'inizio dell'oggetto del messaggio di risposta automatica e viene allegato il file indicato.

La riga "`%SetSubject%=RE: $SUBJECT$`" viene gestita come segue:

1. La porzione `$SUBJECT$` viene estesa e sostituita dal testo dell'oggetto del messaggio originale. La stringa pertanto risulta equivalente a:

   ```
   %SetSubject%=RE: Testo dell'oggetto originale
   ```

2. MDaemon sostituisce l'oggetto originale (memorizzato nei buffer interni) con quello appena calcolato. Successivamente, ogni volta che nello script verrà utilizzato "`$SUBJECT$`" si otterrà il nuovo risultato.

Si noti che le nuove macro sono elencate alla fine dello script di risposta, per evitare effetti collaterali. Se ad esempio la macro `%SetSubject%` fosse collocata prima della macro `$SUBJECT$`, visualizzata nella seconda riga dello script di risposta, il testo dell'oggetto verrebbe modificato prima dell'espansione della macro `$SUBJECT$`. Di conseguenza, anziché essere sostituita con il contenuto dell'intestazione `$SUBJECT$` del messaggio originale, l'intestazione "`Subject:`" viene sostituita dal valore impostato per `%SetSubject%`.

Vedere:

Creazione di messaggi di risposta automatica 857
Risposte automatiche » Account 852
Risposte automatiche » Elenco esenzioni 855
Risposte automatiche » Impostazioni 856
Account Editor » Risposte automatiche 739

5.3.3.5.1 Esempi di messaggi di risposta automatica

Un esempio di file oof.mrk di messaggio di risposta automatica che utilizza diverse macro di risposta automatica:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$
```

È inoltre possibile utilizzare alcune macro sostitutive delle intestazioni per espandere lo script e controllare le intestazioni generate quando il messaggio di risposta automatica viene reinviato a `$SENDER$`:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\foto\mie_vacanze.jpg
```

Utilizzando questo script, viene aggiunto"`RE: `" all'inizio dell'oggetto del messaggio di risposta automatica e viene allegato il file indicato.

La riga "`%SetSubject%=RE: $SUBJECT$`" viene gestita come segue:

1. La porzione `$SUBJECT$` viene estesa e sostituita dal testo dell'oggetto del messaggio originale. La stringa pertanto risulta equivalente a:

   ```
   %SetSubject%=RE: Testo dell'oggetto originale
   ```

2. MDaemon sostituisce l'oggetto originale (memorizzato nei buffer interni) con quello appena calcolato. Successivamente, ogni volta che nello script verrà utilizzato "`$SUBJECT$`" si otterrà il nuovo risultato.

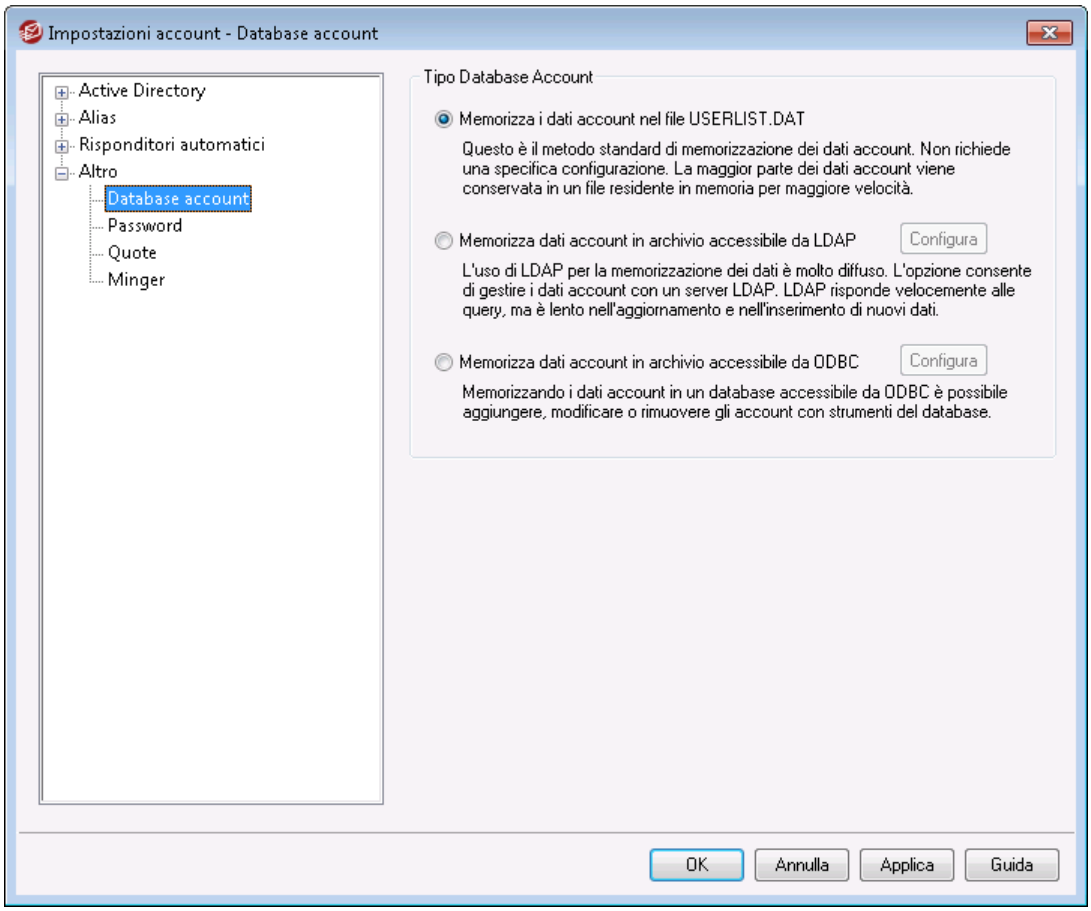
Si noti che le nuove macro sono elencate alla fine dello script di risposta, per evitare effetti collaterali. Se ad esempio la macro `%SetSubject%` fosse collocata prima della macro `$SUBJECT$`, visualizzata nella seconda riga dello script di risposta, il testo dell'oggetto verrebbe modificato prima dell'espansione della macro `$SUBJECT$`. Di conseguenza, anziché essere sostituita con il contenuto dell'intestazione `$SUBJECT$` del messaggio originale, l'intestazione "`Subject:`" viene sostituita dal valore impostato per `%SetSubject%`.

Vedere:

[Creazione di messaggi di risposta automatica](#) 857
[Risposte automatiche » Account](#) 852
[Risposte automatiche » Elenco esenzioni](#) 855
[Risposte automatiche » Impostazioni](#) 856
[Account Editor » Risposte automatiche](#) 739

5.3.4 Altro

5.3.4.1 Database account



La finestra di dialogo Database account (in Account » Impostazioni accountconsente di indicare il metodo desiderato per la gestione degli account utente in MDaemon: ODBC, LDAP o il sistema `USERLIST.DAT` locale.

Tipo database account

Memorizza i dati account nel file USERLIST.DAT
Selezionare questa opzione per abilitare l'uso in MDaemon del file interno `USERLIST.DAT` come database dell'account. Questa impostazione predefinita consente di salvare a livello locale tutte le informazioni sull'account utente di MDaemon. La maggior parte delle informazioni viene memorizzata in un singolo file residente in memoria per aumentare efficienza e velocità.

Memorizza dati account in archivio accessibile da LDAP
Selezionare questa opzione se si desidera che MDaemon utilizzi il server LDAP come database utenti di MDaemon al posto di ODBC o del sistema `USERLIST.DAT` locale. Questo metodo di aggiornamento dei dati dell'account utente può risultare utile se si dispone di più server MDaemon in siti diversi che utilizzano un database utenti condiviso. Ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale. Generalmente, i server LDAP rispondono in modo rapido ed efficiente alle query, ma sono più lenti nell'aggiornamento o nell'inserimento di nuovi dati.

Configura
Quando si seleziona l'opzione relativa a LDAP, questo pulsante consente di aprire la schermata LDAP 844 per la configurazione delle impostazioni del server LDAP.

Memorizza dati account in archivio accessibile da ODBC
Questa opzione consente di utilizzare un database compatibile con ODBC per memorizzare i dati degli account di MDaemon.

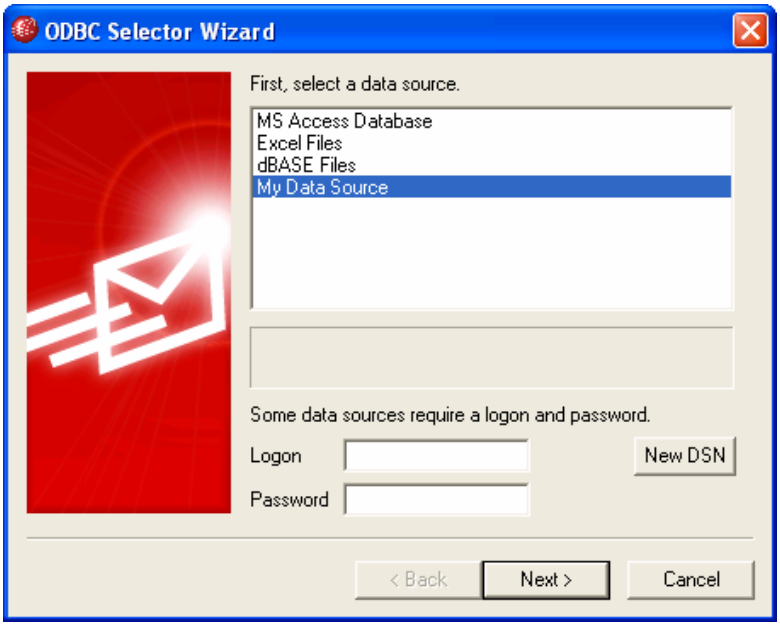
Configura
Quando è specificata l'opzione relativa a ODBC, questo pulsante consente di attivare Selezione guidata ODBC 864 al fine di selezionare e configurare il database compatibile ODBC.

5.3.4.1.1 Selezione guidata ODBC

Selezione guidata ODBC consente di selezionare o configurare un'origine dati compatibile con ODBC da utilizzare come database degli account di MDaemon.

Migrazione del database utenti in un archivio accessibile da ODBC

1. Nella finestra di dialogo Database account (in Account » Impostazioni account » Database account), fare clic su **Memorizza dati account in archivio accessibile da ODBC**, quindi selezionare **Configura** per aprire Selezione guidata ODBC.

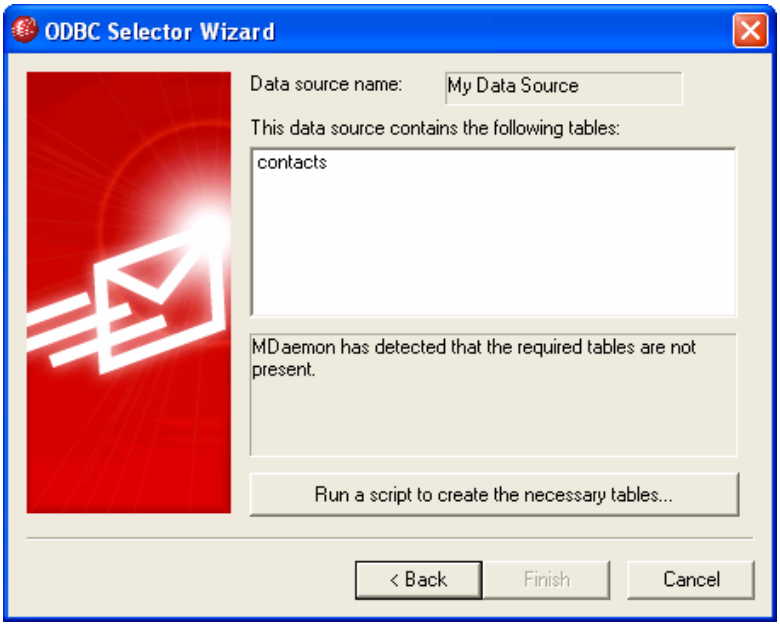


2. Selezionare l'**origine dati** che si desidera utilizzare per il database account. Se questa non è presente nell'elenco, fare clic su **Nuovo DSN** e seguire le indicazioni fornite in **Creazione di una nuova origine dati ODBC** 866.

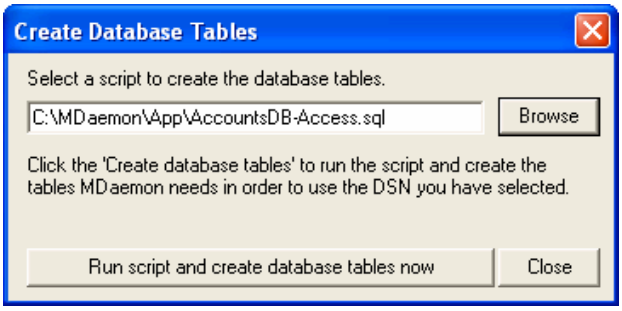
3. Se necessario, inserire l'**ID accesso** e la **Password** dell'origine dati.

4. Scegliere **Avanti**.

5. Se l'origine dati include già le tabelle necessarie per MDaemon, proseguire con il **Passaggio 8.** In caso contrario, fare clic su **Esegui script per creare le tabelle necessarie**.



6. Inserire il percorso (o scegliere **Sfoglia**) del file di script da utilizzare per creare le tabelle dell'applicazione database. Nella cartella `\MDaemon\app\` sono presenti gli script per la maggior parte delle applicazioni database.



7. Scegliere **Esegui script e crea tabelle del database**, quindi **OK** e **Chiudi**.

8. Scegliere **Fine** e fare clic su **OK** per chiudere la finestra di dialogo Database account.

9. Lo strumento di migrazione del database trasferirà tutti gli account utente nell'origine dati ODBC e chiuderà MDaemon. Per iniziare a utilizzare il nuovo database utenti ODBC, scegliere **OK** e riavviare MDaemon.

Per ulteriori informazioni, vedere:

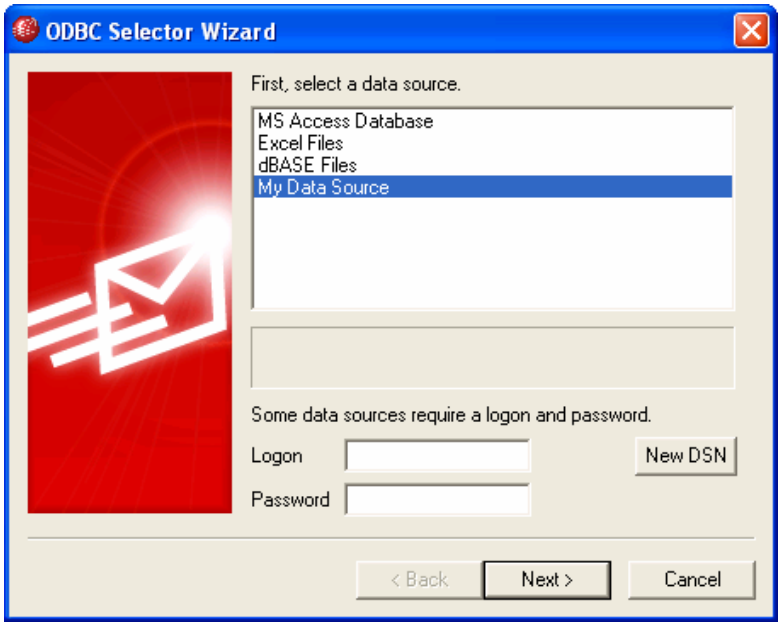
Database account 863
Creazione di una nuova origine dati ODBC 866

5.3.4.1.1.1 Creazione di una nuova origine dati

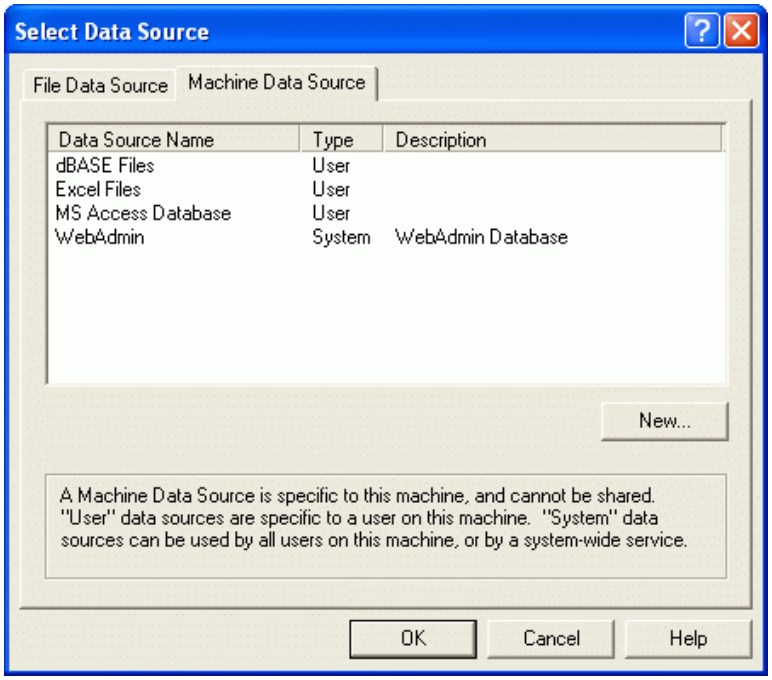
Per creare una nuova origine dati ODBC procedere come segue:

1. Nella finestra di dialogo Database account (in Account » Impostazioni account » Database account), fare clic su **Memorizza dati account in archivio accessibile da ODBC**, quindi selezionare **Configura** per aprire Selezione guidata ODBC.

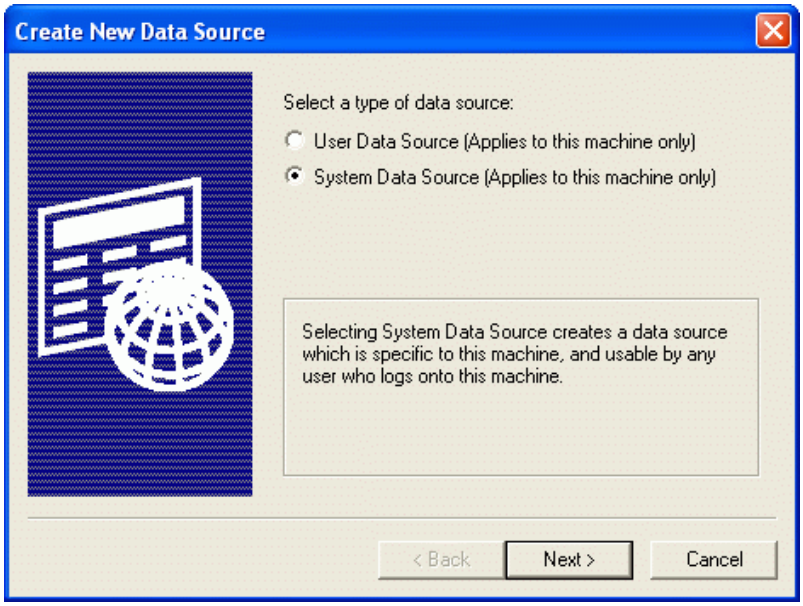
2. Fare clic su **Nuovo DSN** per aprire la finestra di selezione dell'origine dati.



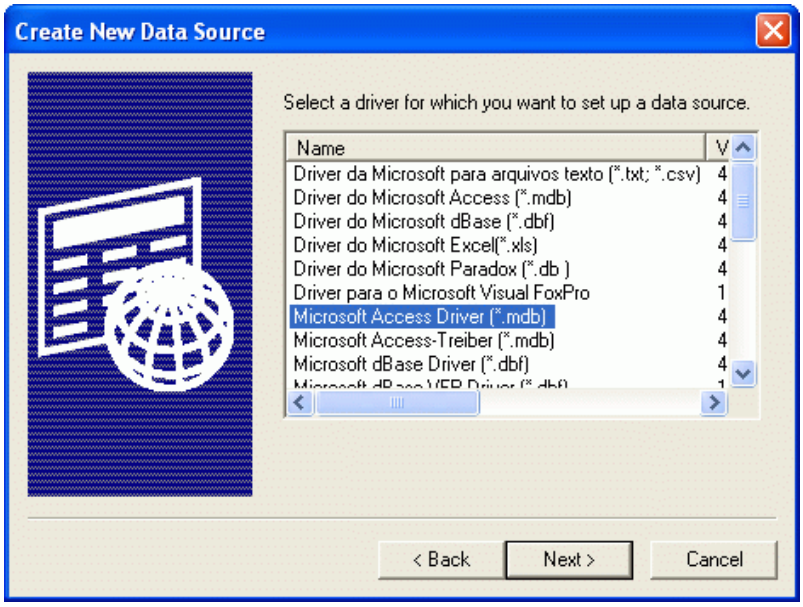
3. Passare alla scheda **Origine dati computer** e fare clic su **Nuova** per aprire la finestra di dialogo Crea nuova origine dati.



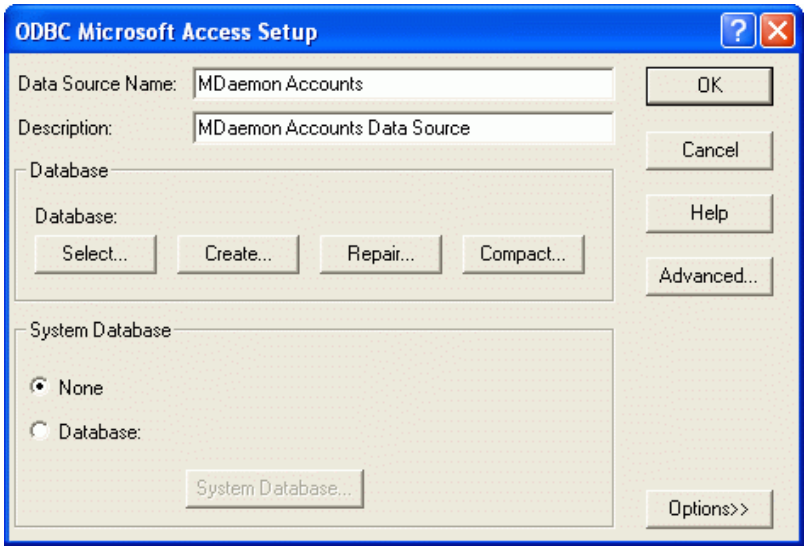
4. Selezionare **Origine dati di sistema** e fare clic su **Avanti**.



5. Selezionare il **driver** di **database** per il quale si desidera configurare l'origine dati, quindi fare clic su **Avanti**.



6. Fare clic su **Fine** per visualizzare la finestra di dialogo per l'impostazione del driver specifico. L'aspetto di questa finestra di dialogo varia a seconda del driver selezionato. Quella visualizzata di seguito è la finestra di dialogo relativa alle impostazioni di accesso Microsoft.



7. Indicare un valore per la nuova origine nel campo **Nome origine dati** e fornire le altre informazioni richieste dalla finestra di dialogo relativa allo specifico driver, quali la creazione o l'indicazione di un database, la scelta di una directory o di un server e così via.

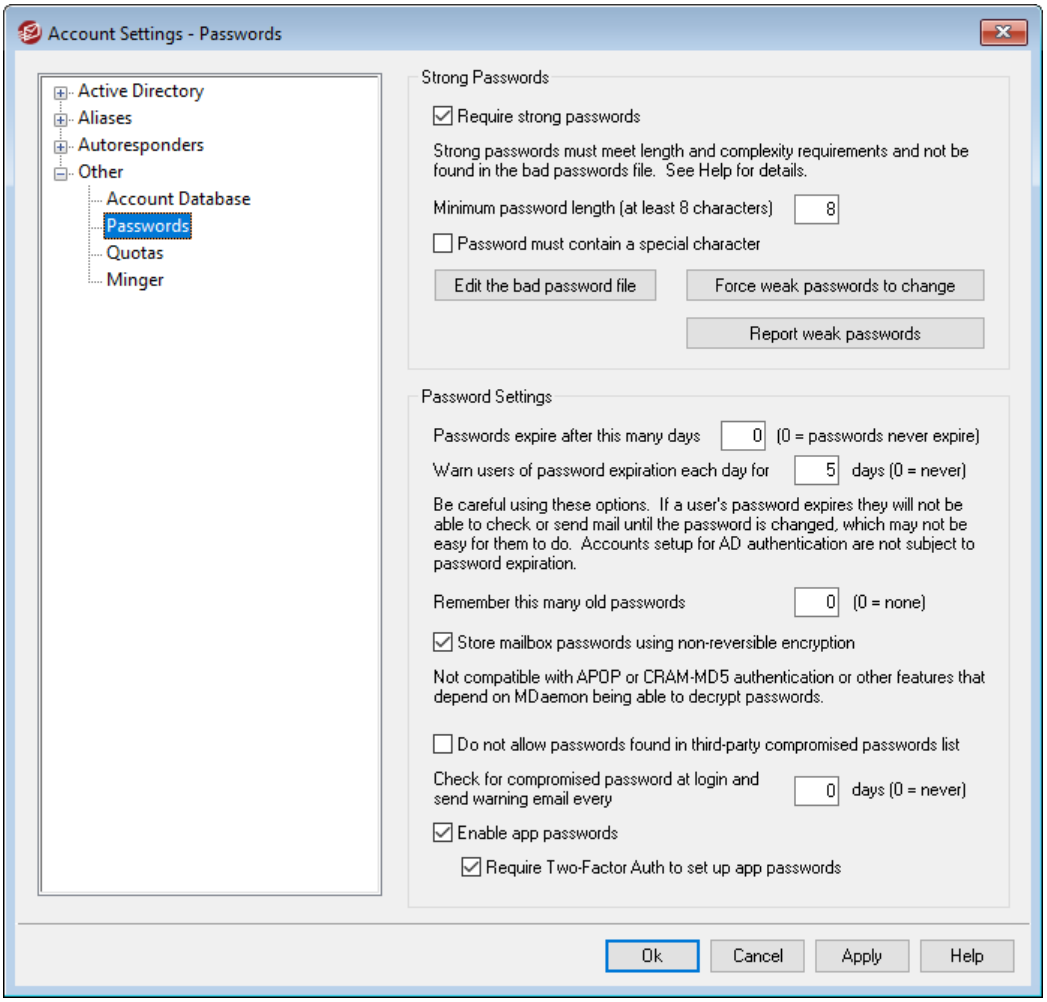
8. Fare clic su **OK** per chiudere la finestra di dialogo del driver.

9. Fare clic su **OK** per chiudere la finestra di dialogo per la selezione dell'origine dati.

Vedere:

Database account 863
Selezione guidata ODBC - Database account 864

5.3.4.2 Password



Password sicure

Richiedi password sicure
Per impostazione predefinita, in fase di creazione di nuovi account o di modifica delle password esistenti MDaemon richiede password sicure. Per disattivare la richiesta di password sicure, deselezionare questa casella di controllo.

Le password sicure devono:
- Soddisfare il requisito di lunghezza minima.
- Contenere lettere maiuscole e minuscole.
- Contenere lettere e numeri.
- Contenere un carattere speciale (se l'opzione per il carattere speciale è impostata di seguito)
- Non contenere il nome completo dell'utente o il nome di una casella postale.
- Non essere presenti nel file delle password non consentite.

Lunghezza minima password (almeno 8 caratteri)
Utilizzare questa opzione per impostare la lunghezza minima della password necessaria per ottenere password sicure. L'impostazione minima è di 8 caratteri, ma è consigliabile impostare un valore più alto. Il valore predefinito per le nuove installazioni di MDaemon è di 10 caratteri. La modifica di questa impostazione non richiede automaticamente una modifica della password da parte degli account che utilizzano password più brevi del nuovo minimo. Tuttavia, quando tali utenti dovranno modificare la password verrà applicata questa impostazione.

Indipendentemente dall'impostazione della lunghezza minima, le password possono essere più lunghe di 72 caratteri quando si seleziona l'opzione "*Memorizza password casella postale mediante crittografia non reversibile*" di seguito. Quando questa opzione è disattivata, le password non possono essere più lunghe di 15 caratteri.

Le password devono contenere un carattere speciale
Per impostazione predefinita, nelle nuove installazioni di MDaemon per le password complesse è richiesto l'uso di almeno uno dei seguenti caratteri speciali: !"#$%&'() *+,-./:;<=>?@[\]^_`{|}~. Disattivare questa opzione se non si desidera richiedere l'uso di caratteri speciali nelle password complesse.

Modifica file password non consentite
Fare clic su questo pulsante per modificare il file password non consentite. Le voci utilizzate in questo file non tengono conto della distinzione tra maiuscole/minuscole e non possono essere utilizzate come password. Per creare voci più complesse o versatili, è possibile utilizzare Espressioni regolari 667. Le voci che iniziano con "!" vengono considerate Espressioni regolari.

Forza modifica password deboli
Fare clic su questo pulsante per forzare tutti gli account con una password debole a modificare la password. In questo modo si bloccano tutti gli account con una password debole fino a che questa non viene modificata. La password può essere modificata da un amministratore mediante l'interfaccia di MDaemon, oppure un utente bloccato può modificare la password via Webmail o attraverso l'interfaccia di Remote Administration. Quando tenta di accedere con la vecchia password, l'utente riceve una richiesta di creazione di una nuova password per poter procedere. **Nota:** questa opzione non è disponibile quando si utilizza l'opzione "*Memorizza password casella postale mediante crittografia non reversibile*" di seguito.

Report password deboli
Fare clic su questo pulsante per generare un report per tutti gli account MDaemon con una password debole. Il report verrà inviato mediante posta elettronica all'indirizzo che si specifica dopo aver fatto clic su OK. **Nota:** questa opzione non è disponibile quando si utilizza l'opzione "*Memorizza password casella postale mediante crittografia non reversibile*" di seguito.

Impostazioni password

Scadenza password dopo il numero di giorni seguente (0=le password non scadono mai)
Questa opzione consente di impostare il numero massimo di giorni in cui è possibile accedere a un account prima che occorra modificarne la password. Il valore predefinito di questa opzione è "0", indicante che le password non scadono mai. Ma se la si imposta, ad esempio, su 30 giorni, l'utente avrà 30 giorni per modificare la password, **a partire dall'ultima modifica della password dell'account**. Di conseguenza, quando si imposta per la prima volta un valore per la scadenza, gli account con una password che non è stata cambiata entro il numero di giorni specificato si troveranno ad avere immediatamente una password scaduta. Quando la password di un utente scade, l'utente non potrà accedere a POP, IMAP, SMTP, Webmail o Remote Administration. Potrà comunque connettersi a Webmail o a Remote Administration e gli verrà richiesto di modificare la password prima di procedere. Per modificare la password non è possibile utilizzare i client di posta elettronica, ad esempio Outlook, Thunderbird e simili. Inoltre, molti client non visualizzano nemmeno un messaggio di errore utile per gli utenti, che potrebbero quindi necessitare dell'assistenza dell'amministratore per comprendere perché l'accesso non riesce.

Affinché gli utenti possano modificare le password via Webmail o Remote Administration, devono prima ottenere l'autorizzazione di accesso Web "...modifica password" nella schermata Servizi Web 814. Prestare attenzione prima di utilizzare questa opzione, in quanto la modifica della password potrebbe creare qualche difficoltà ad alcuni utenti.

Avvisa utenti della scadenza della password ogni giorno per [xx] giorni (0 = mai)
Gli account con una password in scadenza possono ricevere quotidianamente un messaggio e-mail di promemoria. Utilizzare questa opzione per specificare quanti giorni prima della scadenza della password si desidera che MDaemon inizi a inviare e-mail quotidiane.

Ricorda il seguente numero di vecchie password (0 =nessuna)
Utilizzare questa opzione per specificare il numero di password precedenti che si desidera che MDaemon ricordi per ogni utente. Quando gli utenti modificano la password, non sarà loro consentito di riutilizzare le password precedenti. Per impostazione predefinita, questa opzione è impostata su "0" (disabilitata).

Salva le password della casella postale con una crittografia non reversibile
Selezionare questa casella se si desidera archiviare le password utilizzando una crittografia non reversibile. In questo modo le password non possono essere decrittografate da MDaemon, dall'amministratore e da malintenzionati. A tale scopo, MDaemon utilizza la funzione di hashing delle password bcrypt che consente l'utilizzo di password più lunghe (fino a 72 caratteri), nonché di conservarle senza rivelarle durante l'importazione e l'esportazione di account. Alcune funzionalità, tuttavia, non sono compatibili con questa opzione, ad esempio il rilevamento delle password deboli e l'autenticazione APOP e CRAM-MD5 94, perché dipendono dalla capacità di MDaemon di decrittografare le password. Le password irreversibili sono abilitate per impostazione predefinita.

Password compromesse

MDaemon può controllare le password di un utente in base a un elenco di password compromesse fornito da un servizio di terze parti. È in grado di eseguire questa operazione senza trasmettere le password al servizio e se la password di un utente è presente nell'elenco non significa che l'account è stato violato. Significa che qualcuno da qualche parte ha usato gli stessi caratteri di questa password in precedenza e la password è stata visualizzata in una violazione di dati. Le password pubblicate possono essere utilizzate dagli hacker negli attacchi con dizionario, ma le password univoche che non sono mai state utilizzate sono più sicure. Per ulteriori informazioni, vedere Password pwned.

Non consentire password presenti nell'elenco di password compromesse di terze parti
Selezionare questa casella di controllo se non si desidera consentire di impostare la password dell'account su una delle password presenti nell'elenco di password compromesse.

Controlla password compromesse all'accesso e invia e-mail di avviso ogni [xx] giorni (0 = mai)
Con questa opzione è possibile controllare automaticamente la password di ogni utente in base all'elenco di password compromesse ogni numero di giorni specificato, quando ciascun utente esegue l'accesso. Se viene rilevato l'uso di una password compromessa, viene inviata una e-mail di avviso all'account e al postmaster. Le e-mail di avviso possono essere personalizzate modificando i file di modello di messaggio nella cartella `\MDaemon\App`. Poiché le istruzioni per gli utenti su come modificare la password possono dipendere da se l'account usa una password memorizzata in MDaemon o l'autenticazione di Active Directory 835, sono disponibili due file di modelli: `CompromisedPasswordMD.dat` e `CompromisedPasswordAD.dat`. È possibile utilizzare le macro per personalizzare il messaggio, modificare l'oggetto, il destinatario e così via.

Password di applicazione

Password di applicazione 766 è un'opzione che si può utilizzare per rendere più sicuri gli account creando password molto complesse, generate in modo casuale, da utilizzare solo nei client e-mail e nelle app di posta elettronica, poiché tali app non possono essere protette dall'autenticazione a due fattori 735 (2FA). Vedere: Password di applicazione 766.

Attiva password di applicazione
Per impostazione predefinita, tutti gli utenti possono creare password di applicazione per i propri account quando accedono a Webmail utilizzando l'Autenticazione a due fattori. Se non si desidera consentire a un utente specifico di utilizzare la funzionalità delle password di applicazione, è possibile utilizzare l'opzione *...modificare password di applicazione* 735 nella pagina Servizi Web dell'utente.

Richiedi l'autenticazione a due fattori per impostare le password di applicazione
Per impostazione predefinita, gli utenti devono accedere a Webmail utilizzando l'Autenticazione a due fattori 735 (2FA) per creare una nuova password di applicazione. Non è consigliabile disattivare questo requisito. Gli amministratori globali 773 sono esentati da questo requisito in MDRA, ma è comunque consigliabile utilizzare sempre la 2FA quando si accede a MDRA o a Webmail.

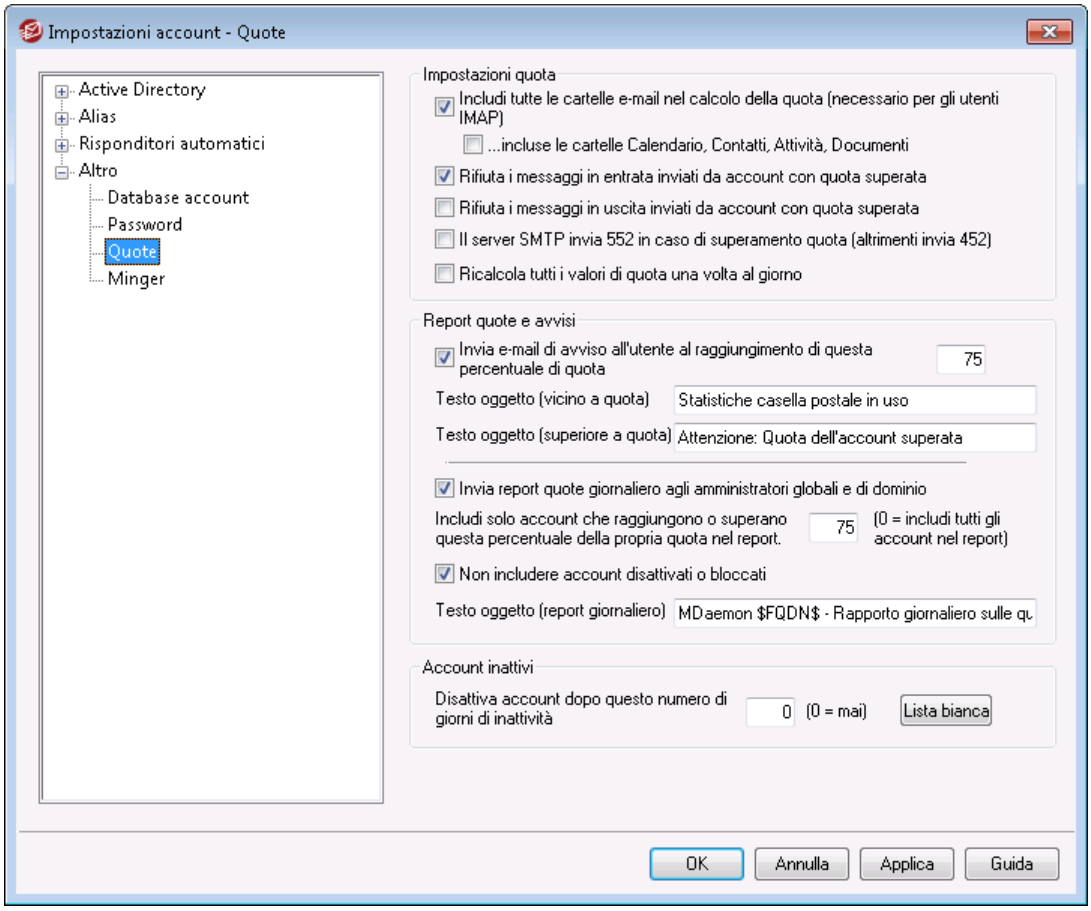
Nella pagina di impostazioni di Account Editor 776 è disponibile un'opzione per gli account: "*Richiedi la password di applicazione per l'accesso a SMTP, IMAP, ActiveSync, ecc.*".

La richiesta di password di applicazione può aiutare a proteggere le password degli account da attacchi a dizionario e a forza bruta via SMTP, IMAP, ecc. La sicurezza è garantita dal fatto che, ove mai con un attacco di questo tipo si riuscisse a indovinare la password reale di un account, questa non funzionerebbe senza che l'aggressore possa accorgersene, perché MDaemon accetta solo una password di applicazione corretta. Inoltre, se gli account in MDaemon utilizzano l'autenticazione con Active Directory 835 e Active Directory blocca un account dopo un certo numero di tentativi non riusciti, questa opzione può aiutare a prevenire il blocco degli account, poiché MDaemon verifica solo le password di applicazione e non tenta l'autenticazione con Active Directory.

Vedere:

Account Editor » Dettagli account 729
Account Editor » Servizi Web 735
Account Editor » Password di applicazione 766
Espressioni regolari 667

5.3.4.3 Quote



Impostazioni della quota

Includi tutte le cartelle e-mail nel calcolo della quota (necessario per gli utenti IMAP)
Quando questa casella è selezionata, per tutti i file dei messaggi in tutte le cartelle e-mail dell'account di un utente verranno applicate le limitazioni relative a numero o dimensioni dei messaggi. In caso contrario, le limitazioni saranno applicate solo ai file dei messaggi presenti nella Posta in arrivo. Questo è in genere necessario solo per gli utenti IMAP.

...includi anche le cartelle Calendario, Contatti, Attività, Documenti
Selezionare questa casella di controllo se si desidera includere nel calcolo delle quote tutte le cartelle relative a calendario, contatti, attività e documenti.

Rifiuta messaggi in arrivo inviati ad account con quota superata
Per impostazione predefinita, se per un account è stato impostato un limite di quota, quando questo limite viene superato, MDaemon non accetta più messaggi in arrivo per l'account finché il titolare non elimina parte dei messaggi di posta memorizzati. Deselezionare questa casella di controllo se non si desidera rifiutare i messaggi in ingresso per account con quota superata.

Rifiuta messaggi in uscita inviati da account con quota superata
Selezionare questa casella di controllo se si desidera rifiutare i messaggi in uscita inviati da account che hanno raggiunto la quota. Un account con quota superata non potrà più inviare la posta fino a quando non elimina alcuni dei messaggi memorizzati. L'opzione è disabilitata per impostazione predefinita.

Il server SMTP invia 552 in caso di superamento quota (altrimenti invia 452)
Per impostazione predefinita, quando un account supera la quota[746] MDaemon invia il codice di errore 452 ("Azione richiesta respinta: spazio su sistema insufficiente") durante l'elaborazione SMTP. Questo codice indica generalmente che il server deve effettuare un tentativo successivo. Selezionando questa casella di controllo invece, viene inviato il codice di errore permanente 552 ("Azione richiesta interrotta: spazio dedicato superato").

Ricalcola tutti i valori di quota una volta al giorno
Per impostazione predefinita, i valori di quota memorizzati nella cache sono azzerati solo quando viene attivata l'opzione "*Invia report quote giornaliero...*". Selezionare questa casella di controllo se invece si desidera che i valori di quota siano ricalcolati nell'ambito della routine di manutenzione giornaliera.

Report quote e avvisi

Inviare una e-mail di avviso all'utente se viene raggiunta questa percentuale di quota
Se, durante l'evento di manutenzione e pulizia quotidiana[501], MDaemon determina che un account supera, sia in relazione al *numero di messaggi memorizzati contemporaneamente* che allo *spazio massimo consentito su disco*, il valore percentuale di limitazione della quota previsto in Account Editor[746], verrà inviato un messaggio di avviso all'account. Utilizzare l'opzione *Testo dell'oggetto (limite quota quasi raggiunto)* riportata di seguito per impostare l'oggetto del messaggio. Nel messaggio verranno inclusi il numero di messaggi memorizzati e la dimensione della casella postale relativi all'account, nonché la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato. Ogni volta che un nuovo messaggio di avviso viene inserito nella Posta in arrivo di un utente, viene creata una voce nel registro di sistema per notificarlo all'utente. Non viene creata alcuna voce di registro quando il messaggio esiste già e viene solo aggiornato. Se una voce di registro viene aggiunta ripetutamente, questo indica che l'utente sta eliminando il messaggio dalla Posta in arrivo. Se non si desidera inviare un messaggio di avviso sulle quote agli utenti, disabilitare questa opzione.

Il modello Messaggio vicino alla quota (disponibile in: MDaemon\app\NearQuota.dat) viene utilizzato per creare il messaggio di avviso di vicinanza ai limiti della quota. Tutte le macro relative agli account utente (ad es. $EMAIL$, $MAILBOX$, $DOMAIN$, ecc.) possono essere usate nel modello.

Testo dell'oggetto (limite quota quasi raggiunto)
Questo è il testo dell'oggetto dei messaggi di avviso inviati a qualsiasi utente che superi la percentuale di quota prestabilita. Tali messaggi vengono inviati ogni giorno

durante gli eventi di manutenzione e pulizia quotidiana che per impostazione predefinita hanno luogo a mezzanotte.

Testo dell'oggetto (limite quota superato)
Analogamente al messaggio "quota quasi raggiunta", verrà inviato un altro messaggio quando l'account di un utente supera la quota. Questo è il testo dell'oggetto del messaggio di avviso "quota superata".

Invia report quote giornaliero agli amministratori globali e di dominio
Selezionare questa casella e specificare un valore se si desidera inviare un report giornaliero delle quote a tutti gli amministratori globali e di dominio. Il report conterrà le statistiche sulle quote di tutti gli utenti che raggiungono o superano la percentuale specificata del propria limite di quota. Utilizzare il valore "0" se si desidera che il report includa le statistiche di quota su tutti.

Non includere account disattivati o bloccati
Per impostazione predefinita, i report quote non includono gli account disattivati o bloccati. Deselezionare questa casella di controllo se si desidera includerli.

Testo dell'oggetto (report giornaliero)
Utilizzare questa opzione per personalizzare il testo dell'oggetto del rapporto giornaliero sulle quote che MDaemon invia agli amministratori. Vedere `QuotaReport.dat` nella cartella `MDaemon\APP` per personalizzare anche il rapporto.

Account inattivi

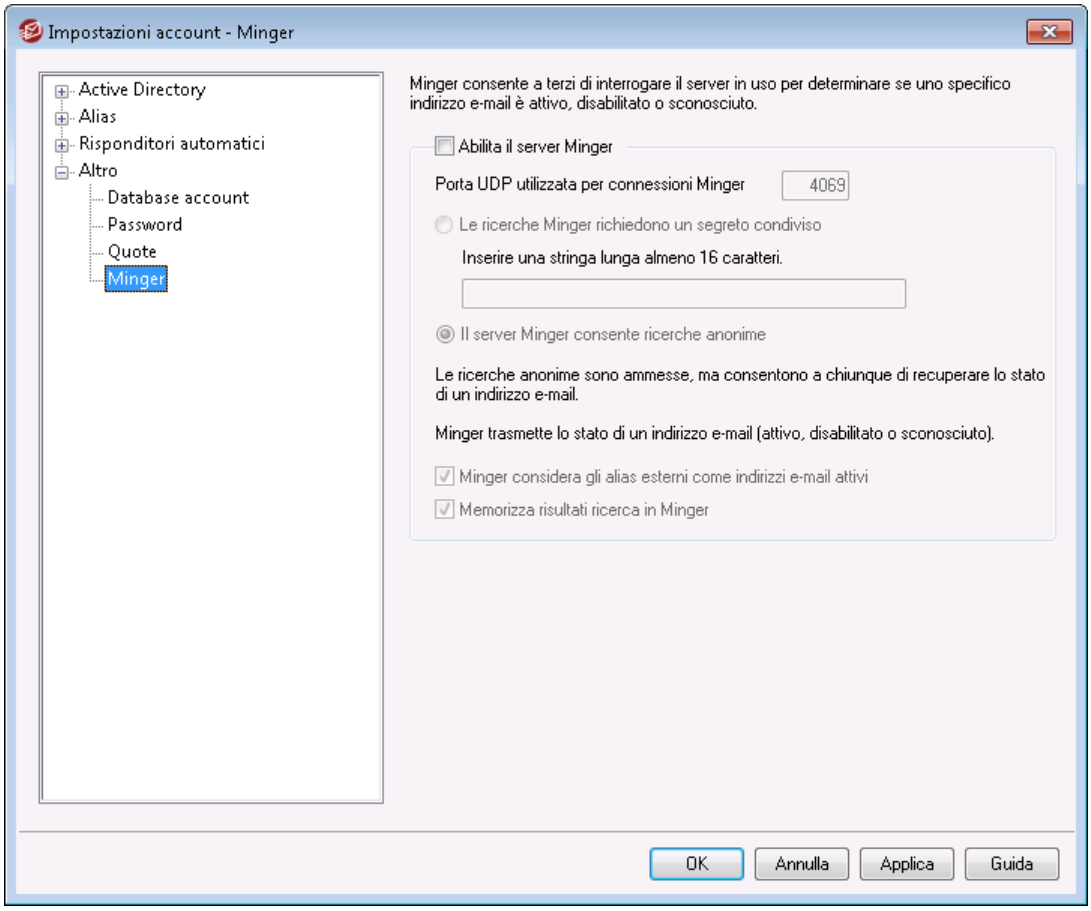
Disattiva account dopo questo numero di giorni di inattività XX (0=mai)
Utilizzare questa opzione per disattivare automaticamente gli account rimasti inattivi per più di un determinato numero di giorni. Una volta raggiunto il numero massimo di giorni di inattività, l'account viene disattivato e viene inviato un messaggio di e-mail al postmaster. Una risposta a tale messaggio e-mail riattiva l'account. L'elaborazione viene eseguita come parte dell'evento di pulizia di mezzanotte ogni notte. Il valore predefinito è 0 (disattivata).

Elenco esenzioni
Gli account aggiunti a questo elenco vengono esentati dalla funzionalità di disabilitazione degli account inattivi.

Vedere:

Account Editor » Quote 746
Gestione account » Quote 825

5.3.4.4 Minger



Disponibile in Account » Impostazioni account, Minger è un protocollo di verifica degli indirizzi e-mail creato da MDaemon Technologies. Ispirato in origine dal protocollo Finger, lo scopo principale di Minger è fornire un semplice ed efficiente meccanismo di interrogazione del server in uso per verificare la validità di un indirizzo e-mail. Minger utilizza il protocollo UDP anziché TCP per motivi di efficienza e, se lo si desidera, richiede l'autenticazione, sebbene supporti anche query anonime. La finestra di dialogo Minger consente di attivare o disattivare il server Minger di MDaemon, di indicare la porta utilizzata (la porta predefinità è 4069) e di scegliere se richiedere l'autenticazione tramite un segreto condiviso oppure se consentire le query anonime.

In MDaemon è disponibile un client Minger, integrato nel sistema Gateway di dominio. Per ulteriori informazioni, vedere Verifica 264. È possibile configurare l'uso di Minger per ogni dominio per il quale MDaemon agisce da server gateway o server di backup. Se si abilita Minger, MDaemon si connette al server remoto per verificare se i destinatari dei messaggi in entrata relativi a tale dominio siano validi. In tal modo, non è più necessario attenersi all'assunto che tutti i destinatari rappresentino indirizzi validi.

Per visualizzare l'ultima specifica relativa al protocollo Minger, visitare il sito:

http://tools.ietf.org/html/draft-hathcock-minger-06

Server Minger

Abilita il server Minger
Fare clic su questa casella di controllo per abilitare il server Minger di MDaemon.

Porta UDP utilizzata per connessioni Minger
Consente di specificare la porta monitorata dal server Minger per le connessioni. L'authority IANA (Internet Assigned Numbers Authority) ha riservato la porta TCP e UDP 4069 ai client e ai server Minger. Non è consigliabile modificare la porta utilizzata, perché è riservata esclusivamente a Minger.

Le ricerche Minger richiedono un segreto condiviso
Se si desidera richiedere l'autenticazione mediante un segreto condiviso, scegliere questa opzione e inserire una stringa di testo lunga almeno almeno 16 caratteri. Se si utilizza questa opzione, il server Minger respinge automaticamente le ricerche prive di autenticazione.

Il server Minger consente ricerche anonime
Selezionare questa opzione se si desidera che il server Minger consenta le ricerche anonime. In questo caso, al client che esegue la connessione non viene richiesto di eseguire l'autenticazione prima della ricerca. Il funzionamento di questa opzione è simile a quanto può essere realizzato utilizzando il comando `SMTP VRFY`, ossia la richiamata o l'inoltro di chiamata SMTP, ma è molto più efficiente e non provoca i problemi relativi a questi metodi, ossia la chiusura di numerose sessioni SMTP su TCP, l'affollamento dei file registro SMTP con le informazioni relative alle sessioni perse e così via.

Minger considera gli alias esterni come indirizzi e-mail attivi
Se si abilita questa casella, Minger considera gli alias esterni, ossia quelli che puntano a indirizzi esterni, come indirizzi attivi noti. Questa è la modalità operativa applicata anche alle interrogazioni eseguite da SecurityGateway in MDaemon, indipendentemente dall'impostazione di questa opzione.

Memorizza risultati ricerca Minger
Per impostazione predefinita, MDaemon memorizza nella cache i risultati della ricerca Minger. Se non si desidera che li memorizzi nella cache, disabilitare questa opzione.

5.4 Importazione degli account

5.4.1 Importazione degli account da un file di testo

Per accedere a questa funzione di generazione degli account, scegliere `Account » Importazione... » Importa account da file di testo delimitato da virgole...` . La stessa funzione può essere attivata facendo clic sul pulsante *Importa* di Account Manager. Si tratta di un metodo semplice per importare e generare automaticamente gli account di posta. MDaemon legge il file di testo e genera i nuovi account utilizzando solo i nomi e i cognomi degli utenti. Se si impostano con attenzione le stringhe di modello per l'account corrette (vedere Valori predefiniti nuovo account 807), è possibile generare

account univoci utilizzando solo i nomi e i cognomi degli utenti. Inoltre, se si desidera ignorare i valori predefiniti del nuovo account, è possibile includere numerose altre opzioni relative a impostazioni specifiche per l'utente. Tutti i campi devono essere separati da virgole.

Ogni riga del file di testo separato da virgole deve contenere una sola voce. La prima riga del file deve essere un'intestazione che fornisce i nomi e la sequenza dei campi delle righe successive. Di seguito è riportato un esempio di file corretto:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"maurizio", "Maurizio Argento", "C:\Mail\Maurizio\", Y
"michele", "Michele Masone", "C:\Mail\Michele\", N
```

I nomi dei campi dell'intestazione vengono esaminati da MDaemon per determinare la sequenza dei dati e possono pertanto comparire in qualunque ordine. Ogni nome di campo deve essere racchiuso tra virgolette.

Tutti i valori di tipo stringa devono essere racchiusi tra virgolette e un valore di tipo "booleano" (true o false viene considerato `FALSE` a meno che il primo carattere sia: `y`, `Y`, `1`, `t` o `T`.

Per ogni nome completo vengono accettati il nome, il secondo nome e il cognome. Tuttavia, questi non possono essere separati da virgole.

Una volta eseguito il processo di importazione, MDaemon crea il file `TXIMPORT.LOG` che contiene i risultati dell'importazione, incluso un elenco degli account importati e non importati. In genere, non è possibile eseguire un'importazione perché vengono rilevati conflitti con la casella postale, il nome o le informazioni di directory di un account esistente, con l'alias esistente di un account oppure con il nome di una lista di distribuzione.

Per ulteriori informazioni sulle corrispondenze tra campi, consultare la descrizione di `MD_ImportUserInfo()` e di `MD_ExportAllUsers()` nel file `MD-API.HTML`, situato nella cartella `\API\`.

Per impostare la corrispondenza con i campi degli account di MDaemon, utilizzare nell'intestazione i valori seguenti:

Nome campo	Tipo
MailBox	stringa
Domain	string
FullName	string
MailDir	string

Password	string
AutoDecode	booleano
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	intero
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	stringa

Per ulteriori informazioni, vedere

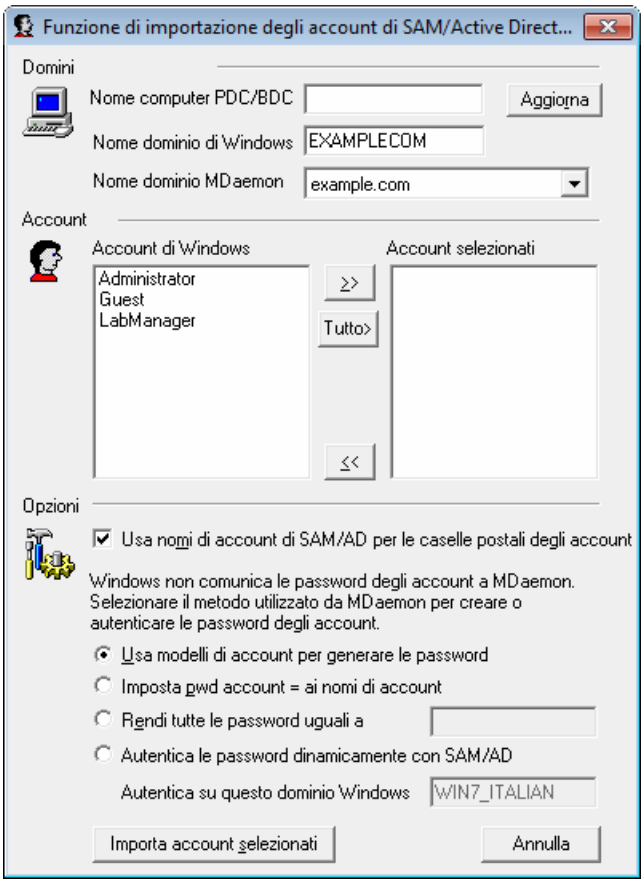
Integrazione con gli account Windows 882

5.4.2 Integrazione con gli account Windows

MDaemon supporta l'integrazione con gli account Windows. Tale supporto consiste in un modulo di importazione da SAM/Active Directory, al quale è possibile accedere dal menu Account di MDaemon (Account » Importazione... » Importa account da SAM/Active directory...). Inoltre, nel codice di gestione degli utenti di MDaemon è stato incorporato il supporto per l'autenticazione di Active Directory (AD) degli utenti. È possibile specificare un dominio Windows nel campo della password di un account in modo che MDaemon autentichi dinamicamente e in tempo reale tale account mediante il sistema di protezione del dominio Windows specificato. Se è in uso uno schema di questo tipo, la modifica della password dell'account nella Gestione utenti di Windows aggiorna automaticamente MDaemon. Di conseguenza, gli utenti devono ricordare solo un set di credenziali di autenticazione. Ciò consente inoltre di semplificare la configurazione delle nuove installazioni.

Il contesto di protezione dell'account che esegue MDaemon deve includere il privilegio **SE_TCB_NAME** (ossia Agisci come parte del sistema operativo). Se è un servizio in esecuzione nell'account *Local System*, il processo dispone di questo privilegio per impostazione predefinita. In caso contrario, è necessario impostare nella gestione utenti di Windows tale privilegio per l'account in cui MDaemon è in esecuzione.

Funzione di importazione degli account di SAM/Active Directory



Domini

Nome computer PDC/BDC

In questo campo è possibile specificare il nome del sistema da cui MDaemon legge le informazioni sul database degli account Windows. Specificando \\<DEFAULT>, MDaemon leggerà i dati dal sistema locale.

Aggiorna

Fare clic su questo pulsante per aggiornare l'elenco degli account Windows.

Nome dominio di Windows

Digitare il nome dominio Windows da cui si desidera importare gli account.

Nome dominio MDaemon

Selezionare dalla casella di riepilogo a discesa il dominio MDaemon in cui importare gli account.

Account

Account di Windows

In questa finestra viene fornito un elenco di tutti i nomi di account raccolti dal database degli account Windows.

Account
In questa finestra vengono riportati tutti i nomi degli account selezionati per l'importazione.

>>
Fare clic su questo pulsante per spostare i nomi account evidenziati dalla finestra "Account di Windows" alla finestra "Account selezionati".

<<
Fare clic su questo pulsante per rimuovere le voci evidenziate dalla finestra "Account selezionati".

Opzioni

Usa nomi di account di SAM/AD per le caselle postali degli account
Selezionare questa casella di controllo per utilizzare il nome dell'account Windows di ciascun utente come valore della relativa casella postale. In questo modo, non è necessario configurare apposite macro per il modello dei nuovi account 812.

Usa modelli di account per generare le password
Se si seleziona questa opzione, MDaemon genererà le password per gli account importati utilizzando le impostazioni del modello di account. Al riguardo, vedere Valori predefiniti account 812.

Imposta pwd account = ai nomi di account
Se si seleziona questa casella di controllo, MDaemon utilizzerà il nome dell'account come password per l'account.

Rendi tutte le password uguali a
Questa opzione consente di specificare un valore di password statico che verrà utilizzato da tutti gli account importati.

Autentica le password dinamicamente con SAM/AD
Questa opzione consente l'autenticazione AD degli account importati. Anziché specificare una password, MDaemon autenticherà in tempo reale i valori USER e PASS forniti dal client di posta mediante il database di NT.

Autentica su questo dominio Windows
Immettere il nome dominio di Windows utilizzato da MDaemon durante l'autenticazione dinamica delle connessioni. **Questo non è il nome computer del controller del dominio, ma il nome effettivo del dominio Windows.**

Quando gli account vengono configurati per l'autenticazione AD, il nome del dominio Windows (preceduto da due caratteri di barra rovesciata) viene utilizzato nel campo `PASSWORD` dell'account e viene memorizzato in formato non crittografato nel file `USERLIST.DAT`. Ad esempio, se un account è configurato per per l'autenticazione AD su un dominio Windows denominato `ALTN`, il campo relativo alla password dell'account

contiene il valore \\ALTN. I due caratteri di barra rovesciata che precedono il nome del dominio indicano a MDaemon che il campo relativo alla password contiene effettivamente il nome di un dominio Windows. MDaemon deve quindi tentare di utilizzare il database degli account del dominio per l'autenticazione dei valori USER e PASS forniti dal client di posta. Per questo motivo, è necessario non inserire password precedute da due barre rovesciate a meno che l'account non sia stato configurato per l'autenticazione AD nel modo appena descritto. In altri termini, le password normali non possono iniziare con due barre rovesciate. Di regola, si presuppone che questo tipo di password rappresenti un nome di un dominio Windows e non una password.

È possibile inserire una combinazione di due caratteri di barra rovesciata e del nome dominio Windows in un campo relativo alla password dell'account nella schermata Dettagli account 729 di Account Editor. Per configurare gli account per l'autenticazione AD non è indispensabile utilizzare la funzione di importazione.

Vedere:

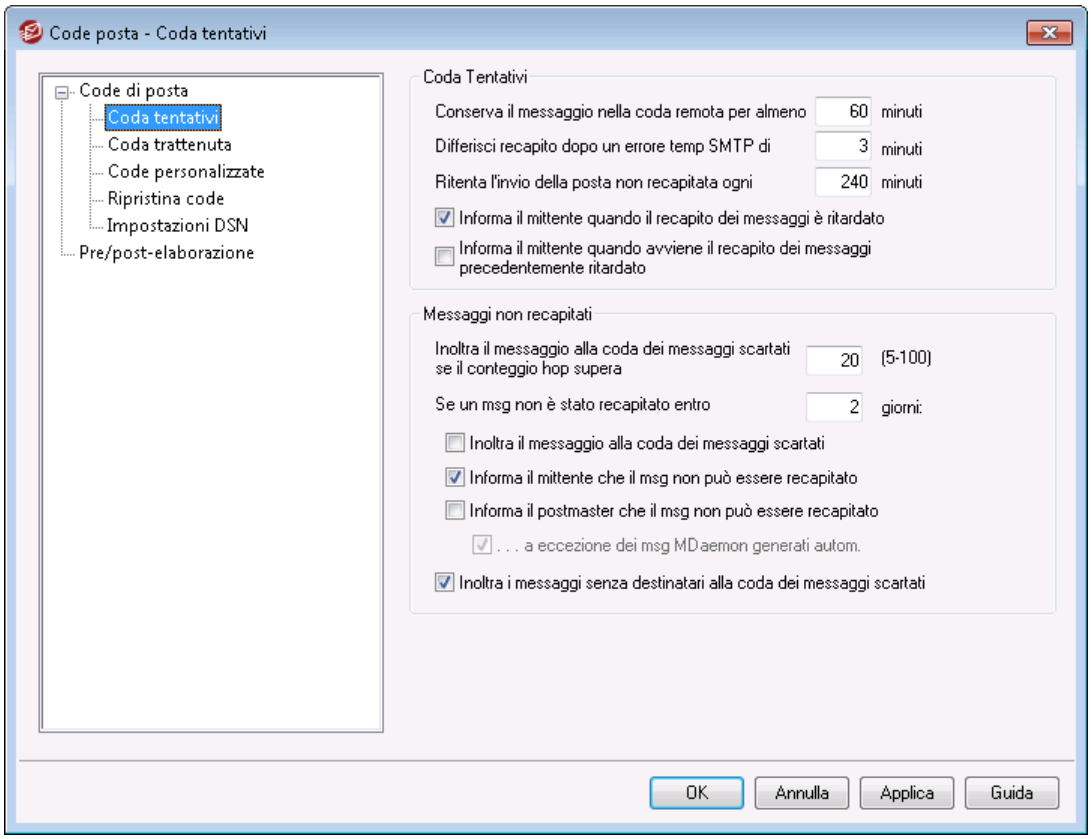
Importazione degli account da un file di testo 879
Account Editor » Account 729

Sezione

6 Menu Code posta

6.1 Code posta

6.1.1 Coda tentativi



La finestra di dialogo Coda tentativi, situata in Code posta » Code posta, consente di indicare a MDaemon come gestire i messaggi che non può consegnare a causa di errori reversibili, ad esempio quando il server ricevente è temporaneamente non disponibile.

Coda tentativi

Conserva il msg nella coda remota per almeno XX minuti
In questo campo si specifica quanto tempo un messaggio deve rimanere nella coda remota prima di essere rimosso e collocato nella coda tentativi. In genere, la coda remota è impostata per tentare di inviare i messaggi più frequentemente rispetto alla coda tentativi.

Differisci recapito dopo un errore temp SMTP di xx minuti
Quando in MDaemon si verifica un errore SMTP temporaneo (4xx) durante il tentativo di recapito di un messaggio, il successivo tentativo di recapito del messaggio sarà ritardato del numero di minuti specificato. Questo consente di evitare che MDaemon tenti di recapitare ripetutamente lo stesso messaggio troppo rapidamente. Per

impostazione predefinita, il ritardo è impostato su 3 minuti. Se si desidera disattivare il ritardo, impostare il valore su "0".

Ritenta l'invio della posta non recapitata ogni XX minuti
Questa impostazione definisce la frequenza con cui vengono elaborati i messaggi presenti nella coda tentativi.

Informa il mittente del ritardo nel recapito del messaggio
Per impostazione predefinita MDaemon informa il mittente quando un messaggio non viene recapitato a causa di un errore temporaneo, che ne causa l'inserimento nella coda tentativi. Deselezionare questa casella di controllo se non si desidera informare il mittente del ritardo.

Informa il mittente quando i messaggi vengono consegnati dopo un ritardo
Selezionare questa casella di controllo se si desidera che il mittente venga informato quando un messaggio viene consegnato dopo un ritardo iniziale. È disabilitata per impostazione predefinita.

Posta non recapitata

Instradare alla coda dei messaggi scartati i messaggi con più del seguente numero di hop (5-100)
In base agli standard RFC, un server di posta è tenuto a contrassegnare ciascun messaggio ogni volta che questo viene elaborato. Questi contrassegni possono essere contati e utilizzati come misura provvisoria per evitare i loop di posta, che in alcuni casi sono causati da configurazioni errate. Se non vengono rilevati, questi loop di consegna dei messaggi esauriranno le risorse del sistema. Calcolando il numero di volte per cui un messaggio viene elaborato, è possibile rilevare tali messaggi e collocarli nella directory dei messaggi scartati. Si presuppone che sia in corso un loop di posta se un messaggio non ha raggiunto il destinatario dopo un certo numero di elaborazioni da parte dei server. L'impostazione predefinita di questo comando dovrebbe essere sufficiente a impedire il verificarsi di loop di posta.

Se un msg non è stato recapitato entro XX giorni
Questa impostazione determina per quanti giorni un messaggio può rimanere nella coda tentativi prima di essere rimosso. Se si inserisce "0", il messaggio verrà rispedito al mittente dopo il primo tentativo di reinvio. Il valore predefinito è 2 giorni.

Sposta in coda messaggi scartati
Quando si abilita questa opzione, il messaggio viene spostato nella coda dei messaggi scartati ogni volta che si raggiunge il limite impostato nell'opzione "*Se un messaggio non è stato recapitato entro XX giorni*".

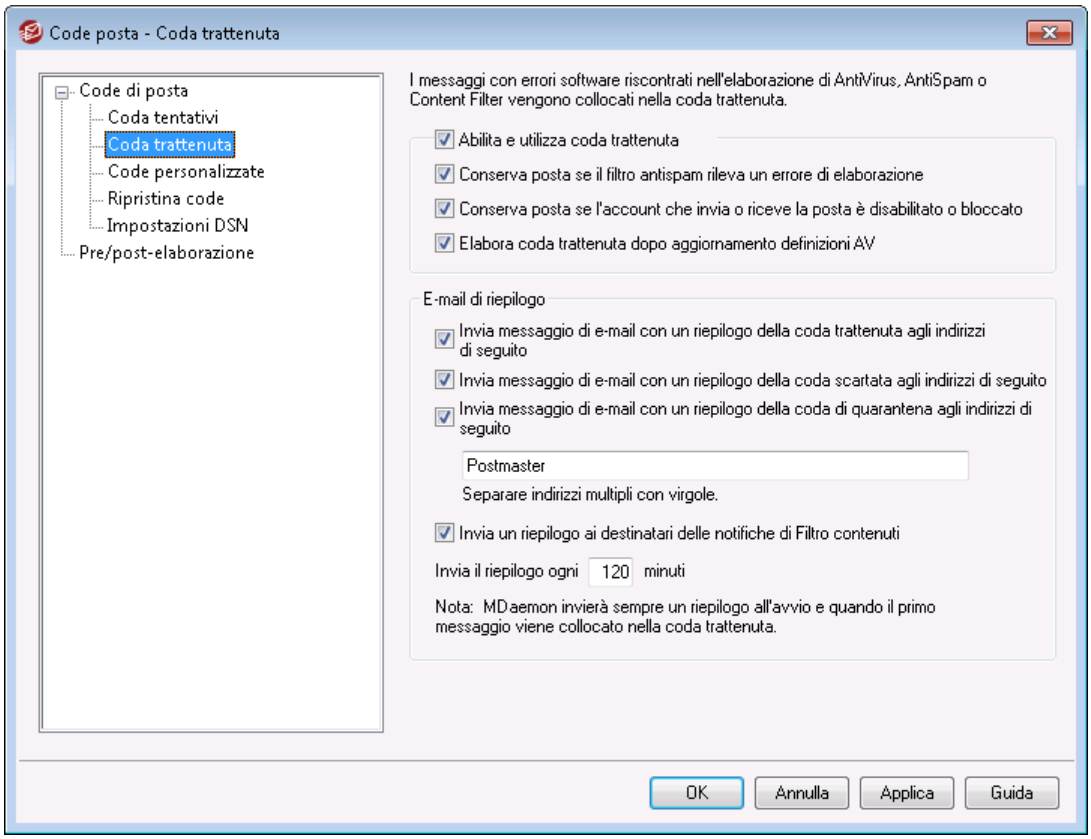
Informa il mittente che il msg non può essere recapitato
Se questa casella è selezionata, una volta scaduto il tempo specificato nel campo "*Se un messaggio non è stato recapitato entro XX giorni:*", MDaemon invierà un messaggio di notifica dello stato di recapito 896 al mittente per informare della rimozione permanente del messaggio dal server.

Informa il postmaster che il msg non può essere recapitato
Se questa casella è selezionata, viene inviato al postmaster un avviso in cui si indica che un messaggio è stato eliminato in maniera definitiva dal sistema tentativi.

. . . a eccezione dei msg MDaemon generati automaticamente
Per impostazione predefinita, il sistema tentativi non informa il postmaster dell'impossibilità di consegnare un messaggio generato automaticamente da MDaemon. Per informare il postmaster anche del mancato recapito di questi messaggi, abilitare questa casella di controllo. Le notifiche di ricevuta di ritorno, i messaggi creati come risposte automatiche e i risultati di gestione di un account sono esempi di messaggi generati automaticamente.

Instradare i messaggi senza destinatari alla coda dei messaggi scartati
Se questa opzione è abilitata, i messaggi senza l'indicazione del destinatario vengono collocati nella coda dei messaggi scartati. Se questa opzione è disabilitata, vengono eliminati. L'opzione è abilitata per impostazione predefinita.

6.1.2 Coda trattenuta



La coda trattenuta, disponibile in Code posta » Code posta, può essere utilizzata per ricevere i messaggi che hanno determinato eccezioni software durante l'elaborazione di AntiVirus, AntiSpam o Filtro contenuti. Qualora si verifichi un errore software durante

l'elaborazione di un messaggio, questo viene spostato nella coda trattenuta senza essere consegnato.

I messaggi collocati nella coda trattenuta vi rimangono finché l'amministratore non li rimuove. L'opzione *Elabora coda trattenuta* è presente sia nella barra degli strumenti di MDaemon sia nella barra di menu Code posta. È possibile elaborare i messaggi anche facendo clic con il pulsante destro del mouse sulla coda trattenuta nell'interfaccia principale e scegliendo la voce "Riaccoda" dal menu di scelta rapida. L'elaborazione della coda trattenuta sposta tutti i messaggi nella coda remota o locale per la normale elaborazione della posta. Se l'errore che ha determinato l'inserimento del messaggio nella coda trattenuta si verifica ancora, il messaggio viene reinserito nuovamente nella coda trattenuta. Se si desidera tentare di consegnare i messaggi della coda trattenuta ignorando eventuali errori, fare clic con il pulsante destro del mouse sulla coda trattenuta dell'interfaccia principale e selezionare dal menu la voce "Rilascia". Quando vengono rilasciati messaggi dalla coda trattenuta, appare un avviso sulla possibilità che alcuni messaggi contengano virus o non siano gestiti dai moduli di Filtro contenuti, AntiSpam e/o AntiVirus.

Coda trattenuta

Abilita e utilizza coda trattenuta
Per attivare la coda trattenuta, selezionare questa casella di controllo. I messaggi che hanno determinato eccezioni software durante l'elaborazione di AntiVirus e Filtro contenuti verranno spostati in questa coda qualora si verifichi un errore.

Conserva posta se il filtro antispam rileva un errore di elaborazione
Fare clic su questa opzione se si desidera spostare nella coda trattenuta i messaggi che determinano errori durante l'elaborazione di Spam Filter.

Conserva posta se l'account che invia o riceve la posta è disabilitato o bloccato
Quando questa opzione è abilitata, MDaemon tratterrà automaticamente i messaggi quando l'account che invia o riceve la posta è disabilitato o bloccato.

Elabora coda trattenuta dopo aggiornamento definizioni AV
Se si attiva l'opzione, la coda in sospeso verrà elaborata automaticamente ogni volta dopo l'aggiornamento delle firme dei virus di AntiVirus 658.

E-mail di riepilogo

Invia messaggio di e-mail con un riepilogo della coda trattenuta agli indirizzi di seguito
Se si desidera inviare un riepilogo dei messaggi contenuti nella coda trattenuta a uno o più indirizzi e-mail a intervalli regolari, fare clic su questa opzione ed elencare gli indirizzi nell'apposito campo.

Invia messaggio di e-mail con un riepilogo della coda scartata agli indirizzi di seguito
Se si desidera inviare un riepilogo dei messaggi contenuti nella coda messaggi scartati a uno o più indirizzi e-mail a intervalli regolari, fare clic su questa opzione ed elencare gli indirizzi nell'apposito campo.

Invia messaggio di e-mail con un riepilogo della coda di quarantena agli indirizzi di seguito
Attivare questa opzione per inviare un riepilogo della coda di quarantena all'intervallo specificato di seguito.

Destinatari messaggio di riepilogo
Utilizzare la casella di testo per specificare gli indirizzi di posta elettronica a cui si desidera inviare i messaggi di riepilogo sul contenuto delle code specificato nelle due opzioni precedenti. Nel caso in cui si elencano più indirizzi, separarli con una virgola.

I messaggi di notifica vengono inviati all'avvio di MDaemon, al primo inserimento di un messaggio nella coda trattenuta e, successivamente, a intervalli regolari (specificati nell'opzione *Invia il riepilogo ogni XX minuti*).

Se il messaggio di notifica genera errori software, non viene consegnato ai destinatari remoti, ma solo ai destinatari locali.

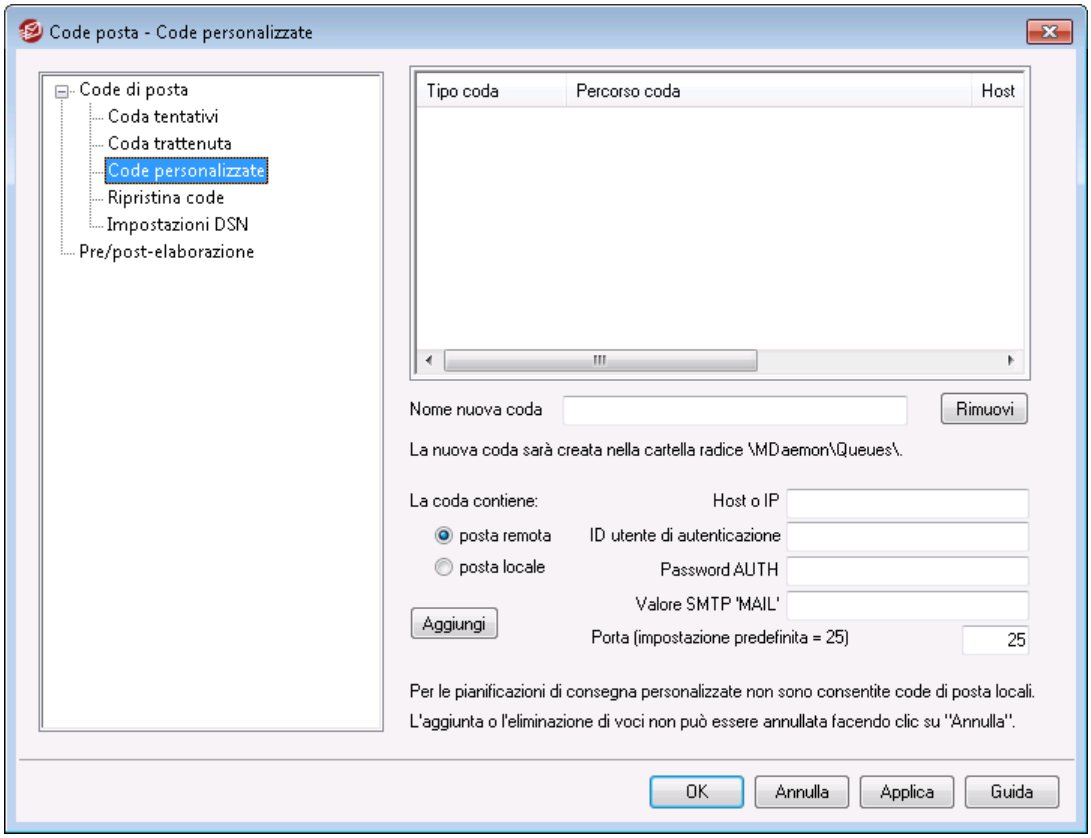
Invia un riepilogo ai destinatari delle notifiche di Filtro contenuti
Fare clic su questa opzione se si desidera che una copia aggiuntiva di ciascun messaggio di notifica venga inviata ai destinatari 680 specificati per le notifiche di Filtro contenuti.

Includere il collegamento dell'azione (rilascio, riaccodamento, eliminazione) nell'e-mail di riepilogo.
Per impostazione predefinita, le e-mail di riepilogo per coda in sospeso, di quarantena e scartati contengono i link per rilasciare, riaccodare o eliminare ciascun messaggio. Disattivare questa opzione se non si desidera includere i collegamenti nelle e-mail di riepilogo.

Per generare i collegamenti, è necessario impostare l'URL di Remote Administration 361.

Invia il riepilogo ogni XX minuti
Scegliere questa opzione per specificare il numero di minuti che devono passare prima che MDaemon invii un messaggio di notifica della coda trattenuta agli indirizzi specificati o ai destinatari delle notifiche di Filtro contenuti.

6.1.3 Code personalizzate



Utilizzare la finestra di dialogo Code personalizzate in Code » Code posta per creare code di posta locali e remote personalizzate. Il supporto per le code personalizzate consente di monitorare diverse posizioni da cui inviare la posta. È possibile creare nuove code sia locali sia remote e utilizzare le funzioni di Filtro contenuti per collocare automaticamente i messaggi nelle code di posta personalizzate. Nel caso di code di posta remote, è possibile utilizzare Pianificazione eventi 388 per creare pianificazioni personalizzate al fine di controllare la frequenza di elaborazione di tali code.

Code personalizzate

Questa area include una voce per ciascuna coda personalizzata che consente di visualizzare il percorso del file associato alla coda e la tipologia di coda (locale o remota).

Rimuovi
Per rimuovere una coda dall'elenco, selezionarla e fare clic sul pulsante *Rimuovi*.

Se si elimina una coda personalizzata, verranno eliminate anche le pianificazioni personalizzate o le regole di Filtro contenuti associate alla coda.

Nome nuova coda
Immettere un nome per la nuova coda di posta. La coda sarà creata nella cartella MDaemon's `\MDaemon\Queues\`.

La coda contiene

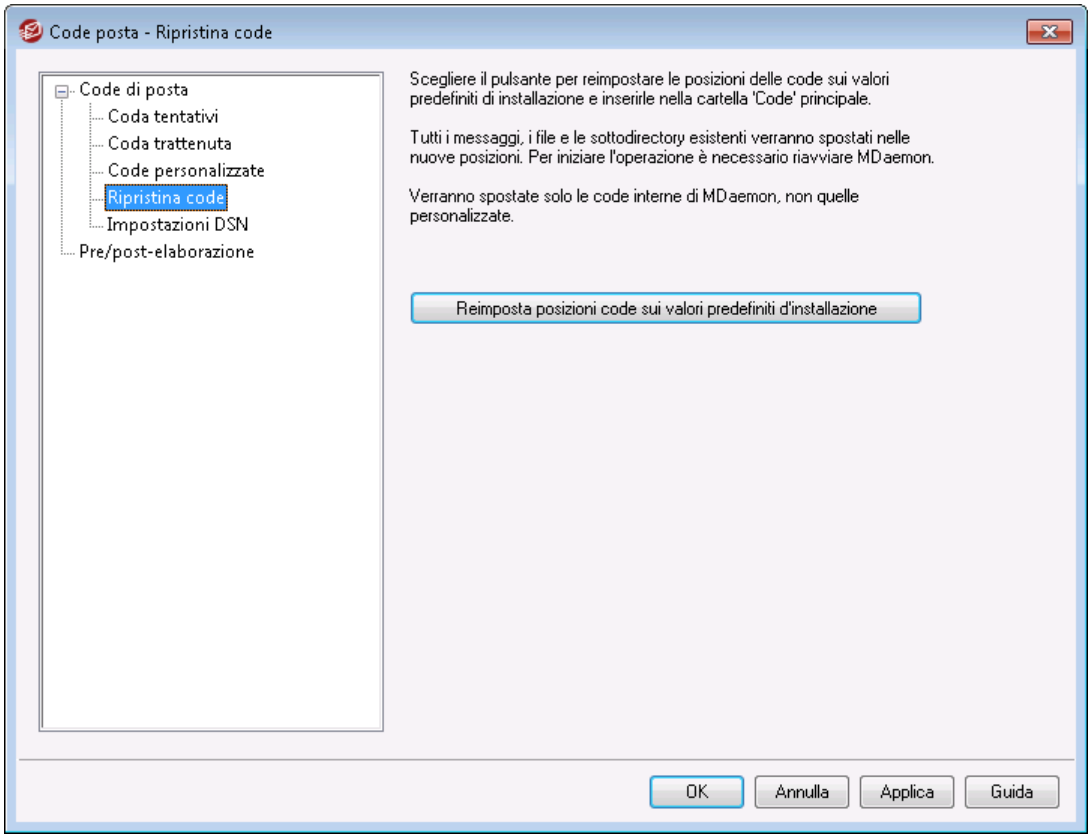
posta remota
Selezionare questa opzione per utilizzare la coda personalizzata per la posta remota.

Credenziali coda
È possibile specificare *Host o IP*, *Accesso/Password AUTH*, *valore 'MAIL' SMTP* e *Porta* per qualsiasi coda remota. Se specificati, tutti i messaggi nella coda sono recapitati usando queste impostazioni. Tuttavia resta ancora possibile in alcune circostanze per i singoli messaggi nella coda avere i propri dati di recapito unici, che avranno priorità su queste nuove impostazioni.

posta locale
Selezionare questa opzione per utilizzare la coda personalizzata per la posta locale.
Nota: Per le pianificazioni di consegna personalizzate non sono consentite code di posta locali.

Aggiungi
Dopo aver scelto il nome e il tipo della coda, fare clic sul pulsante *Aggiungi* per aggiungerla all'elenco di code personalizzate.

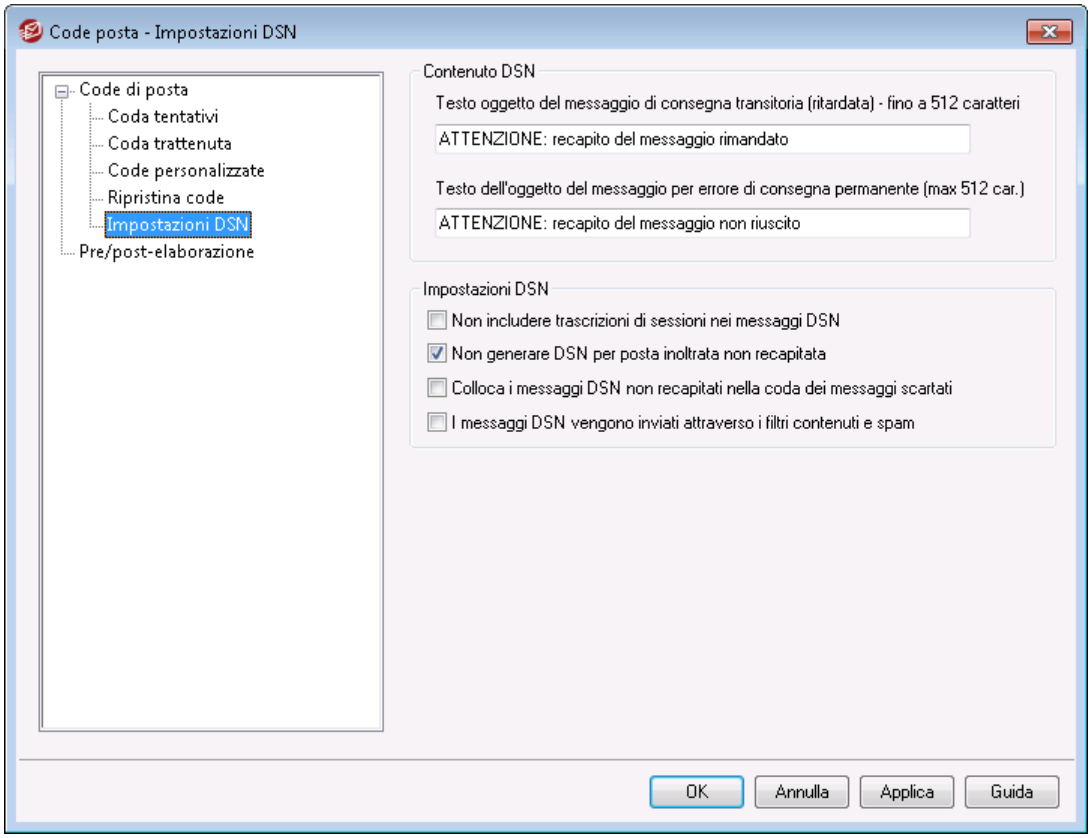
6.1.4 Ripristina code



Reimposta posizioni code su valori predefiniti d'installazione
Per impostazione predefinita, la nuova installazione di MDaemon archivia le code dei messaggi, ad esempio le code remote, locali o RAW, nella sottocartella `\MDaemon\Queues\`. Le precedenti versioni di MDaemon archiviano le code in cartelle differenti. Se l'installazione di MDaemon usa la precedente posizione delle cartelle ma si desidera spostare le code in questa nuova struttura meglio organizzata, fare clic su questo pulsante per spostare tutte le code, i file e i messaggi contenuti. Dopo aver fatto clic su questo pulsante, riavviare MDaemon per implementare le modifiche apportate.

Le code personalizzate 893 non vengono spostate con questa funzionalità.

6.1.5 Impostazioni DSN



Se in MDaemon si verifica un problema durante la consegna di un messaggio, sia esso un errore temporaneo o permanente, viene inviato un messaggio DSN (Delivery Status Notification) al mittente del messaggio. Questa schermata contiene varie opzioni relative ai messaggi DSN. Seguire il percorso: `Code » Code posta/DSN... » Impostazioni DSN`.

Contenuto DSN

Testo oggetto messaggio di consegna transitoria (ritardata) - fino a 512 caratteri
Questa è l'intestazione dell'oggetto del messaggio DSN che viene inviato in caso di un problema transitorio, che provoca un ritardo di consegna del messaggio. Ad esempio, se il server di posta del destinatario non è disponibile nel momento in cui MDaemon tenta di consegnare un messaggio, MDaemon continua a tentare l'invio a intervalli prestabiliti e invia questo messaggio DSN in cui informa il mittente sul problema. Vedere: Personalizzazione messaggi DSN 897.

Testo dell'oggetto messaggio di consegna permanente (non riuscita) - fino a 512 caratteri
Questa è l'intestazione dell'oggetto del messaggio DSN che viene inviato in caso di un problema che rende impossibile la consegna del messaggio. Ad esempio, se il server di posta in entrata respinge il messaggio, dichiarando che l'indirizzo e-mail del destinatario non esiste, MDaemon interrompe l'invio del messaggio e invia un messaggio DSN per informare il mittente che il messaggio non può essere consegnato. Vedere: Personalizzazione messaggi DSN 897.

Impostazioni DSN

Non includere trascrizioni sessioni nei messaggi DSN
Selezionare questa opzione per escludere le trascrizioni delle sessioni SMTP dai messaggi di avviso e di segnalazione di errore nel recapito. L'opzione è disabilitata per impostazione predefinita.

Non generare DSN per posta non consegnabile
Quando si abilita questa opzione, i messaggi inoltrati con i quali si siano verificati errori di consegna permanenti e irreversibili o i messaggi scaduti della Coda tentativi vengono spostati nella coda messaggi scartati, senza che il mittente originale riceva un messaggio DSN. L'opzione è abilitata per impostazione predefinita.

Colloca i messaggi DSN non recapitati nella coda dei messaggi scartati
Selezionare questa casella di controllo se si desidera collocare i messaggi Delivery Status Notification nella coda messaggi scartati anziché tentarne il reinvio.

Questa impostazione viene applicata solo ai messaggi DSN generati da MDaemon.

I messaggi DSN vengono inviati attraverso i filtri di contenuto e anti-spam
Attivare questa opzione per inviare messaggi DSN attraverso i filtri di contenuto e anti-spam. L'opzione è disabilitata per impostazione predefinita.

Personalizzazione messaggi DSN

La parte "leggibile" dei messaggi DSN transitori (ritardati) e permanenti (errore) può essere personalizzata creando un file denominato rispettivamente `DSNDelay.dat` o `DSNFail.dat` nella cartella `\MDaemon\App\`. Modificare il file con un editor di testo come Notepad e immettere il testo che si desidera utilizzare. Nel testo personalizzato è possibile utilizzare le seguenti macro:

$SESSIONID$ - restituisce la stringa di ID della sessione di consegna

$QUEUEID$ - restituisce la stringa di ID della coda di posta del messaggio

$MESSAGEID$ - restituisce il valore dell'intestazione ID del messaggio

$RETRYDAYS$ - tempo di permanenza consentita nella coda (in giorni)

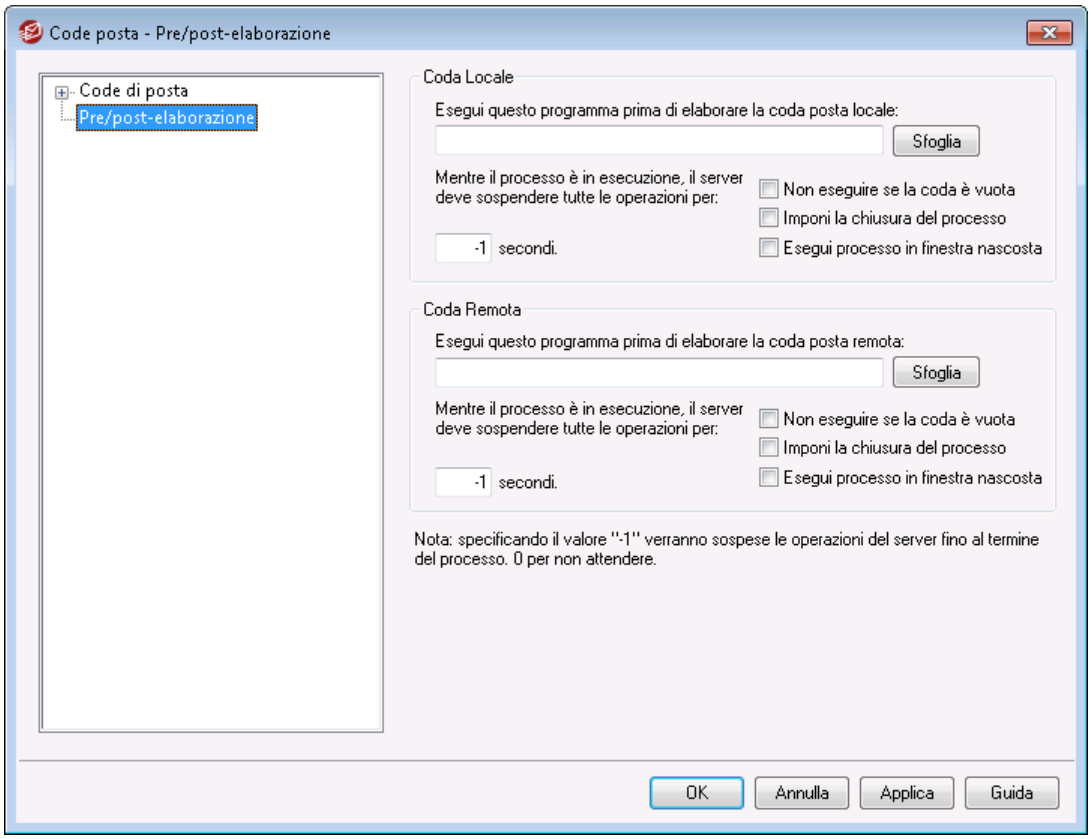
$RETRYHOURS$ - tempo di permanenza consentita nella coda (in ore)

MDaemon deve essere riavviato prima che le modifiche a questi file vengano caricate.

Vedere:

Coda tentativi

6.2 Pre/post-elaborazione



Pre/post elaborazione delle code locali e remote

Esegui questo programma prima di elaborare la coda posta locale
In questo campo vengono specificati il percorso e il nome del programma che verrà eseguito subito prima di elaborare e consegnare qualsiasi messaggio in formato RFC-2822 presente nelle code dei messaggi locali o remote. Se non vengono inserite informazioni di percorso complete, MDaemon cerca l'eseguibile dapprima nella propria directory, quindi nella directory System di Windows, successivamente nella directory Windows e infine nelle directory elencate nella variabile ambientale PATH.

Mentre il processo è in esecuzione, il server deve sospendere tutte le operazioni per XX secondi
Il valore inserito in questo campo determina il comportamento di MDaemon durante l'esecuzione del programma specificato. MDaemon può essere configurato per interrompere momentaneamente il thread di esecuzione per l'intervallo di tempo (in secondi) specificato, in attesa del risultato dell'elaborazione. Se l'elaborazione si riattiva prima che sia trascorso l'intervallo di tempo specificato, MDaemon riprende immediatamente il thread di esecuzione. Specificando il valore "0", MDaemon non effettua alcuna pausa, mentre immettendo "-1" MDaemon attende la ripresa dell'elaborazione, indipendentemente dalla durata dell'attesa.

Non eseguire se la coda è vuota
Selezionare questa casella di controllo se non si desidera che il programma specificato venga eseguito quando la coda è vuota.

Imponi la chiusura del processo
In alcuni casi, il processo da eseguire potrebbe non chiudersi autonomamente. Se questa casella è selezionata, MDaemon impone la chiusura della sessione allo scadere del tempo specificato in *...sospendere tutte le operazioni per xx secondi*. Questo comando non ha alcun effetto se l'intervallo di tempo trascorso è impostato su "-1".

Esegui processo in finestra nascosta
Selezionare questa casella di controllo se si desidera che il processo venga eseguito in una finestra nascosta.

6.3 Gestione delle code e delle statistiche

Il modulo di gestione delle code e delle statistiche di MDaemon è disponibile nel menu Code posta » Gestione code e statistiche. Gestione code e statistiche è una finestra di dialogo composta da quattro schede, ognuna progettata per uno scopo preciso, con un formato intuitivo e di facile utilizzo.

Pagina code 900

La scheda predefinita è *Pagina code*, da cui è possibile accedere con facilità a tutte le code di posta standard di MDaemon, nonché alle cartelle delle caselle postali dell'account utente. Con un semplice clic sulla coda o sull'utente desiderato, è possibile visualizzare un elenco di tutti i file di messaggio contenuti nella coda specificata e alcune informazioni rilevanti su ogni messaggio, ad esempio il mittente, il destinatario, il contenuto dell'intestazione "Deliver-To", l'oggetto, le dimensioni e l'intervallo di tempo per cui il messaggio è rimasto nella posizione corrente. In questa pagina sono inoltre presenti i comandi che consentono di copiare o di spostare i messaggi in cartelle diverse, nonché di eliminarli in modo irreversibile.

Pagina utente 903

Nella *Pagina utente* viene visualizzato l'elenco di tutti gli utenti di MDaemon. Per ogni utente vengono riportati il nome completo, il nome della casella postale, il numero di messaggi presenti nella casella postale, la quantità di spazio su disco occupato e la data in cui è stato effettuato l'ultimo controllo della posta. L'elenco può anche essere salvato su disco come file di testo oppure in formato delimitato da virgole per l'utilizzo nei database.

Pagina registrazioni 905

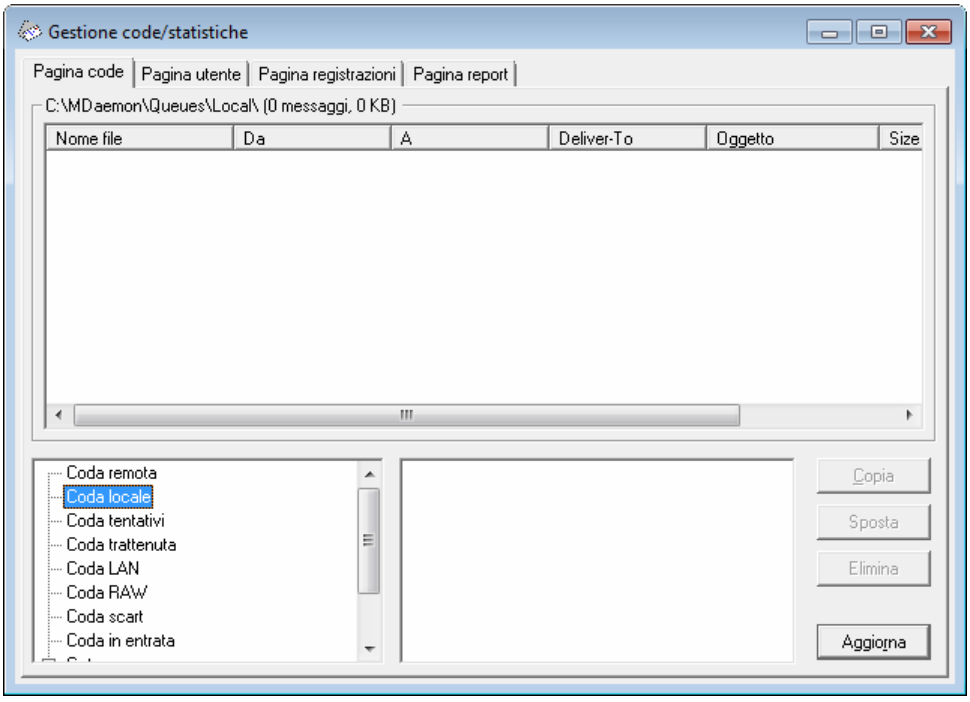
Questa finestra consente di visualizzare i *file registro* di MDaemon in un semplice formato elenco. La funzione risulta utile per esaminare rapidamente la cronologia delle transazioni di posta di MDaemon, perché condensa il *file registro* selezionato in un elenco a colonne che contiene: il tipo di messaggio (POP in entrata, DomainPOP, RFC822 e così via), l'host a cui si è connesso MDaemon durante la transazione, il mittente, il

destinatario, le dimensioni del messaggio, la data di elaborazione di ciascun messaggio e l'esito della transazione. Per esaminare più dettagliatamente le voci del registro, è sufficiente fare doppio clic sulla voce desiderata. Verrà visualizzata la porzione di registro nella quale è stata eseguita la transazione. I registri visualizzati in *Pagina registrazioni* possono essere salvati come file di testo oppure in formato delimitato da virgole per l'utilizzo nei database.

Pagina report 907

L'ultima scheda è *Pagina report*, che consente di creare un report contenente tutte le impostazioni di configurazione di MDaemon in formato leggibile (testo normale). In MDaemon è presente una grande quantità di impostazioni e configurazioni opzionali. Questa funzione consente di accelerare sensibilmente il processo di gestione delle modifiche apportate alla configurazione, nonché di facilitare la diagnosi dei possibili problemi. Inoltre, il report viene visualizzato in un formato di testo modificabile che consente di copiare e incollare le informazioni (mediante il menu di scelta rapida associato al clic con il pulsante destro del mouse) oppure di aggiungere annotazioni e altre specifiche prima di salvare il file.

6.3.1 Pagina code



Casella di riepilogo della pagina code

Quando si sceglie una coda o un utente dall'area *Code* o dalla casella di riepilogo degli utenti, nella casella di riepilogo principale di questa pagina viene visualizzato un elenco di tutti i file di messaggio contenuti nella coda selezionata. Per ogni messaggio, l'elenco contiene il nome del file, il mittente, il destinatario, il contenuto dell'intestazione

"Deliver-To", l'oggetto, la dimensione e l'intervallo di tempo (data e ora) per cui è rimasto nella posizione corrente.

Nell'area soprastante questa casella viene riprodotto il percorso completo della directory correntemente visualizzata, nonché il numero dei messaggi visualizzati e la dimensione della directory stessa.

È possibile copiare, spostare o eliminare uno o più file selezionandoli dall'elenco, quindi facendo clic sul pulsante sottostante appropriato.

Il contenuto dei file può anche essere modificato direttamente dalla casella di riepilogo nella *Pagina code*. Se si fa doppio clic sul file da modificare oppure si sceglie "Modifica" dal menu di scelta rapido associato al clic del pulsante destro del mouse, il file verrà aperto in Blocco note di Windows per consentirne la modifica.

Se si desidera che, per impostazione predefinita, venga aperto un editor diverso da Blocco note, è necessario modificare il file `mdstats.ini` presente nella directory `\MDaemon\app\`. Modificare la chiave "`Editor=`" nella sezione `[QueueOptions]` in `Editor=EditorPersonale.exe`. Se il file `*.exe` non si trova nel percorso corrente, è necessario includere il percorso con il nome file.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. È possibile ordinare le informazioni contenute nella casella di riepilogo *Pagina code* in base a qualunque colonna. Fare clic una volta sulla colonna desiderata per ordinarla in modo ascendente (A-Z, 1-2) oppure doppio clic per ordinarla in modo discendente (Z-A, 2-1). Le colonne possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata.

Selezione dei file

Per selezionare singoli file Fare clic sul file desiderato.

Per selezionare file adiacenti Fare clic sul primo file del gruppo di file adiacenti che si desidera selezionare, quindi, tenendo premuto il tasto MAIUSC, fare clic sull'ultimo file del gruppo.

In alternativa, utilizzare i tasti FRECCIA, HOME, FINE, PAGSU e PAGGIÙ tenendo premuto il tasto MAIUSC.

Per selezionare file non adiacenti Fare clic sui file desiderati nella colonna **Nome file** tenendo premuto il tasto CTRL.

Code dei messaggi
Fare clic su una voce nel riquadro inferiore sinistro per visualizzare nella casella di riepilogo *Pagina code* un elenco di tutti i file contenuti in una determinata coda. Se si fa clic sull'opzione *Cartelle utente*, nella casella di riepilogo degli *utenti* alla destra della sezione relativa alle *code dei messaggi* verrà visualizzato l'elenco di tutti gli utenti di MDaemon.

Casella di riepilogo degli utenti
In questa casella viene visualizzato un elenco di tutti gli utenti MDaemon quando si fa clic sull'opzione *Cartelle utente* all'interno della sezione relativa alle *code dei messaggi* nel riquadro inferiore sinistro. Fare clic sul nome di un utente per visualizzare un elenco di tutti i file messaggio correntemente contenuti nella cartella della casella postale dell'utente.

Aggiorna
Poiché le code di posta vengono modificate dinamicamente mentre MDaemon è attivo grazie al trasferimento costante dei file di messaggio da e per le code, è opportuno fare regolarmente clic su questo pulsante per aggiornare l'elenco di file visualizzato.

È possibile modificare il file `MDstats.ini` in modo che gli elenchi visualizzati vengano aggiornati automaticamente. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e modificare la chiave AutoRefresh in `[QueueOptions]` per farla corrispondere all'intervallo in secondi che deve trascorrere tra un aggiornamento e l'altro. Se si specifica il valore "`0`", l'elenco non verrà aggiornato automaticamente. Esempio: `AutoRefresh=15` (l'elenco viene aggiornato ogni 15 secondi).

Copia
Fare clic su questo pulsante per copiare i file precedentemente selezionati nella cartella della casella postale di un'altra coda o di un altro utente. Una volta fatto clic sul pulsante, viene visualizzata la finestra di dialogo *Copia messaggi*, nella quale è possibile selezionare la posizione in cui si desidera copiare i file selezionati.

Sposta
Fare clic su questo pulsante per spostare i file precedentemente selezionati nella cartella della casella postale di un'altra coda o di un altro utente. Una volta fatto clic sul pulsante, viene visualizzata la finestra di dialogo *Sposta messaggi*, nella quale è possibile selezionare la posizione in cui si desidera spostare i file selezionati.

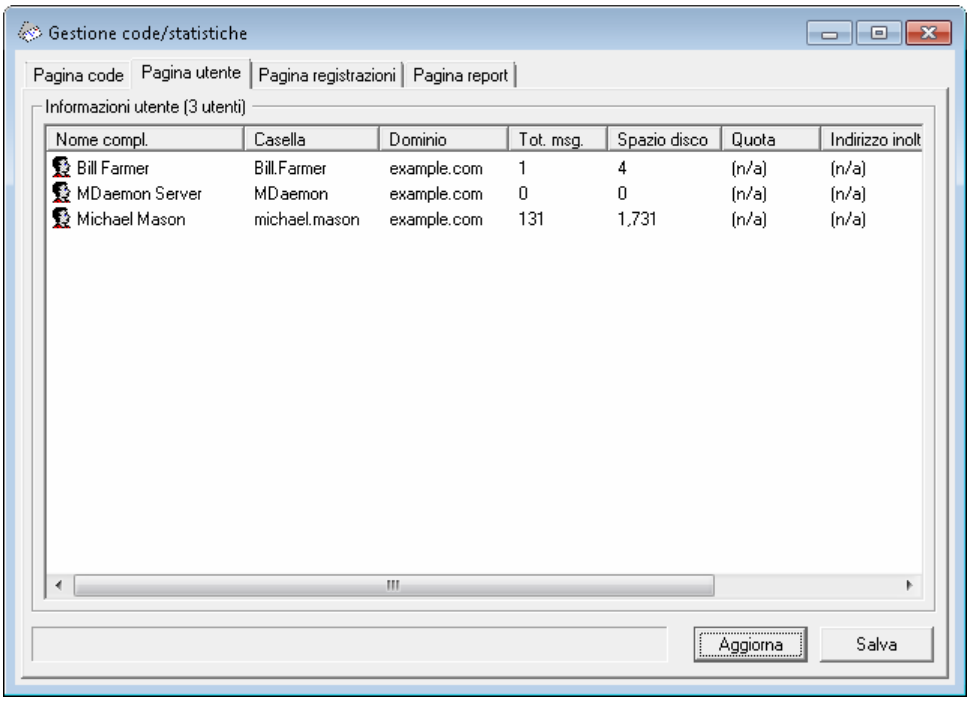
I file copiati o spostati in altre code di solito non conservano il nome originale. Per evitare di sovrascrivere gli eventuali file con lo stesso nome presenti nella coda, MDaemon calcola sempre il nome di file di destinazione in base al file `HIWATER.MRK` contenuto nella cartella di destinazione.

Elimina
Fare clic su questo pulsante per eliminare gli eventuali file selezionati nella casella di riepilogo relativa allo *stato della coda*. Viene visualizzato un messaggio che indica di confermare l'eliminazione dei file selezionati.

Le code di posta vengono modificate dinamicamente mentre MDaemon è attivo grazie al trasferimento costante dei file di messaggio da e per le code. Per tale motivo, è necessario tenere presente che durante la copia, lo spostamento o l'eliminazione dei file può venire visualizzato un messaggio che indica che l'operazione non può essere completata. Questa situazione si verifica quando il file di messaggio su cui si tenta di operare è già stato rimosso da MDaemon. Facendo clic sul pulsante *Aggiorna*, è possibile aggiornare l'elenco corrente dei file visualizzati nella casella di riepilogo.

Per impedire che durante le operazioni di modifica i messaggi vengano spostati all'esterno dalla coda, modificare le impostazioni del file `MDstats.ini`. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e sostituire la chiave `LockOnEdit=No` in `[QueueOptions]` con `LockOnEdit=Yes`. In questo modo, ogni volta che si modifica un messaggio, viene creato un file `LCK` che impedisce che il messaggio soggetto a operazioni venga spostato all'esterno della coda.

6.3.2 Pagina utente



Informazioni utente
Quando si seleziona la *Pagina utente*, nella casella di riepilogo *Informazioni utente*viene caricato l'elenco di tutti gli account MDaemon. Nell'elenco sono specificati il nome completo dell'utente, il nome della casella postale, il dominio a cui appartiene l'account, il numero dei messaggi contenuti nell'account, il formato di posta, la quantità di spazio su disco (in KB) occupato dall'account, l'indirizzo di inoltro e la data relativa all'ultimo controllo della posta. Poiché l'elenco contiene informazioni in costante cambiamento, è opportuno aggiornarlo facendo clic sul pulsante *Aggiorna*.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. Le informazioni contenute nella casella di riepilogo *Informazioni utente* possono essere ordinate in base a qualunque colonna. È sufficiente fare clic una volta sulla colonna desiderata per ordinarla in modo ascendente (A-Z) oppure doppio clic per ordinarla in modo discendente (Z-A). Le colonne possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata. Infine, è possibile fare doppio clic su qualunque voce per passare alla *Pagina code* e visualizzare il contenuto della casella postale corrispondente.

Per impostazione predefinita, nell'elenco viene visualizzato il conteggio dei messaggi (non dei file) e lo spazio utilizzato *dai messaggi* (non da tutti i file della directory). Queste sono le informazioni relative alle *quote* riportate da MDaemon. In alternativa, è possibile visualizzare il conteggio dei *file* e lo spazio su disco utilizzato da tutti i *file* anziché dai messaggi. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e sostituire la chiave `ShowQuota=Yes` di `[UserOptions]` in `ShowQuota=No`.

Le cartelle utenti contengono un file di nome "`hiwater.mrk`" che viene utilizzato per determinare alcune informazioni relative agli utenti. L'eventuale eliminazione di questo file impedirebbe a Gestione code e statistiche di ottenere alcune delle informazioni esposte nella casella di riepilogo *Informazioni utente*.

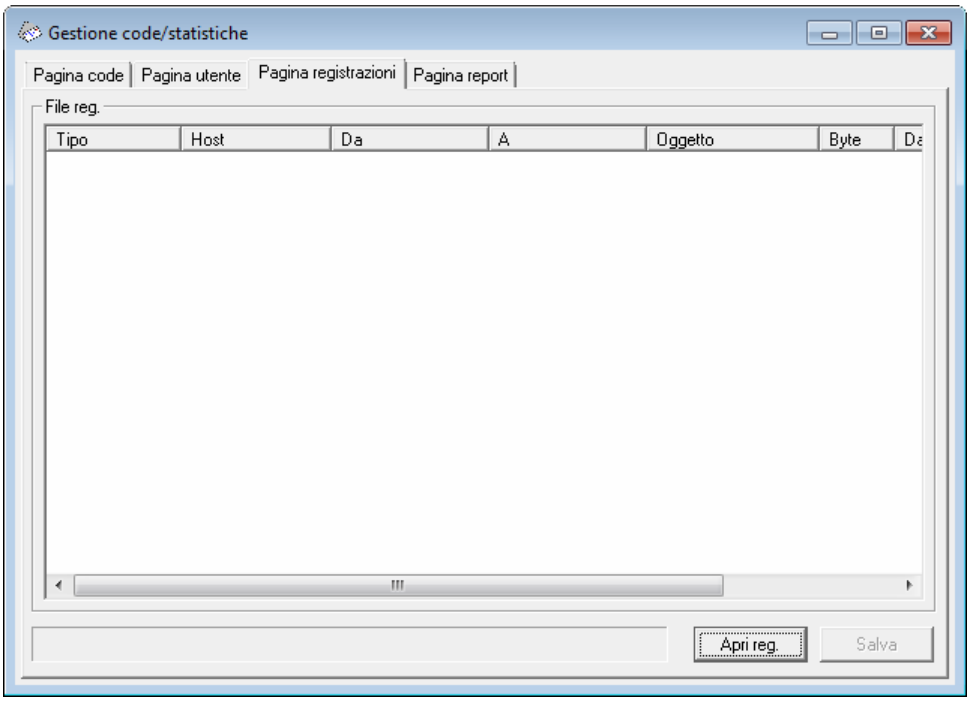
Aggiorna
Alcune statistiche relative agli utenti, ad esempio il numero di messaggi contenuti nella casella postale o la quantità di spazio su disco utilizzato dall'account, cambiano continuamente. È possibile aggiornare i contenuti della casella di riepilogo *Informazioni utente* semplicemente facendo clic sul pulsante *Aggiorna*. Verranno immediatamente visualizzate le informazioni correnti.

Indicatore di avanzamento
Poiché gli elenchi visualizzati nella casella di riepilogo *Informazioni utente* possono raggiungere dimensioni notevoli, sotto la casella di riepilogo *Informazioni utente* è

presente un indicatore di avanzamento che segnala visivamente che il programma è ancora in funzione mentre vengono caricati file di grandi dimensioni.

Salva
Facendo clic su *Salva*, è possibile salvare i contenuti della casella di riepilogo *Informazioni utente* in formato delimitato da virgole, utilizzabile con i database, oppure come file di solo testo ASCII. Una volta scelti il nome e la posizione da assegnare al file nella finestra Salva con nome di Windows, viene richiesto di specificare se salvare il file in formato delimitato da virgole o in formato di testo semplice.

6.3.3 Pagina registrazioni



Report registri
Nella casella di riepilogo *Report registri* vengono visualizzati i file di registro dettagliati di MDaemon selezionabili mediante il pulsante *Apri registro* e la finestra di dialogo Apri di Windows. Il *report dei registri* fornisce un metodo rapido e semplice per esaminare la cronologia delle transazioni di posta elaborate da MDaemon, senza che sia necessario controllare il notevole volume di informazioni che i file di registro di MDaemon talvolta contengono. Quando un *report dei registri* viene visualizzato in questa casella di riepilogo, Gestione code e statistiche lo riduce a un formato più semplice che contiene: il tipo di messaggio (POP in entrata, DomainPOP, RFC822 e così via), l'host a cui si è connesso MDaemon durante la transazione, il mittente, il destinatario, le dimensioni del messaggio, la data di elaborazione di ciascun messaggio e l'esito della transazione.

Per esaminare più dettagliatamente le voci del registro, è sufficiente fare doppio clic sulla voce desiderata. Verrà visualizzata la porzione di registro nella quale è stata

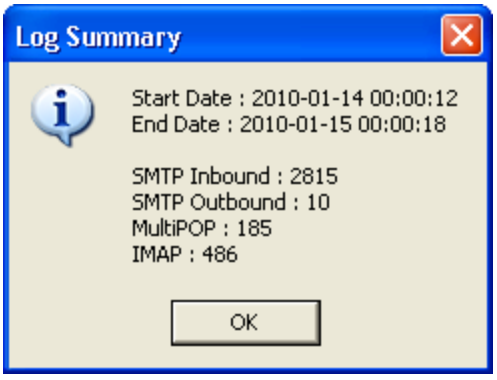
eseguita la transazione. Mediante il menu di scelta rapida associato al clic con il pulsante destro del mouse, è possibile copiare e incollare la porzione dettagliata del registro in un editor di testo, quindi salvarla o modificarla.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. Le colonne della casella di riepilogo possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata.

La scheda *Pagina registrazioni* consente di visualizzare i file registro creati mediante l'opzione *Registra sessioni posta dettagliate* o *Registra il riepilogo delle sessioni di posta* situate in Registrazione » Modalità di registrazione. Tuttavia, è consigliabile utilizzare l'opzione *Registra sessioni posta dettagliate*. Se si utilizza l'opzione *Registra il riepilogo delle sessioni di posta*, le informazioni visualizzate nel *Report registri* sono limitate. Dal momento che la *Pagina registrazioni* condensa il registro dettagliato in una visualizzazione di riepilogo dell'attività di MDaemon fornendo comunque la possibilità di aprire una visualizzazione dettagliata di ogni transazione facendo doppio clic su una voce, non è necessario che MDaemon riepiloghi il file di registro in fase di compilazione.

Apri reg.
Fare clic su questo pulsante per aprire la finestra Apri di Windows e scegliere il file registro da visualizzare. Se si fa clic su questo pulsante quando un *file registro* è già visualizzato nella casella di riepilogo *Report registri*, è possibile aggiungere il nuovo file alla fine di quello visualizzato.

Una volta visualizzato un registro, viene aperta una finestra di messaggio contenente un riepilogo del registro selezionato. Quando si salva un report del registro come file di testo, a questo viene aggiunto il riepilogo del registro.

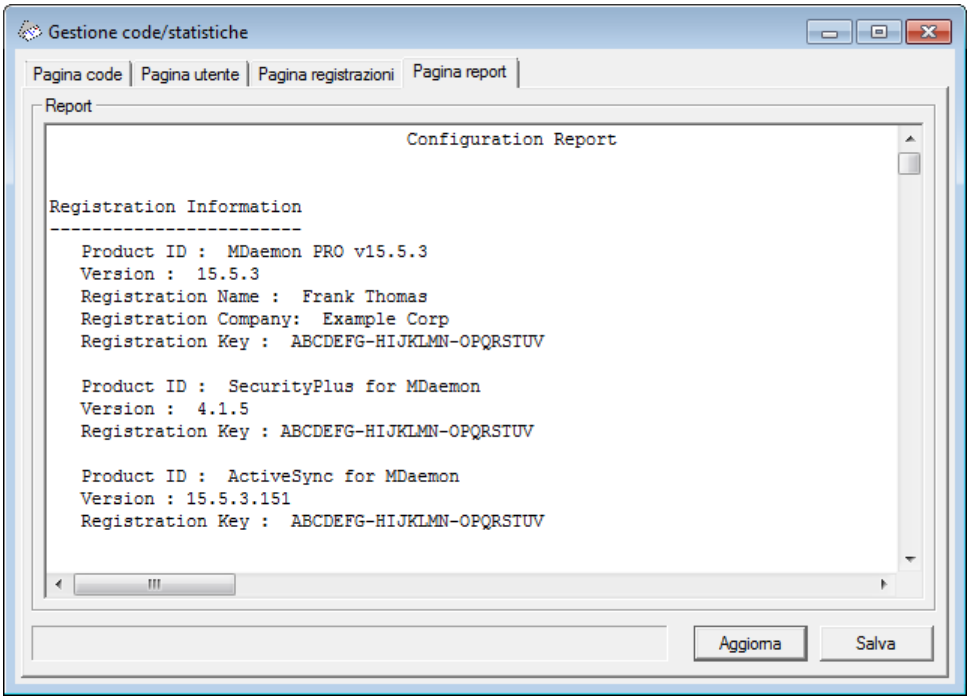


Indicatore di avanzamento
Poiché i *file registro* possono avere dimensioni notevoli, sotto la casella di riepilogo *Report registri* è presente un indicatore di avanzamento che segnala visivamente che il

programma è ancora in funzione durante il caricamento o il salvataggio di file di grandi dimensioni.

Salva
Facendo clic su *Salva*, è possibile salvare i contenuti della casella di riepilogo *Report registri* in formato delimitato da virgole, utilizzabile con i database, oppure come file di solo testo ASCII. Una volta scelti il nome e la posizione da assegnare al file nella finestra Salva con nome di Windows, viene richiesto di specificare se salvare il file in formato delimitato da virgole o in formato di testo semplice.

6.3.4 Pagina report



Report
Facendo clic sulla *Pagina report*, viene prodotto un report esaustivo in cui sono elencate tutte le impostazioni di MDaemon in un formato di testo di facile lettura. Questa funzione consente all'amministratore di velocizzare le operazioni di controllo delle numerose impostazioni di configurazione di MDaemon e facilita la risoluzione dei problemi eventualmente riscontrati.

È possibile spostarsi nel report mediante le barre di scorrimento o i tasti CURSORE. Inoltre, fungendo anche da editor di testo, la visualizzazione del *Report* consente di inserire annotazioni o informazioni supplementari prima che se ne esegua il salvataggio in un file. È anche possibile utilizzare il menu di scelta rapida per tagliare, copiare e incollare in/da questa visualizzazione. A questo scopo, fare clic con il pulsante destro del mouse, quindi selezionare l'opzione desiderata dal menu visualizzato.

Aggiorna
Fare clic su questo pulsante per aggiornare il *report* delle impostazioni di MDaemon correntemente visualizzato.

Indicatore di avanzamento
Analogamente alle altre schede di Gestione code e statistiche, la *Pagina report* contiene un indicatore di avanzamento che offre una rappresentazione visiva del funzionamento del programma mentre vengono caricati o salvati file di grandi dimensioni.

Salva
Fare clic su questo pulsante per salvare il *report* visualizzato. A seguito del clic su questo pulsante, verrà visualizzata una finestra di dialogo Salva con nome, in cui è possibile specificare il nome del file e la posizione in cui salvarlo.

6.3.5 Personalizzazione di Gestione code e statistiche

6.3.5.1 File MDstats.ini

Personalizzazione della funzione di gestione delle code e delle statistiche
Di seguito è riportato un elenco delle impostazioni modificabili dal file `MDstats.ini` presente nella directory `\app\` di MDaemon:

[MDaemon]

AppDir=C:\mdaemon\app\	Percorso della directory \app\ di MDaemon.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor da utilizzare quando si fa doppio clic su un messaggio oppure si seleziona l'opzione Modifica dal menu visualizzato facendo clic con il pulsante destro del mouse.
LockOnEdit=No	Specifica se deve essere creato un file LCK quando si modifica un messaggio. Grazie a questa opzione, è possibile impedire che un messaggio in fase di modifica possa essere rimosso dalla coda.
AutoRefresh=Yes	Intervallo di tempo (in secondi) che deve trascorrere tra un aggiornamento automatico dell'elenco dei messaggi e un altro. Il valore 0 disattiva l'aggiornamento automatico.
ShowDirectories=Yes	Mostra le sottodirectory delle code presenti nella casella di riepilogo, oltre ai messaggi. Le directory

	vengono visualizzate nel formato <NomeDirectory>.
[UserOptions]	
ShowQuota=Yes	Determina se nell'elenco degli utenti debbano essere visualizzate le informazioni sulle quote (calcolo dei messaggi e dello spazio su disco effettuato da MDaemon) o le informazioni sui file (numero di file e spazio su disco totale).
[LogOptions]	
ShowUnknown=Yes	Mostra le sessioni di' cui MDStats non è riuscito a determinare il tipo (in entrata o in uscita, SMTP o POP).
ShowSmtpInbound=Yes	Mostra le sessioni SMTP in entrata.
ShowPopInbound=Yes	Mostra le sessioni POP in entrata (controlli della posta).
ShowSmtpOutbound=Yes	Mostra le sessioni SMTP in uscita.
ShowPopOutbound=Yes	Mostra le sessioni POP in uscita (MultiPOP, DomainPOP).
ShowRFC822=Yes	Mostra le consegne di posta locale RFC822.
ShowSmtpHelo=Yes	Mostra il dominio HELO nella colonna Host per le sessioni SMTP in entrata.
IgnoreEmptyPop=Yes	Ignora i controlli della posta se non è stato consegnato alcun messaggio.
ShowImap=Yes	Mostra le sessioni IMAP.
[Remap]	Rimappatura delle lettere delle unità, utile per eseguire MDStats da un sistema diverso da quello su cui MDaemon è attivo.
C:=\\server\c	Nella lettura di MDaemon.ini, sostituisce "C:" con "\\server\c".
[Special]	
OnlyOneInstance=No	Consente l'esecuzione di una sola istanza di MDStats. Se si tenta di riaprire MdStats, viene

attivata l'istanza già in esecuzione.

Per ulteriori informazioni, vedere:

Parametri della riga di comando di MDStats 910

6.3.5.2 Parametri della riga di comando di MDStats

Nota: Nessun parametro della riga di comando è soggetto alla distinzione tra maiuscole e minuscole.

Numeri da 1 a 8	Consentono di visualizzare una coda specifica nella scheda Pagina code. = Coda remota = Coda locale = Coda tentativi = Coda LAN = Coda RAW = Coda messaggi scartati = Coda SmtpIn = Coda salvataggi
/L[N] [FileInput] [FileOutput]	Crea un report del file registro. Se si specifica la lettera 'N' dopo 'L', il report non viene salvato in formato delimitato da virgole.
/A	Creando un report del file registro, aggiunge le nuove informazioni al file di output anziché sovrascriverlo.

Sezione

7 Caratteristiche aggiuntive di MDaemon

7.1 MDaemon e file di testo

MDaemon utilizza numerosi file di testo al fine di memorizzare i propri dati, i modelli di messaggi generati dal sistema e le impostazioni di configurazione. Questa caratteristica offre un'ampia flessibilità. Per creare nuovi file di testo da MDaemon, selezionare File » Nuovo. Questa funzionalità può rivelarsi particolarmente utile per creare rapidamente dei file di dati da utilizzare con le risposte automatiche e con varie altre funzioni di MDaemon, ad esempio i file RAW.

Modifica dei file di MDaemon

I vari file di dati di MDaemon sono di testo semplice e si possono modificare con Blocco note. È possibile aprire direttamente i file con MDaemon mediante la selezione di menu File » Apri » File testo vuoto. Per impostazione predefinita, con questa selezione vengono cercati nella cartella `\app\` di MDaemon i file con estensione `*.txt`. Per visualizzare gli altri file della cartella, nell'elenco a discesa *Tipo file:* selezionare "Tutti i file".

7.2 Controllo remoto del server via e-mail

Utilizzando il sistema di trasporto e-mail, è possibile accedere a molte funzioni di MDaemon in modalità remota, mediante l'invio di una e-mail formattata in modo speciale all'account del sistema MDaemon "`MDaemon@<dominio MDaemon>`". I messaggi inviati al server vengono memorizzati nella directory messaggi del server, analogamente a quanto avviene per gli utenti normali.

Alcuni di questi messaggi di controllo richiedono un account valido sul server. Per i comandi che richiedono un account valido, è necessario che il messaggio venga autenticato durante l'elaborazione SMTP mediante SMTP AUTH.

I comandi che possono essere utilizzati nei messaggi e-mail rientrano in due categorie generali: Lista di distribuzione 912 ed E-mail generale 915.

Vedere:

Comandi liste di distribuzione 912
Comandi e-mail generali 915

7.2.1 Controllo dei cataloghi e delle liste di distribuzione

Nessuno di questi comandi richiede un account sul server. I parametri racchiusi tra [parentesi quadre] sono opzionali. Ad esempio, "nome [indirizzo]" potrebbe essere immesso semplicemente come "Carlo" oppure con l'aggiunta di un parametro opzionale: "Carlo utente1@esempio.com". I messaggi devono essere inviati a "mdaemon@[dominio

MDaemon]" con ciascun comando e i parametri associati contenuti su una sola riga nel corpo del messaggio.

COMANDO	PARAMETRI	DESCRIZIONE

SUBSCRIBE	nomelista [indirizzo] [{nome reale}] [(password)]	L'originatore viene aggiunto alla lista specificata, purché la lista esista e consenta le iscrizioni remote. Se viene specificato un indirizzo opzionale dopo il nome della lista, tale indirizzo viene aggiunto all'appartenenza della lista anziché all'indirizzo trovato nel campo FROM: del messaggio di iscrizione. È possibile aggiungere il nome reale dell'iscritto racchiudendolo tra parentesi graffe, ad esempio {Roberto R}. Se dopo il comando viene specificata la password della lista (le parentesi sono obbligatorie), il comando viene soddisfatto anche se la funzione per l'iscrizione della lista è disattivata.
		Esempi:
		`SUBSCRIBE lista@esempio.com`
		`SUBSCRIBE lista@esempio.com io@esempio.com {Roberto F}`
		`SUBSCRIBE lista@esempio.com tu@esempio.org (PASS)`

UNSUBSCRIBE o SIGNOFF	nomelista [indirizzo] [(password)]	L'originatore viene rimosso dalla lista specificata, purché la lista esista e contenga l'originatore tra i suoi iscritti. Se viene specificato un indirizzo opzionale dopo il nome della lista, tale indirizzo viene rimosso dall'appartenenza della lista anziché all'indirizzo trovato nel campo FROM: del messaggio di ritiro. Se dopo il comando viene specificata la password della lista (le parentesi sono obbligatorie), il comando viene soddisfatto anche se la funzione per il ritiro dalla lista è disattivata.
		Esempi:
		`UNSUBSCRIBE lista@esempio.com (listPASS)`
		`SIGNOFF lista@esempio.com io@esempio.com`

DIGEST	nomelista [indirizzo]	Consente di impostare la ricezione della posta della lista in formato riassunto per il mittente. Se viene specificato un indirizzo opzionale dopo il nome della lista, tale indirizzo viene impostato in modalità riassunto. Esempi:

		DIGEST lista@esempio.com DIGEST lista@esempio.com utente1@esempio.cc
NORMAL	nomelista [indirizzo]	Il mittente viene impostato per ricevere la posta dalla lista in formato normale (non riassunto). Se viene specificato un indirizzo opzionale dopo il nome della lista, tale indirizzo (non il mittente originale) viene impostato per ricevere la posta in formato normale. Esempi: NORMAL lista@esempio.com NORMAL lista@esempio.com utente1@altn.com
NOMAIL	nomelista [indirizzo]	Questo comando imposta la modalità nomail (no posta) per l'indirizzo. L'account viene posto in stato di sospensione e non riceve più il traffico della lista. Se non viene specificato alcun indirizzo, viene utilizzato l'originatore del messaggio. Esempio: NOMAIL lista@esempio.com io@esempio.com
MAIL	nomelista [indirizzo]	Questo comando reimposta la modalità normale (consegna della posta) per l'indirizzo precedentemente in modalità nomail. Se non viene specificato alcun indirizzo, viene utilizzato l'originatore del messaggio. Esempi: MAIL lista@esempio.com MAIL lista@esempio.com io@esempio.com
REALNAME	nomelista [indirizzo] {nome reale}	Questo comando imposta sul valore specificato il nome reale di "indirizzo", iscritto alla lista "nomelista". Il nome reale deve essere racchiuso tra i caratteri "{" e "}". Esempio: REALNAME lista@esempio.com {Roberto Rossi}
LIST	[nome lista] [password lista]	Offre informazioni sulla lista di distribuzione. Se il nome della lista non viene indicato, viene restituito un riepilogo di tutte le liste. Se per le liste si indica una password, vengono restituite maggiori informazioni. Esempio: LIST lista@esempio.com Lz$12

Per ulteriori informazioni, vedere:

Controllo remoto del server via e-mail 912
Comandi e-mail generali 915

7.2.2 Comandi e-mail generali

I comandi e-mail generali possono essere inviati all'account di sistema mediante messaggi e-mail. I messaggi devono essere inviati a "mdaemon@[dominio MDaemon]" con ciascun comando e i parametri associati contenuti su una sola riga nel corpo del messaggio.

COMANDO	PARAMETRI	DESCRIZIONE
`HELP`	nessuno	Una copia di NEWUSERHELP.DAT viene elaborata e reinviata all'originatore del messaggio.
`STATUS`	nessuno	Un report sullo stato delle operazioni del server e sulle condizioni correnti viene reinviato all'originatore del messaggio. Poiché le informazioni contenute nel rapporto sullo stato sono considerate private, l'utente che richiede il rapporto deve essere autenticato come amministratore. Esempio: `STATUS`

Per ulteriori informazioni, vedere

Controllo remoto del server via e-mail 912
Comandi liste di distribuzione 912

7.3 Specifica dei messaggi RAW

7.3.1 Specifica dei messaggi RAW

MDaemon incorpora il supporto per un formato di messaggi e-mail semplice e potente, noto come RAW. Il sistema di posta RAW fornisce un formato semplice e standard, utilizzabile dai sistemi software come MDaemon per creare messaggi compatibili con il più complesso metodo RFC-2822. L'utilizzo di un sistema MTA come RAW fa sì che il software client deleghi al server la responsabilità della conformità con gli standard della posta Internet.

La posta RAW consiste in una serie di intestazioni testuali necessarie e opzionali seguite da un corpo del messaggio. La maggior parte delle intestazioni è costituita da un token seguito da un valore compreso tra i simboli <>. Ciascuna riga dell'intestazione termina con una combinazione <CRLF> di caratteri. Le intestazioni sono separate dal corpo del

messaggio da una riga bianca e non sono sensibili alla distinzione tra maiuscole e minuscole. Inoltre, le intestazioni *Da* e *A* sono le uniche necessarie. Tutti gli elementi di testo, sia dell'intestazione che del corpo, sono in testo ASCII semplice e devono essere contenuti in un file con estensione "RAW", ad esempio "mio-messaggio.raw". Quindi, per accodare il messaggio per la consegna, collocare il file con estensione *.raw nella coda RAW di MDaemon, che in genere si trova in "C:\MDaemon\Queues\Raw".

Come ignorare Filtro contenuti

Per impostazione predefinita, i messaggi RAW vengono trasferiti tramite il Filtro contenuti come messaggi normali. Se si desidera che il filtro ignori un determinato messaggio RAW, è necessario che il nome del file inizi con "p" o con "P". Ad esempio, "P_mio-messaggio.raw" verrà ignorato da Filtro contenuti che, al contrario, elaborerà normalmente "mio-messaggio.raw".

Ignorando il Filtro contenuti, non è possibile applicare ai messaggi una firma DKIM. Se MDaemon è stato configurato per firmare tutti i messaggi, ciò potrebbe provocare alcuni problemi di consegna. Se si desidera che MDaemon firmi i messaggi RAW configurati per ignorare il Filtro contenuti, è possibile utilizzare l'opzione x-flag=sign descritta di seguito.

Intestazioni RAW

Da <casellapostale@esempio.com>	Questo campo contiene l'indirizzo e-mail del mittente.
To <casellapostale@esempio.com [, casellapostale@esempio..com]>	Questo campo contiene gli indirizzi e-mail dei destinatari. È possibile specificare più destinatari separandoli con una virgola.
ReplyTo <casellapostale@esempio.com>	Un indirizzo e-mail opzionale a cui vengono dirette le risposte al messaggio.
CC <casellapostale@esempio.com[, casellapostale@esempio.com]>	Un elenco opzionale di destinatari in copia conoscenza del messaggio. È possibile specificare più destinatari separandoli con una virgola.
Subject <testo>	Un oggetto opzionale per il messaggio.
Header <intestazione: valore>	Consente di inserire esplicitamente delle combinazioni intestazione/valore nel messaggio. Ciò consente di sostituire intestazioni personalizzate o non standard nei messaggi RAW

Campi speciali previsti dalla specifica RAW

Allegati di file e codifica

```
x-flag=attach <percorsofile, metodo> [-x]
```

Esempio: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

X-FLAG specifica il valore "ATTACH" insieme a due parametri compresi tra i caratteri <>. Il primo parametro è il percorso completo del file da allegare al messaggio. Il secondo parametro, separato dal primo mediante una virgola, specifica il metodo di codifica da utilizzare per allegare il messaggio. In MDaemon sono supportati due valori per questo parametro. Il metodo MIME segnala al server di utilizzare il metodo standard Internet Base64 di codifica dei messaggi. Il metodo ASCII segnala al server di importare semplicemente il file nel messaggio. Il parametro -X opzionale alla fine della stringa indica al server di rimuovere il file dal disco una volta allegato.

Notifica dello stato della consegna

```
x-flag=confirm_delivery
```

Quando si converte in RFC-2822 un messaggio RAW che contiene questo flag, la stringa viene trasformata nel costrutto "Return-Receipt-To:@ <mittente@esempio.com>".

Inserimento di specifiche combinazioni intestazione/valore nel messaggio RFC-2822

```
header <Intestazione: valore>
```

Per inserire una combinazione intestazione/valore specifica nel messaggio RFC-2822 generato da un file RAW, è necessario utilizzare la macro HEADER indicata nella sezione Intestazioni RAW. Ad esempio, per inserire l'intestazione "Delivered-By: sistema-posta@esempio.com" nel messaggio RFC-2822, inserire: "header <Delivered-By: sistema-posta@esempio.com>" nel messaggio RAW. Per la macro "header" sono necessari sia il campo che il valore. In un messaggio RAW è possibile inserire un numero illimitato di macro "header".

Messaggi RAW con firma DKIM

```
x-flag=sign
```

L'inclusione di questo comando speciale in un file con estensione `RAW` consente di applicare una firma DKIM al messaggio RAW. Questo comando può essere utilizzato solo nei messaggi RAW configurati per ignorare il Filtro contenuti, ossia quelli il cui nome file inizia con "`p`" o con "`P`". Non è necessario utilizzare questo comando nel caso di messaggi RAW normali, elaborati tramite il filtro, che verranno firmati normalmente.

In tutti i messaggi RAW generati da Filtro contenuti viene utilizzato automaticamente il comando `x-flag=sign`.

Esempi di messaggi di posta RAW

Esempio 1:

```
from <mdaemon@altn.com>
to <utente01@esempio.com>

Ciao John!
```

Esempio 2:

```
da <utente01@esempio.com>
a <utente09@esempio.net>
oggetto <File richiesti>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X

Ecco tutti i file richiesti.
```

7.4 File semaforo

MDaemon offre il supporto per i file semaforo che possono essere utilizzati per diversi scopi, tra cui determinare specifiche azioni di MDaemon. MDaemon esegue una scansione periodica della sottocartella \APP\ per verificare l'esistenza di questi file. Se ne individua uno, viene attivato il comportamento appropriato e il file semaforo viene rimosso. Si tratta di un semplice meccanismo che consente agli amministratori e/o agli sviluppatori di gestire MDaemon senza utilizzarne l'interfaccia. Di seguito è riportato un elenco di tutti i file semaforo e delle azioni a essi associate:

NOME FILE	AZIONE
ACLFIX.SEM	Esegue la routine di pulizia dei file ACL.
ADDUSER.SEM	Questo file semaforo consente di creare nuovi account. Viene utilizzato per imporre a MDaemon di associare nuovi record alla fine del file USERLIST.DAT senza avviare una ricostruzione completa del database utenti, che potrebbe richiedere un periodo di tempo eccessivo. Ogni riga del file deve costituire un record di account completo nella forma specificata nella sezione Account Management Functions dell'API di MDaemon (vedere MD-API.html nella sottocartella \docs\API\ di MDaemon). È possibile specificare più account nuovi, un record di account per riga. MDaemon elabora il file una riga per volta e aggiunge un nuovo account. È possibile creare un file ADDUSER.LCK per bloccare il file in corso di aggiornamento in modo che MDaemon non

tocchi ADDUSER.SEM fino a quando ADDUSER.LCK è stato eliminato. Per visualizzare un campione del file ADDUSER.SEM, aprire ADDUSER.SMP nella directory APP con un editor di testo.

ALERT.SEM — Visualizza in una finestra a comparsa il contenuto del file Semaphore per tutti gli utenti di Webmail connessi al momento della creazione del file. La finestra, tuttavia, non viene visualizzata immediatamente da tutti gli utenti, ma singolarmente da ciascuno degli utenti quando il suo browser invia una richiesta al server Webmail.

Nota: a differenza degli altri file Semaphore, questo file è specifico di Webmail. e anziché nella directory \app\, deve essere inserito nella directory \MDaemon\WorldClient\.

ALIAS.SEM — Carica nuovamente i file di dati degli alias.

AUTORESPEXCEPT.SEM — Ricarica i file delle eccezioni della risposta automatica.

BATV.SEM — Carica nuovamente i file di dati della protezione backscatter (BATV).

BAYESLEARN.SEM — Questo file semaforo avvia manualmente il processo di apprendimento bayesiano, così come avviene facendo clic sul pulsante Apprendi nella scheda Bayesiano di Spam Filter. Nota: con questa operazione, la procedura di apprendimento bayesiano si avvia anche se l'apprendimento bayesiano è disattivato.

BLACKLIST.SEM — Ricarica i file di dati della lista nera.

CFILTER.SEM — Ricarica le regole di Filtro contenuti, cancella i dati di Filtro contenuti presenti nella cache, ricarica il file Lista consentiti (nessun filtro)[708].

CLEARQUOTACOUNTS.SEM — I risultati delle verifiche delle quote relative agli utenti vengono conservati nel file quotacounts.dat. Se si desidera cancellare il valore della quota relativa a un utente memorizzato nella cache, aggiungere l'indirizzo e-mail dell'utente nel file SEM e collocarlo nella cartella \app\. Se in una riga è presente solo un asterisco

(*), l'intero file verrà eliminato invalidando tutti i conteggi delle quote memorizzate nella cache.

DELUSER.SEM — È possibile utilizzare questo file semaforo per eliminare uno o più account utente. Creare un file di testo contenente gli indirizzi di ciascun account che si desidera eliminare (un indirizzo per riga), denominare il file DELUSER.SEM, quindi spostarlo nella directory \app\ di MDaemon. MDaemon elimina dapprima gli account, quindi il file DELUSER.SEM. Per eliminare un account senza eliminare la cartella della posta, aggiungere "^" all'indirizzo (ad esempio, frank@example.com^).

DNS.SEM — Ricarica le impostazioni Server DNS Windows[108] e DNS Spam Filter.

DOMAINSHARING.SEM — Carica nuovamente il file di dati di Condivisione dominio.

EDITUSER.SEM — Questo semaforo viene utilizzato per aggiornare dei record utente specifici del file USERLIST.DAT senza ricorrere a una ricostruzione completa che potrebbe richiedere molto tempo. Per aggiornare i record utente specifici in USERLIST.DAT, creare un file denominato EDITUSER.SEM che contenga un record sostitutivo completo, uno per ogni riga, per ciascuno dei record utente che si desidera sostituire. Ognuno dei record deve essere costruito nel formato di USERLIST.DAT descritto nell'articolo della Knowledge Base Userlist File Format (Formato del file Userlist), ma deve iniziare con l'indirizzo e-mail originale del record seguito da una virgola. MDaemon elabora il file EDITUSER.SEM una riga per volta. È possibile creare un file EDITUSER.LCK per bloccare il file in corso di aggiornamento in modo che MDaemon non tocchi EDITUSER.SEM fino a quando EDITUSER.LCK è stato eliminato. Per visualizzare un campione del file EDITUSER.SEM, aprire EDITUSER.SMP nella directory \APP\ con un editor di testo.

EXITNOW.SEM — Chiude MDaemon.

GATEWAYS.SEM — Per offrire migliori prestazioni, MDaemon conserva nella memoria l'elenco dei gateway. Per ricaricare in MDaemon il file gateways.dat, creare il file GATEWAYS.SEM nella directory APP di MDaemon.

GREYLIST.SEM	Carica nuovamente i file di dati Greylisting.
GROUPS.SEM	Carica nuovamente i file di dati dei gruppi di account.
GRPLIST.SEM	Carica nuovamente la cache interna con i nomi delle liste di distribuzione.
HANGUPG.SEM	Impone un'interruzione condizionata del dispositivo RAS. MDaemon attende la chiusura delle eventuali sessioni di posta in sospeso, quindi interrompe la sessione RAS.
HANGUPR.SEM	Impone un'interruzione incondizionata del dispositivo RAS. Si tratta di un'interruzione immediata e incondizionata, che prescinde delle sessioni di posta eventualmente in corso sulla connessione.
HOSTSCREEN.SEM	Carica nuovamente i file di dati di Vaglio host.
IPSCREEN.SEM	Carica nuovamente i file di dati di Vaglio IP.
IPSHIELD.SEM	Il file IPShield.dat viene conservato nella memoria cache per aumentare la velocità di accesso. Utilizzare IPSHIELD.SEM per ricaricare il file nella memoria
LDAPCACHE.SEM	Carica nuovamente i file di dati degli utenti relativi a LDAP e gateway.
LOCKSEMS.SEM	Impedisce l'elaborazione di tutti i file semaforo fino alla sua rimozione.
LOGSETTINGS.SEM	Carica nuovamente le impostazioni del file di registro.
MDSPAMD.SEM	Ricarica la lista consentiti per lo Spam Filter e MDSPAMD, forzando la reinizializzazione di tutti i dati di configurazione.
MINGER.SEM	Arresta e riavvia il server Minger 878.
MXCACHE.SEM	Carica nuovamente i file di dati della cache MX.

NODNSBL.SEM	Ricarica il file della lista consentiti DNSBL.
NOPRIORITY.SEM	Impone a MDaemon di ricaricare il file `NoPriority.dat`.
ONLINE.SEM	MDaemon crea questo file di semaforo quando stabilisce una connessione all'ISP mediante RAS e lo rimuove al termine della connessione. Il file si rivela utile per sapere se MD sta utilizzando il sottosistema RAS.
POSTDIAL.SEM	MDaemon crea questo file immediatamente dopo la chiusura della connessione effettuata in precedenza.
PREDIAL.SEM	MDaemon crea questo file immediatamente prima che si tenti di utilizzare il servizio di accesso remoto (RAS/DUN). in modo che gli altri programmi software liberino la porta di connessione quando questa deve essere utilizzata da MDaemon.
PRIORITY.SEM	Carica nuovamente i file di dati della posta prioritaria.
PROCBAD.SEM	Avvia la consegna del contenuto della coda dei messaggi scartati.
PROCDIG.SEM	Avvia la creazione e la consegna dei riassunti della lista di distribuzione.
PROCHOLDING.SEM	Avvia la consegna del contenuto della coda trattenuta.
PROCNOW.SEM	Avvia il controllo della posta remota e la consegna di quella in coda.
PROCREM.SEM	MDaemon passa immediatamente in modalità di elaborazione della posta ed effettua le transazioni relative a tutta la posta remota.
PROCRETR.SEM	Avvia la consegna del contenuto della coda tentativi.
PRUNE.SEM	Carica nuovamente le impostazioni di sfoltimento automatico.

PUBLICSUFFIX.SEM	Ricarica il file dei suffissi pubblici 559.
QUEUE.SEM	Questo file semaforo si utilizza per abilitare/disabilitare le code di posta. Il file può contenere un qualsiasi numero di righe, ma ciascuna di queste deve contenere una delle seguenti stringhe (una per riga): ENABLE INBOUND, ENABLE REMOTE, ENABLE LOCAL o DISABLE INBOUND, DISABLE REMOTE, DISABLE LOCAL.
RESTART.SEM	Arresta e riavvia MDaemon.
RESTARTCF.SEM	Arresta e riavvia `CFEngine.exe`, ossia il file eseguibile di Filtro contenuti.
RESTARTWC.SEM	Arresta e riavvia MDaemon Webmail. Questo file funziona solo quando Webmail viene eseguito sul relativo server Web incorporato 330.
RELOADCACHE.SEM	Ricarica tutte le impostazioni e tutti i file memorizzati nella cache, ad eccezione delle impostazioni e dei file di Filtro contenuti.
REVERSEEXCEPT.SEM	Carica nuovamente il file delle eccezioni della ricerca inversa.
SCHEDULE.SEM	Carica nuovamente i file di dati della pianificazione.
SPAMHONEYPOTS.SEM	Carica nuovamente i file di dati delle trappole spam.
SPF.SEM	Carica nuovamente i file di dati relativi alle funzionalità SPF, DKIM e VBR.
SUPPRESS.SEM	Ricarica le impostazioni della lista bloccati e cancella le impostazioni del dominio memorizzate nella cache.
TARPIT.SEM	Carica nuovamente i file di dati relativi a tarpit e a vaglio dinamico.
TRANSLAT.SEM	Ricarica il file di dati della traduzione delle intestazioni.

TRAY.SEM	Ridisegna l'icona di MDaemon nella barra delle applicazioni.
TRUST.SEM	Per offrire migliori prestazioni, i domini accreditati e gli indirizzi IP vengono conservati nella memoria residente. Per ricaricare manualmente tali impostazioni, creare TRUST.SEM.
UPDATEAV.SEM	Avvia l'aggiornamento delle definizioni virus.
UPDATESA.SEM	Avvia l'aggiornamento di Spam Filter.
USERLIST.SEM	Carica nuovamente il file USERLIST.DAT. Utilizzare questo file quando si effettuano delle modifiche a USERLIST.DAT ed è necessario che MDaemon lo ricarichi.
WATCHDOG.SEM	MDaemon cerca e rimuove questo semaforo dalla directory APP ogni 10-20 secondi circa. Questo file può essere utilizzato dalle applicazioni esterne per verificare se MDaemon è in esecuzione. Se questo file rimane nella directory APP per più di 20 secondi, è probabile che MDaemon non sia più in esecuzione.

7.5 Route Slip

Di solito, all'interno di un file di messaggio in attesa in una coda sono contenute tutte le informazioni necessarie perché il messaggio venga consegnato alla destinazione appropriata. All'interno del file, inoltre, sono memorizzate le intestazioni, ad esempio X-MDaemon-Deliver-To, che forniscono a MDaemon le istruzioni sulla destinazione e sul destinatario del messaggio. In alcuni casi può tuttavia essere necessario o opportuno ignorare queste informazioni e fornire delle alternative specifiche sulla destinazione e sul destinatario di un messaggio. Il route slip fornisce esattamente questo meccanismo. Un route slip è un file che fornisce a MDaemon delle informazioni molto specifiche sulla destinazione e sul destinatario di un messaggio. Se per un particolare messaggio è presente un route slip, la destinazione e il destinatario del messaggio verranno controllati in base alle impostazioni del route slip e non a quelle del file .MSG stesso.

I route slip hanno estensione RTE. Ad esempio, se un file di messaggio in attesa di invio è denominato "MD0000.MSG", il route slip corrispondente avrà il nome MD0000.RTE e dovrà trovarsi nella stessa directory (coda di posta) del file di messaggio.

Un route slip presenta il seguente formato:

```
[RemoteHost]
DeliverTo=esempio.net
```

Questa sezione di un route slip indica a MDaemon il server a cui deve essere inviato il file `.MSG` corrispondente. MDaemon tenta sempre di stabilire una connessione diretta all'host cercando di instradare il messaggio nel più breve tempo possibile. È possibile specificare un solo host.

```
[Port]
Port=xxx
```

Questo comando specifica la porta utilizzata per i tentativi di connessione TCP/IP e di consegna. La porta predefinita per la posta SMTP è la porta 25.

```
[LocalRcpts]
Rcpt0=indirizzo@esempio.com
Rcpt1=secondo-indirizzo@esempio.com
Rcpt2=terzo-indirizzo@esempio.com

[RemoteRcpts]
Rcpt0=indirizzo@esempio.net
Rcpt1=secondo-indirizzo@esempio.net
Rcpt2=terzo-indirizzo@esempio.net
```

Queste sezioni del route slip consentono di specificare il numero desiderato di destinatari locali e remoti per la ricezione di una copia del file `.MSG` associato. Gli indirizzi dei destinatari locali e remoti devono essere tenuti separati all'interno delle rispettive sezioni `[LocalRcpts]` e `[RemoteRcpts]`.

Benché forniscano un efficace meccanismo di consegna o reindirizzamento della posta elettronica, generalmente i route slip non sono necessari. MDaemon, ad esempio, utilizza i route slip per i messaggi di una lista di distribuzione "instradata". Quando una lista di distribuzione viene impostata per instradare una sola copia del messaggio di lista a un host remoto, viene utilizzato un route slip. Si tratta di un metodo molto efficace per consegnare la posta in caso di indirizzi collettivi. Per una singola copia del messaggio può infatti essere specificato un numero illimitato di destinatari. Tuttavia, non tutti gli host remoti consentono questo tipo di instradamento. Poiché in ultima istanza rappresentano i sistemi incaricati di consegnare una copia del messaggio a ciascun indirizzo, alcuni host pongono un limite sul numero di destinatari specificabili.

Sezione

8 Creazione e uso dei certificati SSL

Se la creazione di certificati avviene mediante la finestra di dialogo SSL & TLS, MDaemon genera certificati autofirmati. In altre parole, l'autorità emittente o CA (Certificate Authority, autorità di certificazione) coincide con il proprietario del certificato. Questa impostazione è perfettamente valida e consentita, ma poiché la CA non sarà già presente negli elenchi delle CA affidabili degli utenti, ogni volta che si connetteranno all'URL HTTPS di Webmail o Remote Administration gli utenti riceveranno una richiesta di conferma prima di procedere al sito e/o installare il certificato. Dopo aver dato la conferma per l'installazione del certificato e aver accreditato il dominio di Webmail come CA valida, il messaggio dell'avviso di protezione non viene più visualizzato quando ci si connette a WorldClient o Remote Administration.

Quando si effettua una connessione a MDaemon attraverso un client di posta come Microsoft Outlook, non viene tuttavia offerta la possibilità di installare il certificato. È possibile scegliere se proseguire o meno nell'uso temporaneo del certificato, anche se non convalidato. Ogni volta che il client di posta viene avviato e si effettua una connessione al server, è necessario scegliere se continuare a utilizzare il certificato non convalidato. Per evitarlo è possibile ottenere un certificato da una CA, ad esempio Let's Encrypt 605 oppure esportare il certificato autofirmato e distribuirlo agli utenti via e-mail o mediante altri mezzi. Gli utenti potranno quindi installare manualmente il certificato e accreditarlo per evitare eventuali messaggi di avviso.

Creazione di un certificato

Per creare un certificato da MDaemon, seguire le istruzioni descritte di seguito.

1. Passare alla finestra di dialogo SSL e TLS in MDaemon (fare clic su **Sicurezza » Impostazioni di sicurezza » SSL e TLS » MDaemon**).
2. Selezionare la casella, **Abilita SSL, STARTTLS e STLS**.
3. Fare clic su **Crea certificato**.
4. Nella casella di testo **Nome host**, inserire il dominio cui appartiene il certificato (ad esempio, "*mail.esempio.com*").
5. Nella casella di testo "*Nome organizzazione/azienda*", digitare il nome dell'organizzazione o dell'azienda cui appartiene il certificato.
6. In "*Nomi host alternativi*...", digitare tutti i nomi dei domini utilizzati dagli utenti per accedere al server (ad esempio, "`*.esempio.com`", "`esempio.com`", "`wc.altn.com`" e così via).
7. Scegliere la lunghezza della chiave crittografica dalla casella di riepilogo a discesa.
8. Scegliere il paese o la regione in cui si trova il server.
9. Fare clic su **OK**.

Uso di certificati emessi da un'altra autorità di certificazione

Se si è acquistato o creato un certificato con un'origine diversa da MDaemon, è possibile utilizzarlo importandolo tramite Microsoft Management Console nell'archivio certificati di MDaemon. A questo scopo, utilizzando Windows XP:

1. Nella barra degli strumenti di Windows, fare clic su **Start** » **Esegui** e inserire "**mmc /a**" nella casella di testo.
2. Fare clic su **OK**.
3. In Microsoft Management Console, fare clic su **File** » **Aggiungi/Rimuovi snap-in** nella barra dei menu o premere la combinazione di tasti **CTRL+M** sulla tastiera.
4. Nella scheda Autonomo, fare clic su **Aggiungi...**
5. Nella finestra di dialogo *Aggiungi snap-in autonomo*, fare clic su **Certificati** e quindi su **Aggiungi**.
6. Nella finestra di dialogo *Snap-in certificati*, selezionare **Account del computer** e quindi fare clic su **Avanti**.
7. Nella finestra di dialogo *Selezione computer*, selezionare **Computer locale** e quindi fare clic su **Fine**.
8. Fare clic su **Chiudi** e quindi su **OK**.
9. In *Certificati (computer locale)* situato nel riquadro di sinistra, se il certificato da importare è autofirmato, fare clic su **Autorità di certificazione fonti attendibili** e quindi su **Certificati**. In caso contrario, fare clic su **Personale**.
10. Nella barra dei menu, fare clic su **Azione** » **Tutte le attività** » **Importa** e quindi su **Avanti**.
11. Inserire il percorso del file del certificato da importare, utilizzando il pulsante Sfoglia se necessario, quindi fare clic su **Avanti**.
12. Fare clic su **Avanti** e quindi su **Fine**.

MDaemon consente di visualizzare solo certificati con chiavi private che utilizzano il formato Personal Information Exchange (PKCS #12). Se il certificato importato non viene visualizzato nell'elenco, è necessario importare un file con estensione `PEM` che contiene sia la chiave del certificato che la chiave privata. Eseguendo l'importazione del file PEM con lo stesso processo descritto in precedenza, il file viene convertito automaticamente nel formato PKCS #12.

Utilizzo di Let's Encrypt per la gestione del certificato

Let's Encrypt è un'autorità di certificazione (CA) che fornisce certificati gratuiti mediante un processo automatizzato che si pone la finalità di eliminare i processi più complessi di creazione, convalida, firma, installazione e rinnovo manuali dei certificati per i siti Web sicuri.

Per supportare l'utilizzo del processo automatico di Let's Encrypt per la gestione di un certificato, è disponibile la schermata Let's Encrypt[605] che consente di configurare ed eseguire facilmente lo script PowerShell incluso nella cartella "`MDaemon\LetsEncrypt`". L'esecuzione dello script imposterà ogni elemento per Let's Encrypt e posizionerà i file necessari nella cartella HTTP di Webmail per completare il test http-01. Viene utilizzato il nome host SMTP[188] del dominio predefinito[185] come dominio per il certificato, che comprende gli eventuali *nomi host alternativi*, poi recuperato e configurato in Windows, quindi viene configurato MDaemon in modo che il certificato sia valido per MDaemon, Webmail e Remote Administration. Quindi, lo script crea un file di registro nella cartella "`MDaemon\Logs\`", denominato `LetsEncrypt.log`. Questo file di registro viene rimosso e creato di nuovo ad ogni esecuzione dello script e contiene la data e l'ora di avvio dello script. Inoltre, in caso di errori e se si specifica una *E-mail amministratore per notifiche*, vengono inviati dei messaggi e-mail di notifica. Vedere l'argomento Let's Encrypt[605] per ulteriori informazioni.

Vedere:

SSL e TLS[585]

Sezione

9 Glossario

ACL - Acronimo di **A**ccess **C**ontrol **L**ists. È un'estensione del protocollo Internet Message Access Protocol (IMAP4) che consente di creare un elenco di accesso per ogni cartella di messaggi IMAP disponibile, accordando diritti di accesso a tali cartelle anche agli altri utenti che dispongono di un account sullo stesso server di posta. Le autorizzazioni possono essere impostate in modo da limitare o estendere il livello di controllo che ciascun utente può esercitare su tali cartelle. È ad esempio possibile specificare se un utente è autorizzato a eliminare dei messaggi, a contrassegnarli come letti o non letti, a copiare i messaggi nelle cartelle, a creare delle nuove sottocartelle e così via. Solo i client e-mail che supportano ACL possono essere utilizzati per condividere l'accesso e impostare le autorizzazioni. Se il client di posta elettronica in uso non supporta ACL, sarà comunque possibile impostare queste autorizzazioni dall'interfaccia di MDaemon.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII - Acronimo di "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". Si tratta del codice standard utilizzato a livello mondiale per rappresentare tutte le lettere (maiuscole e minuscole) dell'alfabeto latino, nonché i numeri e i segni di interpunzione sotto forma di numeri binari a 7 cifre. A ogni carattere è assegnato un numero compreso tra 0 e 127 (da 0000000 a 1111111). Ad esempio, il codice ASCII per la lettera M maiuscola è 77. La maggior parte dei computer utilizza i codici ASCII per rappresentare il testo, in modo da poter trasferire i dati ad altri sistemi. La maggior parte degli editor e degli elaboratori di testo è in grado di memorizzare i file in formato ASCII (definiti, talvolta, semplicemente file ASCII). Tuttavia, la maggior parte dei file di dati, in particolare quelli che contengono dati numerici, non viene memorizzata in formato ASCII.

Diversi set di caratteri utilizzano 8 bit anziché 7 e dispongono quindi di 128 caratteri supplementari. Questi caratteri aggiuntivi sono utilizzati per rappresentare i simboli e i caratteri non appartenenti all'alfabeto inglese. Il sistema operativo DOS utilizza un set ASCII superiore, denominato ASCII esteso o "high ASCII". Uno standard riconosciuto a livello quasi universale è ISO Latin 1, utilizzato da numerosi sistemi operativi e browser Web.

ATRN - Vedere ETRN e ODMR più avanti.

Allegato - Un file allegato a un messaggio e-mail. Poiché la maggior parte dei sistemi di gestione e-mail supporta solo l'invio di file di testo, se l'allegato è costituito da un file binario o da un file di testo formattato (ad esempio, un documento creato con un elaboratore di testo), deve essere codificato come testo prima dell'invio e decodificato dopo la ricezione. Esistono numerosi schemi di codifica: i più diffusi sono le codifiche MIME (Multipurpose Internet Mail Extensions) e Uuencode (Unix-to-Unix). Per i messaggi in arrivo, MDaemon si può configurare in modo da lasciare il processo di decrittografia al client e-mail del destinatario oppure da decrittografare automaticamente gli allegati e memorizzarli in una posizione specifica prima di consegnare il messaggio all'utente locale.

Dorsale - Una linea o una serie di connessioni che formano il percorso principale di una rete. Si tratta di un termine alquanto relativo, dal momento che a volte una linea non di dorsale di una grande rete può avere dimensioni superiori alla dorsale di una rete più piccola.

Larghezza di banda - Quantità di dati che è possibile trasmettere in un intervallo prefissato di tempo mediante una connessione di rete o via modem, misurata generalmente in bit al secondo (o bps, bits-per-second). Una pagina intera di testo equivale a circa 16.000 bit, trasferibili da un modem veloce in circa 1 o 2 secondi. Un video a pieno schermo richiede quasi 10.000.000 bps, a seconda della compressione utilizzata.

La larghezza di banda può essere equiparata a un'autostrada. L'autostrada rappresenta la connessione, mentre i veicoli che la percorrono rappresentano i dati. Più larga è l'autostrada (quindi, maggiore è la larghezza di banda), maggiore è il numero di veicoli che possono percorrerla.

Baud - La velocità in baud rappresenta una misura della frequenza con cui i segnali portanti cambiano valore su una linea telefonica. Si riferisce alla velocità a cui un modem trasmette i dati. Solitamente, i modem più lenti vengono descritti in termini di velocità in baud, mentre quelli più veloci vengono classificati mediante bit al secondo. I due termini non sono necessariamente sinonimi, poiché ciascun segnale è in grado di codificare più di un bit nelle connessioni ad alta velocità.

Bit - Abbreviazione di **B**inary dig**it**. ovvero dell'unità di dato minima: un numero a cifra singola a base 2 (0 o 1). Il bit viene solitamente abbreviato con una "b" minuscola, come accade in "bps" (bits per second). Una pagina intera di testo corrisponde a circa 16.000 bit.

Bitmap - La maggior parte delle immagini visualizzate su un computer, comprese quelle presenti in Internet, è costituita da bitmap. Una bitmap è sostanzialmente una mappa di punti (o bit) che ha l'aspetto di un'immagine, almeno finché non viene osservata troppo da vicino o non viene ingrandita in misura eccessiva. I tipi di file bitmap più comuni sono BMP, JPEG, GIF, PICT, PCX e TIFF. Le immagini bitmap sono costituite da una serie di punti. Se vengono ingrandite, appaiono a blocchi e risultano poco uniformi. La grafica vettoriale, in genere creata nei formati CorelDraw, PostScript o CAD, consente invece un ingrandimento migliore, poiché è costituita da forme geometriche generate matematicamente anziché da punti disposti in modo apparentemente "casuale".

Bps - Acronimo di "**B**its **P**er **S**econd" (bit al secondo). È la misura della velocità con cui i dati possono essere trasferiti da una posizione all'altra. Ad esempio, un modem a 33,6 kbps è in grado di trasferire 33.600 bit al secondo. Kilobit (1000 bit) al secondo e Megabit (1.000.000 bit) al secondo vengono abbreviati rispettivamente in "Kbps" e "Mbps".

Browser - Abbreviazione di "Web browser". Si tratta di un'applicazione utilizzata per visualizzare le pagine Web. È in grado di interpretare codice HTML, testo, collegamenti ipertestuali, immagini, JavaScript e così via. I browser più diffusi sono Internet Explorer e Netscape Communicator.

Byte - Set di bit (di solito otto) che rappresenta un singolo carattere. Un byte contiene 8 o più bit, a seconda della modalità di misurazione. Il termine "byte" viene abbreviato con una "b" maiuscola.

Cache - Esistono diversi tipi di cache, ma tutti vengono utilizzati per memorizzare i dati più recenti, così che a questi sia possibile accedere con maggiore rapidità in un secondo momento. Ad esempio, un browser Web utilizza una cache per memorizzare pagine, immagini, URL e altri elementi relativi a un sito Web visitato di recente. Quando si accede una seconda volta a una pagina memorizzata nella cache, il browser non deve scaricare di nuovo tali elementi. Poiché l'accesso alla cache sul disco fisso è molto più veloce dell'accesso a Internet, la consultazione delle pagine viene considerevolmente accelerata.

La cache IP di MDaemon memorizza l'indirizzo IP dei domini ai quali sono stati di recente recapitati messaggi. In questo modo, MDaemon non deve cercare nuovamente tali indirizzi per consegnare eventuali altri messaggi agli stessi domini. Questo consente di velocizzare in modo sostanziale il processo di recapito.

CGI - Acronimo di Common **G**ateway **I**nterface. Si tratta di un insieme di regole che descrivono il modo in cui un server Web comunica con altri programmi sullo stesso sistema e il modo in cui questi ultimi (i cosiddetti "programmi CGI") comunicano con il server Web. Un programma CGI è una qualunque applicazione che gestisce l'input e l'output in base allo standard CGI. Si tratta generalmente di un programma di piccole dimensioni che preleva i dati dal server Web e li elabora, ad esempio inserendo il contenuto di un modulo in un messaggio e-mail. I programmi CGI vengono spesso memorizzati nella directory "cgi-bin" di un sito Web e di solito sono visualizzati nell'URL utilizzato per accedervi.

cgi-bin - Il nome più comune per la directory di un server Web in cui sono memorizzati i programmi CGI. La porzione "bin" di "cgi-bin" è l'abbreviazione di "binary": precedentemente infatti numerosi programmi venivano considerati "binari". In realtà, la maggior parte dei programmi cgi-bin è costituita da file di testo, ovvero script eseguiti da programmi residenti altrove.

CIDR - Acronimo di "**C**lassless **I**nter-**D**omain **R**outing". Si tratta di un nuovo sistema di indirizzi IP che sostituisce il precedente, basato sulle classi A, B e C. Gli indirizzi IP CIDR hanno l'aspetto di normali indirizzi IP seguiti da una barra e da un numero, il cosiddetto prefisso IP. Ad esempio,

123.123.0.0/12

Il prefisso IP definisce il modo in cui molti indirizzi vengono coperti dall'indirizzo CIDR, con i numeri più bassi che coprono più indirizzi. Nell'esempio precedente il prefisso IP "/12" può essere utilizzato per indirizzare 4.096 indirizzi della precedente classe C.

Gli indirizzi CIDR riducono le dimensioni delle tabelle di instradamento e rendono più indirizzi IP disponibili all'interno delle organizzazioni.

Il sistema CIDR viene descritto nelle RFC 1517-1519, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Client - Programma utilizzato per accedere, nonché per ottenere e inviare dati da e a un programma *server*. Il server si trova di solito su un altro computer, che non deve necessariamente appartenere alla rete locale. Ciascun programma *client* è progettato per funzionare con uno o più tipi specifici di programmi *server*. Ciascun server richiede un tipo specifico di client. Un *browser* Web è un tipo specifico di client che comunica con i *server* Web.

Common Gateway Interface - Vedere CGI.

Cookie - Nella terminologia informatica, un *cookie* rappresenta una serie di dati inviati da un server Web al browser. Queste informazioni vengono salvate e successivamente utilizzate per diversi scopi, quando l'utente accede di nuovo allo stesso sito o ne visita una pagina diversa. Quando un server Web riceve da un browser Web una richiesta in cui è incluso un cookie, può utilizzare le informazioni del cookie per conseguire lo scopo per cui è stato progettato, ad esempio personalizzare i dati che invia all'utente o mantenere un registro delle richieste dell'utente. Di solito, i cookie vengono utilizzati per memorizzare password, nomi utente, preferenze, informazioni sui carrelli degli acquisti e altri dati associati al sito a cui i cookie corrispondono. In questo modo, il sito "riconosce" l'utente e riesce a tenere traccia delle relative attività.

A seconda delle impostazioni del browser, è possibile accettare o meno i cookie, nonché decidere per quanto tempo debbano essere conservati. I cookie sono in genere impostati per scadere dopo un determinato periodo e vengono preservati in memoria fino alla chiusura del browser, quando è possibile che vengano salvati sul disco.

I cookie **non** sono in grado di leggere dal disco rigido. Tuttavia, possono essere utilizzati per raccogliere informazioni sull'utente e le attività che questi esegue nel particolare sito a cui appartengono.

Connessione di accesso remoto - Componente di Windows che consente di connettere il computer alla rete mediante un modem. Se il computer non è connesso a una rete LAN con accesso a Internet, è necessario configurare l'accesso remoto (definito anche DUN, Dial-Up Networking) al fine di connettersi a un POP (Point of Presence) e accedere al provider di servizi Internet (o ISP, Internet Service Provider). Successivamente, sarà possibile ottenere l'accesso a Internet. Può essere necessario che il provider fornisca determinate informazioni, quali l'indirizzo del gateway e l'indirizzo IP del computer.

La connessione di accesso remoto è selezionabile facendo doppio clic sull'icona Risorse del computer. È possibile configurare un profilo di accesso differente per ciascun servizio online utilizzato. Una volta configurato, è possibile copiare sul desktop un collegamento al profilo. Per stabilire la connessione, sarà sufficiente doppio clic sull'icona del collegamento.

Predefinito - Termine utilizzato per fare riferimento al valore preimpostato per le opzioni dei programmi. Le impostazioni predefinite vengono utilizzate quando l'utente non specifica alcuna impostazione personalizzata. Ad esempio, l'impostazione predefinita per i caratteri in Netscape Communicator è "Times". L'impostazione

rimarrà invariata finché non viene modificata dall'utente. La maggior parte degli utenti si avvale in genere delle impostazioni predefinite.

I valori *predefiniti* vengono frequentemente utilizzati se un'impostazione personalizzata non funziona oppure se al programma mancano alcuni dati per completare un'operazione.

DHCP - Acronimo di "**D**ynamic **H**ost **C**ontrol **P**rotocol". I server di rete utilizzano questo protocollo per assegnare dinamicamente gli indirizzi IP ai computer in rete. Un server DHCP attende che un computer stabilisca la connessione, quindi assegna al computer un indirizzo IP prelevandolo da un elenco presente in memoria.

Il sistema DHCP viene descritto nella RFC-2131, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2131.txt

Gateway di dominio - Vedere Gateway più avanti.

Nome dominio - Nome univoco che identifica un sito Web su Internet. Ad esempio: "mdaemon.com" è il nome di dominio di MDaemon Technologies. Ciascun nome dominio contiene due o più porzioni separate da punti: la porzione all'estrema sinistra è la più specifica mentre quella all'estrema destra è la più generica. Ciascun nome dominio punta all'indirizzo IP di un solo server, ma un server può avere più nomi dominio. Ad esempio, "mail.mdaemon.com", "smtp.mdaemon.com" ed "esempio.com" possono puntare tutti allo stesso server di "mdaemon.com", ma "mdaemon.com" non può puntare a due server diversi. Esistono tuttavia dei metodi per specificare dei server alternativi a cui i client vengono reindirizzati se il server principale è guasto o non disponibile.

Comunemente un nome di dominio viene registrato ma non effettivamente connesso a un sistema. Di solito, questo si verifica perché il proprietario del nome di dominio non ha ancora creato il sito Web oppure perché desidera disporre di indirizzi di posta elettronica presso uno specifico dominio senza dover gestire un sito Web. In quest'ultimo caso, deve esistere un sistema Internet vero e proprio che gestisca la posta associata al nome dominio.

Infine, è frequente che il termine "nome dominio" venga abbreviato in "dominio". Tuttavia, poiché "dominio" ha altri significati e può fare riferimento ad altri elementi (ad esempio, un dominio di Windows NT o una classe di valori), è opportuno conoscere la distinzione al fine di evitare confusione.

I nomi dominio vengono descritti nelle RFC 1034-1035, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP — Sviluppato da MDaemon Technologies come componente del server MDaemon, DomainPOP consente di fornire servizi e-mail dalla casella postale POP di un singolo ISP per un'intera LAN o per un intero gruppo di lavoro. In precedenza, a meno che il server di posta elettronica di un'azienda non disponesse di una connessione a Internet permanente, l'unico modo per fornire i servizi di posta Internet a un gruppo di lavoro consisteva nell'assegnare a ciascun utente una

propria casella postale sull'ISP aziendale dalla quale l'utente poteva poi raccogliere la posta. Con DomainPOP è sufficiente una sola casella postale. Tutti i pool ISP inviano la posta per il nome di dominio dell'azienda alla casella postale dalla quale viene periodicamente raccolta da DomainPOP. Quindi, analizza la sintassi dei messaggi per determinarne i destinatari e distribuirli alle caselle postali degli utenti locali. Così i messaggi e-mail sono forniti per l'intera rete da un singolo account dialup ISP.

Download (o scaricamento) - Processo mediante il quale il computer ottiene o recupera i dati da un altro computer. Le informazioni, ad esempio, vengono ottenute da Internet *scaricandole* da altri computer. L'operazione opposta allo scaricamento è il *caricamento*. Per inviare dati a un altro computer, è necessario *caricarli* nel computer in questione.

Driver - Programma di dimensioni ridotte che comunica con un determinato dispositivo hardware. I driver contengono le informazioni necessarie al computer e ad altri programmi per controllare e riconoscere il dispositivo. Nei computer Windows spesso i driver sono contenuti in un file DLL (Dynamic Link Library). La maggior parte dei dispositivi hardware utilizzati dai computer Mac non richiede driver. Tuttavia, nel caso fosse necessario, il driver presenterebbe la forma di un'estensione di sistema.

DUN - Vedere Connessione di accesso remoto.

E-mail - Abbreviazione di **"**Electronic mail" (posta elettronica). Il termine compare anche nelle forme "E-mail", "Email", "e-mail" ed "email". Si tratta della trasmissione di messaggi di testo mediante le reti di comunicazione. La maggior parte delle reti dispone di un sistema e-mail. Alcuni sono confinati su una rete composta da un solo computer, altri dispongono di gateway per accedere a reti diverse (comunicazione con più posizioni specifiche) o a Internet (comunicazione con qualunque luogo del mondo).

La maggior parte dei sistemi e-mail include sia un *client e-mail* (definito anche *client di posta* o semplicemente *client*) contenente un editor di testo e altri strumenti per la composizione di messaggi, sia uno o più *server* che ricevono i messaggi dai client e li instradano alla destinazione appropriata. Di solito, un messaggio viene composto mediante il client, quindi trasferito al server per essere consegnato all'*indirizzo e-mail* specificato e infine instradato dal server a un altro server che si occupa della memorizzazione dei messaggi destinati a tale indirizzo. Se la destinazione del messaggio è un indirizzo locale di cui è responsabile il server originale, il messaggio può essere conservato su questo anziché essere instradato a un altro server. Infine, il destinatario del messaggio si connette al proprio server e ritira il messaggio mediante il proprio client e-mail. L'intero processo di trasferimento di un messaggio e-mail dal client al server di destinazione richiede solitamente pochi secondi o minuti.

Oltre al testo semplice, i messaggi e-mail possono contenere anche degli *allegati*, che possono essere costituiti da file di qualsiasi tipo: immagini, file di testo, file di programma, altri messaggi e-mail, e così via. Tuttavia, poiché la maggior parte dei sistemi e-mail supporta solo l'invio dei file di testo, gli allegati devono essere codificati (cioè, convertiti in formato di testo) prima di poter essere inviati, quindi decodificati quando raggiungono la destinazione finale. Questo processo viene di solito eseguito automaticamente dai client di posta di invio e di ricezione.

Tutti gli ISP offrono servizi e-mail. La maggior parte inoltre, supportando i gateway, consente di scambiare messaggi e-mail con altri sistemi di posta. Benché sistemi

diversi possano elaborare la posta utilizzando protocolli diversi gli uni dagli altri, esistono tuttavia standard comuni che consentono di scambiare messaggi con gli utenti di praticamente qualunque sistema.

Indirizzo e-mail - Nome o stringa di caratteri che identifica una specifica casella postale elettronica presente su una rete a cui è possibile inviare dei messaggi e-mail. Gli indirizzi e-mail rappresentano le posizioni a cui e da cui vengono inviati i messaggi e-mail. Gli indirizzi e-mail sono necessari ai server e-mail per instradare i messaggi alle destinazioni appropriate. Benché a diversi tipi di rete corrispondano diversi formati di indirizzi e-mail, su Internet tutti gli indirizzi e-mail hanno la forma seguente: "casellapostale@esempio.com".

Ad esempio:

```
Michele.Masone@altn.com
```

Client e-mail - Definito anche *client di posta* (o semplicemente *client*), il *client e-mail* è un'applicazione che consente di inviare, ricevere e gestire la posta elettronica. È chiamato client perché i sistemi e-mail sono basati su un'architettura client-server: il client viene utilizzato per comporre il messaggio e-mail e inviarlo a un server, che lo invia quindi al server del destinatario dal quale sarà recuperato dal client del destinatario. In genere, i client di posta elettronica sono applicazioni software separate installate sul computer dell'utente, ma prodotti come MDaemon contengono un client Webmail integrato che viene "servito" al browser Web dell'utente. In questo modo, è possibile utilizzare come client i browser senza doverne installare uno nel computer. Ne risulta una maggiore portabilità e una migliore efficienza del sistema e-mail.

Crittografia - Si tratta di una misura di *sicurezza* basata sulla codifica delle informazioni di un file, che possono quindi essere lette solo se decodificate o decrittografate. La crittografia viene spesso utilizzata nella posta elettronica per impedire che un messaggio eventualmente intercettato da una terza parte possa essere letto. Il messaggio viene crittografato in fase di invio e decifrato al momento della ricezione.

Ethernet - Il tipo più diffuso di connessione utilizzata nelle LAN (Local Area Network). Le forme di Ethernet più usate sono 10BaseT e 100BaseT. Una connessione Ethernet 10BaseT è in grado di trasferire i dati a una velocità pari a 10 mbps (megabit al secondo) via cavo o connessione wireless (senza fili). Una connessione Ethernet 100BaseT trasferisce i dati a una velocità massima di 100 mbps. Una connessione Ethernet Gigabit è in grado di effettuare trasferimenti a una velocità pari a 1000 mbps ed è utilizzata da alcuni computer Apple.

ETRN - Acronimo di **E**xtended **T**U**RN**. Si tratta di un'estensione al protocollo SMTP che consente a un server SMTP di inviare a un altro server SMTP, che ne conserva la posta, una richiesta di invio della posta, ossia di annullamento dell'accodamento dei messaggi. Poiché il solo SMTP non è in grado di richiedere la posta, generalmente richiesta mediante i protocolli POP e IMAP, il server SMTP che effettua la richiesta ETRN comunica al server remoto di avviare una sessione SMTP e di iniziare l'invio all'host specificato nella richiesta della posta memorizzata.

Il comando `TURN` utilizzato a tale scopo sollevava un rischio di sicurezza, poiché provocava l'inversione della direzione della sessione SMTP avviando immediatamente l'invio della posta memorizzata senza alcuna verifica o autenticazione dell'identità del

server che emetteva la richiesta. ETRN avvia una nuova sessione SMTP anziché invertirne la direzione. In questo modo, se il server che emette la richiesta è un host "mascherato", il server di invio tenta comunque di consegnare la posta al vero host. Attualmente, è in corso di valutazione la proposta di un nuovo standard. Questo dovrebbe introdurre il comando Authenticated TURN (ATRN), il quale, analogamente a TURN, inverte la direzione della sessione SMTP ma, diversamente da TURN, richiede prima l'autenticazione. Lo standard in questione è ODMR (On-Demand Mail Relay). MDaemon supporta sia ETRN che ATRN di ODMR.

Il sistema ETRN viene descritto nella RFC-1985, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1985.txt

Il sistema ODMR viene descritto nella RFC-2645, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ - Acronimo di "**F**requently **A**sked **Q**uestions". Si tratta di documenti in cui vengono raccolte le risposte alle domande sollevate più di frequente su un determinato argomento. Di solito vengono presentati in formato di elenco, in cui a ogni domanda segue la risposta corrispondente. Nelle FAQ più estese è probabile che tutte le domande vengano elencate all'inizio del documento con i riferimenti (o i collegamenti ipertestuali, nel caso delle FAQ su Internet) alla posizione di ciascuna coppia di domanda e risposta all'interno del documento. Le FAQ vengono spesso utilizzate prima di consultare il supporto tecnico e le istruzioni operative, in modo da risparmiare tempo.

File Transfer Protocol - Vedere FTP più avanti.

Firewall - Nella terminologia informatica, un *firewall* esiste quando si adottano delle misure di sicurezza (sia software che hardware) per suddividere una rete di computer in due o più parti o per limitarne l'accesso a determinati utenti. Ad esempio, è possibile consentire a chiunque di visualizzare la home page di un sito Web presente sulla rete ma autorizzare all'accesso ad alcune aree speciali solo specifici utenti. A prescindere dal metodo utilizzato (la richiesta di una password, la restrizione d'accesso per determinati indirizzi IP e così via), le aree speciali vengono definite "protette da firewall".

FTP - Acronimo di "**F**ile **T**ransfer **P**rotocol". Si tratta di un metodo particolarmente efficiente e alquanto diffuso per trasferire i file via Internet da un computer a un altro. A questo scopo, sono state sviluppate apposite applicazioni client/server, denominate "server FTP" e "client FTP" (uno dei client più diffusi è FileZilla). Di solito, i client FTP sono in grado di eseguire diverse altre funzioni oltre al semplice trasferimento dei file. Inoltre, alcuni browser Web includono il supporto per il File Transfer Protocol, benché talvolta tale supporto consenta solo lo scaricamento. In aggiunta, alcuni server FTP sono di tipo "anonymous" (anonimo), il che significa che chiunque può accedervi per scaricare i file, solitamente specificando "anonymous" come nome utente e il proprio indirizzo e-mail come password. Spesso, i siti FTP anonimi consentono di scaricare i file senza che l'utente esegua l'accesso: è sufficiente fare clic su un collegamento. Per i browser che supportano l'FTP, di solito è sufficiente connettersi al sito FTP specificando "ftp://..." anziché "http://..." nell'URL.

Il protocollo FTP viene descritto nella RFC-959, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc959.txt

Gateway - Componente hardware o software che converte i dati tra due applicazioni o reti dotate di protocolli diversi. Il termine "gateway" viene utilizzato anche per indicare qualsiasi metodo che consente di accedere da un sistema a un altro. Ad esempio, il provider di servizi Internet è un gateway per Internet.

Grazie alla funzionalità Gateway di dominio, il server di messaggistica MDaemon può fungere da gateway e-mail per altri domini. Opera infatti come intermediario, o gateway, raccogliendo la posta di un dominio e conservandola finché il dominio in questione non provvede a ritirarla. Si tratta di una funzione utile sia per i domini che non mantengono una connessione continua a Internet, sia per i domini che richiedono un server di backup nel caso il proprio sia soggetto a guasti.

GIF - Acronimo di "**G**raphics **I**nterchange **F**ormat". Si tratta del formato per i file di immagine più utilizzato su Internet. I file GIF utilizzano i colori indicizzati o una tavolozza composta da un determinato numero di colori, così che le dimensioni risultano estremamente ridotte, soprattutto quando l'immagine contiene grandi aree dello stesso colore. La dimensione ridotta velocizza il trasferimento dei file di immagine tra i sistemi e rende questo formato molto popolare su Internet. Poiché la formula di compressione GIF è stata originariamente sviluppata da CompuServe, spesso le immagini GIF vengono indicate come CompuServe GIF.

Interfaccia grafica utente - Vedere GUI.

GUI - Acronimo di "**G**raphical **U**ser **I**nterface" (Interfaccia grafica utente). La GUI rende possibile l'interazione con il computer o un'applicazione poiché impiega un dispositivo di puntamento per selezionare gli elementi grafici sullo schermo anziché richiedere di digitare del testo nella riga di comando. I sistemi operativi Microsoft Windows e Apple Mac sono entrambi basati su GUI, ma, benché introdotto originariamente da Apple, il concetto di interfaccia utente grafica è stato sviluppato da Xerox.

Host - Qualunque computer in rete che funge da server per gli altri computer della stessa rete. Il sistema host può essere eseguito come server Web, come server di posta o come servizio di altro tipo. Di norma, fornisce più servizi contemporaneamente.

Nelle reti peer-to-peer è frequente che i sistemi siano contemporaneamente host e client. Ad esempio, un computer può fungere da host per la stampante di rete ed essere simultaneamente utilizzato come client per raccogliere la posta e scaricare i file da un altro host.

HTML Acronimo di "**H**yper**t**ext **M**arkup **L**anguage". Si tratta del linguaggio di codifica utilizzato per creare i documenti ipertestuali presenti sul World Wide Web. In termini semplici, un documento HTML è un documento di testo semplice che contiene tag e codici di formattazione il browser web dell'utente interpreta e presenta come pagina Web completa di testo formattato e colori. Ad esempio, un browser che riceve un documento HTML contenente il testo "<B>Testo</B>" visualizza il termine "Testo" in grassetto. Poiché sono molto piccoli, i file di testo possono essere trasferiti molto rapidamente su Internet.

HTTP - Acronimo di **H**yper**t**ext **T**ransfer Protocol. Si tratta del protocollo utilizzato per trasferire i file *ipertestuali* tra i computer collegati a Internet. Il protocollo HTTP richiede un programma client a un'estremità (di solito, un browser Web) e un server HTTP all'altra.

Il protocollo FTP viene descritto nella RFC-2616, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2616.txt

Ipertesto - Qualunque testo che contiene un collegamento ipertestuale a un altro documento o a un altro punto dello stesso documento. Talvolta, il testo viene definito collegamento ipertestuale, collegamento o link. L'ipertesto può essere costituito da una parola o da una frase e incorpora il collegamento in modo che, facendo clic su di esso, l'utente può spostarsi in corrispondenza del punto "contrassegnato" o visualizzare il documento collegato. Di solito, i collegamenti ipertestuali sono evidenti perché il testo è sottolineato e di colore diverso, anche se questo non è obbligatorio. In alcuni casi, l'ipertesto non presenta un aspetto diverso dal testo normale, ma in genere risulta distinguibile dalla variazione grafica del puntatore che consegue dal posizionamento del mouse sul testo che funge da collegamento.

Hypertext Markup Language - Vedere HTML.

IMAP - Sviluppato dall'università di Stanford, il protocollo IMAP, **I**nternet **M**essage **A**ccess **P**rotocol viene utilizzato per gestire e recuperare i messaggi e-mail. La versione più recente è IMAP4 ed è simile a POP3, pur includendo una serie di caratteristiche aggiuntive. IMAP4 è particolarmente conosciuto come protocollo utilizzato per gestire la posta sul server anziché sul sistema locale dell'utente: i messaggi possono essere cercati in base alle parole chiave, organizzati in cartelle e specificamente selezionati per essere scaricati o per consentire altre funzioni mentre si trovano ancora sul server. Il protocollo IMAP risulta meno impegnativo per il sistema dell'utente. Inoltre, centralizza la posta elettronica, consentendo così di accedervi da posizioni diverse.

Il protocollo IMAP viene descritto nella RFC-2060, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2060.txt

Estensione IMAP4 ACL - Vedere ACL.

Internet - Internet è stata creata nel 1969 dall'esercito degli Stati Uniti, originariamente come rete di comunicazione indistruttibile in caso di conflitto nucleare. Oggi è costituita da milioni di computer e reti in tutto il mondo. Internet è decentralizzata, ovvero non è controllata da alcuna azienda, organizzazione o nazione. Ciascun host (o computer) su Internet è indipendente dagli altri ed è in grado di fornire qualsiasi informazione o servizio reso disponibile dai propri operatori. Ciononostante, la maggior parte delle informazioni trasferite su Internet in qualche punto passa attraverso delle "dorsali", connessioni a larga banda e ad alta velocità, controllate dai maggiori provider e dalle maggiori organizzazioni. La maggior parte degli utenti accede a Internet attraverso un servizio online come AOL o per mezzo di un provider di servizi Internet (ISP, Internet Service Provider), che gestisce o si connette a una di queste dorsali.

Molti credono che il *World Wide Web* (WWW) e Internet siano la stessa cosa, ma non è così. Il World Wide Web è solo una parte di Internet. Si tratta della parte di Internet più visibile e conosciuta, generalmente gestita e strutturata in base a dettati commerciali, ma non coincide con l'interezza di Internet.

Intranet - In termini semplici, un'intranet è una piccola Internet privata utilizzata solo all'interno della rete di un'azienda o di un'organizzazione. Benché varino sensibilmente da un'organizzazione all'altra, le intranet possono integrare qualunque funzione disponibile su Internet. Possono ad esempio includere sistemi e-mail, directory di file, pagine Web da consultare, articoli da leggere e così via. La differenza principale tra un'intranet e Internet risiede nel fatto che un'intranet è relativamente piccola e comunque confinata a un'organizzazione o un gruppo.

IP - Acronimo di "**I**nternet **P**rotocol", come in TCP/IP. I protocolli Internet rendono possibile il trasferimento dei dati tra i diversi sistemi connessi a Internet. Indipendentemente dalla piattaforma o sistema operativo di ciascun computer,se viene utilizzato lo stesso protocollo Internet da tutti i computer, sarà possibile lo scambio di dati tra i vari computer. Il termine "IP" viene spesso utilizzato come ulteriore abbreviazione di "indirizzo IP". Lo standard corrente del protocollo Internet è IP versione 4 (IPv4).

Il protocollo Internet viene descritto nella RFC-791, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc791.txt

Indirizzo IP - Talvolta definito anche numero IP, l'indirizzo IP (**I**nternet **P**rotocol) viene utilizzato per identificare una specifica rete TCP/IP e gli host o i sistemi che la compongono. Si tratta di un indirizzo numerico a 32 bit contenente quattro numeri compresi tra 0 e 255, separati da punti, ad esempio "127.0.0.1". All'interno di una rete isolata, ciascun nome di computer deve avere un indirizzo IP univoco, a volte assegnato in modo casuale. In Internet ogni computer deve invece disporre di un indirizzo IP registrato per evitare duplicazioni. Gli indirizzi IP di Internet possono essere statici o dinamici. I primi non cambiano e rappresentano sempre la stessa posizione o lo stesso sistema su Internet. I secondi cambiano e vengono solitamente assegnati da un ISP a quei computer che si trovano su Internet solo temporaneamente (ad esempio, quando un utente accede a Internet mediante un account di accesso remoto). Tuttavia, è possibile che a un account di accesso remoto venga assegnato un indirizzo IP statico.

I provider e le grandi organizzazioni cercano di solito di acquisire una gamma o un set di indirizzi IP dall'InterNIC Registration Service, in modo che tutti i client o gli utenti delle proprie reti abbiano indirizzi simili. Questi set vengono suddivisi in tre classi: A, B e C. I set di classe A e B vengono utilizzati dalle organizzazioni molto grandi e supportano rispettivamente 16.000.000 e 65.000 host. I set di classe C sono destinati alle reti più piccole e supportano 255 host. Poiché i set di classe A e B sono oggi molto difficili da ottenere a causa della scarsità di indirizzi disponibili, gran parte delle aziende devono accontentarsi dei set di classe C. A causa di questa scarsità di indirizzi IP, un nuovo protocollo per gli indirizzi IP, denominato CIDR (Classless Inter-domain Routing), sta gradualmente sostituendo quello classico.

Il protocollo Internet standard corrente, Ipv4, viene descritto nella RFC-791, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc791.txt

Il protocollo Internet versione 6 (IPv6) viene descritto nella RFC-2460, consultabile all'indirizzo

http://www.rfc-editor.org/rfc/rfc2460.txt

Il protocollo CIDR viene descritto nelle RFC 1517-1519, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Numero IP - Vedere *Indirizzo IP*.

ISP - **I**nternet **S**ervice **P**rovider (Provider di servizi Internet). L'ISP, o più comunemente il provider, è un'azienda che fornisce accesso e servizi Internet agli utenti finali. La maggior parte degli ISP fornisce ai propri clienti più servizi Internet, ad esempio l'accesso al World Wide Web, la posta elettronica, l'accesso ai newsgroup e ai server news e così via. In genere, gli utenti si collegano all'ISP mediante una connessione di accesso remoto o di altro tipo. Successivamente, l'ISP collega gli utenti a un router, che a sua volta li instrada alla dorsale Internet.

Java - Sviluppato da Sun Microsystems, Java è un linguaggio di programmazione orientato alle reti con una sintassi molto simile a quella di C/C++, ma strutturata sulle classi anziché sulle funzioni. Nelle applicazioni Internet viene comunemente utilizzato per programmare le applet, ovvero i piccoli programmi incorporati nelle pagine Web. Questi programmi possono essere scaricati automaticamente ed eseguiti dal browser di un utente al fine di fornire una vasta gamma di funzioni, che non sarebbero possibili con l'utilizzo del semplice HTML o di altri linguaggi di script e senza il rischio di infezioni da virus o danni al computer. Poiché Java è sia efficiente che facile da utilizzare, sta diventando molto popolare tra gli sviluppatori software e hardware.

JavaScript - Da non confondersi con Java. JavaScript è stato sviluppato da Netscape come linguaggio di script progettato per estendere le capacità dell'HTML e creare pagine Web interattive. Si tratta di un linguaggio di programmazione semplificato, più facile da utilizzare rispetto a Java e ad altri linguaggi, ma anche più limitato. Nonostante i limiti, si rivela molto utile per aggiungere elementi interattivi ai siti Web. Ad esempio, JavaScript può essere efficientemente utilizzato quando si desidera che i dati vengano pre-elaborati prima di essere inviati al server oppure che le pagine rispondano all'interazione da parte dell'utente con collegamenti o altri elementi di forma. Può inoltre essere utilizzato per controllare i plug-in e le applet che si basano sulle selezioni dell'utente, nonché per eseguire numerose altre funzioni. JavaScript è incluso nel testo dei documenti HTML e, affinché le funzioni vengano eseguite, deve essere interpretato dai browser Web.

JPEG - Formato di file grafico più efficiente del GIF nella compressione delle immagini a 65.536 colori e di quelle fotografiche. Mentre il formato GIF rappresenta la soluzione ottimale per le immagini contenenti forme regolari e grandi aree di motivi di colore ripetuti, il JPEG risulta più adatto per le immagini con motivi irregolari e grandi

quantità di colori. JPEG è il formato più utilizzato per le immagini a 65.536 colori e le immagini fotografiche su Internet. È l'acronimo di "**J**oint **P**hotographic **E**xperts **G**roup", il gruppo che ha sviluppato il formato.

Kbps - Unità di misura utilizzata comunemente per le velocità dei modem (ad esempio, 56 Kbps). È l'acronimo di "**K**ilo**b**its **P**er **S**econd (kilobit al secondo)". Misura la quantità di kilobit (1000 bit) di dati che vengono spostati o elaborati ogni secondo. Si tratta di *kilobit* e non di *kilobyte*: la dimensione di un kilobyte è infatti otto volte quella di un kilobit.

Kilobyte - Un kilobyte (abbreviato in K o KB) corrisponde a mille byte di dati. Tecnicamente, equivale a 1024 byte (2^10 = 1024), tuttavia nell'uso comune viene solitamente approssimato a 1000.

LAN - Una LAN (**L**ocal **A**rea **N**etwork) è una rete di computer limitata a un singolo edificio o area, i cui nodi (computer o workstation) sono di solito connessi l'uno con l'altro con una configurazione di fili, cavi o altri tipi di supporto. La maggior parte delle grandi aziende dispone di reti LAN, poiché semplificano considerevolmente la gestione e la condivisione delle informazioni tra i dipendenti e gli uffici. La maggior parte delle reti LAN utilizza un sistema e-mail o chat e condivide i dispositivi, ad esempio le stampanti, che non devono pertanto essere installati in ogni stazione. Quando i nodi della rete sono connessi mediante linee telefoniche, onde radio o collegamenti satellitari, la LAN viene definita WAN (Wide Area Network).

Latenza - Tempo impiegato da un pacchetto di dati per spostarsi lungo una connessione di rete. Mentre un pacchetto di dati viene inviato, si sviluppa un tempo "latente" durante il quale il computer mittente attende conferma dell'avvenuta ricezione del pacchetto. Insieme alla larghezza di banda, la latenza è uno dei fattori che determinano la velocità di una connessione.

LDAP - Acronimo di **L**ightweight **D**irectory **A**ccess Protocol. Si tratta di una versione semplificata del protocollo per servizi di elenchi in linea DAP (Directory Access Protocol). Il sistema di directory è una struttura gerarchica composta dai livelli seguenti: la directory principale o iniziale, il Paese, l'organizzazione, l'unità organizzativa e l'individuo all'interno dell'unità. Ogni voce LDAP è una raccolta di attributi con un identificatore univoco, definito DN (Distinguished Name). Poiché si tratta di un protocollo aperto e distribuibile su più server, LDAP può in ultima analisi consentire a qualunque applicazione o piattaforma in qualunque parte del mondo di accedere alle informazioni dell'elenco in linea per individuare gli indirizzi e-mail, le organizzazioni, i file e così via.

Il protocollo LDAP viene descritto nella RFC-2251, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2251.txt

Link - Vedere *Ipertesto*.

Server list - Applicazione server utilizzata per distribuire i messaggi e-mail a più destinatari specificando un solo indirizzo. In termini semplici, quando viene indirizzato a una *lista di distribuzione* gestita dal server list, un messaggio e-mail viene automaticamente trasmesso a tutti i membri della lista. Le liste di distribuzione hanno di solito un solo indirizzo e-mail normale (ad esempio, nomelista@esempio.com), che fa riferimento a un intero elenco di destinatari anziché a una persona o a una casella

postale specifica. Quando un utente *si iscrive* a una lista di distribuzione, il server list ne aggiunge automaticamente l'indirizzo alla lista e distribuisce i futuri messaggi diretti alla lista a tale indirizzo (o membro) e a tutti gli altri. Quando un utente annulla l'iscrizione, il server list semplicemente rimuove l'indirizzo, in modo che non riceva più messaggi di lista.

Spesso, il termine "listserv" viene genericamente usato per indicare il server di una lista di distribuzione. Tuttavia, Listserv® è un marchio registrato di L-Soft international, Inc. ed è un programma specifico sviluppato da Eric Thomas di BITNET nel 1986. Oltre ad altri list server, MDaemon è dotato di un'intera suite di funzionalità per i list server o le liste di distribuzione.

Logon - Codice univoco o serie di caratteri da utilizzare per ottenere l'accesso o identificarsi presso un server o un computer. Nella maggior parte dei casi, l'accesso viene consentito solo se al nome di logon viene associata una password.

Esistono numerosi sinonimi di "logon", come *login*, *nomeutente*, *nome utente*, *ID utente*, *accesso* e altri, ad esempio "*accedo* al server della posta". In tale contesto, tuttavia, resta più corretto dire "eseguo il *logon* al server della posta".

Casella postale - Area della memoria o di un dispositivo di memorizzazione assegnata a uno specifico indirizzo e-mail, in cui vengono archiviati i messaggi e-mail. A prescindere dal tipo di sistema e-mail in uso, ciascun utente dispone di una casella postale privata in cui vengono memorizzati i messaggi man mano che il server di posta li riceve. Il termine "casella postale" viene spesso utilizzato per indicare la porzione alla destra di un indirizzo e-mail. Ad esempio, "utente01" in "utente01@esempio.com" rappresenta la casella di posta, mentre "esempio.com" è il nome di dominio.

Lista di distribuzione - Definita anche gruppo e-mail, la lista di distribuzione è un elenco o un gruppo di indirizzi e-mail identificati da un unico indirizzo e-mail, ad esempio "nomelista@esempio.com". Di solito, quando il server delle liste riceve un messaggio e-mail indirizzato a una delle proprie liste di distribuzione, il messaggio viene automaticamente distribuito a tutti i membri della lista, ovvero agli indirizzi inclusi nella lista. MDaemon è dotato di una vasta gamma di funzioni di gestione delle liste di distribuzione che possono essere utilizzate per rendere le liste pubbliche o private (l'invio dei messaggi è aperto a chiunque o riservato ai soli membri) oppure moderate (ogni messaggio deve essere approvato da qualcuno prima di essere inviato alla lista), nonché per inviarle in formato riassunto o come messaggi singoli.

Megabyte - Benché dal punto di vista tecnico corrisponda a 1.048.576 byte (o 1024 kilobyte), un megabyte è generalmente approssimato a un milione di byte. Megabyte è abbreviato in "MB", come in "20 MB".

MIME - Definito nel 1992 dalla Internet Engineering Task Force (IETF), il MIME (**M**ultipurpose **I**nternet **M**ail **E**xtensions) è un metodo di codifica standard utilizzato per allegare i file non testuali ai messaggi e-mail standard. Poiché di solito solo i file di testo semplice possono essere trasferiti via e-mail, i file non testuali devono essere dapprima codificati in formato di testo semplice, quindi decodificati una volta raggiunta la propria destinazione. Pertanto, un programma e-mail viene considerato compatibile con MIME se invia e riceve i file mediante lo standard MIME. Quando viene inviato un allegato con codifica MIME, come parte del messaggio vengono di solito specificati sia il tipo di file inviato che il metodo da utilizzare per ripristinarne la

forma originale. Esistono molti tipi di contenuto MIME predefiniti, ad esempio "image/jpeg" e "text/plain". È tuttavia possibile definire anche dei tipi MIME personalizzati.

Lo standard MIME viene utilizzato anche dai server Web per identificare i file inviati ai browser Web. Poiché supportano vari tipi di MIME, i browser Web sono in grado di visualizzare o produrre file in formato non HTML. Inoltre, aggiornando gli elenchi MIME-Types del browser e del software utilizzato per la gestione di ciascun tipo, è possibile supportare immediatamente nuovi formati di file.

Il sistema MIME viene descritto nelle RFC 2045-2049, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

Mirror - Server, di solito di tipo FTP, in cui è contenuta una copia dei file presenti su un altro server. Viene in genere utilizzato per fornire una posizione alternativa da cui scaricare i file, se il server originale diventa indisponibile. Il termine "mirror" (specchio) fa anche riferimento a una configurazione in cui le informazioni vengono scritte su più dischi fissi contemporaneamente . Di norma, tale configurazione viene utilizzata come misura di ridondanza per consentire il funzionamento del sistema e impedire la perdita di dati importanti nel caso si verifichi un guasto in uno dei dischi.

Modem - Acronimo derivato da **mo**dulator-**dem**odulator. Si tratta di un dispositivo connesso a un computer che consente di trasferire dati ad altri computer tramite le linee telefoniche. Il modem converte in formato analogico (modulazione) i dati digitali del computer e successivamente li trasferisce a un altro modem, che esegue l'operazione inversa (demodulazione). In altri termini, il modem è un convertitore da analogo a digitale e viceversa. La velocità con cui vengono trasferiti i dati viene espressa sia in termini di velocità in baud, ad esempio 9.600 baud, sia in termini di kilobit al secondo, ad esempio 28,8 kbps.

MultiPOP — Un componente di MDaemon che può essere configurato per raccogliere la posta con il protocollo POP3, contemporaneamente da diversi server e-mail, per conto degli utenti MDaemon. In questo modo, i titolari degli account di MDaemon provvisti di altri account e-mail su server e-mail diversi possono raccogliere la posta con l'e-mail dell'account di MDaemon in modo da archiviare tutti i messaggi e-mail in un'unica cassetta postale.

NAT - Acronimo di Network Address Translation. Vedere Conversione degli indirizzi di rete più avanti.

Rete - Due o più computer connessi tra loro. Una rete viene appositamente progettata per consentire la condivisione di risorse e di informazioni tra più sistemi.

Ne sono esempi significativi i sistemi composti da più computer che condividono stampanti, unità DVD-ROM o dischi fissi.

Esistono molti tipi di rete, ma le più diffuse sono le LAN (Local Area Network) e le WAN (Wide Area Network). In una LAN, i singoli computer (detti nodi) sono vicini geograficamente, spesso nello stesso edificio. Inoltre, sono solitamente connessi direttamente mediante cavi, benché ultimamente si stiano affermando anche le connessioni senza fili. I nodi di una WAN sono di solito più lontani (ubicati in edifici o città diverse) e connessi mediante linee telefoniche, collegamenti satellitari o altri mezzi.

Internet è una rete, spesso indicata come rete di reti.

Conversione degli indirizzi di rete - Definita anche NAT (Network Address Translation). Si tratta di un sistema che consente a un'unica rete di utilizzare due set di indirizzi IP: uno per il traffico esterno e uno per quello interno. Questo tipo di sistema viene principalmente utilizzato come firewall per la sicurezza della rete. Il computer di un utente mostra ai computer esterni alla LAN un determinato indirizzo IP, mentre l'indirizzo IP effettivo è completamente diverso. I sistemi hardware o software posti tra la rete e Internet eseguono le conversioni tra i due indirizzi. Grazie a questo metodo, è probabile che più computer in una LAN possano condividere un unico indirizzo IP aziendale. In questo modo, nessuno al di fuori della rete è in grado di conoscere l'indirizzo del computer di un utente o collegarvisi se non è stato autorizzato o autenticato durante la conversione.

Scheda di interfaccia di rete - Definita anche NIC (Network Interface Card). Si tratta di una scheda a circuito che consente a un computer di collegarsi a una rete. Le schede NIC forniscono connessioni di rete permanenti, mentre i modem (utilizzati per collegare in rete con accesso remoto gran parte dei computer domestici) forniscono di solito solo connessioni temporanee. La maggior parte delle schede NIC è progettata per tipi specifici di reti e protocolli, quali Ethernet o Token Ring e TCP/IP.

Network News Transfer Protocol - Vedere NNTP più avanti.

NIC - Acronimo di Network Interface Card. Vedere Scheda di interfaccia di rete.

NNTP - Acronimo di **N**etwork **N**ews **T**ransfer Protocol. Si tratta del protocollo utilizzato per trasferire e distribuire i messaggi nei newsgroup USENET. I browser e i client e-mail più diffusi incorporano client NNTP.

Il sistema NNTP viene descritto nella RFC-977, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc977.txt

Nodo - Qualunque computer singolo connesso a una rete.

ODMR - Acronimo di On-**D**emand **M**ail **R**elay è un nuovo protocollo che consente ai server di posta che dispongono solo di una connessione intermittente a un provider di servizi, e che non sono dotati di un indirizzo IP statico, di ricevere la posta in modo simile ai server che invece ne dispongono e utilizzano il comando `ETRN`. Se il sistema è dotato di indirizzo IP statico, è possibile utilizzare il comando ESMTP ETRN. Tuttavia, i sistemi sprovvisti di indirizzi IP dinamici non dispongono di una soluzione efficace. ODMR risolve questo inconveniente. Tra le altre cose, ODMR introduce il

comando Authenticated TURN (ATRN) che causa l'inversione del flusso di una sessione SMTP (come il precedente comando TURN) ma con la sicurezza aggiunta di richiedere l'autenticazione del server richiedente. In questo modo, un server SMTP con un indirizzo IP dinamico è in grado di connettersi al proprio ISP e ricevere la posta di uno o più host mediante SMTP anziché raccoglierla mediante POP o IMAP. In questo modo, è possibile fornire una soluzione a basso costo alle aziende che richiedono un server proprietario, ma non possono permettersi un indirizzo IP statico o una presenza online dedicata.

Il sistema ODMR viene descritto nella RFC-2645, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM - Acronimo di **O**riginal **E**quipment Manufacturer. Si tratta di un termine spesso confuso e frainteso. Un OEM è un'azienda che utilizza l'attrezzatura o i prodotti di un'altra azienda nei propri prodotti, confezionati e venduti con un marchio o un nome aziendale diverso. Ad esempio, HyperMegaGlobalCom, Inc. è un OEM, poiché acquista componenti di computer da uno o più produttori diversi, li assembla in un unico prodotto personalizzato e li rivende sotto il marchio "HyperMegaGlobalCom". L'azienda che ha venduto i propri componenti a HyperMegaGlobalCom può essere anch'essa un OEM, se a sua volta ha acquistato i componenti da un altro produttore. Il termine "OEM" è utilizzato spesso in modo improprio, perché gli OEM non sono in realtà i produttori originali, bensì le aziende che "personalizzano" il software o lo incorporano nei propri prodotti. Ciononostante, il termine "OEM" viene spesso utilizzato per fare riferimento ai produttori hardware.

Al volo - Il termine "al volo" (talvolta anche "on the fly") ha di solito due significati. Nel primo caso, indica un'operazione che può essere effettuata "di fretta" o facilmente durante l'esecuzione di un'altra operazione. Ad esempio, un prodotto per la creazione dei segnalibri può supportare la creazione di account "al volo" durante l'immissione di cifre relative alle vendite, come "Interrompere l'immissione delle cifre, fare clic sul pulsante X, immettere un nome, quindi continuare con l'immissione di altre cifre". Un'operazione viene definita "al volo" anche quando può essere generata dinamicamente o automaticamente anziché manualmente o staticamente. Ad esempio, utilizzando le informazioni memorizzate in un "cookie", è possibile generare "al volo" una pagina Web personalizzata, non appena un utente accede di nuovo a un sito Web. Anziché richiedere la creazione manuale di una pagina personalizzata in base ai gusti dell'utente, la pagina viene generata dinamicamente in base alle operazioni eseguite dall'utente durante la navigazione.

Original Equipment Manufacturer - Vedere OEM.

Pacchetto - Unità di dati informatici inviati su una rete. I dati che si ricevono da un altro computer connesso alla LAN o a Internet hanno la forma di "pacchetti". Il file o il messaggio originale viene dapprima suddiviso in pacchetti, quindi trasmesso e infine ricombinato, quando raggiunge la destinazione finale. Ogni pacchetto include un'intestazione contenente l'origine e la destinazione, un blocco di dati e un codice di verifica degli errori. Al pacchetto viene inoltre assegnato un numero, con cui è possibile collegarlo ai pacchetti correlati inviati. Il processo di invio e ricezione dei pacchetti è noto come "commutazione di pacchetto". I pacchetti sono denominati anche "datagrammi".

Commutazione di pacchetto - Processo di invio e ricezione di pacchetti su una rete o su Internet. A differenza della commutazione di circuito, ad esempio quella dei telefoni analogici, che invia i dati con un flusso continuo su un singolo percorso o circuito, la commutazione di pacchetto trasmette i dati suddividendoli in "pacchetti", che non seguono necessariamente lo stesso percorso per giungere a destinazione. Inoltre, poiché i dati sono in unità separate, più utenti possono contemporaneamente inviare file diversi sullo stesso percorso.

Parametro - Un parametro è una caratteristica o un valore. In termini di elaborazione, rappresenta qualunque valore che viene passato a un programma da un utente o da un altro programma. Sono parametri i nomi, le password, le impostazioni, le dimensioni dei font e così via. In termini di programmazione, un parametro è un valore che viene passato a una subroutine o a una funzione per l'elaborazione.

PDF - Acronimo di **P**ortable **D**ocument Format. Si tratta di un formato di file multi-piattaforma a elevata compressione sviluppato da Adobe Systems Incorporated, in grado di catturare la formattazione, il testo e le immagini dei documenti creati con una vasta gamma di applicazioni. Diversamente da molti elaboratori di testo, consente di ottenere una visualizzazione e una stampa fedeli di un documento su più computer e piattaforme diverse. La visualizzazione dei file PDF richiede Adobe Acrobat Reader, un'applicazione distribuita gratuitamente da Adobe Systems. È comunque disponibile anche un plug-in che consente di visualizzare i file PDF direttamente nel browser Web. Il plug-in consente di visualizzare i file PDF pubblicati su un sito Web in modo diretto, senza che sia necessario scaricarli e aprirli con un programma separato.

Analisi sintattica - In campo linguistico, l'analisi sintattica è la suddivisione di una struttura linguistica nei suoi componenti grammaticali, ad esempio verbi, aggettivi e sostantivi.

In informatica, per analisi sintattica (o "parsing") si intende la suddivisione di un'istruzione in parti che possono rivelarsi utili per il computer. Un analizzatore sintattico (o "parser") di un compilatore suddivide ciascuna istruzione scritta da uno sviluppatore in parti che possono essere utilizzate per sviluppare ulteriori operazioni o per creare le istruzioni che compongono un programma eseguibile.

MDaemon e altri prodotti effettuano spesso l'analisi sintattica dei messaggi e-mail per determinarne la destinazione o per elaborarli mediante filtri e altri strumenti.

Ping - Acronimo di **P**acket **In**ternet **G**roper. Si tratta di un programma Internet di base che determina se un determinato indirizzo IP è raggiungibile e accetta le richieste. Questa analisi viene eseguita inviando una richiesta ECHO ICMP (Internet Control Message Protocol) a cui deve seguire una risposta. Per eseguire il "ping" di un indirizzo IP, è sufficiente digitare "ping" seguito dall'indirizzo IP o dal dominio sul prompt dei comandi DOS, ad esempio "Ping 192.0.2.0."

I protocolli ICMP ed Echo vengono descritti rispettivamente nella RFC-792 e nella RFC-862, consultabili su Internet agli indirizzi:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP - Acronimo di **P**ost **O**ffice **P**rotocol. Il protocollo POP (spesso indicato anche come POP3) è il protocollo e-mail più utilizzato per ritirare i messaggi da un server e-mail. La maggior parte dei client e-mail utilizza il protocollo POP, benché alcuni supportino anche il più recente protocollo IMAP. POP2, diventato uno standard verso la metà degli anni Ottanta, richiedeva SMTP per l'invio dei messaggi. La versione con cui è stato sostituito, ovvero POP3, può essere utilizzata anche senza SMTP.

Il protocollo POP3 viene descritto nella RFC-1939, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1939.txt

Porta - Nelle reti TCP/IP e UDP e su Internet, la porta costituisce il punto finale di una connessione logica ed è identificata da un numero compreso tra 0 e 65536. Le porte da 0 a 1024 sono riservate per alcuni protocolli e servizi privilegiati. Di solito, i server Web sono presenti sulla porta 80, i server SMTP comunicano mediante la porta 25 e i server POP inviano e ricevono la posta mediante la porta 25. In genere, una determinata porta su ciascun sistema può essere utilizzata da un solo programma alla volta. Quando si naviga in Internet, è probabile che alcuni server vengano eseguiti su porte non predefinite. In questi casi, è necessario specificare la porta nell'URL, preceduta da un segno di due punti. Ad esempio, "www.esempio.com:3000".

Una porta può essere utilizzata anche per fare riferimento ai socket di un computer utilizzato per la connessione di periferiche e altri dispositivi hardware, ad esempio porte seriali, porte parallele o porte USB.

Infine, il concetto di porting (in inglese, "to port") viene spesso impiegato per descrivere il processo in base al quale un programma progettato per una piattaforma specifica viene eseguito su un'altra piattaforma.

Post - Nella messaggistica Internet, indica un singolo messaggio immesso nel sistema di comunicazione di rete per essere condiviso, ad esempio un messaggio visualizzato in un newsgroup, in una lista di distribuzione o in un forum.

PPP - Acronimo di "Point to Point Protocol". Si tratta dello standard Internet per le connessioni di accesso remoto. PPP è un set di regole che definisce il modo in cui la connessione via modem scambia i pacchetti di dati con gli altri sistemi su Internet.

Il protocollo PPP viene descritto nella RFC-1661, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocollo - In informatica, un protocollo è costituito da un set di indicazioni o standard in base a cui comunicano i server e le applicazioni. Esistono numerosi tipi di protocollo, utilizzati per scopi diversi: TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP e così via.

Registro - Database utilizzato da Microsoft Windows per memorizzare le informazioni di configurazione relative al software installato nel computer, ad esempio le impostazioni personalizzate, le associazione delle estensioni dei file, gli sfondi del desktop, gli schemi colori e così via. Il registro è suddiviso nelle seguenti parti:

HKEY_User - Memorizza le informazioni relative a ciascun utente del sistema.

HKEY_Current_User - Memorizza le preferenze dell'utente corrente.

HKEY_Current_Configuration - Memorizza le impostazioni dello schermo e delle stampanti.

HKEY_Classes_Root - Include le associazioni dei file e le informazioni OLE.

HKEY_Local_Machine - Memorizza le impostazioni per l'hardware, il sistema operativo e le applicazioni installate.

HKEY_Dyn_Data - Include i dati relativi alle prestazioni.

Quando si installano dei programmi nel computer, il programma di installazione scrive automaticamente alcune informazioni nel registro. Anche se il registro può essere modificato manualmente, è preferibile utilizzare il programma regedit.exe fornito da Windows. Si consiglia di eseguire questa operazione con attenzione perché la modifica non corretta di un'impostazione può dare origine a gravi malfunzionamenti del computer.

RFC - Acronimo di **R**equest **F**or Comments. Si tratta del nome assegnato al processo di creazione di uno standard su Internet e al relativo risultato. Ogni nuovo standard o protocollo viene proposto e pubblicato su Internet sotto forma di "Request For Comments" (Richiesta di commenti). L'IETF (Internet Engineering Task Force) promuove il dibattito sul nuovo standard, che diventa ufficiale solo successivamente. Anche quando è perfettamente definito e non vengono più richiesti commenti, lo standard conserva l'acronimo RCF insieme al numero di identificazione. Ad esempio, RFC-822 (ora sostituito da RFC-2822) è lo standard ufficiale, o RFC, per l'e-mail. Tuttavia, ai protocolli ufficialmente adottati come "standard" è comunque associato un numero standard ufficiale, riprodotto nel documento Internet Official Protocol Standards (il quale è a sua volta indicato come STD-1 e, correntemente, come RFC-3700). È possibile trovare RFC su Internet in molti siti, ma la fonte autorevole è The RFC Editor, all'indirizzo http://www.rfc-editor.org/.

Il documento Internet Official Protocol Standards è consultabile all'indirizzo:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF - Acronimo di **R**ich **T**ext Format. Si tratta di un formato di file universale sviluppato da Microsoft e supportato da quasi tutti gli elaboratori di testo. A differenza del formato di testo semplice, il formato RTF consente di conservare la formattazione, le informazioni sui font, il colore del testo e così via. La dimensione dei file RTF può essere molto superiore a quella di altri formati, quali il formato di Microsoft Word (*.doc e *.docx) e Adobe PDF.

Server - Computer o programma che fornisce uno specifico tipo di servizio al software client in esecuzione su altri computer. Il termine può fare riferimento a un particolare software, ad esempio un server SMTP, oppure a un sistema su cui quel software viene eseguito. Su un singolo *sistema* server possono essere in esecuzione più *programmi* server. Ad esempio, sul server di una rete possono essere contemporaneamente in esecuzione un server Web, un server e-mail, un server FTP, un server fax e altri ancora.

SMTP - Acronimo di **S**imple **M**ail **T**ransfer **P**rotocol. Si tratta del protocollo principale utilizzato per inviare la posta elettronica su Internet da un server all'altro o da un client a un server. Il protocollo SMTP è composto da un insieme di regole con cui

viene gestita l'interazione tra un programma che invia i messaggi e un programma che li riceve. Una volta che un server ha ricevuto dei messaggi via SMTP, li conserva finché non vengono ritirati da un client mediante il protocollo POP, IMAP o altro.

Il sistema SMTP viene descritto nella RFC-2821, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam - Posta indesiderata su Internet. Il termine "spam" viene generalmente utilizzato per indicare messaggi collettivi non richiesti e non desiderati. Si definisce "spammer" colui che, dopo aver ottenuto centinaia, migliaia o persino milioni di indirizzi di posta elettronica da varie fonti, utilizza tali indirizzi per inviare messaggi o richieste di vario tipo. Con "spam" si indica anche la pubblicazione di messaggi non richiesti o contenenti annunci pubblicitari non correlati alla discussione nell'ambito di un newsgroup o un forum di discussione pubblica.

Il fenomeno legato allo spamming è ormai diventato un problema, perché comporta notevoli sprechi di tempo e risorse server. Gli spammer usano tecniche molto diverse e sofisticate per tentare di mascherare l'origine dei propri messaggi, ad esempio utilizzando gli indirizzi e-mail altrui o inoltrando lo spam in modo occulto attraverso più server di posta. La prevenzione di questo fenomeno si rivela pertanto alquanto difficile. Il server MDaemon di MDaemon Technologies è dotato di numerose funzioni appositamente progettate per impedire lo spamming, ad esempio liste bloccati DNS (DNS-BL), schermatura IP, filtro IP, controllo dell'inoltro e altre ancora.

L'origine del termine "spam" è ancora oggetto di discussione. Secondo la versione più accreditata, deriva da un famoso sketch del gruppo comico inglese Monty Python in cui la parola "spam" viene continuamente ripetuta e periodicamente accompagnata da un coro di Vichinghi che canta "Spam spam spam spam, spam spam spam spam...". Tuttavia, qualcuno afferma che si tratti semplicemente di un paragone poco lusinghiero con la carne in scatola Spam della Hormel che, secondo un'opinione diffusa negli Stati Uniti, tutti prima o poi mangiano, anche se a nessuno piace.

TCP/IP - Acronimo di **T**ransmission **C**ontrol **P**rotocol/**I**nternet Protocol. Il protocollo TCP/IP viene definito come la struttura fondamentale di Internet. Si tratta della suite di protocolli di comunicazione utilizzati per connettere gli host sia su Internet che sulle reti LAN. È un sistema a due livelli: quello superiore, TCP, gestisce il disassemblaggio e l'assemblaggio dei file in pacchetti per la trasmissione sulla rete; quello inferiore, IP, gestisce l'indirizzamento dei pacchetti in modo che raggiungano la destinazione corretta. I protocolli TCP e IP vengono discussi rispettivamente nella RFC-793 e nella RFC-791, consultabili su Internet agli indirizzi:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet - Comando e programma utilizzati per collegarsi ai siti Internet che supportano l'accesso Telnet. Tramite il comando Telnet, l'utente visualizza il prompt di accesso del server Telnet. Se l'utente dispone di un account su tale server, può accedere alle risorse autorizzate (file, messaggi e-mail e così via). Telnet presenta dei limiti: si tratta infatti di un programma da riga di comando che utilizza i comandi Unix.

Il protocollo TELNET viene descritto nelle RFC 854-855, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminale - Dispositivo che consente di inviare comandi a un computer remoto, ad esempio una tastiera, uno schermo, un circuito semplice, nonché un computer in emulazione.

Tiff - Acronimo di **T**agged **I**mage **F**ile **F**ormat. Si tratta di un formato di file grafico creato per fungere da convertitore grafico universale tra più piattaforme di elaborazione. Il formato TIFF è in grado di gestire intensità di colore da 1 a 24 bit.

UDP - Acronimo di **U**ser **D**atagram Protocol. È uno dei protocolli che compongono la suite di protocolli TCP/IP per il trasferimento dei dati. Il protocollo UDP è noto come protocollo senza stato, poiché non riconosce l'avvenuta ricezione dei pacchetti inviati.

Il protocollo UDP viene descritto nella RFC-768, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc768.txt

Unix - Anche UNIX. Sistema operativo creato da Bell Labs negli anni Sessanta. Progettato per essere utilizzato da più utenti contemporaneamente, rappresenta il sistema operativo più popolare per i server su Internet. Esistono ormai molti sistemi operativi basati su UNIX: Linux, GNU, Ultrix, XENIX e altri.

URL - Acronimo di **U**niform **R**esource **L**ocator. Ogni file o server su Internet è dotato di un URL, ovvero dell'indirizzo che gli utenti immettono nel browser Web per accedere al file o al server in questione. Gli URL non possono contenere spazi e utilizzano sempre le barre normali (/). Sono costituiti da due parti, separate da "://": la prima rappresenta il protocollo utilizzato o la risorsa a cui ci si collega, ad esempio http, telnet, ftp e così via, mentre la seconda è l'indirizzo Internet del file o server, ad esempio www.altn.com o 127.0.0.1.

Uuencode - Set di algoritmi utilizzato per convertire i file in una serie di caratteri ASCII a 7 bit per la trasmissione su Internet. Nonostante rappresenti l'abbreviazione di Unix-to-Unix Encode (codifica da Unix a Unix), Uuencode non è più un protocollo esclusivo del sistema UNIX, ma è diventato universale. Consente la trasmissione di file tra piattaforme diverse. Si tratta di un metodo di codifica utilizzato comunemente nella posta elettronica.

WAN - Acronimo di **W**ide **A**rea **N**etwork. Una rete WAN è analoga a una LAN (Local Area Network), ma in genere si estende tra più edifici o città. Le reti WAN sono spesso costituite da LAN di dimensioni più piccole interconnesse. Internet può essere descritta come la più grande WAN del mondo.

Zip - Si riferisce a un file compresso, di solito con l'estensione di file ".`zip`". Per estensione, "zippare" significa comprimere uno o più file in un unico file di archivio. Questa procedura consente di risparmiare spazio o di effettuare un trasferimento più rapido a un altro computer. Per utilizzare un file zip, è necessario decomprimerlo con un apposito programma, quale PKZIP o WinZip. Molti siti Web consentono di scaricare utilità di compressione/decompressione, sia shareware che freeware.

Indice

- 2 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -