Manual del Usuario

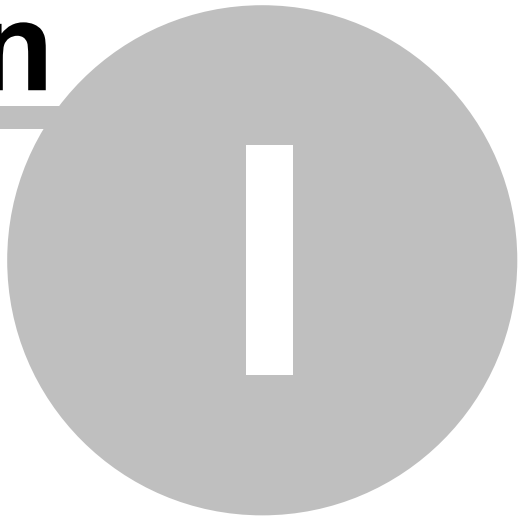
Private Cloud 12.0

MDaemon Private Cloud
Manual del Usuario

v12.0.0 - agosto 2024

Tabla de Contenidos

Sección



1 MDaemon Private Cloud 12.0

Introducción

El Servidor de Mensajería MDaemon es un servidor de correo basado en los estándares SMTP/POP3/IMAP que soporta Windows 7, Server 2008 R2, o superior y ofrece las funcionalidades más completas requeridas para un servidor de correo. MDaemon está diseñado para administrar las necesidades de correo de cualquier cantidad de usuarios individuales e incluye un poderoso conjunto de herramientas integradas para administrar cuentas de correo y formatos de mensajes. MDaemon ofrece servicios escalables SMTP, POP3 y IMAP4 junto con soporte a LDAP y Active Directory, cuenta con un cliente de correo integrado que funciona en cualquier navegador, filtrado de contenido, filtros de Spam, una amplia gama de funciones de seguridad y mucho más.

Funcionalidades de MDaemon

MDaemon está equipado con muchas funcionalidades además del procesamiento SMTP, POP3, y IMAP4. A continuación presentamos la lista de algunas de estas funcionalidades.

- Soporte completo para escaneo de virus y protección disponible como complemento a su licencia de MDaemon o MDaemon Private Cloud. Este complemento proporciona acceso en tiempo real a Outbreak Protection 640 y MDaemon AntiVirus 668. Los mensajes se pueden escanear y ser limpiados o eliminados automáticamente antes de que lleguen a sus usuarios destino. Más aun, puede configurar MDaemon para enviar un mensaje al administrador, al remitente y/o al destinatario del mensaje infectado, notificándoles sobre el virus.
- MDaemon cuenta con una suite completa de funciones para Listas de Distribución y administración de Grupos lo que permite la formación de un número ilimitado de listas de distribución que pueden contener miembros locales y/o remotos. Las listas se pueden configurar para permitir o rechazar solicitudes de suscripción, ser públicas o privadas, generar respuestas tanto a la lista como al emisor de cualquier mensaje, hacer envíos en forma de resumen, junto con muchas otras opciones.
- Webmail 321 es un componente integrado en MDaemon. Este componente permite a sus usuarios tener acceso a su correo utilizando su navegador web favorito a diferencia de los clientes de correo que corren sobre el equipo local. Esta herramienta es perfecta para personal móvil y usuarios

que no cuentan con una computadora dedicada donde tener acceso a su correo.

- MDaemon Webmail está equipado con una suite completa de funcionalidades de cliente de correo. Le permite: enviar y recibir correo, revisar la ortografía de los mensajes, administrar el correo en múltiples carpetas personales, desplegar la interface en cualquiera de 18 lenguajes, programar reuniones y citas y compartir calendarios y tareas con otros usuarios, administrar la configuración de su cuenta de correo (cuando se utiliza junto con Administración Remota 354), administrar contactos y mucho más. Webmail también está equipado con MDaemon Mensajería Instantánea (MDIM) 322, pequeña utilería que se puede descargar e instalar en el equipo del usuario. Este programa da un acceso fácil a su correo y carpetas y verifica la llegada de mensajes nuevos sin tener que abrir el navegador web. También incluye un sistema completo de Mensajería Instantánea que se puede utilizar para "conversar" con otros usuarios de MDaemon que estén utilizando MDIM u otro cliente XMPP 374.
- MDaemon está equipado con muchas funcionalidades diseñadas para ayudar a hacer más seguro su sistema de correo. El Filtro de Spam y las Listas DNS de Bloqueo le ayudarán a terminar con la mayor parte del "Spam" que intenta ingresar a su dominio. El monitoreo de Ip y Hosts y las Listas de Bloqueo de Direcciones permiten monitorear e impedir que ciertas direcciones y dominios se conecten o envíen correo a través de su sistema. También permiten que se conecten direcciones IP específicas mientras que se monitorean todas las demás.
- Equipado con soporte a Lightweight Directory Access Protocol (LDAP), MDaemon puede mantener su servidor LDAP actualizado con sus cuentas de usuario. Esto le permite mantener una libreta de direcciones LDAP actualizada de manera que otros usuarios con clientes de correo que soporten LDAP, las puedan consultar. Puede también utilizar Active Directory o su servidor LDAP como base de datos de cuentas de MDaemon en lugar de utilizar alguna base tipo ODBC o la base local del sistema `USERLIST.DAT`. Así, puede configurar múltiples servidores MDaemon en ubicaciones distintas para que compartan la misma base de datos de cuentas.
- MDaemon cuenta con funcionalidades de segmentación de encabezados que le permiten dar servicios de correo para una LAN completa utilizando tan solo un buzón POP3 proporcionado por su ISP. Esto permite dar servicios de correo a una red completa por una fracción del costo asociado normalmente.
- Los Alias de Direcciones le permiten enrutar a una cuenta válida o Lista de Distribución, mensajes de correo dirigidos a buzones "ficticios". Esto permite que cuentas individuales y listas tengan múltiples direcciones de correo en uno o más dominios.
- Las Puertas de Enlace de Dominios dan la opción de configurar dominios separados para varios departamentos o grupos que pueden ser locales en su red o estar localizados en otra ubicación en Internet. Utilizando esta funcionalidad, todo el correo dirigido al dominio para el que MDaemon funciona como Puerta de Enlace, será colocado en el buzón de correo de ese dominio en MDaemon. De ahí, puede ser recolectado ya sea por el servidor MDaemon de ese dominio o por un cliente de correo para luego ser distribuido a los usuarios del dominio. Esta funcionalidad también se puede utilizar para permitir que MDaemon actúe como servidor de respaldo para otros dominios.
- Administración remota vía web. El componente de Administración Remota 354 de MDaemon, está integrado en MDaemon y Webmail y permite a los

usuarios visualizar y editar la configuración de sus cuentas vía su navegador web. Usted puede definir qué parámetros pueden editar los usuarios y asignar permisos de acceso por cuenta. La Administración Remota también puede ser utilizada por el Administrador (y quién quiera que usted designe) para revisar o editar cualquier parámetro de MDaemon y cualquier otro archivo que desee permitir que muestre el sistema de Administración Remota.

- El sistema interno de transporte de mensajes conocido como correo RAW proporciona un método sencillo de colocar mensajes en el flujo del correo y simplifica el desarrollo de opciones personalizadas. Al utilizar RAW, se puede diseñar un sistema completo de correo utilizando un editor de textos y un par de archivos batch.
- El sistema de Filtro de Contenido es muy versátil y le permite personalizar el comportamiento de su servidor en base al contenido de los mensajes entrantes y salientes. Puede insertar y eliminar encabezados de mensajes, agregar texto al pie de los mensajes, eliminar adjuntos, enrutar copias a otros usuarios, hacer que se envíe un mensaje de Mensajería Instantánea a algún usuario, ejecutar otros programas y más.

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) es una edición especial de MDaemon Servidor de Mensajería desarrollada específicamente para revendedores y proveedores de servicios de TI que desean utilizar MDaemon para proporcionar a sus clientes servicios de correo. A diferencia de MDaemon, que se vende para uso en sitio, MDPC fue construido con un nuevo esquema de licenciamiento diseñado específicamente para ser utilizado en un ambiente de hospedaje. MDaemon Private Cloud incluye todas las funcionalidades de MDaemon, así como las opciones siguientes:

- Nuevo sistema de licenciamiento y facturación (por usuario/por mes)
- Soporte a Outlook
- Control de multidominios mejorado
- Personalización por dominio
- Reportes por dominio
- Cuentas de prueba no facturables (cuentas que no se incluirán en el total de cuentas facturables)
- Outbreak Protection, MDaemon Antivirus y el motor antivirus ClamAV (opcionales con costo adicional)
- ActiveSync para MDaemon (opcional con costo adicional).

Requerimientos del Sistema

Para obtener información actualizada de los requerimientos y recomendaciones del sistema, visite la página Requerimientos del Sistema en mdaemon.com.

Marcas Registradas

Apple es una marca registrada de Apple Inc. Windows Mobile, Microsoft y Outlook son marcas registradas de Microsoft Corporation. Todas las otras marcas registradas son propiedad de sus respectivos propietarios.

Ver:

Lo nuevo en MDaemon Private Cloud 12.0 15
Actualizando a MDaemon Private Cloud 12.0.0 71
Pantalla principal de MDaemon 80
Obtener Ayuda 76

1.3 Lo nuevo en MDaemon Private Cloud 12.0

Lo nuevo en MDaemon Private Cloud 12.0.0

- MDaemon Private Cloud 12.0.0 incluye MDaemon 24.0.1 con MDaemon Connector 8.0.1.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 24.0.1.

Para una lista de todos los cambios a MDaemon Connector, ver las Notas de la versión de MDaemon Connector 8.0.1.

Lo nuevo en MDaemon 24.0

Cambios y Nuevas Funcionalidades

MDaemon Server

- MDaemon puede recolectar y enviar datos anónimos de uso a MDaemon Technologies. Utilizaremos esta información para mejorar el producto y sus funcionalidades para satisfacer mejor las necesidades de nuestros clientes. Esto se puede des habilitar quitando la marca en la casilla "Enviar datos de uso anónimos" en Inicio | Preferencias | Misceláneos 503. Vea nuestra política de privacidad para obtener más información.
- La opción DKIM para firmar mensajes de listas de distribución 532 ya no requiere procesamiento del filtro de contenido para cada mensaje individual de la lista.
- El correo con el Resumen de la Cola de Erróneos 874 ahora cuenta con una liga para eliminar todos los mensajes. Como con las otras ligas en los mensajes resumen de colas, esto requiere que esté habilitada la opción

"*Incluir liga de acción en el correo resumen*[874]" y qiue la URL de Administración Remota[356] esté configurada.

- Protocolo ARC (Authenticated Received Chain)[537] - ARC es un protocolo de autenticación de correo electrónico que permite que los servidores de correo firmen digitalmente los resultados de autenticación de un mensaje. Esto proporciona una "cadena de custodia" autenticada para el mensaje, permitiendo que cada servidor que procesa el mensaje vea qué servidores lo procesaron previamente y si fue o no autenticado en cada paso. Cuando un servidor de correo de salida hace una verificación DMARC y encuentra que fallaron SPF o DKIM (debido a reenvío o a modificaciones de listas de distribución, por ejemplo), puede consultar los resultados ARC de un servidor confiable y utilizarlos para decidir si se acepta el mensaje. La verificación y firma ARC se puede habilitar en el nuevo diálogo Ajustes ARC[537] en Autenticación de Remitente. Para mas información sobre el protocolo ARC vea: RFC 8617: The Authenticated Received Chain (ARC) Protocol.
- Se agregó soporte a archivos SEM[902] sin "blacklist" o "whitelist" en sus nombres: `BLOCKLIST.SEM`, `SENDERBLOCKLIST.SEM`, `RCPTBLOCKLIST.SEM`, `CREDSMATCHEXEMPTLIST.SEM`, `DMARCEXEMPTLIST.SEM`.
- Se modificó el correo de notificación de cuenta congelada por la Detección de Secuestro[568] para incluir la razón exacta por la que la cuenta fue congelada.
- MDaemon deshabilita el cliente de auto-actualización[400] de MDaemon Connector en versiones previas a la 7.0.6, para resolver un error del auto-actualizador en esas versiones.

Administración Remota (MDRA)

- **Ligas de Documentos** - Esta funcionalidad permite que los usuarios de Webmail generen ligas temporales apuntando a archivos específicos en su carpeta personal de documentos. Estas ligas se pueden compartir con cualquiera, estarán activas por 30 días y serán eliminadas automáticamente luego de ese periodo. El ajuste global por omisión para esta opción se puede encontrar en la página Ajustes de Webmail[345]. También se puede configurar por dominio en el Administrador de Dominios[201] o por usuario en el Administrador de Cuentas[760]. Los Administradores Globales pueden utilizar le página Ligas de Documentos para ver qué ligas se están compartiendo, cuando fueron creadas, cuantas veces se ha descargado el archivo en la liga y la última descarga. También pueden utilizar esta página para revocar cualquier liga.
- La página Estatus ahora despliega el estatus de la licencia y el número de cuentas utilizadas para MDaemon, MDaemon Connector, AntiVirus y ActiveSync. Esta información también se despliega en la página de Registro (dar clic en **Acerca** y luego en **Registro** en la barra de herramientas).
- Ahora se cuenta con un Ajuste en Webmail[345] para "*Deshabilitar hipervínculos en spam y mensajes que fallen la autenticación DMARC DNSBL o SPF*", que se habilita por omisión. Opcionalmente también puede exentar mensajes de esta funcionalidad cuando el encabezado From coincide con un contacto en la lista de contactos permitidos del dominio o del usuario. También se agregó una opción para exentar esta función para los Remitentes Permitidos en la opción "*Bloquear imágenes HTML*" en la misma página.
- Se agregó una opción para Personalizar Webmail[354] para cargar una imagen de fondo personalizada para la página de inicio de Webmail.

- Ahora puede configurar MDaemon para "*Permitir que el inicio de sesión WebAuthn omita la página de Autenticación de Dos Factores*" en la página principal de Ajustes de Webmail 345 y en la página correspondiente Administrador de Dominios de Webmail 201. Dado que WebAuthn ya es una forma de autenticación multi-factor, el utilizar otra forma de Autenticación de Dos Factores (2FA) cuando ya se ha utilizado el inicio de sesión de WebAuthn se puede ver como redundante o excesivo para algunos usuarios o administradores.
- Se modificó la lista de credenciales registradas en la página de ajustes de usuario para solo desplegar las credenciales del Inicio de Sesión sin Contraseña y se agregó el mismo tipo de lista a la porción Dispositivos de Autenticación de Dos Factores para incluir las credenciales registradas. Puede acceder a la página de ajustes de usuario dando clic en su nombre de cuenta el la esquina superior derecha del menú de navegación.
- Se movieron los ajustes de proxy del actualizador de AV a Inicio | Ajustes de Servidor | Ajustes Proxy 174.
- Se agregó el botón **Eliminar** en la páginaBúsqueda de Mensajes bajo el menú de Mensajes y Colas. Los Administradores pueden usarla para eliminar mensajes del buzón del usuario. Los Administradores Globales también pueden ahora buscar en **Todos los Buzones** para un dominio dado.

Webmail

Tema Pro

- El tema Pro ahora cuenta con una opción para permitir a los usuarios crear ligas temporales a archivos individuales en su carpeta de Documentos, que se pueden compartir con cualquier persona. En la lista de documentos, el usuario crea la liga dando clic al ícono Liga a la derecha de cualquier archivo listado. Al utilizar el mismo ícono, el usuario puede eliminar una liga creada previamente o reemplazar la liga con una nueva, dado que las ligas se eliminarán automáticamente luego de 30 días. Si existe una liga para un archivo, aparecerá un ícono antes del nombre del archivo en la lista de documentos. En MDRA, la opción "*Permitir a los usuarios crear ligas temporales a documentos personales*" que administra esta funcionalidad, se localiza en la página Ajustes de Webmail 345 (las opciones correspondientes se encuentran también en los Administradores de Dominio 201 y Cuentas 760) y hay una página **Ligas de Documentos** para visualizar y administrar las ligas que han creado sus usuarios.
- Al visualizar un mensaje al que ha respondido o reenviado previamente, aparece una nota bajo los encabezados mencionando la fecha y hora en que respondió o lo reenvió.
- Ahora hay un ícono de campana de notificación en la esquina superior derecha de la barra de navegación, para revisar y "marcar como visto" sus Recordatorios de eventos y tareas pasados. Si desea eliminar el ícono de campana de la barra de navegación, puede deshabilitar la funcionalidad en la opción "*Desplegar recordatorios de eventos y tareas en la barra de navegación*" en la página Ajustes | Notificaciones en Webmail.
- Ahora se cuenta con la opción "Mostrar Detalles de Encabezado" en Ajustes | Personalizar para siempre mostrar los detalles del encabezado en la vista de mensajes.
- Se agregaron instrucciones sobre como utilizar la IU de disponibilidad en el diálogo Publicar Programa.

- Se actualizó el editor HTML, TinyMCE, de la versión 6.0 a la versión 6.8.
- Se actualizaron las traducciones en el navegador, de la mensajería instantánea.
- Se agregó una opción de fuente en la página Ajustes | Personalizar.
- Se agregó la facilidad de arrastrar y soltar ligas de descarga de adjuntos y documentos al escritorio. Solo funciona con navegadores basados en Chrome.
- Se agregó una flecha para habilitar/deshabilitar los campos CC y CCO en la vista de redacción.
- Se redujo el espacio ocupado por listas y menú para los distintos tamaños de navegador de escritorio.
- Luego de copiar o mover un mensaje a otra carpeta, la siguiente vez que abra el menú copiar/mover, contendrá una nueva liga para Copiar o Mover a la misma carpeta utilizada anteriormente. Por ejemplo, si copia un mensaje a la Bandeja de Entrada, la siguiente vez que abra el menú rápido, habrá una nueva opción "***Copiar a Bandeja de Entrada**" abajo de la opción normal **Copiar**.
- Se actualizó el texto en la página Publicar Programa para usar "Duplicar" en lugar de "Copiar" para agregar a otros días la disponibilidad existente.
- Se actualizó la página Acciones de Carpeta.

Otras Mejoras

- Se mejoró el desempeño reduciendo la cantidad de Lectura/Escritura a disco.
- Ahora se eliminarán hrefs vacíos en marcas HTML en correos, para prevenir comportamiento inválido.
- Se creó una carpeta pública Remitentes Permitidos que se verifica por las opciones "**No Bloquear Imágenes para Remitentes Permitidos**" y "*No Deshabilitar Hipervínculos para Remitentes Permitidos*". Actualmente esta carpeta solo la utiliza Webmail, no el servidor MDaemon o el Filtro de Spam.
- Se agregaron las opciones de usuario "*Solicitar Confirmación de Entrega*" y "*Solicitar Confirmación de Lectura*" en Ajustes | Redacción. Cuando se configura a **Sí**, las casillas correspondientes son activadas en la vista de Redacción.
- Se agregó una opción para "*No Deshabilitar Hipervínculos para Remitentes Permitidos*" en Ajustes | Personalizar. Cuando se deshabilitan los hipervínculos en un mensaje, se desplegará "*Hipervínculos deshabilitados. Dé clic aquí para habilitarlos*" en la parte superior de la ventana del mensaje.
- Se agregó la facilidad de definir el color de un calendario en el tema Pro. El ajuste está disponible dando clic derecho en el calendario en la vista de Calendarios, yendo a Ajustes | Carpetas y dando clic en un calendario de la lista de carpetas y al crear un calendario nuevo en el diálogo Carpeta Nueva. El ajuste de color se respeta en los temas LookOut y WorldClient.
- Se modificó la lista de credenciales registradas en la página Ajustes | Seguridad para solo desplegar las credenciales de Inicio de Sesión sin Contraseña y se agregó el mismo tipo de lista a la porción de la página donde se encuentran los Dispositivos de Autenticación de Dos Factores para las credenciales registradas relacionadas.

- Se modificó el ícono "Importar Mensajes" a una flecha hacia abajo en lugar de una flecha hacia arriba.
- Se agregó más contraste en el estatus de leído/no leído en la lista de mensajes.
- Se actualizó CKEditor a la versión v4.22.1.

ActiveSync

- Se mejoró la Operación SmartForward/SmartReply cuando **NO** se especifica <ReplaceMime/>.

  Versiones anteriores contenían código que cumplía con la especificación EAS 2.5 Spec para SmartForward. Más aún, SmartReply no soportaba imágenes en línea en la respuesta de mensaje. Este nuevo código soporta esto. El fragmento del estilo css que controla la división dentro de la que se coloca el mensaje al que se respondió o se reenvió, sigue siendo personalizable. Vea las Muestras de operación ActiveSync_DomainSettings_*.xml y ActiveSync_GlobalSettings.xml. A menos que se especifique explícitamente, los ajustes de dominio utilizarán los ajustes globales de formateo.
- Las modificaciones en la Administración de ActiveSync ahora se registra en el archivo AirSync-Mgmt.
- El servidor ActiveSync respeta la opción de Webmail de utilizar el encabezado X-Forwarded-For.

Otros

- XMLAPI - Se agregó la administración de Contraseñas de App.
- Filtro de Contenido - Se agregó soporte de caracteres extranjeros en la edición y consultas de reglas. Los archivos de configuración del Filtro de Contenido (CFilter.ini y CF*.dat) han sido convertidos a UTF-8. Si requiere revertir a una versión anterior y tener caracteres No-ASCII en esos archivos, conviértalos a ANSI o restáurelos de un respaldo.
- Se actualizaron los archivos de DQS SpamAssassin por contenido y correcciones HBL.
- Monitoreo Dinámico - Si encuentra errores "No se encontró la ruta de red", edite en el registry HKLM\SOFTWARE\Alt-N Technologies\MDaemon\DynamicScreening\Configuration y defina el Servidor como "." y UseCustomServer (DWORD) como 1.
- Se actualizó ClamAV a la versión 1.0.6 LTS.
- MDaemon Connector se actualizó a la versión 8.0.0.
- Cambios en la Administración de ActiveSync ahora se registran en el archivo AirSync-Mgmt.
- El servidor ActiveSync respeta a opción de Webmail de utilizar el encabezado X-Forwarded-For.

Notas de la versión del Servidor MDaemon

Para una lista completa de estas y otras adiciones, cambios y correcciones incluidas en MDaemon 24.0.0, vea las Notas de la Versión.

Lo nuevo en MDaemon Private Cloud 11.5.0

- MDaemon Private Cloud 11.5.0 incluye MDaemon 23.5.2 con MDaemon Connector 7.0.7.
- Se corrige en MDRA: las funciones de la nube, como los Servidores Administrados, no aparecen en el menú.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 23.5.2.

Para una lista de todos los cambios a MDaemon Connector, ver las Notas de la versión de MDaemon Connector 7.0.7.

Lo nuevo en MDaemon 23.5

Cambios y Nuevas Funcionalidades

Webmail

Soporte a WebAuthn 345

MDaemon soporta la API de Autenticación Web (también conocida como WebAuthn), que los usuarios de Webmail pueden utilizar para tener una experiencia de inicio de sesión más segura y sin contraseña, permitiéndoles utilizar biométricos, llaves de seguridad USB, Bluetooth y más para autenticación. WebAuthn también se puede utilizar para la Autenticación de Dos Factores 345 (2FA), aunque si está utilizando tanto la autenticación sin contraseña como la 2FA, no puede utilizar el mismo método de autenticación para las dos opciones. Puede encontrar los ajustes para WebAuthn en la página de Ajustes 345 de Webmail en la interface web de MDaemon Administración Remota (MDRA) 354.

Visite: webauthn.guide, para más información sobre WebAuthn y como funciona.

Funcionalidades IA en Mensajes 352

A partir de MDaemon 23.5.0, el tema Pro del cliente Webmail de MDaemon incluye varias funciones de Inteligencia Artificial (IA) para ayudar a sus usuarios a administrar su correo e incrementar la productividad. Con estas funciones, en MDaemon Webmail puede utilizar IA (específicamente ChatGPT de OpenAI) para obtener resúmenes de los contenidos de algún mensaje de correo, sugerir la respuesta a un mensaje con base en los criterios que se elijan y ayudar a redactar mensajes nuevos con base en textos propios y otros criterios.

Las funciones IA de Webmail están deshabilitadas por omisión para todos los dominios. Se pueden habilitar utilizando la opción "*Habilitar las funciones IA en Mensajes*" en la página de Ajustes 345 de Webmail o en la página del Administrador de Dominios de Webmail 201. Las funciones IA de Webmail también están deshabilitadas por usuario por omisión. Puede habilitarlas por usuario en la página de Servicios Web 720 del Editor de Cuentas o como parte de un Grupo 781 controlado por una Plantilla de Cuentas 791. Cuando el ajuste de Dominio está deshabilitado, tiene precedencia sobre el ajuste de usuario.

Por esto, ninguno de los usuarios del dominio podrá utilizar las funciones IA de mensajes, sin importar el ajuste en el usuario.

Ver: Funciones IA en Mensajes en Webmail 352, para obtener más información y advertencias sobre su uso. Más aún, puede encontrar la Política de Uso de Inteligencia Artificial de MDaemon Technologies en nuestra Página de Información sobre Inteligencia Artificial (IA). En esa misma página se encuentra una liga a los Términos de Uso de OpenAI.

Mejoras en Temas

- Pro y WorldClient: Ahora se tiene una opción para eliminar todos los adjuntos de un mensaje dado.
- Pro y WorldClient: Se agregó la columna Descripción a la vista de Documentos.
- Pro: El selector de contactos en la vista de Redacción ahora cuenta con un diálogo para agregar un contacto con tres campos (Nombre, Correo, Celular).
- Pro: Se tienen nuevas opciones de Estilo en: Ajustes | Personalizar.
- Pro: Ahora se soportan múltiples recordatorios de eventos.

Otras mejoras a Webmail

- Se agregó una opción para Programación Pública, de manera que los usuarios pueden permitir a otros programar una reunión.
- Se separó el proceso de configuración de la verificación por correo para la Autenticación de Dos Factores, del proceso de configuración para la verificación de la app de autenticación.
- La funcionalidad de Recuperación de Contraseña ahora envía un correo sin revelar al usuario a donde se envió. La Autenticación de Dos Factores ocurre luego de dar clic en la liga de recuperación en el mensaje.
- Se modificó como se autentica Webmail con el servidor SMTP de MDaemon de manera que no se requiere la contraseña del usuario.
- Se agregó una opción a "Marcar como leídos los mensajes eliminados" en: Ajustes | Personalizar.
- Ahora se cuenta con un botón para habilitar/deshabilitar Todos en la vista de Documentos.

Administración Remota (MDRA)

Verificación de Salud 510

Ahora se cuenta con una página para Verificación de Salud en MDRA en: Seguridad | Verificación de Salud. Esta página proporciona una lista conveniente de ajustes de seguridad importantes, consolidados en una sola página y despliega el valor actual de cada ajuste y su valor por omisión. Cuando los valores difieren, se resalta el ajuste de manera que los Administradores Globales pueden revisar rápidamente esos ajustes en particular y restaurar cualquiera de ellos a los valores por omisión si se desea. Cada grupo de ajustes también tiene a un lado un ícono de acceso rápido, de manera que puede ir rápidamente a la página en que se localiza cada ajuste. Adicionalmente, también puede visualizar una lista de todos los cambios en la

Verificación de Salud, hechos durante la sesión actual del navegador y deshacer cualquiera de ellos si fuera necesario.

Otras mejoras en MDRA

- Se agregaron opciones gráficas de edición para la edición directa de archivos.
- Ahora se cuenta con un ícono "**X**" en el que puede dar clic para ocultar cualquier gráfica en el resúmen Tráfico y Buzones resumen reportes. Para restaurar el reporte oculto, dé clic en el nombre de su cuenta en la esquina superior derecha de la página y luego clic en la asilla al lado del reporte que desea restaurar.
- Se agregó el botón **Eliminar Todos** en la página Miembros de la Lista de Distribución 280.
- Al igual que en Webmail, se agregó soporte a WebAuthn en MDRA, lo que proporciona a los usuarios un método seguro de autenticación sin contraseña que también se puede utilizar como método de Autenticación de Dos Factores. Las opciones WebAuthn en MRDA se localizan en la páginaAjustes de Administración Remota 356. Ver: Soporte a WebAuthn 20 en la sección de Webmail arriba.
- El Editor de Carpetas Públicas 314 y el Editor de Carpetas Compartidas 743 ahora cuenta con la opción **Anidar Abajo** para elegir la carpeta padre bajo la que se anidarán las carpetas públicas o compartidas seleccionadas.
- Se agregó texto en la página Listas de Distribución para explicar que el usuario puede aparecer como miembro de una lista de distribución, por pertenecer a un Grupo 781.
- En la Consulta de Mensajes y Colas, se agregó la facilidad de visualizar el mensaje de correo, en adición a poder visualizar su fuente. Los mensajes RAW todavía se muestran solo en texto plano.
- Se agregaron ligas a las Colas en la página Estatus.
- Se agregó la facilidad de incluir múltiples direcciones (separadas por comas) luego de agregar nuevos Permisos de Acceso a una Carpeta Pública en la página Control de Acceso 316. No puede agregar direcciones al editar los permisos existentes.

Seguridad

- Se agregó soporte a HTTPS para Outbreak Protection 640.
- Se actualizó ClamAV a la versión 1.0.3.
- LetsEncrypt - Se agregó soporte para TLS 1.3
- Se actualizó SpamAssassin a la versión 4.0.0.

XMLAPI

MDaemon 23.5.0 incluye muchas adiciones y mejoras a XMLAPI. Vea las Notas de la Versión para obtener una lista completa de estas mejoras.

Otros

- Se agregó una opción de Contraseñas de Apps[855] para eliminar las contraseñas de app de una cuenta cuando se modifica la contraseña de la cuenta. Esta nueva opción se habilita por omisión.
- Se agregó una página de Restricciones[810] a las Plantillas de Cuentas. Cuando se elimina una cuenta de un grupo con una plantilla de cuenta que controla restricciones, las restricciones de la cuenta se revierten a sus valores previos o posiblemente a la plantilla de cuentas de otro grupo, si la cuenta es miembro de varios grupos.
- En el Monitoreo de Localizaciones[572] la opción "Se aceptan conexiones SMTP pero la autenticación está bloqueada" ahora se habilita por país en lugar de global. Bloquear conexiones SMTP protege al servidor de recibir correo de un país dado. Al permitir conexiones SMTP con la autenticación deshabilitada, se permite al servidor recibir correo de un país bloqueando al mismo tiempo ataques de fuerza bruta y diccionario. No se afectan los protocolos distintos a SMTP.
- Se eliminó de la Interface de Usuario la opción obsoleta "Redactar en una nueva ventana del navegador".
- LetsEncrypt - Se agregó soporte a TLS 1.3.

MDaemon Server Notas de la Versión

Para una lista completa de estas y otras adiciones, cambios y correcciones incluidas en MDaemon 23.5.2, vea las Notas de la Versión.

Lo nuevo en MDaemon Private Cloud 11.0.0

- MDaemon Private Cloud 11.0.0 incluye MDaemon 23.0.2 con MDaemon Connector 7.0.7.
- MDaemon deshabilita la actualización automática del cliente de MDaemon Connector en versiones previas a la 7.0.6, para resolver un fallo de la actualización automática en esas versiones.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 23.0.2.

Para una lista de todos los cambios a MDaemon Connector, ver las Notas de la versión de MDaemon Connector 7.0.7.

Lo nuevo en MDaemon 23.0

Cambios nuevas funcionalidades

Servidor MDaemon

- (23.0.2) Se agregó una opción en Configuración | Ajustes de Servidor | MultiPOP[151] para enviar un mensaje de notificación luego de múltiples fallos al verificar una cuenta MultiPOP. Dado que son comunes los fallos temporales, existe una opción para definir cuantos fallos consecutivos toma

para detonar una notificación. También hay una opción para definir cuantos días esperar entre notificaciones, para evitar enviar demasiados mensajes. El contenido y destinatarios del correo de notificación se puede personalizar editando el archivo \MDaemon\App\MPOPFailureNotice.dat. Por omisión las notificaciones se envían luego de 5 fallos, no más de una vez cada 7 días, al propietario de la cuenta MultiPOP.

- Se incluye una nueva página MultiPOP[151] bajo Ajustes del Servidor. Desde esta página puede habilitar/deshabilitar el servidor MultiPOP de MDaemon y utilizar la opción "*MultiPOP siempre elimina el correo...*" (localizada anteriormente en la página Recolección MultiPOP[383] para ignorar para todos los usuarios la opción *Dejar una copia del mensaje en el servidor POP*[739]. Esta página nueva también contiene las opciones de soporte a OAuth 2.0 para la recolección MultiPOP desde Gmail y Office 365.

  Soporte MultiPOP OAuth 2.0 para recolectar correo desde Gmail y Office 365[153] — OAuth 2.0 es autentificación moderna, que requieren estos servicios al deshabilitar la autentificación básica/tradicional. A fin de que la funcionalidad MultiPOP de MDaemon utilice OAuth 2.0 para recolectar correo desde Gmail u Office 365 para sus usuarios, se debe registrar el servidor MDaemon con Google o Microsoft respectivamente, creando una aplicación OAuth 2.0 utilizando la Consola Api de Google o Azure Active Directory de Microsoft. Este es similar al procedimiento requerido para utilizar en MDaemon la Integración con Dropbox[337] para sus usuarios de Webmail. Vea el tema MultiPOP[153] en la ayuda para más información sobre como configurar el soporte a OAuth 2.0.

- El servidor IMAP de MDaemon ahora soporta marcas de palabras clave. Esto permite a los clientes de correo tal como Mozilla Thunderbird, almacenar Marcas de Mensajes en el servidor, lo que permite visualizar las marcas en una instancia de un cliente, que fueron configurada en otra instancia del cliente.

- Se mejoró el desempeño del servidor IMAP al abrir carpetas de correo grandes.

Seguridad

- (23.0.2) Se agregó soporte para el Servicio de Consulta de Datos Spamhaus (DQS) en Seguridad | Filtro de Spam[675]. Para más información sobre Spamhaus DQS visite https://info.spamhaus.com/getting-started-with-dqs

- Se incluye una nueva opción *Bloquear Violación de Políticas al Inicio de Sesión* en el Monitoreo Dinámico[610], que puede utilizar si desea bloquear cualquier dirección IP que intenta iniciar sesión sin utilizar la dirección de correo completa. Esta opción está deshabilitada por omisión. Vea la página Sistemas[494] para más información en la opción correspondiente, "*Los servidores requieren autenticación con la dirección de correo completa*".

- Se agregó la opción *Solo para cuentas válidas* para expandir la opción *Ignorar intentos de autentificación usando contraseñas idénticas* en la página Rastreo de Fallos Auth[615]. Active esta opción si solo desea ignorar intentos de autentificación contraseña duplicada, cuando intentan iniciar sesión a una cuenta válida. Esto significa que si, por ejemplo, un usuario actualiza su contraseña en un cliente pero en otro cliente aún utiliza la contraseña anterior, estos intentos de inicio de sesión de ese cliente serán ignorados, dado que tendrá el nombre de inicio de sesión correcto. Un bot intentando inicios de sesión aleatorios con contraseñas similares, no tendrá ese beneficio y será bloqueado tan pronto como supere el umbral de fallos auth. Esto ayudará a derrotar a los bots más rápidamente. También se

actualizó la operación XML API DynamicScreen para reflejas estas nuevas funcionalidades.

- Se agregó la opción Filtro de Contenido » Adjuntos[657] para *"Agregar advertencias en la parte superior del cuerpo del mensaje si se elimina el adjunto".* Cuando MDaemon elimina un adjunto de un mensaje, por ejemplo porque se detectó un virus, agregará un mensaje de advertencia en la parte superior del cuerpo del mensaje. También se cuenta con un botón **Advertencia** a utilizar si desea revisar o modificar la plantilla de ese mensaje. Esta opción está habilitada por omisión.
- Se agregó la opción a *Excluir IPs confiables del escaneo de AntiVirus*[668].
- MDaemon envía un mensaje de advertencia a los admins cuando están por expirar los Certificados SSL[575] configurados para uso de MDaemon[577], Webmail[580], o Administración Remota[584].
- MTA-STS[590] ahora cuenta con una lista de exentos, de manera que dominios problemáticos pueden exentarse en lugar de que MTA-STS tenga que deshabilitarse cuando los fallos afectan las entregas.
- Se actualizó el componente de ClamAV AntiVirus a la versión 0.105.2 (MDaemon 23.0.1).

Webmail

- Integración con Google Drive[340] — Webmail ahora se puede vincular a las cuentas de Google de sus clientes permitiéndoles grabar adjuntos de mensajes directamente a su cuenta de Google Drive, así como editar y trabajar con los documentos almacenados ahí. A fin de habilitar esto se requieren las **Llave API**, **CID de Cliente** y **Secreto de Cliente**. Se obtienen directamente de Google creando una App utilizando la Consola Google Api y registrando su MDaemon en ese servicio. Esta app tiene un componente de autentificación OAuth 2.0, lo que permite a sus usuarios de Webmail iniciar sesión en Webmail y luego autorizar el acceso a su cuenta de Google Drive desde MDaemon. Una vez autorizados, los usuarios pueden visualizar las carpetas y archivos que se encuentran en Google Drive. Más aún, pueden subir, descargar, mover, copiar, renombrar y eliminar archivos, así como copiar/mover archivos de y hacia las carpetas locales de documentos. Si un usuario desea editar un documento, al dar clic en la opción de visualizar el archivo en Google Drive, el usuario podrá editarlo de acuerdo con los permisos establecidos en Google Drive. El proceso de configuración de Google Drive es similar a las funcionalidades Integración con Dropbox[337] y a la Integración MultiPOP OAuth[151]. Vea Integración con Google Drive[340] para más información.
- Se agregó una opción en todos los temas excepto el Lite para "*Habilitar Arrastrar y Soltar para mover carpetas*". La nueva opción se localiza en Webmail en la página **Carpetas** bajo el menú Opciones y se habilita por omisión.
- Se hizo la cookie de sesión segura sobre HTTPS.
- Ahora se envían a MDaemon notificaciones de cambio de Categorías
- WorldClient ya no modifica el archivo robots.txt al iniciar sesión.
- El servidor web integrado impide la descarga de archivos .dll del directorio HTML.

- Se agregó uno al maxlength del campo de contraseña nueva de manera que se mostrará cuando no se cumpla el requerimiento "Máximo 15 caracteres".
- Se agregó reporteo a intentos de inicio de sesión sin la dirección de correo completa, para soportar la nueva opción del Monitoreo Dinámico Política de Bloqueo de Inicio de Sesión 610.
- (23.0.2) Se hizo más visible la opción para dejar de posponer un mensaje con un resaltado naranja.

Tema Pro

- Se agregó soporte a las Confirmaciones de Lectura.
- Se agregó una opción para deshabilitar el menú contextual del editor HTML
- Se agregó la facilidad de ajustar el tamaño de la lista de carpetas.

Administración Remota (MDRA)

23.0.2

- Se agregó una casilla de verificación para "Excluir IPs confiables del escaneo AntiVirus 668"
- Se agregó la opción No permitir autentificación en el puerto SMTP 523
- Se agregó una opción para el Nombre de Despliegue ActiveSync en Configuración | Carpetas Públicas | Administración de Carpetas Públicas 314 | Editar
- Se agregaron cuatro más opciones de filtrado en la lista de usuarios 712. Solo Admins, Solo No-Admins, Solo Admins Globales y Solo Admins del Dominio
- Se agregó la página DQS en el Filtro de Spam 675 | Servicio de Consulta de Datos. Para más información sobre Spamhaus DQS visite https://info.spamhaus.com/getting-started-with-dqs

23.0.0

- En el Administrador de Dominios, ahora existe un Ajuste de Webmail 345 para "*Permitir a los usuarios recibir por correo los códigos de verificación de la Autentificación de Dos Factores*", de manera que los usuarios pueden recibir su código de verificación mediante una dirección de correo alternativa en lugar de utilizar la app Google Authenticator. Este ajuste se habilita por omisión.
- Se modificaron los permisos por omisión al agregar un nuevo registro ACL para Consultar y Leer.
- Los botones **Probar** en: Filtro de Spam » DNS-BL » Hosts 701 y Configuración » Active Directory » Autentificación 825 ahora se deshabilitan cuando se ejecuta el proceso.
- El servidor web integrado impide la ejecución y descarga de archivos .dll en el directorio Templates.
- Los usuarios ahora pueden personalizar la apariencia de la interface web de Administración Remota dando clic en el nombre del usuario (ej. frank.thomas) en la esquina superior derecha de la ventana. Se tienen opciones para cambiar la interface a Modo Oscuro, definir el Tipo de Font y elegir el Lenguaje preferido.

- Se modificar la confirmación de eliminación de cuenta para utilizar la funcionalidad de confirmación personalizada.
- Se agregó reporteo del Monitoreo Dinámico de intentos de inicio de sesión sin la dirección de correo completa.

ActiveSync

- Se agregó una opción en los Ajustes de Cliente para *Bloquear el Remitente al mover correo a la carpeta de Correo No Deseado* 421. Cuando se habilita, si un cliente mueve un mensaje a la carpeta de Correo no Deseado de la cuenta, el servicio agregará al remitente o la dirección De de ese correo a la carpeta de Remitentes Bloqueados.
- Ahora puede deshabilitar el Botón Borrado Completo 460 para clientes ActiveSync si lo decide, de manera que no pueda hacer un borrado completo de un dispositivo ActiveSync sin primero deshabilitar la nueva opción No Permitir Restablecimiento a valores de fábrica 421.
- Se hicieron legibles los datos BodyPreferences para facilitar la resolución de problemas de sincronización.
- Se mejoró el desempeño en el cierre de sistema cuando los clientes están sincronizando buzones grandes.
- Se agregó la facilidad de definir un nombre de despliegue personalizado en el buzón y las carpetas públicas.
- Se mejoró el desempeño en el cierre del sistema.
- Los clientes ActiveSync ahora pueden enviar mensajes a las Listas de Distribución Personales en la carpeta de Contactos.
- Se modificó la disposición del Diálogo de Ajustes de Cliente en la IU para agregar espacio a nuevos ajustes.

Otros

- (23.0.2) Filtro de Contenido - $LIST_ATTACHMENTS_REMOVED$ 663 se puede utilizar como acción en una regla (ej. "enviar nota", "agregar advertencia...")
- En la IU de MDaemon, se modificaron los permisos por omisión al agregar un nuevo registro ACL para Consultar y Leer.
- En la IU de MDaemon, se agregó una pantalla emergente de advertencia si intenta definir valores de puertos en conflicto en los servidores Webmail, Administración Remota, o XMPP BOSH.
- XMLAPI - Se agregó la operación Editor que se puede utilizar para editar varios archivos INI de MDaemon.
- Se modificaron varios complementos para permitir que las nuevas versiones se ejecuten y los clientes puedan probar posibles versiones con parches/hotfixes.

Notas de la Versión del Servidor MDaemon

Para obtener una lista completa de adiciones, cambios y correcciones incluidos en MDaemon, ver las Notas de la versión de MDaemon 23.0.

Lo nuevo en MDaemon Private Cloud 10.0.2

- MDaemon Private Cloud 10.0.2 incluye MDaemon 22.0.5 con MDaemon Connector 7.0.7.

CONSIDERACIONES ESPECIALES

- Outbreak Protection 640 ha sido restablecido. Por favor revise sus ajustes de Outbreak Protection ya que pueden haber regresado a los valores por omisión.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 22.0.5.

Lo nuevo en MDaemon Private Cloud 10.0.1

- MDaemon Private Cloud 10.0.1 incluye MDaemon 22.0.4 con MDaemon Connector 7.0.7.

CONSIDERACIONES ESPECIALES

- Cyren Anti-Virus ha sido reemplazado con IKARUS Antivirus. Cyren anunció recientemente sus planes para descontinuar operaciones, sin aviso previo. Esto nos obligó a encontrar un nuevo socio antivirus. Después de una profunda evaluación, IKARUS se destacó por su excelente tasa de detección y su velocidad. IKARUS Antivirus actualiza automáticamente sus definiciones cada 10 minutos.
- Cyren Outbreak Protection ha sido eliminado. Cyren anunció recientemente sin previo aviso sus planes de descontinuar operaciones. Estamos investigando y evaluando activamente opciones viables de tecnología antispam como adiciones adecuadas a los mecanismos antispam actuales disponibles en nuestros productos de software.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 22.0.4.

Lo nuevo en MDaemon Private Cloud 10.0.0

- MDaemon Private Cloud 10.0 incluye MDaemon 22.0.3 con MDaemon Connector 7.0.7.

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 22.0.

Para una lista de todos los cambios a MDaemon Connector, ver las Notas de la versión de MDaemon Connector 7.0.7.

Lo nuevo en MDaemon 22.0

Cambios y Nuevas Funcionalidades

Webmail

Tema Pro

- Al visualizar un mensaje, puede pasar el puntero sobre el nombre del remitente para abrir una pantalla emergente, que contiene opciones para agregar el remitente a sus Contactos y a las carpetas de Remitentes Permitidos o Bloqueados.
- Las vistas de Redacción, Mensajes, Eventos, Contactos, Tareas y Notas ahora se abren en una nueva ventana.
- Ahora puede abrir el siguiente mensaje no leído en el panel de vista previa de mensajes y en la vista de mensajes.
- Se agregaron fragmentos de mensajes a la lista de mensajes cuando se utiliza el modo multi-línea.
- Ahora puede habilitar la opción *Editar los Nombres de Despliegue de Alias* para usuarios del tema Pro, ubicada en Ajustes » Redacción. Permite a los usuarios editar el nombre de despliegue de cualquier alias asociado con su cuenta. Utilice la nueva opción "*Permitir a los usuarios editar sus nombre de despliegue de alias*" en Ajustes de Webmail 345 si desea permitir esto. **Nota:** Esta opción solo está disponible en la interface web de MDaemon Administración Remota (MDRA) 354.
- Las opciones y ligas que decían "lista blanca" o "lista negra" de remitentes ahora dicen remitente "permitido" o "bloqueado". Adicionalmente las carpetas Lista Blanca y Lista negra ahora se llaman "Remitentes Permitidos" y "Remitentes Bloqueados".
- La Lista de Mensajes se puede ordenar por la columna Marca.
- En la Lista de Tareas, las tareas vencidas ahora aparecerán en rojo.
- Se actualizó el cliente XMPP a la versión 4.4.0.

Otros

- Cuando se requieren contraseñas fuertes, ahora hay una lista de requerimientos de contraseñas que se despliega en verde y se deshabilita conforme al usuario cumple con los requerimientos. También se agregaron mensajes de error más descriptivos sobre qué es lo que es incorrecto en una contraseña inválida al ingresarla.
- Las Opciones de Redacción ahora contienen opciones para seleccionar la dirección "De" por omisión que se utilizará al redactar, responder o reenviar un mensaje.
- Se agregó un ajuste de "1 minuto" a la opción Tiempo para Refrescar la Lista, ubicada en la página Opciones » Personalizar.
- Se agregó soporte a tokens CSRF en la página de inicio de sesión de Webmail. Esto se habilita en la página Ajustes de Webmail » Servidor Web 326, al habilitar la opción "*Utilizar tokens CSRF (Cross Site Request Forgery)*". Si utiliza plantillas personalizadas en Webmail, agregue una entrada oculta en la

forma de Inicio de Sesión como sigue: `<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />`

- Calendario Público - Se modificó la vista de Lista para iniciar en la fecha actual y mostrar los siguientes 30 días.
- Se agregó una conversión automática de URLs a hipervínculos en la vista de mensajes.
- Los nombres de las carpetas por omisión (Borrador, Mensajes Enviados, etc.) se traducen al lenguaje del usuario en Webmail, sin importar en qué lenguaje se haya instalado MDaemon (anteriormente solo MDaemon en inglés hacía esto).
- Ahora hay una opción para enviar códigos de verificación de Autentificación de dos Factores a una dirección de correo secundaria.
- Temas LookOut y WorldClient - Se modificó el comportamiento de despliegue de la lista de categorías.
- Las carpetas Remitentes Permitidos y Bloqueados ahora tienen íconos diferentes para indicar que son carpetas especiales.

Administración Remota (MDRA)

- Se agregó la página IPs de Excepción de Autentificación de Dos Factores en MDRA, localizada bajo el menú de Inicio. Esto permite a los usuarios iniciar sesión en Administración Remota o Webmail sin requerir 2FA, al conectarse desde alguna de las IPs especificadas.
- En MDRA, en Ajustes de Webmail 345 ahora se tiene la nueva opción "*Permitir a los usuarios editar sus nombre de despliegue de alias*". Active esta opción si desea permitir a los usuarios editar el nombre de despliegue de cualquier alias asociado con su cuenta. Pueden hacerlo utilizando la opción *Editar Nombres de Despliegue de Alias*, localizada en el tema Pro de Webmail.
- Se modificó autocompletar="off" a autocompletar="contraseña nueva" en los campos de contraseña para impedir que Firefox auto-complete contraseñas fuera de la página de inicio de sesión.
- Se agregó el Editor de Mensajes de Notificación en la página Notificaciones 659 del Filtro de Contenido.
- Se agregó soporte a tokens CSRF en la página de inicio de sesión. Esto se habilita con la opción "*Utilizar tokens CSRF (Cross Site Request Forgery)*" en la página Ajustes de Administración Remota en MDRA.
- Cualquier Cola Personalizada 877 local o remota que haya creado se puede administrar bajo la sección Mensajes y Colas en MDRA.

Seguridad

- MDaemon ahora soporta TLS 1.3 en versiones recientes de Windows. Windows Server 2022 y Windows 11 tienen habilitado TLS 1.3 por omisión. Las versiones de Windows 10 2004 (OS Build 19041) y superiores cuentan con soporte TLS 1.3 experimental que se puede habilitar para conexiones entrantes al agregar lo siguiente en el registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityPro
   viders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0
```

```
Enabled (DWORD) = 1
```

- MDaemon registra la suite cipher (ej. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) utilizada por conexiones SSL/TLS.
- Se agregó una opción en Contraseñas 855 para que las contraseñas fuertes requieran un caracter especial. Se habilita por omisión en instalaciones nuevas y se deshabilita por omisión en instalaciones existentes.
- Escaner AV de Buzones - Cuando se encuentra un mensaje infectado durante el escaneo de buzones, se incrementará el contador de infectados de MDaemon.
- AntiVirus - Se actualizó ClamAV a la versión 0.104.3.

ActiveSync

- Se mejoró el desempeño de FolderSync.
- El Diálogo de Monitoreo de Conexiones ActiveSync cuenta con un nuevo menú al dar clic derecho para terminar una sesión y bloquear al cliente.
- Se agregó una opción al diálogo Ajustes de Cliente 460 para permitir a Outlook enviar correo utilizando alias. Si el campo Reply-To lleva un alias válido para la cuenta remitente, el mensaje se enviará desde ese alias.
- Se agregó soporte para el comando Find EAS 16.1. Se eliminó la restricción de protocolo 432 que impide que iOS utilice EAS 16.1

Otros

- Filtro de Contenido - Se agregó soporte a las macros $CONTACT...$ en la acción "Agregar una firma corporativa 648". Estas macros se pueden utilizar para personalizar la firma con información de contacto del remitente de la carpeta de contactos públicos. Ver: Macros de Firmas 143 para una lista de las macros soportadas.
- Filtro de Contenido - Se agregó una acción para extraer adjuntos 648 y agregar una liga de adjuntos 366 en el mensaje.
- Correos Resumen 874 para las colas de retención, cuarentena y de erróneos ahora tienen ligas para liberar, re-encolar o eliminar cada mensaje. Esta nueva opción "*Incluir liga de acción*" se encuentra habilitada por omisión. Nota: La URL de Administración Remota 356 debe estar configurada par que se generen las ligas.
- LetsEncrypt 594 - Se actualizó el script para funcionar con PS 7.
- Se agregó una opción de Entrega Diferida en Recuperación de Mensajes 130 para reemplazar el encabezado 'Fecha:' con la fecha y hora actual cuando se libera un mensaje de la Cola Diferida. Se encuentra deshabilitada por omisión.
- MDaemon Connector 387 se actualizó a la versión 7.0.7.
- XMLAPI - Se agregó soporte para programar reenvíos.

Notas de la versión de MDaemon Servidor de Correo

Para una lista completa de adiciones, cambios y correcciones incluidos en MDaemon, ver las Notas de la versión de MDaemon 22.0.

Lo nuevo en MDaemon Private Cloud 9.5.0

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

Para una lista de todos los cambios a MDaemon, ver las Notas de la versión de MDaemon 21.5.

Para una lista de todos los cambios a MDaemon Connector, ver las Notas de la versión de MDaemon Connector 7.0.6.

Lo nuevo en MDaemon 21.5

Principales Funcionalidades Nuevas

Contraseñas de Apps 751

Las Contraseñas de Apps son contraseñas muy fuertes, generadas aleatoriamente, para utilizar en clientes de correo y apps, para ayudar a que sus apps de correo sean seguras dado que no pueden ser protegidas por la Autentificación de Dos Factores 720 (2FA). 2FA es una forma segura de que un usuario inicie sesión en Webmail o en MDaemon Administración Remota (MDRA), pero una app de correo no la puede utilizar porque la app debe poder darle acceso a su correo en segundo plano sin tener que registrar un código de su app de autentificación. Las funcionalidad Contraseñas de Apps le permite crear contraseñas fuertes y seguras para utilizar en sus apps, manteniendo la contraseña de su cuenta segura con 2FA. Las Contraseñas de Apps solo pueden ser utilizadas en apps de correo, no se pueden utilizar para iniciar sesión en Webmail o en MDRA. Esto significa que aun cuando una Contraseña de App estuviera comprometida de alguna forma, el usuario no autorizado no podría ingresar a su cuenta para modificar la contraseña u otros ajustes, pero el usuario, sin embargo, si podría iniciar sesión en su cuenta con la contraseña regular y 2FA, para eliminar la Contraseña de App comprometida y crear una nueva si fuera requerido.

Requerimientos y recomendaciones de las Contraseñas de Apps

- A fin de crear Contraseñas de Apps, 2FA debe estar habilitado para la cuenta (aunque el requerimiento se puede deshabilitar 855 si usted lo decide).
- Las Contraseñas de Apps solo pueden ser utilizadas por apps de correo—no se pueden utilizar para iniciar sesión en Webmail o MDRA.
- Cada Contraseña de App se despliega solo una vez, cuando es creada. No hay manera de recuperarla después, de manera que los usuarios deberán estar listo para ingresarla en su app cuando es creada.
- Los usuarios deben utilizar una Contraseña de App distinta para cada app de correo y deberán revocar (eliminar) su contraseña siempre que dejen de utilizar una app o cuando el dispositivo se extravíe o sea robado.
- Cada Contraseña de App indica cuando fue creada, cuando se utilizó por última vez y la dirección IP desde la que se ingresó a la cuenta de correo. Si un usuario encuentra algo sospechoso en los datos de Último Uso o Última IP, deberá revocar esa Contraseña de App y crear una nueva para esa app..

- Cuando una contraseña de cuenta se modifica, todas las Contraseñas de Apps se eliminan en automático—el usuario no puede seguir usando sus Contraseñas de App anteriores.

Requerir Contraseñas de App para SMTP, IMAP, ActiveSync y más

Existe una opción de cuenta en la página Ajustes del Editor de Cuentas 760 que puede utilizar para "*Requerir contraseñas de app para iniciar sesión en SMTP, IMAP, ActiveSync, etc.*"

Requerir Contraseñas de Apps puede ayudar a proteger la contraseña de la cuenta de ataques de diccionario y fuerza bruta vía SMTP, IMAP, etc. Esto es más seguro porque aun cuando un ataque de ese tipo adivinara la contraseña actual de la cuenta, no podría funcionar y el atacante no lo sabría, porque MDaemon solo aceptaría una Contraseña de App correcta. Adicionalmente, si sus cuentas en MDaemon utilizan la autenticación víaActive Directory 822 y Active Directory está configurado para bloquear una cuenta luego de un número de intentos fallidos, esta opción puede ayudar a prevenir que las cuentas sean bloqueadas, porque MDaemon solo verificará las Contraseñas de Apps y no intentará autentificar con Active Directory.

Otras Mejoras y Funcionalidades Nuevas

Tema Pro

- El Tema Mobile ahora se llama **Pro**. Se expandió y mejoró para ser responsivo y adaptable para uso en distintos tipos de dispositivos y tamaños de pantalla, sin sacrificar funcionalidades.
- Se agregaron tokens tipo Cross-Site-Request-Forgery para transacciones más seguras. Esta funcionalidad está deshabilitada por omisión. Para habilitarla desde MDRA vaya a Inicio | Ajustes de Webmail | Servidor Web 326 y active la opción "Utilizar tokens Cross-Site-Request-Forgery".
- Se agregó una opción en Ajustes | Personalizar para habilitar el modo Oscuro, para desplegar el tema Pro con un fondo oscuro.
- Se agregó una lita para "Rastrear mi paquete" en mensajes abiertos.
  - Los número de rastreo de transportistas monitoreados por omisión son: USPS, UPS, OnTrac, FedEx y DHL.
  - El archivo de configuración por omisión se encuentra en: `\MDaemon\WorldClient\package_tracking.json`
  - Los Administradores pueden agregar más transportistas creando el archivo: `\MDaemon\WorldClient\package_tracking.custom.json`, utilizando el mismo formato que el archivo por omisión `package_tracking.json`. Se requiere al menos un nombre de servicio, una URL de rastreo y al menos una expresión regular válida. Incluya nombres de servicio que pueden aparecer en un mensaje para reducir la posibilidad de coincidencias falso positivas.
- Se agregó el diálogo Distribución de la Lista de Mensajes para tamaños de navegador menores. Solo se despliega el ajuste Densidad de la Lista de Mensajes.
- Se agregó un medidor de fuerza de contraseña.
- Se agregó la funcionalidad de presentación de imágenes en la Vista de Mensajes

- Se agregó una vista de tarjeta para la lista de Contactos.
- Se movió el botón "Elemento Nuevo" de la barra de herramientas al espacio sobre la lista de carpetas para los tamaños de pantalla de escritorio.
- Se agregó un ícono "+" junto a "Personal" para crear un calendario nuevo en la vista de calendarios.
- Se agregó un mensaje emergente con las opciones Editar y Enviar un Mensaje a la opción Participante.
- Se hizo que la barra de búsqueda siempre sea visible para ventanas de navegador con anchos de 1200px o mayor.
- Se agregó un diálogo para permitir a los usuarios eliminar un contacto de la Lista Negra al agregarlos a la Lista Blanca y viceversa.
- Se agregó un mensaje cuando ocurre un error al crear o renombrar una carpeta.
- Se agregó soporte para notas HTML en Eventos, Contactos, Tareas y Notas.
- Se reemplazó el editor HTML actual (CKEditor) con Jodit.
- Se modificó la vista básica de encabezado para mostrar la dirección de correo De.
- Se agregó la Grabadora de Voz.

Otras Mejoras a Webmail

- Se agregó una liga para Desuscribir al lado de la dirección "De" cuando existe el encabezado List-Unsubscribe en un mensaje. Esto se puede deshabilitar en Webmail en Ajustes | Personalizar.
- Se agregó la facilidad para importar correo a la lista de mensajes actual.
- Se actualizó la integración con Dropbox para utilizar el token de refresco proporcionado por Dropbox para reconectar usuarios sin interacción del diálogo OAuth. Cuando el token de acceso expira, Webmail intentará utilizar el token de refresco para obtener un nuevo token de acceso. Los ajustes que ya no son necesarios se han eliminado de la página Apps Cloud. El Administrador NO requiere hacer cambios en la app de Dropbox en Dropbox.com.
- Las peticiones de búsqueda en Todas /Subcarpetas ya no buscan en carpetas no suscritas cuando están ocultas.
- Se agregó una casilla de verificación denominada "Omitir Búsqueda" para excluir carpetas específicas de las peticiones Buscar Todas / Subcarpetas.
- Se agregó un ajuste en Administración Remota que permite que la casilla de verificación de Autentificación de Dos Factores para Recuérdame esté oculta.
- Se agregó un efecto de difuminado para el fondo cuando expira la sesión del usuario.
- Se agregó una funcionalidad automática CC y CCO en Ajustes | Redacción.
- Se agregó una opción en: `WorldClient\Domains.ini [Default:Settings] PreventComposeWithAlias`, para impedir la redacción de mensajes con un alias. El ajuste se encuentra deshabilitado por omisión.

- Tema Lite - Se agregó la funcionalidad grabado automático para borradores en la vista de Redacción.
- Se agregó una opción en la vista Opciones | Carpetas para permitir a los usuarios omitir carpetas de contactos en las búsquedas de auto-completar. Se agregó la opción en el menú de clic derecho también.
- Se agregó una entrada al registro de Webmail para el User-Agent cuando un usuario inicia sesión.
- Se agregó una notificación en la vista de Redacción si un destinatario local tiene su autorespuesta habilitada.
- Tema WorldClient - Se agregó un ícono de sujetapapeles en las cuadrículas de eventos que contienen adjuntos.
- El tamaño máximo de Adjuntos se configura en 25 MB para instalaciones nuevas.
- Se modificó la acción de carpeta "Borrar Todo" por "Vaciar Carpeta"
- Tema WorldClient - Se agregaron botones "Modificar Contraseña" y Modificar Correo de Recuperación" en la página Seguridad

Administración Remota (MDRA)

- Se agregó la facilidad de arrastrar y soltar en las reglas del filtro de contenido. Los botones copiar, editar y eliminar ahora se encuentran respectivamente en cada regla.
- Se agregaron tokens Cross-Site-Request-Forgery para transacciones más seguras. La funcionalidad se habilita por omisión. Para deshabilitarla vaya a:Inicio | Ajustes de Administración Remota | Ajustes y deshabilite "Utilizar tokens Cross-Site-Request-Forgery".
- Se agregó un medidor de fortaleza de contraseña a algunos campos de contraseña.
- Se agregó la opción: "Habilitar Autentificación de Dos Factores Recuérdame" en Configuración | Administrador de Dominios | Editar | Ajustes de Webmail 201 y en Inicio | Ajustes de Webmail | Ajustes 345.
- Se agregaron reportes de IPs Bloqueadas y Rechazadas en el Monitoreo Dinámico.
- Se agregaron vistas de Grupos 468 y Tipos de Cliente 475 bajo ActiveSync.
- Se actualizaron las páginas de Diagnósticos 430 y Ajustes 418 de ActiveSync.
- Se agregó una gráfica y tabla de uso de navegador por Sistema Operativo en Reportes | Tráfico | Estadísticas de Inicio de Sesión de Webmail.
- Se agregaron botones para abrir una pantalla emergente para visualizar Usuarios y Grupos, para agregarlos a listas de distribución, en: Inicio | Listas de Distribución | Editar | Nueva 280. Solo los Administradores Globales o de Dominio 757 tienen acceso a esos botones.
- Se agregaron opciones de Solo Borrar Cuentas en Inicio | Mi Cuenta | Clientes ActiveSync y en ActiveSync | Administración de Clientes 460
- Se agregaron registros de Cambios. Se registrará toda modificación que se realice vía Administración Remota.
- Se actualizó Recuperación de Mensajes 130 para coincidir con la IU de MDaemon.

- Se agregó la opción "Extraer adjuntos de winmail.dat" en Seguridad | Filtro de Contenido | Compresión 666.
- Se agregó el lenguaje Esloveno en MDaemon Administración Remota.

Otras mejoras a MDaemon

- Se agregó soporte a Canalización de comandos SMTP (SMTP Command Pipelining - RFC 2920). MDaemon enviará comandos MAIL, RCPT y DATA en lotes en lugar de individualmente, lo que mejora el desempeño sobre conexiones de red de alta latencia. La canalización SMTP siempre se habilita para conexiones entrantes. Se encuentra habilitada por omisión para conexiones salientes, pero se puede deshabilitar en Configuración | Servidor Ajustes | Servidores & Entrega | Servidores 100.
- Se agregó soporte para SMTP CHUNKING (RFC 3030). CHUNKING (trozos) permite que se transfieran mensajes no orientados en línea. Se encuentra habilitado por omisión para conexiones entrantes pero deshabilitado por omisión para conexiones salientes. Cambios de línea (line feeds) en mensajes recibidos se convierten en inicio de línea (carriage return) por omisión. Estos valores por omisión se pueden modificar definiendo `[Special] SMTPChunkingInbound=Yes/No`, `SMTPChunkingOutbound=Yes/No` y `SMTPChunkingAllowBareLF=Yes/No` en `\MDaemon\App\MDaemon.ini`.
- Filtro de Contenido - Se actualizó la lista por omisión de adjuntos restringidos 657.
- Filtro de Contenido - Se agregó una acción en las reglas para agregar adjuntos a un mensaje 648.
- Servidor ActiveSync - Los registros de Iniciar/Detener se escriben en el registro de Sistema de MDaemon.
- Clústeres - Se agregó soporte para recordatorios de sincronización para nodos secundarios.
- Monitoreo Dinámico - Se agregó una opción de Registrar Ubicaciones utilizando Códigos ISO-3166 610 en lugar de nombres.
- XMLAPI - Se agregó soporte para el ajuste de ActiveSync AlwaysSendMeetingUpdates.
- XMLAPI - Se agregó soporte para la creación de archivos semáforo.
- XMLAPI - Se agregó soporte para reportar/modificar ajustes en Configuración/Servidor Ajustes/Registro.
- MDaemon Mensajería Instantánea - Se mejoró la funcionalidad de chats de grupo agregando la capacidad de selección múltiple de contactos para chat de grupo. También se agregó una opción para auto-aceptar peticiones de cuartos de chat.
- Monitoreo de Localizaciones 572 cuenta con una opción nueva para controlar si el encabezado `X-MDOrigin-Country` se agrega o no a los mensajes. Se encuentra habilitada por omisión.
- Ahora existe un ajuste de Cuentas para permitir a los usuarios iniciar sesión utilizando alias, localizada en: Cuentas | Ajustes de Cuentas | Alias | Ajustes 836. Se encuentra habilitada por omisión.
- MDaemon Connector se actualizó a la versión 7.5.0.

- El mensaje de texto por omisión para confirmación de entrega (en \MDaemon\App\Receipt.dat) se ha modificado para utilizar la macro $HEADER:X-RCPT-TO$ en lugar de $RECIPIENT$ para evitar revelar la dirección actual a la que resuelve un alias.

Notas de la versión del Servidor de Correo MDaemon

Para una lista completa de todas las adiciones, cambios y correcciones incluidos en MDaemon, ver las Notas de la versión de MDaemon 21.5.

Lo nuevo en MDaemon Private Cloud 9.0.0

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

Para obtener una lista de todos los cambios de MDaemon, vea las Notas de la versión de MDaemon 21.0.

Para una lista de todos los cambios de MDaemon Connector, vea las Notas de la versión de MDaemon Connector 7.0.4.

Lo Nuevo en MDaemon 21.0

Principales Funcionalidades Nuevas

Cuartos de Chat Persistentes

El servidor XMPP de MDaemon, ahora soporta cuartos de chat persistentes, que no tienen que ser creados cada vez que todos los usuarios salen del chat. Configúrelos en: Configuración | Web & Servicios IM | XMPP.

Reporte de clasificaciones erróneas de Virus/Spam

Al ubicarse en las pantallas de las colas de Cuarentena, Erróneos o Trampa de Spam en la IU de MDaemon, dando clic derecho aparecerá un menú emergente para reportar mensajes a MDaemon.com como falsos positivos o faltos negativos. Se agregaron opciones similares en MDaemon Administración Remota. Los mensajes serán analizados y se pasarán a los proveedores para que tomen acciones correctivas.

Interface de Usuario para el Cliente de Migración de ActiveSync (ASMC)

Se ha creado una Interface de Usuario (IU) como ayuda al ejecutar ASMC (`ASMCUI.exe` en la carpeta de MDaemon `\app\`). Le permite almacenar sus opciones y recuperarlas después. ASMC soporta migración de correo, calendarios, tareas, notas y contactos desde servidores ActiveSync que soportan la versión 14.1 del protocolo. Puede encontrar documentación al respecto en la carpeta de Documentos de MDaemon, en: `\MDaemon\Docs\ActiveSync Migration Client.html`.

Mejoras al tema Móvil de Webmail

Se expandió y mejoró el Tema Móvil para usuarios de Webmail. Ver `RelNotes.html` localizado en la carpeta de MDaemon `\Docs\` para obtener una lista completa de las muchas nuevas funcionalidades que se agregaron.

Mejoras al servicio de Clúster 407

Se realizó un número significativo de mejoras al Servicio de Clúster de MDaemon:

- Se agregó una opción de Enrutamiento de correo Multi-Nodo 412, donde se comparten las colas de correo entre nodos del clister. Al tener múltiples máquinas procesando y entregando los mensajes, dividen el trabajo de mejor manera y se impide que se atoren los mensajes en las colas de las máquinas que estén fuera de línea.
- Ahora se replican los certificados SSL del nodo primario a los secundarios.
- Las Colas en los nodos secundarios se congelan durante la replicación inicial de datos, lo cual mejora la respuesta al iniciar el sistema.
- La Replicación se pausa tan pronto como inicia el apagado de MDaemon, eliminando retrasos en el apagado relacionados con el clister.
- Los nodos del Clúster se pueden agregar utilizando direcciones IP o nombres DNS.
- Ahora se administran más fácilmente las rutas compartidas de red desde la nueva pantalla Rutas de Red Compartidas.
- Se proporcionan herramientas para registro y diagnóstico en la nueva pantalla Diagnósticos.

Otras nuevas Funcionalidades y Cambios

Administración Remota (MDRA)

Se agregaron muchas opciones a la interface de MDaemon Administración Remota. Para obtener una lista de estas opciones y otros cambios en MDRA vea `RelNotes.html` localizado en la carpeta de MDaemon `\Docs\`.

Filtro de Contenido

Se agregó la facilidad de hacer búsquedas en archivos restringidos 657 dentro de archivos comprimidos tipo 7-Zip.

Autorespuestas 838

Las Autorespuestas ahora soportan Unicode (UTF-8), permitiendo que el texto se registre en cualquier lenguaje.

Filtros IMAP 737

Las reglas de filtrado IMAP ahora pueden buscar texto específico en el cuerpo de los mensajes.

Webmail

- Ahora puede adjuntar un evento a un correo nuevo dando clic derecho en el evento y seleccionando la opción "Enviar" en los temas WorldClient y LookOut y desde la vista previa del evento en el tema Mobile.
- Todas las funcionalidades de Creación de Cuentas Nuevas han sido eliminadas.
- Cuando publica un calendario (compartir una liga de Acceso Público apuntando a él), las nuevas opciones le permiten definir la vista por omisión del calendario (ej. mes/semana/día) y publicar una liga del calendario Libre/Ocupado.
- Se agregó una opción para omitir la verificación de Persistencia de IP por usuario. En MDRA edite la cuenta del usuario y en Servicios Web se habilita "Omitir verificación de persistencia de IP para las sesiones de Webmail".
- Se agregó la facilidad de buscar en el campo CC en la búsqueda avanzada.
- Se agregó Máximo de Mensajes enviados por día en las cuotas desplegadas.

Interface de Usuario

- Configuración | Administración de Dispositivos Móviles se eliminó y reemplazó por el diálogo Administración ActiveSync en Configuración | ActiveSync.
- La pantalla Ajustes de Cliente ActiveSync ha sido eliminada. Personalice ajustes de cliente en las pantallas Ajustes, Dominios, Grupos, Cuentas y Clientes.
- La pantalla Tipo de Cliente ActiveSync cuenta con un menú de comandos para poner en lista blanca y negra los tipos de cliente.
- Se agregaron pantallas en Configuración | Indexación de Mensajes para la configuración de mantenimiento en tiempo real y nocturno de los índices de búsqueda utilizados por Webmail, ActiveSync y Administración Remota.
- Varios complementos ahora comparten la pantalla de configuración Diagnósticos.
- Los sistemas de ayuda en navegador para MDRA y Webmail han sido actualizados con un nuevo tema responsivo para hacerlos más utilizables en diferentes tipos de dispositivos.

XML API

- La apariencia del portal de documentación de XML API se puede personalizar globalmente y por dominio. Vea el documento "Cambios y notas de desarrollo" en el portal de ayuda (http[s]://ServerName[:MDRAPort]/MdMgmtWS) o vea el archivo \MDaemon\Docs\API\XML API\Help_Readme.xml en disco utilizando Internet Explorer para más información. Se proporciona un directorio de muestra company.mail en \MDaemon\Docs\API\XML API\Samples\Branding.
- Se agregaron operaciones de Alias para simplificar su administración, resolución y reporte.
- Se agregó la acción de Búsqueda por Carpeta en la búsqueda en mensajes.

- Se agregó soporte al servicio de Clúster para QueryServiceState y ControlServiceState.

Archivado 138

- Cuando un mensaje se envía entre cuentas locales, se crean copias en las carpetas "entrante" y "saliente" si se encuentran habilitadas las dos opciones "Archivar correo entrante" y "Archivar correo saliente".
- La opción para archivar mensajes de Spam, que se eliminó en la versión 20.0, ha regresado.
- Los mensajes de Spam liberados de la Trampa de Spam, son archivados.

Actualizaciones de Componentes

- MDaemon Connector ha sido actualizado a la versión 7.0.0.
- Filtro de Spam: Se actualizó a SpamAssassin 3.4.4. y se eliminaron los ajustes obsoletos en el archivo local.cf.
- AntiVirus: ClamAV se actualizó a la versión 0.103.0 y el motor de Cyren AV se actualizó a la versión 6.3.0.2.
- Servidor XMPP: Se actualizó la base de datos a la versión SQLite 3.33.0.

MDaemon Server Notas de la versión

Para una lista completa de adiciones, modificaciones y correcciones incluidas en MDaemon, ver las Notas de la versión de MDaemon 21.0.

Lo nuevo en MDaemon Private Cloud 8.0

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

Para obtener una lista de todos los cambios de MDaemon, vea las Notas de la versión de MDaemon 20.0.

Para una lista de todos los cambios de MDaemon Connector, vea las Notas de la Versión de MDaemon Connector 6.5.2.

Lo Nuevo en MDaemon 20.0

MDaemon Servicio Clúster 407

El nuevo Servicio Clúster de MDaemon fue diseñado para compartir su configuración entre dos o más servidores de MDaemon en su red. Esto le permite utilizar hardware o software para balanceo de cargas, para distribuir la carga del servicio de correo entre múltiples servidores MDaemon lo que puede mejorar la velocidad y eficiencia reduciendo la congestión de la red y sobrecarga y maximizando sus recursos de correo. También ayuda a asegurar redundancia en sus sistemas de correo si es que alguno de sus servidores tiene una falla de hardware o software. Ver: Servicio Clúster 407, para más información para configurar un clúster de MDaemon en su red.

Nuevas Extensiones SMTP

RequireTLS (RFC 8689) 590
Finalmente se ha concluido el esfuerzo en la IETF para definir el estándar RequireTLS y se ha implementado su soporte en MDaemon. RequireTLS le permite marcar mensajes que **deben** ser enviados utilizando TLS. Si no es posible TLS (o si los parámetros del intercambio de certificado TLS son inaceptables), los mensajes serán rechazados en lugar de entregarse de manera insegura. RequireTLS se habilita por omisión, pero solo los mensajes que sean sujetos al procesamiento RequireTLS se marcan específicamente con una regla del Filtro de Contenido utilizando una nueva Acción del Filtro de Contenido 648, "*Marcar mensaje para REQUIRETLS...*", o mensajes enviados a `<local-part>+requiretls@domain.tld` (por ejemplo, `arvel+requiretls@mdaemon.com`). Todos los demás mensajes se tratan como si el servicio estuviera deshabilitado. Adicionalmente, se deben cumplir varios requerimientos a fin de se envíe un mensaje utilizando RequireTLS. Si no se cumple cualquiera de ellos, el mensaje será devuelto en lugar de ser enviado. Para más información sobre estos requerimientos y como configurar RequireTLS, ver: Extensiones SMTP 590. Para una descripción completa de RequireTLS, ver: RFC 8689: SMTP Require TLS Option.

SMTP MTA-STS (RFC 8461) - Strict Transport Security 592
Se ha concluido el esfuerzo de la IETF para definir el estándar MTA-STS y se ha implementado soporte para esto en MDaemon. SMTP MTA Strict Transport Security (MTA-STS) es un mecanismo que permite a los proveedores de servicio de correo (SPs) declarar su capacidad de recibir conexiones SMTP seguras utilizando TLS (Transport Layer Security) y especificar si los servidores SMTP remitentes deben rechazar la entrega a hosts MX que no ofrezcan TLS con un certificado de servidor confiable. El soporte a MTA-STS se encuentra habilitado por omisión. Ver: Extensiones SMTP 590 para más información sobre como configurar esto, así mismo MTA-STS se describe a detalle en RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

Reporteo SMTP TLS (RFC 8460) 592
El Reporteo TLS permite a los dominios que utilizan MTA-STS ser notificados sobre fallos para recuperar las políticas MTA-STS o negociar un canal seguro utilizando STARTTLS. Al habilitarse, MDaemon enviará un reporte diario a cada dominio que tenga habilitado STS al que haya enviado (o intentado enviar) correo ese día. Existen varias opciones para configurar la información que contendrán los reportes. El Reporteo TLS se encuentra deshabilitado por omisión y se discute en RFC 8460: SMTP TLS Reporting.

Encripción MDPGP a nivel Dominio/Empresa con una sola llave

MDPGP 629 ahora soporta encripción de mensajes entre dominios utilizando una única llave de encripción para todos los usuarios. Por ejemplo, supongamos que 'Dominio-a' y 'Dominio-b' desean encriptar todos los mensajes enviados entre ellos pero no desean configurar y administrar llaves individuales de encripción para cada una de las cuentas de usuarios de ambos dominios. Esto ahora se puede realizar como sigue:

'Dominio-a' y 'Dominio-b' intercambian una llave pública de encripción vía el método que deseen. Por ejemplo, pueden enviar las llaves por correo dando clic derecho en una llave pública existente en la IU MDPGP y seleccionando 'Exportar & Enviar llave'. Si desean crear llaves nuevas para este fin, pueden dar clic en el botón 'Crear llaves para un usuario específico' y elegir el elemento '_Domain Key (domain.tld)_

<anybody@domain.tld>' que se ha colocado ahí para este fin (aunque cualquier llave funcionará). Una vez que cada parte haya recibido la llave de la otra, darán clic en el botón 'Importar Llave del Dominio' en la IU MDPGP y registrarán el nombre del dominio para el que todos los mensajes se enviarán encriptados utilizando la llave recibida. el sistema no crea una llave en el menú desplegable para cada uno de sus dominios. Puede utilizar la llave proporcionada para todos sus dominios o puede crear llaves específicas por dominio, si lo desea.

Si cualquiera de las partes ya cuenta con una llave pública que deseen utilizar y ya se encuentra en el llavero, pueden darle clic derecho en la IU MDPGP y seleccionar 'Configurar como llave del Dominio'. Sin embargo, no utilice una llave para la que también cuenta con la llave privada correspondiente. Si lo hace, MDPGP encriptará el mensaje e inmediatamente verá que la llave de desencripción es conocida y desencriptará el mensaje.

En este punto, MDPGP crea una regla en el Filtro de Contenido denominada 'Encrypt all mail to <domain>' que invocará la operación de encripción para cada mensaje enviado a ese dominio. Utilizar el Filtro de contenido significa que puede controlar este proceso habilitando o deshabilitado la regla ahí definida. También la puede modificar para afinar los criterios que desea aplicar antes de que se encripten los mensajes (por ejemplo, quizá desee hacer lo mismo para dos dominios o solo para ciertos destinatarios de un dominio). El Filtro de Contenido proporciona gran flexibilidad para lograr esto.

Encriptar Correo Saliente con base en la dirección IP Receptora

MDPGP 629 cuenta con una casilla de verificación y un botón de configuración donde puede mapear direcciones IP con llaves de encripción específicas. Cualquier sesión SMTP saliente que entregue un mensaje a alguna de esas IPs encriptará primero el mensaje utilizando la llave asociada, justo antes de la transmisión. Si el mensaje ya va encriptado con otra llave, no se realiza ninguna acción. Esto es útil (por ejemplo) en situaciones donde quiere asegurarse de que todos los mensajes enviados a ciertos destinatarios clave, proveedores, filiales, etc., se envían siempre encriptados.

Macros para mensajes de Listas de Distribución

La pantalla Editor de Listas de Distribución » Enrutamiento 300 cuenta con nuevas opciones que permitirán el uso de macros dentro del cuerpo de mensajes posteados a la lista. Esto le permitirá (por ejemplo) personalizar cada mensaje de la lista. Las Macros han sido soportadas desde hace mucho tiempo en los archivos del encabezado y pie del correo de la lista, pero nunca se habían soportado en el cuerpo del mensaje. Dado que las macros se relacionan con miembros individuales de la lista, esta opción solo es compatible con listas que están configuradas para "*Entregar correo de la lista individualmente a cada miembro*." Adicionalmente, con fines de seguridad, se puede configurar esta opción para que requiera que se proporcione la contraseña de la lista a fin de utilizar macros en el cuerpo del mensaje. Si decide no requerir la contraseña, cualquier miembro de la lista que tenga permisos de enviar a la lista, podrá utilizar las macros. Vea la pantalla Enrutamiento de la Lista de Distribución 300 para más información y para una lista de las macros que se pueden utilizar.

Sistema de Detección de Cuentas Secuestro Mejorado

La Detección de Cuentas Secuestradas 568 cuenta con opciones nuevas para ayudar a prevenir que las cuentas se utilicen para enviar spam debido a que sus contraseñas han sido robadas. Una característica común del correo spam es que

con frecuencia los mensajes se envían a un gran número de destinatarios inválidos, debido a que el spammer intenta enviarlos a direcciones de correo antiguas o intenta adivinar cuentas nuevas. Por esto, si una cuenta de MDaemon empieza a enviar mensajes a un número notable de destinatarios inválidos en un periodo de tiempo corto, es un buen indicador de que la cuenta ha sido secuestrada y se está utilizando para enviar spam. Para impedir esto, MDaemon ahora puede rastrear el número de veces que un usuario autentificado intenta enviar un mensaje a un destinatario inválido. Si esto ocurre demasiadas veces en un rango de tiempo muy corto, se puede hacer que MDaemon congele la cuenta (el postmaster recibe un mensaje sobre esto y puede responder para rehabilitar la cuenta). Esto puede ayudar a detener automáticamente una cuenta secuestrada, antes de que haga mucho daño. **Nota**: Como parte de este trabajo, las opciones de modificación del encabezado From se movieron a su propia página Monitoreo del Encabezado From 574 , para hacer espacio para las nuevas opciones de Detección de Secuestro.

Cola de Mensajes Diferidos y Recuperación de Mensajes Mejorada 130

Para ayudar a mejorar la eficiencia del sistema de Recuperación de Mensajes y el soporte al encabezado Deferred-Delivery, MDaemon ahora cuenta con una cola dedicada a los mensajes diferidos. Anteriormente, la Cola Entrante se saturaba con mensajes diferidos, lo que podría alentar la entrega de mensajes no diferidos. La nueva cola de Diferidos ayuda a resolver este problema. El sistema ahora coloca los mensajes en la Cola de Diferidos y llevan codificado en el nombre del archivo la fecha en que deben enviarse. MDaemon verifica la cola una vez por minuto y cuando es momento de que los mensajes dejen la cola, los mueve a la Cola de Entrantes y pasan al proceso normal de procesamiento/entrega de mensajes.

Adicionalmente, MDaemon ahora rastrea el encabezado Message-IDs del mensaje más reciente enviado por cada usuario local autentificado, lo que significa que los usuarios ahora pueden recuperar el último mensaje que enviaron (pero solo el último que enviaron), simplemente colocando RECALL (solamente) como Asunto en un mensaje enviado a la cuenta de sistema mdaemon@. No hay necesidad de encontrar y pegar el Message-ID del mensaje que desea recuperar, cuando es el último enviado. Para recuperar cualquier otro mensaje se sigue requiriendo incluir el Message-ID en el texto del Asunto o el mensaje original tomado de la carpeta de Enviados, agregado como adjunto a la petición de recuperación.

Además de recordar el mensaje enviado más recientemente por cada usuario autentificado, MDaemon también recuerda las ubicaciones y Message-ID de los últimos 1000 mensajes enviados por todos los usuarios autentificados. Consecuentemente, esto posibilita recuperar mensajes directamente de los buzones de los usuarios aun cuando hayan sido entregados. Así, los mensajes desaparecerán de los clientes de correo de los usuarios y de sus teléfonos, si son recuperados. **Nota**: Esto, por supuesto, solo es posible para mensajes enviados a otros usuarios locales; una vez que MDaemon ha entregado un mensaje a otro servidor ya no está bajo control de MDaemon y no puede ser recuperado.

Registro de Fallos de Autentificación

Ahora existe un nuevo archivo de registro de Fallos de Autentificación que contiene una línea con detalles para cada inicio de sesión SMTP, IMAP y POP que falla. La información incluye el protocolo utilizado, el campo SessionID para que pueda consultar otros archivos de registro, la IP del ofensor, el valor que intentaron utilizar (en ocasiones es un alias) y la Cuenta que coincide con el inicio de sesión (o 'ninguna' si no coincide con ninguna cuenta).

Autentificación al Reenviar/Enrutar Correo

Existen varias opciones de reenvío en MDaemon donde ahora puede agregar credenciales de autentificación. Esto significa que varios archivos en la carpeta \APP\ (i.e. `forward.dat`, `gateways.dat`, `MDaemon.ini` y todos los archivos `.grp` de las listas de distribución) ahora tienen el potencial de contener datos ocultos en un estado débilmente encriptado. Como siempre, debe utilizar las herramientas del sistema operativo, así como cualesquiera otras medidas que elija, para proteger el equipo donde reside MDaemon y la estructura de directorios, para prevenir accesos no autorizados. Las opciones de credenciales de autentificación se agregaron a: Correo Desconocido 111, Enrutamiento de Listas de Distribución 300, Editor de Puertas de Enlace » Reenvío 268, Editor de Puertas de Enlace » Desencolamiento 269 y Editor de Cuentas » Reenvío 729.

Autentificación de Host 132

La Autentificación de Host es una pantalla nueva donde puede configurar los valores de puerto, inicio de sesión y contraseña, para cualquier host. Cuando MDaemon envía correo SMTP a ese host, se utilizarán las credenciales asociadas a ese host registradas ahí. Por favor note que esas credenciales son una opción alterna y solo se utilizan cuando no están disponibles credenciales específicas para ciertas tareas. Por ejemplo, si configura el inicio de sesión/contraseña Auth utilizando las nuevas opciones Editor de Cuentas » Reenvío 729 o Administrador de Puertas de Enlace » Desencolamiento 269, entonces se utilizan esas credenciales y tienen prevalencia sobre las configuradas aquí. Esta funcionalidad aplica solo para nombres de host (no direcciones IP).

Colas Personalizadas Mejoradas y Enrutamiento de Mensajes 877

Ahora puede especificar un host, inicio de sesión, contraseña, SMTP return-path y puerto para cualquier cola remota. Si se proporcionan, todos los mensajes en la cola se entregan utilizando los estos nuevos ajustes. Sin embargo, por diseño aún es posible que mensajes individuales en la cola tengan sus propios datos únicos de entrega, que tendrán prioridad sobre estos nuevos ajustes. Adicionalmente, ahora puede configurar tantas colas remotas como lo desee, filtrar correo utilizándolas a través del Filtro de Contenido, con base en cualquier criterio que usted elija, dar a cada cola su propio horario de entrega y realizar un enrutamiento completamente distinto con base en lo que usted requiera.

Dominios Compartidos Mejorados 123

Durante algún tiempo la funcionalidad de Dominios Compartidos ha realizado búsquedas del valor SMTP MAIL del remitente conforme se requería. Sin embargo, con frecuencia se rechazaban mensajes con el mensaje 'Authentification Required' aunque no hubiera manera de que se realizara la autentificación cuando la cuenta remitente residía en un servidor distinto. Esto se ha resuelto y MDaemon puede aceptar correo sin requerir autentificación para cuentas que existen en otros servidores. Esto se puede deshabilitar con la nueva opción del Administrador de Seguridad en: Autentificación de Remitente » Autentificación SMTP 523. Si prefiere no ejecutar consultas para Dominios Compartidos con base en el valor SMTP MAIL del remitente, puede deshabilitarlo con una opción de Dominios Compartidos.

Los Dominios Compartidos también cuentan con una nueva opción que habilita compartir listas de distribución. Cuando llega un mensaje dirigido a una lista de distribución, se crea una copia para cada host de Dominios Compartidos que cuenta con una versión de esa lista (se hace una consulta para verificar). Cuanto estos hosts reciben sus copias, harán la entrega a todos los miembros de esa lista que

soportan. De esta manera las listas de distribución pueden estar divididas a lo largo de múltiples servidores sin pérdida de funcionalidad. Para que funcione esto cada host de Dominios Compartidos debe incluir las direcciones IP de los otros hosts en su configuración de IPs Confiables 520.

Finalmente, los Dominios Compartidos cuentan con el botón Avanzado que abre un archivo donde puede configurar los nombres de dominio que pueden utilizar Dominios Compartidos. Cuando el archivo está vacío (la condición por omisión) entonces todos sus dominios pueden utilizar Dominios Compartidos. Vea las instrucciones en la parte superior de ese archivo para obtener más información.

Control Mejorado sobre Reenvío de Mensajes

Preferencias » Misceláneos 503 cuenta con una nueva opción que permite a los administradores impedir que una cuenta reenvíe mensajes fuera del dominio. Si un usuario configura el reenvío de mensajes para su cuenta a fin de enviar mensajes a dominios externos, el mensaje se colocará en la Cola de Erróneos. Este ajuste solo aplica a mensajes que se reenvían utilizando las opciones de reenvío de correo para la cuenta.

Editor de Cuentas » Reenvío 729 cuenta con un nuevo botón de *Programación* que le permite a las cuentas configurar una programación para el inicio y fin de reenvíos. Esto también se incluye en la pantalla correspondiente en Plantillas de Cuentas 808. Estos ajustes configuran la fecha y hora en que inicia el reenvío y la fecha y hora en que se detiene; el reenvío solo ocurrirá en los días de la semana que usted seleccione.

El campo Dirección de Reenvío en la Plantilla de Cuentas Nuevas 792 ahora funciona con macros de cuentas. Las únicas macros con datos al momento de creación de cuentas nuevas, son aquellas relativas al nombre completo, dominio, buzón y contraseña de la cuenta. Así (por ejemplo), si desea que todas las cuentas nuevas reenvíen a la misma dirección de correo pero a un dominio diferente, puede colocar esto en el campo Dirección de Reenvío: `$MAILBOX$@example.com`. Las Macros también funcionan con los campos *Send As*, *AUTH Logon* y *AUTH Password*.

Al reenviar un mensaje ahora se actualiza la hora del último acceso de la cuenta que reenvía. Esto significa que las cuentas que no hacen otra cosa más que reenviar correo ya no son potencialmente borradas por inactividad. **Nota**: El reenvío debe ocurrir y no puede ser detenido por otras opciones de configuración tales como restricciones sobre si el usuario que reenvía puede enviar correo o está 'fuera de horario'. El solo tener la cuenta de reenvío configurada no marca automáticamente la cuenta como activa.

Autentificación SMTP Mejorada

Autentificación de Remitente » Autentificación SMTP 523 cuenta con dos opciones nuevas. Primero, la opción "*No permitir autentificación en el puerto SMTP*" deshabilitará completamente el soporte AUTH sobre el puerto SMTP. AUTH no se ofrecerá en la respuesta EHLO y será tratado como un comando desconocido si es proporcionado por el cliente SMTP. La otra opción es "*...agregar la dirección IP al Monitoreo Dinámico si lo intentan de todas formas*". Esta opción agregará al Monitoreo Dinámico 625 la dirección IP de cualquier cliente que intente autentificar cuando AUTH está deshabilitado. La conexión se terminará inmediatamente. Estos ajustes son útiles en configuraciones donde todas las cuentas legítimas están utilizando el puerto MSA (u otro) para enviar correo autentificado. En esas configuraciones se asume que cualquier intento de autentificar en el puerto SMTP debe provenir de un atacante.

Administración de Cuentas Mejorada

Se han expandido las opciones de filtrado del Administrador de Cuentas. Ahora puede elegir desplegar cuentas con base en si están o no Habilitadas, están utilizando MultiPOP, están cerca de su cuota (70% o 90%) o no están reenviando. También puede buscar cualquier texto en el campo de descripción de la cuenta y seleccionar cuentas con base en eso. Más aun, el menú de acceso rápido/clic derecho cuenta con opciones nuevas para agregar o eliminar todas las cuentas seleccionadas de o para listas de distribución o grupos. También cuenta con una opción para Copiar una cuenta existente a fin de crear una cuenta nueva. Todos los ajustes de la cuenta existente se copian a la cuenta nueva excepto el Nombre Completo, Buzón, Contraseña y Carpeta de Correo. Finalmente, la pantalla de Filtros IMAP 737 del Editor de Cuentas tiene un botón nuevo llamado Publicar para agregar una regla nueva a la cuenta que se está editando y a cualquier otra cuenta en el dominio de la misma. Esto puede ahorrar tiempo cuando se necesita una regla nueva para todos.

Habilitar el "No Molestar" para el domino completo 192

La pantalla Nombre de Host & IP 192 del Administrador de Dominios cuenta con un ajuste nuevo que le permite habilitar "No Molestar" para un dominio. Cuando está activo, el dominio rechazará todas las conexiones de todos los usuarios para todos los servicios, pero aceptará mensajes entrantes del mundo exterior. Más aun, puede programar cuando inicia y termina 'No Molestar'. Por ejemplo, si configura Mayo 1, 2020 a Junio 30, 2020 de 5:00pm a 7:00am, Lunes a Viernes, esto significa que no habrá servicios de correo disponibles para los usuarios de ese dominio en esos días de la semana a partir de las 5:00pm y restableciéndose a las 7:01am, en tanto la fecha actual se encuentre entre Mayo 1 y Junio 30 del 2020. Si se borra la fecha de inicio programada, se desactiva la programación y tiene el efecto de **configurar el dominio en 'No Molestar' para siempre.**

Archivo Mejorado 138

El sistema simple de archivo de mensajes de MDaemon se ha modificado para ser más eficiente y consistente. El archivo ahora funciona como sigue: Cuando se entrega un mensaje desde la(s) Cola(s) Local(es) a la carpeta de correo del usuario, se genera una copia en el archivo en ese momento (en la carpeta IN del destinatario, si así está configurado). Cuando un mensaje se toma de la(s) cola(s) Remota(s) para entrega SMTP (ya sea que la entrega tenga éxito o no), se genera una copia en ese momento (en la carpeta 'OUT' del remitente, si así está configurado). Usted verá líneas como "ARCHIVE message: pgp5001000000172.msg" en el archivo de registro de Enrutamiento o puede ver líneas como "* Archived: (archives)\company.test\in\frank@company.test\arc5001000000023.msg" en el archivo de registro de Enrutamiento cuando se procesa el correo Local y Remoto. Así mismo, ahora existe una cola 'ToArchive' como cola del sistema (no se expone en la interface gráfica). Esta cola se verifica en intervalos regulares buscando mensajes que hayan sido colocados ahí (manualmente, por un complemento o de otra manera). Cuando se encuentran mensajes ahí, se archivan y eliminan inmediatamente. Si se encuentran mensajes que no son elegibles para archivar, entonces simplemente se eliminan. El nombre de la cola es \MDaemon\Queues\ToArchive\. La pantalla/archivo de Enrutamiento mostrará detalles siempre que un mensaje sea archivado exitosamente. Así mismo, el Archivado de mensajes encriptados ahora se maneja de forma más consistente. Por omisión, se almacenan en el archivo copias desencriptadas de los mensajes encriptados. Si un mensaje no se puede desencriptar, se almacenará la forma encriptada. Si prefiere almacenar versiones encriptadas, ya existe una opción para permitirle hacer eso. Adicionalmente, ahora hay una opción para archivar mensajes

enviados a direcciones de remisión públicas, que se encuentra habilitada por omisión. finalmente, los tipos siguientes de mensajes nunca se archivan: tráfico de Listas de Distribución, Spam (la opción para hacerlo es obsoleta y ha sido eliminada), mensajes con virus, mensajes a nivel de sistema y autorespuestas.

Archivos de Registro más Eficientes

MDaemon ya no genera archivos de registro vacíos. Cuando se deshabilitan elementos en la pantalla de Ajustes, su archivo de registro asociado no se genera al iniciar el sistema. Los archivos de registro que ya existen cuando se deshabilita un elemento, se quedan en su lugar (no se eliminan). Si un archivo de registro no se encuentra cuando se habilita un elemento, entonces se crea instantáneamente el archivo requerido. Este cambio aplica a todos los archivos de registro que maneja el motor de MDaemon. Los archivos de registro para el Monitoreo Dinámico, Mensajería Instantánea, XMPP, WDaemon y Webmail, corren de manera externa a MDaemon y por esto no se han modificado. Varios otros cambios relacionados a registro incluyen: hacer que los registros de sesiones ATRN se vean correctos, hacer que todos los registros sean consistentes en cuanto a los colores y como despliegan ID ´s de Sesión e Hijos, y el servidor MultiPOP ya no descompone las sesiones para cuentas que ya sobrepasaron su cuota y por esto ya no hay desperdicio en los registros en estos casos. Finalmente, el registro del Enrutamiento solo registraba la segmentación de mensajes en las colas ENTRANTE y LOCAL. Ahora también registra la segmentación de la cola REMOTA cuando se hacen intentos de entrega. De esta manera no se tiene que buscar en el registro de Enrutamiento y en el de SMTP-saliente para ver cuando se procesó un mensaje.

Integración mejorada con Active Directory

Ahora puede configurar la funcionalidad de integración de MDaemon con Active Directory para crear una cuenta en MDaemon cuando agregue a alguien en un grupo de Active Directory y cuando elimine a alguien de un grupo de Active Directory la cuenta correspondiente en MDaemon será deshabilitada (pero no eliminada). Para utilizar esta funcionalidad, debe usar un filtro de búsqueda alternativo de Active Directory. Ver: Active Directory » Autentificación, para más información.

En la pantalla de Autentificación de Active Directory ahora hay una opción separada denominada "*Filtro de Búsqueda de Contactos*" para búsquedas de contactos. Previamente, la búsqueda de contactos se hacía utilizando el filtro de búsqueda de usuarios. También hay un botón de prueba separado para el filtro de búsqueda de contactos. Las búsquedas en Active Directory se han optimizado de manera que cuando los filtros de búsqueda son idénticos una sola consulta actualiza todos los datos. Cuando son distintos, son necesarias dos consultas separadas.

Los campos siguientes se han agregado al archivo de plantillas ActiveDS.dat, de manera que se incluyen en los registros de contactos cuando el monitoreo de Active Directory crea o actualiza las libretas de direcciones: `abTitle=%personalTitle%`, `abMiddleName=%middleName%`, `abSuffix=%generationQualifier%`, `abBusPager=%pager%`, `abBusIPPhone=%ipPhone%` y `abBusFax=%FacsimileTelephoneNumber%`.

Los contactos en Carpetas Públicas ahora se eliminan por omisión cuando la cuenta asociada se elimina de Active Directory. Sin embargo, el contacto solo se elimina si fue creado por la funcionalidad de integración de Active Directory. El ajuste para controlar esto se localiza en la pantalla Monitoreo de Active Directory.

Cuando el sistema de monitoreo de Active Directory crea o actualiza una cuenta y encuentra un valor de buzón demasiado largo para el tamaño de espacio limitado del valor del buzón en MDaemon, truncará el valor del buzón como antes pero ahora

también creará un alias utilizando el valor completo del buzón. Así mismo, cuando se crea una cuenta o alias, la sección de notas de la pantalla Roles Administrativos 757 se actualiza para fines de auditoría.

La pantalla Active Directory 305 del Administrador de Listas de Distribución ahora le permite registrar un atributo de Active Directory para el campo de nombre completo de los miembros de la lista.

Los cambios en las propiedades de las cuentas en Active Director pueden detonar una recreación de una cuenta en MDaemon, aun cuando la cuenta haya sido eliminada previamente desde MDaemon. Para evitar que se vuelvan a crear cuentas de esa manera, se agregó una nueva opción en Monitoreo de Active Directory 828. Por omisión, las cuentas no serán creadas de nuevo cuando sean eliminadas manualmente desde MDaemon.

Monitoreo mejorado del encabezado From 574

Las opciones "*Modificación del Encabezado From*" se movieron de la pantalla de Detección de Secuestro a su propia pantalla Monitoreo del Encabezado From 574 y se agregaron nuevas opciones. Por ejemplo, el Monitoreo del Encabezado From ahora puede validar los nombres de despliegue del encabezado "From:" buscando cualquier cosa que parezca una dirección de correo. Si se encuentra una y no coincide con la dirección del remitente, entonces la dirección que se despliega se puede reemplazar con la dirección de correo real. Por ejemplo, si está utilizando esta funcionalidad y el encabezado "From:" se ve como esto: "`From: 'Frank Thomas <friend@friend.test>' <enemy@enemy.test>`" entonces se modificará a: "`From: 'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>`".

Validación de Contraseñas Comprometidas 855

MDaemon ahora puede verificar las contraseñas de usuario contra una lista de contraseñas comprometidas provenientes de un servicio de terceros. Puede hacer esto sin transmitir la contraseña al servicio, si la contraseña del usuario se encuentra en la lista no significa que la cuenta haya sido hackeada. Significa que alguien en algún lugar ha utilizado los mismos caracteres como contraseña y esta ha aparecido en una violación de datos. Las contraseñas publicadas pueden ser utilizadas por hackers en ataques de diccionario, en cambio contraseñas únicas que nunca se han utilizado en otro lugar son más seguras. Ver Pwned Passwords para más información.

En la pantalla Contraseñas 855 de los Ajustes de Seguridad, MDaemon ahora cuenta con una opción para impedir que la contraseña de una cuenta se configure como una que se encuentre en la lista de contraseñas comprometidas. También puede validar la contraseña cada cierto número de días cuando inician sesión y si la encuentra, envía un correo de advertencia al usuario y al postmaster. Los mensajes de advertencia se pueden personalizar editando los archivos de plantillas de mensajes en la carpeta `\MDaemon\App`. Dado que las instrucciones de cómo puede el usuario cambiar su contraseña pueden depender de si la cuenta utiliza una contraseña almacenada en MDaemon o se está utilizando la autentificación de Active Directory, se tienen dos archivos de plantilla: `CompromisedPasswordMD.dat` y `CompromisedPasswordAD.dat`. Se pueden utilizar Macros para personalizar el mensaje, cambiar el asunto, los destinatarios, etc.

Funcionalidades Adicionales y Mejoras

Se han incluido más de 250 nuevas funcionalidades y mejoras en MDaemon 20, muchas de ellas no se enlistan en esta sección. Para una lista completa de

adiciones, modificaciones y correcciones incluidas en MDaemon, ver las Notas de la versión de MDaemon 20.0.

Lo nuevo en MDaemon Private Cloud 7.5

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

Para obtener una lista de todos los cambios de MDaemon, vea las Notas de la Versión de MDaemon 19.5.3.

Para una lista de todos los cambios de MDaemon Connector, vea las Notas de la Versión de MDaemon Connector 6.5.1.

Lo Nuevo en MDaemon 19.5

Nuevo tema Móvil en Webmail

El tema Móvil de Webmail ha sido reemplazado con una interface de usuario más moderna y con nuevas funcionalidades. Las funcionalidades de Listas de Mensajes incluyen categorías personalizadas, opción de posponer mensajes, ordenamiento por marcados/no leídos/pospuestos, reordenamiento de columnas y recuperación de mensajes. Las funcionalidades del Calendario ahora incluyen Importar/Exportar eventos como archivos csv o ics, agregar calendarios externos, ligas de acceso privado, publicar calendarios y visualizar múltiples calendarios al mismo tiempo. Las funcionalidades de redacción incluyen entrega diferida, múltiples firmas, mensajes en texto/html y plantillas de correo.

Otras funcionalidades incluyen filtros de correo con funcionalidad de arrastrar y soltar, editor de múltiples firmas, más opciones de administración de carpetas, notificaciones, administración de columnas y categorías con funcionalidad de arrastrar y soltar y más. Si Webmail se ejecuta en IIS, se requieren pasos adicionales de configuración para utilizar el tema Móvil. Ver el artículo de la Base de Conocimientos Knowledge Base article 1236 para más información.

Administración de Firmas de Clientes 147

Ahora puede configurar firmas de correo para ser entregadas a sus usuarios de Webmail y MDaemon Connector. Se puede establecer una Firma de Cliente por Omisión 147 o se puede configurar por dominio en la pantalla Firmas de Cliente 215 del Administrador de Dominios. Utilice macros de firmas 148 como `$CONTACTFULLNAME$`, `$CONTACTEMAILADDRESS$`, para personalizar la firma con datos tomados del contacto del usuario en la carpeta Pública de Contactos del dominio. Utilice la macro `$ATTACH_INLINE:filename$` para imágenes en línea en la firma HTML. Luego de registrar el texto de la firma, aparecerá en las opciones de Redacción de Webmail como firma del "Sistema" y se convertirá en la firma por omisión del usuario. Se puede habilitar/deshabilitar para Webmail por omisión bajo Ajustes de Webmail 345, o por dominio en el Administrador de Dominios 201. Para MDaemon Connector, el nombre de la firma y los ajustes relacionados se pueden configurar en los ajustes de Cliente de MC en la pantalla Firma 404. Esta funcionalidad requiere MDaemon Connector 6.5.0 o superior.

Página de Categorías 344

La interface de Administración Remota de MDaemon (MDRA) ahora cuenta con una página de Categorías 344 bajo las opciones de Webmail, para configurar las Categorías del Dominio y las Categorías Personales por omisión.

Mejoras Adicionales a MDRA

Muchas opciones que anteriormente solo podían manejarse desde la interface gráfica de MDaemon, se han agregado a MRDA. Para obtener una lista completa, vea las Notas de la Versión.

Cambios y Funcionalidades Adicionales

MDaemon 24.0 cuenta con muchas nuevas funcionalidades y cambios. Vea `RelNotes.html` que se localiza en la subcarpeta `\Docs\` de MDaemon para obtener una lista completa de todas las nuevas funcionalidades, cambios y correcciones para MDaemon respecto a la versión anterior.

Lo nuevo en MDaemon Private Cloud 7.0

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

Para obtener una lista de todos los cambios de MDaemon, vea las Notas de la Versión de MDaemon 19.0.2.

Para una lista de todos los cambios de MDaemon Connector, vea las Notas de la Versión de MDaemon Connector 6.0.1.

Lo Nuevo en MDaemon 19.0

Soporte a TLS Server Name Indication (SNI) 577

MDaemon ahora soporta la extensión Server Name Indication (SNI) del protocolo TLS que permite que se utilice un certificado distinto para cada uno de los nombres de host en su servidor. MDaemon revisará los certificados activos y elegirá el que contenga el nombre de host solicitado en el campo Subject Alternative Names (puede especificar los nombres alternos al crear el certificado). Si el cliente no solicita un nombre de host o no encuentra un certificado coincidente, se utiliza el certificado por omisión.

XML-API para administración de Carpetas y Elementos

XML-API ha sido expandida para incluir la capacidad de administrar carpetas de correo y elementos en las carpetas. Las carpetas pueden ser creadas, eliminadas, renombradas y movidas utilizando la API. Las operaciones de Elementos soportan correo, calendario, contactos, tareas y notas. Los Elementos pueden ser creados, eliminados y movidos utilizando la API. Puede encontrar documentación completa sobre este tema en la carpeta `MDaemon\Docs\API\XML-API\`.

Mejoras a Administración Remota

La interface web de la Administración Remota de MDaemon (MDRA) se ha expandido para incluir acceso a funcionalidades que anteriormente solo podían ser administradas utilizando la sesión de Configuración (i.e. la interface de aplicación de MDaemon) y ahora cuenta con varias opciones a las que solo se puede acceder vía MDRA. Consecuentemente, para las nuevas instalaciones de MDaemon, el acceso directo para "Iniciar MDaemon" abrirá MDaemon Administración Remota en lugar de abrir la sesión de configuración. Si desea modificar esto, edite el archivo `\MDaemon\App\MDaemon.ini` y configure `[MDLaunch] OpenConfigSession=Yes/No` y `OpenRemoteAdmin=Yes/No`. Si la URL autogenerada no funciona o si MDRA se ejecuta en un servidor web externo, defina la *URL de Administración Remota* en Configurar » Web & Servicios IM » Administración Remota » Servidor Web 356 .

Si no es posible determinar una URL funcional, se abrirá una sesión de Configuración. Finalmente, bajó el menú Inicio de Windows, en el grupo de programas MDaemon, ahora se encuentras accesos directos a *Abrir Sesión de Configuración de MDaemon* y *Abrir Administración Remota de MDaemon*.

Mejoras a Webmail

- A los usuarios de Webmail con la opción *Mostrar las Carpetas de Búsqueda guardadas* (localizada en Webmail bajo Opciones » Carpetas) ahora se les preguntará si desean agregar una carpeta de Búsquedas Guardadas para "Todos los No leídos" y "Todos los Marcados", a su lista. Se les preguntará en una sola ocasión, la primera vez que se inicie sesión. Si un usuario selecciona "No" aún puede crear fácilmente esas Búsquedas Guardadas dando clic en los botones *Crear la Búsqueda Guardada Todos los No Leídos* y *Todos los Marcados* (que también se localiza bajo Opciones » Carpetas). Los Administradores pueden impedir que Webmail pregunte a los usuarios si desean crear esas búsquedas agregando `DefaultSavedSearchesCheck=Yes` bajo `[Default:UserDefaults]` en el archivo `MDaemon\WorldClient\Domains.ini`.
- Se modificaron algunos íconos del tema *WorldClient* para facilitar su visualización.
- Se agregó "(EXPIRADO)" al título de la pestaña del navegador cuando la sesión expira, de manera que, si un usuario no se encuentra en la pestaña de Webmail, aun se enterará de que su sesión ha expirado.
- Se agregó un ícono de eliminar para remover los contactos comunes de la lista de autocompletar.

Lo nuevo en MDaemon Private Cloud 6.5

- MDaemon Private Cloud 6.5 incluye MDaemon 18.5.1 y MDaemon Connector 5.6.0.

Para una lista de todos los cambios de MDaemon, vea el archivo Notas de la versión MDaemon 18.5.1.

Para una lista de todos los cambios de MDaemon Connector vea el archivo Notas de la versión de MDaemon Connector 5.6.0.

Lo nuevo en MDaemon 18.5

Macros de Firmas

Las firmas de MDaemon ahora soportan macros que insertan en la firma la información de contacto del remitente, tomándola de la información del remitente disponible en la Carpeta Pública de Contactos del dominio. Esto permite que las firmas por omisión y de dominio sean personalizadas con la información del remitente. `$CONTACTFULLNAME$`, por ejemplo, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Los valores en blanco se utilizan si no existe contacto para el remitente. Las macros disponibles se enlistan en la página Firmas por Omisión.

Los usuarios también pueden controlar la colocación de las firmas de MDaemon en los mensajes utilizando la macro `$SYSTEMSIGNATURE$` para colocar la firma por omisión o del dominio y `$ACCOUNTSIGNATURE$` para colocar la firma de la cuenta.

MDaemon Mensajería Instantánea en Webmail

Los temas WorldClient y LookOut ahora incluyen un cliente XMPP basado en el navegador, que permite a los usuarios contar con mensajería instantánea sin la necesidad de ejecutar la aplicación de escritorio MDaemon Mensajería Instantánea o alguna otra aplicación cliente XMPP. Los usuarios pueden habilitarla en la pantalla Opciones | Personalizar de Webmail, utilizando la opción "Habilitar en el navegador la funcionalidad MDaemon Mensajería Instantánea". Los Administradores pueden habilitar o deshabilitar la mensajería instantánea por dominio utilizando el Administrador de Dominios, por cuenta utilizando el Editor de Cuentas o por grupo utilizando el Administrador de Grupos.

MDaemon incluye un nuevo servidor BOSH para soportar la mensajería instantánea en Webmail. Sus ajustes se pueden configurar en la pantalla XMPP. (**nuevo en 18.5.1)**.

Webmail se exenta del Monitoreo de Localizaciones

Se agregó una opción de usuario en Webmail para exentar del Monitoreo de Localizaciones los inicios de sesión con Autentificación de Dos Factores. Si un usuario tiene habilitada la variable `BypassLocationScreeningTFA=Yes` en la sección `[User]` de su archivo `User.ini` file y la Autentificación de Dos Factores está habilitada para el usuario, se omite el Monitoreo de Localizaciones. Esto permite a los usuarios iniciar sesión en Webmail en países que normalmente serían bloqueados por el Monitoreo de Localizaciones.

Integración AD Mejorada

Los usuarios cuyas cuentas están configuradas para utilizar la autentificación con Active Directory (AD) ahora pueden modificar su contraseña en AD desde Webmail si el ajuste "AllowADPasswordChange" está habilitado en \MDaemon\WorldClient\Domains.ini. Se encuentra deshabilitado por omisión.

MDRA Ampliado

Interface web de Administración Remota de MDaemon se ha ampliado para incluir acceso a muchas funcionalidades que formalmente solo se podrían administrar utilizando la interface gráfica de MDaemon.

Lo nuevo en MDaemon Private Cloud 6.0

- MDaemon Private Cloud 6.0 incluye MDaemon 18.0.2 y MDaemon Connector 5.5.2.

Para una lista de todos los cambios de MDaemon, vea el archivo Notas de la versión MDaemon 18.0.2.

Para una lista de todos los cambios de MDaemon Connector vea el archivo Notas de la versión de Outlook Connector 5.5.2.

Lo nuevo en MDaemon 18.0

DNSSEC 593

La nueva opción DNSSEC (DNS Security Extensions) permite a MDaemon actuar como un Resolutor de Seguridad de Segmentos (Stub) no Validador, que se define en las RFCs 4033 y 4035 como "una entidad que envía consultas de DNS, recibe respuestas de DNS y es capaz de establecer un canal seguro apropiado hacia un servidor de nombres recursivo seguro de que proporcionará estos servicios por parte del resolutor de segmentos". Esto significa que durante las consultas DNS de MDaemon, este puede hacer una petición DNSSEC a sus servidores DNS, estableciendo el bit AD (Authentic Data) en las consultas y validando las respuestas. Esto puede proporcionar un nivel adicional de seguridad durante el proceso de DNS para algunos mensajes, aunque no para todos dado que DNSSEC aún no está soportado por todos los servidores de DNS o para todos los dominios de primer nivel.

Cuando se habilita, el servicio DNSSEC solo se aplica a mensajes que cumplen con sus criterios de selección; se puede solicitar o requerir tan amplia o restrictivamente como prefiera. Simplemente defina cualquier combinación de "`Header Value`" en la pantalla DNSSEC y MDaemon hará la petición al servicio DNSSEC, al hacer consultas DNS, para cualquier mensaje que cumpla los criterios establecidos. Cuando los resultados del DNS no incluyen datos autentificados el resultado no tiene consecuencias negativas; MDaemon simplemente regresa a la conducta normal para la consulta de DNS. Sin embargo, si desea *requerir* DNSSEC para ciertos mensajes, agregue "SECURE" a la combinación encabezado/valor (ej.. `Para *@example.net SECURE)`. Para esos mensajes, cuando los resultados de DNS no incluyen datos autentificados, el mensaje se regresará al remitente. **Nota:** Dado que las consultas DNSSEC requieren mayor tiempo y recursos y como DNSSEC no es soportado por todos los servidores, MDaemon no está configurado para aplicar DNSSEC por omisión para la entrega de todos los mensajes. Si desea requerir DNSSEC para todos los mensajes, lo puede hacer incluyendo "`Para *`" en sus criterios.

Escaneo de Buzones con AntiVirus

Existe una nueva opción *Escanear todos los mensajes cada [n] día(s)* en Seguridad » AntiVirus 668 que se puede utilizar para escanear periódicamente todos los mensajes almacenados, para detectar cualquier mensaje infectado que haya pasado por el sistema antes de que estuviera disponible la actualización más reciente de firmas del antivirus para interceptarlo. Los mensajes infectados serán movidos a la carpeta de cuarentena y se insertará un encabezado `X-MDBadQueue-Reason`, para que usted pueda ver la explicación cuando visualice la cola en MDaemon. Los mensajes que no puedan ser escaneados no se enviarán a la cuarentena. También se tiene una opción *Configurar escaneo de buzones* para especificar la frecuencia

con la que desea que se escaneen los mensajes y si desea que se escaneen todos o solo aquellos que tengan menos de ciertos días. También puede ejecutar manualmente el escaneo de buzones de manera inmediata.

Exentar del Monitoreo de Localizaciones Dispositivos ActiveSync conocidos

Habilite la nueva opción Exentar del Monitoreo de Localizaciones[460] en la pantalla de ajustes de un cliente ActiveSync si desea que el dispositivo pueda omitir la validación del Monitoreo de Localizaciones[572]. Esto permite que un usuario válido siga teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentre viajando en una ubicación que de otra manera estaría bloqueada de intentos de autentificación. A fin de exentar el dispositivo debe haberse conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configura en el ajuste Eliminar clientes inactivos luego de estos días[418] ubicado en la pantalla de puesta a punto. Al exentar un dispositivo del Monitoreo de Localizaciones, también se tiene una opción para poner en lista blanca la dirección IP remota dese la que se está conectando. Esto puede ser útil para permitir a otros clientes que podrían conectarse desde la misma dirección IP.

Nuevas funcionalidades de Webmail y MDRA

Recuérdame

Ahora puede habilitar la casilla "Recuérdame" para las páginas de inicio de sesión en MDaemon Webmail y MDaemon Administración Remota (MDRA), vía las opciones localizadas en la Pantalla de Ajustes[345] de Webmail y la Pantalla de Servidor Web[356], de MDRA respectivamente. Cuando se habilita esta opción, los usuarios que inicien sesión vía el puerto https verán la casilla de verificación. Si los usuarios habilitan esta casilla, sus credenciales serán recordadas para ese dispositivo. Así, en cualquier momento en que utilicen ese dispositivo para conectarse a Webmail o MDRA en el futuro, su sesión iniciará en automático, hasta el momento en que cierren la sesión manualmente o expire su token de Recuérdame. La opción *Recuérdame* se encuentra deshabilitada por omisión y aplica a todos los dominios. Si desea omitir este ajuste para ciertos dominios en Webmail, utilice el ajuste *Recuérdame* localizado en la pantalla Webmail[201] en el Administrador de Dominios, en la interface gráfica de MDaemon.

Por omisión, las credenciales del usuario serán recordadas durante 30 días antes de que se obligue a que inicien sesión de nuevo, pero puede utilizar la opción *Expirar los tokens de Recuérdame luego de estos días* (localizada en MDRA) para definir el número de días que usted defina. Puede establecer esta opción para hasta 365 días. **Nota:** Autentificación de Dos Factores[720] (2FA) cuenta con su propia llave de vencimiento de Recuérdame (`TwoFactorAuthRememberUserExpiration=30`), localizada en la sección `[Default:Settings]` del archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. Por esto, 2FA se requerirá nuevamente al iniciar sesión cuando expire el token 2FA Recuérdame, aun cuando el token regular siga siendo válido.

En MDRA también hay un botón *Recuérdame* que puede utilizar si sospecha que una cuenta ha tenido un fallo de seguridad. Esto restablecerá los tokens Recuérdame para todos los usuarios haciendo que tengan que iniciar sesión de nuevo.

Posponer correo (Snooze)

En MDaemon Webmail ahora puede posponer un correo en su lista de mensajes. Un mensaje pospuesto estará oculto durante un lapso predeterminado. Para posponer un mensaje, de clic derecho sobre él y seleccione la opción "Posponer por..." en el menú contextual. Luego elija cuanto tiempo desea que se posponga el mensaje. La opción "Elegir fecha y hora" solo está disponible para navegadores que soportan el registro de fecha y hora. Los mensajes ocultos se pueden visualizar en el tema LookOut dando clic en el ícono "Ver Mensajes Pospuestos" en la barra de herramientas; en el tema WorldClient deberá elegir "ver ocultos" en la vista del menú desplegable en la barra de herramientas. Esta funcionalidad está habilitada por omisión. Para deshabilitarla vaya a Opciones | Personalizar en Webmail, en los Ajustes de Bandeja de Entrada. Deshabilite la casilla "Habilitar Posponer Mensajes". No existen controles para posponer mensajes en los temas Lite y Mobile, pero los mensajes pospuestos se mantienen ocultos.

Calendarios Públicos

En MDaemon Webmail los usuarios ahora pueden publicar un calendario en una liga accesible públicamente, además, tienen la opción de proteger con contraseña ese calendario. Para publicar un calendario, en los temas LookOut o WorldClient de Webmail vaya a Opciones | Carpetas y de clic en el botón "Compartir Carpeta" al lado del calendario que desea publicar. Luego, abra la pestaña Acceso Público y si lo desea, registre el nombre de despliegue o el requerimiento de contraseña y de clic en el botón "Publicar Calendario". Se desplegará un diálogo de confirmación; luego de dar clic en OK una alerta desplegará la nueva URL donde estará disponible el calendario. También se presentará una liga en la página una vez que el calendario haya sido publicado. Para deshabilitar la publicación del calendario, dé clic en el botón "Despublicar Calendario". Para modificar la contraseña o el nombre de despliegue, dé clic en el botón "Actualizar".

Si desea deshabilitar esta funcionalidad globalmente, modifique el valor de la llave `EnablePublicCalendars` a **No** en la sección `[Default:Settings]` del archivo `Domains.ini` file. Para deshabilitarla por usuario, agregue `CanPublishCalendars=No` al archivo `User.ini` de cada usuario.

Lo nuevo en MDaemon Private Cloud 5.5

- MDaemon Private Cloud 5.5 incluye MDaemon 17.5.2 y Outlook Connector 5.0.1.

Para una lista de todos los cambios de MDaemon, vea el archivo Notas de la versión MDaemon 17.5.2.

Para una lista de todos los cambios de Outlook Connector vea el archivo Notas de la versión de Outlook Connector 5.0.1.

Lo nuevo en MDaemon 17.5

Monitoreo de Localizaciones

El Monitoreo de Localizaciones es un sistema de bloqueo geográfico que puede utilizar para bloquear conexiones entrantes SMTP, POP o IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Administración Remota, CalDAV/CardDAV y Minger provenientes de regiones del mundo no autorizadas por usted. MDaemon

determina el país asociado con la dirección IP que intenta conectarse, bloquea la conexión si pertenece a una localización restringida y agrega una línea al registro del Monitoreo. En el caso de SMTP, el Monitoreo de Localizaciones puede bloquear opcionalmente las conexiones utilizando AUTH. Esto es útil, por ejemplo, si no tiene usuarios en un país en específico, pero desea poder recibir correo de ahí. De esa manera solo bloqueará a aquellos intentando abrir sesión en su servidor.

La carpeta `\MDaemon\Geo\` contiene los archivos de base de datos que se utilizan como base de datos maestra de IP´s por país. Estos archivos fueron proporcionados por MaxMind (www.maxmind.com) y es posible descargar actualizaciones de ese sitio si se desea.

Monitoreo Dinámico para todos los Protocolos y Servicios 610

El sistema de Monitoreo Dinámico de MDaemon se ha expandido de manera considerable para operar con SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Administración Remota, CalDAV/CardDAV, XMPP y Minger. Los fallos de autentificación se rastrean a través de esos servicios y las direcciones IP pueden bloquearse para todos ellos. El Monitoreo Dinámico puede configurarse en el nuevo diálogo multi-pestañas que se encuentra bajo el menú Seguridad.

Adjuntos PIM

Los elementos PIM (calendario, contactos, tareas, notas) ahora soportan archivos adjuntos. Estos se pueden agregar a un elemento PIM vía Webmail, Outlook Connector o CalDAV/CardDAV. Al programar una reunión, los adjuntos se enviarán a los asistentes a ella.

PGP Key-exchange Durante SMTP 629

El diálogo MDPGP contiene una nueva opción para habilitar la transmisión automática de llaves públicas como parte del proceso SMTP de entrega de mensajes. para hacerlo, el servidor SMTP de MDaemon respetará el comando SMTP denominado RKEY. Al enviar un mensaje a un servidor que soporta RKEY, MDaemon le ofrecerá al servidor destino transmitir la llave pública preferida del usuario remitente. El servidor responderá indicando ya sea que ya tiene esa llave ("250 2.7.0 Key already known") o que la requiere, en cuyo caso la llave se transfiere inmediatamente en un formato ASCII protegido ("354 Tecla Intro, terminar con CRLF.CRLF") tal como un mensaje de correo. Las llaves que han expirado o han sido revocadas nunca se transmiten. Si MDaemon cuenta con múltiples llaves para el remitente, siempre enviará la llave marcada en el momento como preferida. Si no hay una llave preferida entonces se enviará la primera que se encuentre. Si no hay llaves válidas disponibles, no se hace nada. Solo se ofrecen llaves públicas pertenecientes a usuarios locales.

La transferencia de llaves públicas ocurre como parte de la sesión SMTP que entrega el mensaje proveniente del usuario. A fin de que sean aceptadas las llaves públicas transmitidas de esta manera, la llave pública debe enviarse junto con un mensaje que lleve Firma DKIM 532 del dominio del propietario de la llave con el parámetro i=set apuntando a la dirección del propietario de la llave, que debe coincidir exactamente con el encabezado From:, del cual solo puede existir uno. El "propietario de la llave" se toma de la llave misma. Así mismo, el mensaje debe llegar al servidor destino en la ruta SPF 526 del remitente. Finalmente, el propietario de la llave (o su dominio entero vía el uso de comodines), debe ser autorizado por RKEY agregando un registro apropiado en el archivo de reglas MDPGP (las instrucciones para esto se encuentran en el archivo de reglas), indicando que el dominio es confiable para el intercambio de llaves. Toda la verificación se realiza

automáticamente pero debe tener habilitados DKIM 529 y la verificación SPF 526 o no podrá realizarse ninguna acción.

El registro del servicio MDPGP muestra los resultados y detalles de todas las llaves importadas o eliminadas y el registro de la sesión SMTP también rastrea esta actividad. Este proceso rastrea la eliminación de llaves existentes y la selección como preferidas de llaves nuevas y actualiza a todos los servidores participantes a los que envía mensajes de correo cuando algo se modifica.

Administrar Complementos de Outlook para usuarios de Outlook Connector 406

La nueva pantalla Complementos en el diálogo de Ajustes del Cliente OC, permite administrar el estado de los complementos de Outlook utilizados por sus usuarios de Outlook Connector. Puede permitir que se utilicen normalmente cualquiera o todos los complementos, o puede deshabilitar el complemento que desee. Esta funcionalidad puede ser útil específicamente en casos donde usted sabe de complementos específicos que tienen conflicto con el Cliente de Outlook Connector, permitiéndole deshabilitarlo para evitar problemas. La funcionalidad de Complementos requiere Outlook Connector 5.0 o superior.

Modificaciones a Webmail

Importar/Exportar Grupos/Listas de Distribución
En los temas LookOut y WorldClient, se agregó una opción para exportar e importar Grupos/Listas de Distribución de y hacia una carpeta de contactos en Webmail. El formato es específico para MDaemon Webmail, dado que Outlook no soporta la exportación/importación de Grupos. El formato es el siguiente:

Columnas: **Group GUID**, **Group Name**, **GUID**, **Full Name**, **Email**

Cada línea que contiene ya sea un Nombre de Grupo o un GUID de Grupo se considera el inicio de un grupo nuevo. Cualquier GUID, Nombre Completo o Cuenta de correo en esa línea se considera el primer miembro del grupo/lista.

Ejemplo de Excel:

Group GUID	Group Name	GUID	Full Name	Email
	Los Jedis		Anakin Skywalker	ani@jedi.mail
			Leia Organa	leia.organa@jedi.mail
			Luke Skywalker	luke.skywalker@jedi.mail
			Yoda	yoda@jedi.mail
	Los Siths		Darth Maul	darth.maul@sith.mail
			Darth Vader	darth.vader@sith.mail
			Emperor Palpatine	emperor.palpatine@sith.mail

Al realizar la importación, el GUID del Grupo se reemplaza con uno nuevo. Si no se incluye Nombre de Grupo, el nombre se desplegará sin traducción como "ImportedFromCSV_%GUID%", donde %GUID% se reemplaza con los primeros cinco caracteres del GUID. Si se dejan vacías las celdas a la derecha de un nombre de

grupo vacío, el resultado será que la siguiente línea será el primer miembro del grupo/lista. El campo Email se requiere para que el miembro sea agregado.

Grabación de Voz
Se agregó la funcionalidad de Grabación de Voz en los temas LookOut y WorldClient. Requiere de un micrófono y solo está disponible para ciertos navegadores. Puede ser deshabilitada por el Administrador o autorizada a nivel usuario agregando `EnableVoiceRecorder=No` en el archivo User.ini. Los usuarios están limitados a cinco grabaciones de cinco minutos cada una. Si se intenta grabar más de 5, el resultado será que ya sea la grabación seleccionada o la primera grabación, serán reemplazadas con la nueva (se le preguntará al usuario). Cuando se detiene la grabación (ya sea automáticamente o por el usuario), la grabación se convierte a formato mp3 y se carga al servidor. Los usuarios cuentan con cuatro opciones respecto a cada grabación:

- Grabar en el Escritorio
- Grabar en la carpeta de Documentos por omisión de WorldClient
- Enviar en un correo utilizando un diálogo rápido que solo incluye los campos Para, CC, CCO, Asunto y el cuerpo de mensaje en formato de texto plano.

  Solo se requiere el campo Para. Se cuenta con frases genéricas para el Asunto y el Cuerpo del mensaje que se utilizan cuando el usuario no registra valores para estos campos.
- Abrir una nueva ventana de Redacción con la grabación adjunta.

Los usuarios solo pueden actuar sobre una grabación a la vez. Por ejemplo, solo se puede enviar una grabación en un mensaje. Si el usuario desea enviar varias grabaciones en un mensaje, deberá guardar cada una de ellas en la carpeta de documentos y luego agregarlas como adjunto manualmente.

Nuevas funcionalidades de Administración de Carpetas
Los temas LookOut y WorldClient tienen nuevas funcionalidades para administración de carpetas e la vista Opciones » Carpetas y en la vista principal de la lista de carpetas.

En la vista de la lista de carpetas (panel izquierdo):

- Los usuarios pueden arrastrar y soltar para mover carpetas de una carpeta padre a otra.
- Los usuarios pueden renombrar carpetas y darles apodos dando clic sobre ellos por segunda vez (luego de seleccionar la carpeta)
- Ahora es posible Mostrar Carpetas por Tipo en el tema LookOut
- Si ya existe por lo menos una carpeta favorita (porque los favoritos están ocultos hasta que se agrega uno), los usuarios pueden arrastrar y soltar una carpeta en favoritos a fin de agregarla (si se arrastra una carpeta fuera de favoritos no ocurre nada).
- Los diálogos carpeta nueva y renombrar carpeta se agregaron al tema LookOut

En la vista Opciones » Carpetas, el árbol de carpetas ahora es colapsable y el diálogo Carpeta Nueva se ha movido a una ventana externa similar al tema WorldClient.

Lo nuevo en MDaemon Private Cloud 5.0

- MDaemon Private Cloud 5.0 incluye MDaemon 17.0.2 y Outlook Connector 4.5.
- Se actualizó a la versión más reciente del motor antivirus Cyren AV.
- Los Administradores del Dominio ahora pueden administrar los servicios web en Administración Remota desde MDPC.

Para una lista de todos los cambios de MDaemon, vea el archivo Notas de la versión MDaemon 17.0.2.

Para una lista de todos los cambios de Outlook Connector vea el archivo Notas de la versión de Outlook Connector 4.5.

Lo nuevo en MDaemon 17.0

Soporte para XMPP 374 en WorldClient Mensajería Instantánea 322 (WCIM)

WCIM ahora utiliza el protocolo XMPP para mensajería instantánea en lugar del protocolo propietario de WorldClient. Esto permite que el cliente de escritorio de WCIM se comunique no solo con otros clientes WCIM, sino con cualquier otro cliente XMPP de terceros (incluyendo clientes móviles) conectados a su servidor XMPP. Adicionalmente, WCIM ahora cuenta con dos tipos de conexiones: "WCMailCheck" y "WCIMXMPP." WCMailCheck se conecta con WorldClient para la recepción de notificaciones de correo nuevo y el conteo de mensajes. WIMXMPP se conecta al servidor XMPP para la mensajería instantánea. Consecuentemente, los usuarios WCIM ahora cuenta con una entrada para cada tipo de conexión listada en la pantalla Conexiones del cliente (ej. "Example.com Mail" y "Example.com WCIM"). Al actualizar a la versión 17, WCIM creará automáticamente una conexión WCIMXMPP para dar continuidad a su conexión WCMailCheck previamente existente y migrará sus contactos IM del nuevo sistema a XMPP. El aspecto y funcionamiento del nuevo cliente WCIM es esencialmente el mismo, pero existen algunas diferencias, tales como la manera en que se administran las conversaciones con contactos o grupos. Vea la Ayuda en el cliente WCIM para más información sobre lo que se ha modificado.

Integración de WorldClient con Dropbox 337

WorldClient ahora está equipado con soporte directo para Dropbox, lo que permite a los usuarios grabar archivos adjuntos en sus cuentas Dropbox, e insertar ligas directas a archivos en Dropbox en los mensajes salientes. Para proporcionar esta funcionalidad a sus usuarios de WorldClient, debe configurar WorldClient como app de Dropbox en la Plataforma de Dropbox. Este es un proceso sencillo, que solo requiere que se firme a su cuenta Dropbox, crear un nombre único para la app con acceso total a Dropbox, especificar la URI de Redireccionamiento hacia WorldClient y modificar un ajuste por omisión. Luego, debe copiar y pegar la AppKey y App Secret de Dropbox en las opciones de la pantalla Dropbox en MDaemon. Luego de eso, sus usuarios podrán ligar sus cuentas Dropbox con WorldClient la siguiente ocasión que inicien sesión en WorldClient. Para instrucciones paso a paso sobre cómo crear su app de Dropbox y ligarla a WorldClient, vea: Crear y Ligar su App de Dropbox 339.

Cuando crea su app de Dropbox, tendrá un estatus inicial de "Desarrollo". Esto permite hasta a 500 usuarios de WorldClient ligar sus cuentas de Dropbox a la app. De acuerdo con Dropbox, sin embargo, "una vez que su app ligue a 50 usuarios de Dropbox, le quedarán dos semanas para solicitar y recibir estatus de Producción antes de que la capacidad de su app para ligar usuarios adicionales de Dropbox se congele, sin importar cuantos usuarios entre 0 y 500 haya ligado su app". Esto significa que hasta que reciba aprobación de estatus Producción, la integración con Dropbox continuará funcionando, pero usuarios adicionales no podrán ligar sus cuentas. La obtención de aprobación para pasar al estatus de Producción es un proceso directo para asegurar que su app cumple con los lineamientos y términos de servicio de Dropbox. Para más información, vea la sección Aprobación para Producción en la Guía para Desarrolladores de la plataforma Dropbox.

Una vez que su app de WorldClient haya sido creada y configurada correctamente, cada usuario de WorldClient tendrá la opción de conectar su cuenta con la de Dropbox, al iniciar sesión en WorldClient. Se solicita al usuario iniciar sesión en Dropbox y otorgar permisos para que la app tenga acceso a la cuenta de Dropbox. Entonces el usuario será redirigido de vuelta a WorldClient utilizando una URI que se dio a Dropbox durante el proceso de autentificación. Para mayor seguridad, esa ruta debe coincidir con alguna de las URIs de redireccionamiento que se especificaron en la página de información de la app en Dropbox.com. Finalmente, WorldClient y Dropbox intercambiarán un código de acceso y un token de acceso que le permitirá a WorldClient conectarse a la cuenta de Dropbox del usuario de manera que el usuario pueda grabar archivos adjuntos ahí. El token de acceso expira cada siete días, lo que significa que el usuario debe reautorizar periódicamente la cuenta para utilizar Dropbox. Alternativamente, los usuarios pueden desconectar manualmente su cuenta de Dropbox o reautorizarla cuando sea necesario, desde la pantalla de opciones Cloud Apps en WorldClient.

Integración con Let's Encrypt 594 vía script de PowerShell

Para soportar SSL/TLS y HTTPS 575 para MDaemon 577, WorldClient 580 y la Administración Remota 584, se requiere contar con un certificado SSL/TLS. Los certificados son pequeños archivos emitidos por una Autoridad de Certificación (Certificate Authority -CA), que se utilizan para verificar que un cliente o navegador está conectado al servidor pretendido y para habilitar SSL/TLS/HTTPS para realizar conexiones seguras al servidor. Let's Encrypt es un CA que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los complejos procesos actuales para crear, validar, firmar, instalar y renovar manualmente certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar certificados, MDaemon incluye un script de PowerShell en la carpeta "`MDaemon\LetsEncrypt`". Una dependencia del script, el módulo ACMESharp, requiere PowerShell 5.1 y .Net Framework 4.7.2, lo que significa que el script no funcionará con Windows 2003. Adicionalmente, WorldClient debe estar escuchando en el puerto 80 o la validación HTTP no podrá completarse y el script no funcionará. Usted deberá configurar correctamente la política de ejecución de PowerShell antes de que le permita ejecutar este script. Al ejecutarlo, se configurará todo para Let's Encrypt, incluyendo colocar los archivos necesarios en la carpeta HTTP de WorldClient, para completar la validación http-01. Utiliza el nombre de host SMTP 192 del dominio por omisión 190 como dominio para el certificado, recupera el certificado, lo importa hacia Windows y configura MDaemon para utilizar el certificado para MDaemon, WorldClient y la Administración Remota.

Si tiene configurado un FQDN 192 como su dominio por omisión, que no apunta al servidor MDaemon, este script no funcionará. Si desea configurar nombres de host

alternativos en el certificado, lo puede hacer introduciéndolos en la línea de comando.

Ejemplo de uso:

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

No necesita incluir el FQDN para el dominio por omisión en la lista `AlternateHostNames`. Por ejemplo, suponga que su dominio por omisión es "`example.com`" configurado con el FQDN "`mail.example.com`" y desea utilizar un nombre alterno de servidor como por ejemplo "`imap.example.com`". Cuando ejecute el script, solo le pasará el valor "`imap.example.com`" como nombre alterno de host- Más aun, si pasa nombres alternos de host, se requerirá completar una validación HTTP para cada uno de ellos. Si las validaciones no se completan entonces el proceso no concluirá correctamente. Si no desea utilizar ningún nombre alterno de host, entonces no incluya el parámetro `-AlternateHostNames` en la línea de comando.

Si está ejecutando WorldClient vía IIS; deberá parar a este script el nombre de su sitio utilizando el parámetro `-IISSiteName`. Debe contar con las Web Scripting Tools de Microsoft a fin de que el certificado se configure en automático en IIS.

Finalmente, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script. El registro incluye la fecha y hora de inicio del script, pero no la fecha/hora de cada acción. Así mismo, es posible enviar correos de notificación cuando ocurre un error. Esto se realiza utilizando la variable `$error`, que es creada y configurada automáticamente por PowerShell. Si no desea recibir correos de notificación cuando ocurre un error, no incluya el parámetro `-To` en la línea de comando.

Opción para almacenar contraseñas de buzones utilizando encripción no-reversible

Existe una nueva Opción de Contraseñas 855 para almacenar contraseñas de buzones utilizando encripción no-reversible. Esto impide que las contraseñas sean desencriptadas por MDaemon, el administrador o un posible atacante. Cuando se habilita, MDaemon utiliza la función de hashing bcrypt, que permite contraseñas largas (hasta 72 caracteres) y que las contraseñas se graben, pero no se revelen al exportar e importar cuentas. Sin embargo, algunas funcionalidades no son compatibles con esta opción, tal como la detección de contraseñas débiles y la autentificación APOP & CRAM-MD5, ya que dependen de que MDaemon pueda desencriptar las contraseñas. Las contraseñas no-reversibles están habilitadas por omisión.

Aprobación de cliente ActiveSync

Se cuenta con un nuevo ajuste de ActiveSync que puede utilizar para requerir que los "Clientes nuevos deben ser autorizados por el administrador antes de sincronizarse" con una cuenta. La lista de Clientes 460 indica los clientes en espera de autorización y el administrador puede autorizarlos desde la misma pantalla. Esta opción está disponible en las pantallas de Ajustes de Cliente Global 421 y de Cuentas 765. La opción global se encuentra deshabilitada por omisión y la opción de cuenta está configurada para "Heredar".

Notificaciones ActiveSync

Se han agregado dos tipos de notificaciones administrativas a ActiveSync: Sync Rollback y Corrupt Message.

Notificaciones de Sync Rollback

El Servicio ActiveSync ahora puede notificar a los administradores si un cliente está enviando repetida/frecuentemente Sync Keys expiradas en operaciones Sync.

Esto informa meramente al administrador que el servidor emitió un rollback para una colección dada porque el cliente hizo una petición de sincronización con la llave Sync expirada más recientemente. El asunto dice "ActiveSync Client Using expired Sync Key". Esto puede ocurrir por errores de red o algo sobre el contenido enviado previamente al cliente en esa colección. En algunos casos, se encontrará el ID del ítem, esto depende meramente de si la sincronización previa sobre esa colección envió o no cualesquiera elementos.

Las advertencias de Rollback no significan que el cliente no está Sincronizado, significan que el cliente tiene el potencial de dejar de sincronizar y que nuestro sistema interno lo detectó. Las advertencias de Rollback se emiten para una colección no más de una vez en un periodo de 24 horas. Las llaves siguientes se pueden editar en el encabezado [System] en el archivo `\MDaemon\Data\AirSync.ini`:

[System] SendRollbackNotifications=[0|1|Yes|No|True|False]

- [System] RollbackNotificationThreshhold=[1-254] : Número de rollbacks que deben ocurrir sobre una colección dada antes de que se envíe una notificación al administrador. Recomendamos un valor por lo menos de 5 aquí dado que las intermitencias de red juegan una parte en esto.
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Si se deberá o no enviar copia al usuario cuyo cliente envió esa llave Sync expirada.

Notificaciones ActiveSync de Mensajes Corruptos

El servicio ActiveSync ahora puede notificar a los administradores si no fue posible procesar un mensaje en particular. Estas notificaciones se envían en tiempo real para informar al admin de un elemento de correo que no pudo ser segmentado y que no es posible realizar acciones posteriores sobre él. El asunto dice "Notificación de Mensaje Corrupto". Estos elementos, en versiones anteriores, podían originar un fallo inesperado del servidor ActiveSync. En la mayoría de los casos, el contenido del archivo msg no serán datos MIME. Si son datos MIME, lo más probable es que esté corrupto. Puede elegir enviar copia de estas notificaciones al usuario afectado con la llave CMNCCUser para que esté consciente de que llegó un mensaje ilegible a su buzón. La acción correcta para esto es remover el archivo msg del buzón del usuario y analizarlo para determinar por qué no fue posible segmentarlo y como llegó a existe en el estado en que se encuentra. Las llaves siguientes se pueden editar en el encabezado [System] en el archivo `\MDaemon\Data\AirSync.ini`:

- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False] (Default is Enabled)
- [System] CMNCCUser==[0|1|Yes|No|True|False]

Lo nuevo en MDaemon Private Cloud 4.5

- MDaemon Private Cloud 4.5 incluye MDaemon 16.5.2 y Outlook Connector 4.0.1.
- Para el plugin ClamAV se agregó la opción de colocar en cuarentena los archivos que no es posible escanear. También se agregó una opción para permitir pasar archivos protegidos con contraseña que no pueden ser escaneados. Si se permiten archivos no-escaneados, en encabezado "X-CAV-Result:" puede contener "encriptado" (archivo protegido con contraseña), "no-escaneado" (no pudo ser escaneado), o "error de escaneo" (error durante el escaneo).

Para una lista de todos los cambios de MDaemon, vea el archivo Notas de la versión MDaemon 16.5.

Para una lista de todos los cambios de Outlook Connector vea el archivo Notas de la versión de Outlook Connector 4.0.1.

Lo nuevo en MDaemon 16.5

Mejoras a MDPGP

Soporte a Servidor de Llaves

WorldClient

WorldClient ahora puede actuar como un servidor de llaves públicas básico. Habilite esta nueva opción de MDPGP a "*Enviar llaves públicas sobre HTTP (WorldClient)*", entonces WorldClient responderá a las peticiones de llaves públicas de sus usuarios. El formato de la URL para hacer la petición es este: "`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`". Donde `<WorldClient-URL>` es la ruta de su servidor WorldClient (por ejemplo, "`http://wc.example.com`") y `<Key-ID>` es el key-id de dieciséis caracteres de la llave que requiere (por ejemplo, "`0A1B3C4D5E6F7G8H`"). La key-id se construye a partir de los últimos 8 bytes de la huella de la llave - 16 caracteres en total.

DNS (PKA1)

Habilite la nueva opción de MDPGP en "*Obtener llaves públicas del DNS (pka1) y conservar en cache durante [xx] horas*" si desea que MDPGP consulte las llaves públicas del destinatario de un mensaje en el DNS utilizando PKA1. Esto es útil porque automatiza el proceso de obtener las llaves públicas de algunos destinatarios, previniendo que usted o sus usuarios tengan que obtener e importarlas manualmente a fin de enviar mensajes encriptados. Cuando las consultas PKA1 se realizan, cualquier llave URI que se encuentre se recolectará inmediatamente, validará y agregará al llavero. Las llaves recolectadas e importadas exitosamente al llavero utilizando este método expirarán en automático luego del número de horas especificadas en esta opción o de acuerdo con el valor TTL del registro PKA1 que las entregó, el valor que sea mayor.

Manejo de Llaves

Rastreo de Llaves

MDPGP ahora siempre rastrea las llaves por sus key-ids primarios en lugar de que lo haga en ocasiones por el key-id y en otras ocasiones por el sub-key-id. Consecuentemente, el diálogo en MDPGP que enlista las llaves se ha depurado para eliminar dos columnas innecesarias. Más aun, MDPGP ahora controla de manera más estricta los contenidos de su carpeta "exportación". Como resultado de esto siempre encontrará aquí copias exportadas de las llaves de los usuarios locales. Aun cuando las llaves privadas están encriptadas, para seguridad adicional deberá utilizar herramientas del SO para proteger esta carpeta (y de hecho proteger la estructura completa de carpetas PEM) para evitar accesos no autorizados.

Llaves Preferidas

Previamente, cuando se encontraban en el llavero múltiples llaves diferentes para la misma dirección de correo, MDPGP encriptaba los mensajes utilizando la primera llave encontrada. Ahora puede dar clic derecho en cualquier llave y definirla como preferente, de manera que MDPGP utilizará esa llave cuando encuentre múltiples llaves. Si no se declara una llave de preferencia, MDPGP utilizará la primera que encuentre. Al desencriptar un mensaje MDaemon intentará con cada llave.

Llaves Deshabilitadas

Las llaves deshabilitadas y eliminadas ahora se rastrean en un nuevo archivo denominado `oldkeys.txt`. Previamente, se daba seguimiento a las llaves deshabilitadas en el archivo `plugins.dat`.

Verificación de Firmas MDPGP

MDPGP ahora puede verificar firmas incrustadas en mensajes que no están encriptados. Previamente no podía verificar firmas a menos que el mensaje estuviera firmado y encriptado. Al visualizar un mensaje con una firma verificada en WorldClient, se despliega un ícono nuevo para indicar que el mensaje fue verificado. La verificación de firmas se habilita por omisión para todos los usuarios no-locales o puede especificar exactamente qué direcciones de correo pueden o no utilizar el servicio (ver: *"Configurar exactamente quién puede o no utilizar los servicios MDPGP"* en el diálogo MDPGP 629).

Servidor de Mensajería Instantánea XMPP 374

MDaemon ahora está equipado con un servidor XMPP (Extensible Messaging and Presence Protocol) denominado en ocasiones servidor Jabber. Esto permite a sus usuarios enviar y recibir mensajería instantánea utilizando clientes XMPP, de terceros tales y como Pidgin, Gajim, Swift y muchos otros.

Los clientes están disponibles para la mayoría de los sistemas operativos y plataformas de dispositivos móviles. El sistema de mensajería instantánea XMPP de MDaemon es completamente independiente del sistema de Mensajería Instantánea de WorldClient; los dos sistemas no se pueden comunicar entre ellos y no comparte las listas de contactos.

El servidor XMPP se instala como servicio de Windows y los puertos que utiliza por omisión son el 5222 (SSL vía STARTTLS) y 5223 (SSL dedicado). El servidor XMPP utilizará la configuración SSL de MDaemon si se encuentra habilitada en él. Así mismo, algunos clientes XMPP utilizan registros DNS SRV para autodescubrimiento de

nombres de host. Por favor consulte: http://wiki.xmpp.org/web/SRV_Records para más información.

Los usuarios ingresan utilizando su dirección de correo y contraseña en el cliente XMPP. Sin embargo, algunos clientes requieren que la dirección de correo se divida en dos componentes separados al iniciar la sesión. Por ejemplo, en lugar de "`frank@example.com`," algunos clientes requieren que utilice "`frank`" como Login/Nombre de Usuario y "`example.com`" como el Dominio.

Para el servicio de chat multiusuario/grupo, los clientes típicamente los manejan como "cuartos" o "conferencias". Cuando quiera iniciar una sesión de chat, cree un cuarto/conferencia (dándole un nombre) y luego invite a los otros usuarios a ese cuarto. La mayoría de los clientes no requieren que registre la localización del servidor para la conferencia; solo necesita darle un nombre. Cuando se le solicite hacerlo, sin embargo, utilice "`conference.<your domain>`" como ubicación (ej. `conference.example.com`). Algunos clientes le requieren que registre el nombre y ubicación juntos con la forma: "`room@conference.<your domain>`" (ej. `Room01@conference.example.com`).

Algunos clientes (tales como Pidgin), soportan el servicio de búsqueda de usuarios, permitiéndole buscar usuarios en el servidor, por nombre o dirección de correo, lo que facilita agregarlos como contactos. Usualmente no tendrá que proporcionar una ubicación de búsqueda, pero si se le solicita hacerlo, utilice "`search.<your domain>`" (ej. `search.example.com`). Al buscar, se puede utilizar el símbolo % como comodín. Por esto, podría utilizar "%@example.com" en el campo de la dirección de correo para desplegar una lista de todos los usuarios con una dirección de correo que termine en "@example.com."

Administración Centralizada de Ajustes del Cliente OC

Utilice el diálogo de Ajustes del Cliente OC para administrar centralizadamente los ajustes de cliente de sus usuarios de Outlook Connector. Configure cada pantalla con los ajustes deseados y MDaemon los entregará a las pantallas correspondientes del cliente conforme sea necesario, cada vez que los usuarios de Outlook Connector se conecten al servidor. Los Ajustes de Cliente OC solo se envían a los clientes cuando alguno de esos valores se ha modificado desde la última vez que el cliente se conectó y los recibió. Si se habilita la opción "*Permitir a los usuarios de OC omitir los ajustes entregados*" los usuarios pueden ignorar los ajustes entregados a sus clientes individuales. Si se deshabilita esa opción, entonces todas las pantallas de clientes se bloquean; los usuarios de Outlook Connector no podrán hacer cambios.

Para permitir que ciertos ajustes sean diferentes para cada usuario o dominio, los Ajustes de Cliente OC soportan macros tales como `$USERNAME$`, `$EMAIL$` y `$DOMAIN$`. Estas macros se convertirán a datos específicos para el usuario o dominio cuando se entreguen los ajustes al cliente. Tenga cuidado de no colocar valores fijos en ninguno de los campos si utiliza una macro, tal como colocar algo como "Frank Thomas" en el campo Su Nombre. Si lo hace, se modificará el nombre de todo usuario de Outlook Connector que se conecte a MDaemon a "Frank Thomas". Para su conveniencia existe un botón de Referencia a Macros en la pantalla General, que despliega una lista de las macros soportadas.

Para aquellos que utilizan MDaemon Private Cloud (MDPC), existe otro diálogo en los Ajustes del Cliente OC en el Administrador de Dominios, para controlar los ajustes del cliente de Outlook Connector con base en el dominio.

Esta funcionalidad se encuentra deshabilitada por omisión y funciona solo con los clientes de Outlook Connector versión 4.0.0 o superior.

Protección/Modificación del Encabezado "From:" 568

Esta nueva función de seguridad modifica el encabezado "From:" en los mensajes entrantes para hacer que la porción del nombre en el encabezado contenga tanto el nombre como la dirección de correo. Esto se realiza para combatir la táctica común utilizada por el spam y ataques donde el mensaje aparenta provenir de alguien más. Al desplegar una lista de mensajes, los clientes de correo comúnmente despliegan solo el nombre del remitente en lugar del nombre y la dirección de correo. Para ver la dirección de correo, el destinatario primero debe abrir el mensaje o realizar alguna otra acción, tal como dar clic derecho en el registro o pasar el puntero sobre el nombre. Por esta razón los atacantes comúnmente construyen la dirección de correo de manera que aparece el nombre de una persona o empresa legítima en la porción visible del encabezado "From:" mientras que la dirección de correo ilegítima se encuentra oculta. Por ejemplo, el encabezado "From:" verdadero de un mensaje podría ser: `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, pero su cliente podría desplegar como remitente solo `"Honest Bank and Trust"`. Esta funcionalidad modifica la porción visible del encabezado para desplegar ambas partes, con la dirección de correo primero. En el mensaje de arriba el remitente se mostraría ahora como `"lightfingers.klepto@example.com -- Honest Bank and Trust,"` dándole una clara indicación de que el mensaje es fraudulento. Esta opción solo aplica a mensajes dirigidos a usuarios locales y se encuentra deshabilitada por omisión.

Monitor de IP Mejorado 562

La pantalla Monitor de IP ahora contiene un botón Importar que puede utilizar para importar direcciones IP de archivos tipo APF o .htaccess. El soporte de MDaemon a este tipo de archivos se limita a lo siguiente:

- Se soportan "rechazar de" y "permitir de"
- Solo se importan valores IP (no nombres de dominio)
- Se permite notación CIDR, pero no se permiten direcciones IP parciales
- Cada línea puede contener cualquier número de direcciones, separadas por espacios o por coma. Por ejemplo: "rechazar de 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5" y similar.
- Se ignoran las líneas que inician con #.

Instalación Automática de Actualizaciones de Producto 501

Utilizando la funcionalidad de Actualizaciones Automáticas, puede configurar MDaemon para informar al postmaster siempre que se encuentre disponible una actualización de alguno de los productos instalados, o puede descargar e instalar esas actualizaciones automáticamente. Esto incluye MDaemon, SecurityPlus y Outlook Connector. La instalación automática de productos se puede controlar por separado para cada producto y se requiere un reinicio de servidor cada vez que un producto se actualiza. Los archivos instalables se descargan cuando se detecta la actualización, pero la instalación y reinicio pueden ocurrir más tarde dependiendo de la hora designada para ello. Toda la actividad de instalación se registra en el sistema de Logs de MDaemon y se informa al postmaster después de que ha ocurrido la actualización. Vea el dialogo Actualizaciones 501 para más información.

Cambios a WorldClient

Categorías 344

WorldClient soporta categorías para el correo electrónico en los temas LookOut y WorldClient. Los usuarios pueden agregar la columna Categorías a la lista de mensajes desde "Opciones » Columnas" y marcando "Categorías" en la sección Lista de Mensajes. Para seleccionar categorías para uno o varios mensajes, seleccione los mensajes y dé clic derecho en uno de ellos. Utilice el menú contextual para establecer la categoría.

- Los Administradores pueden crear categorías personalizadas Existen dos archivos para ese fin: `DomainCategories.json` y `PersonalCategories.json`.
- Las categorías por Dominio se habilitan globalmente por omisión. Para deshabilitarlas abra el archivo `MDaemon\WorldClient\Domains.ini` y en la sección `[Default:Settings]` modifique el valor de "`DomainCategoriesEnabled=`" de "`Yes`" a "`No`".
- Los usuarios pueden agregar y editar sus propias categorías por omisión. Si desea deshabilitar esta opción, puede hacerlo por usuario o globalmente modificando el valor de "`CanEditPersonalCategories=`" de "`Yes`" a "`No`". La opción del usuario se localiza en la sección `[User]` del archivo `User.ini` y la opción global en el archivo `Domains.ini` en la sección `[Default:UserDefaults]`.
- Si se habilitan las Categorías por Dominio y al usuario no se le permite editar sus categorías personales, solo podrá ver las categorías enlistadas en `DomainCategories.json`.
- Si se deshabilitan las Categorías por Dominio y al usuario no se le permite editar sus categorías personales, el usuario verá las categorías enlistadas en `PersonalCategories.json`.
- El archivo `CustomCategoriesTranslations.json` se utiliza para soportar los nombres personalizados de categorías en múltiples lenguajes. Agregue la traducción del nombre de cualquier categoría personalizada para permitir a WorldClient reconocer una categoría grabada de un evento, nota o tarea en un idioma y su equivalente en otro lenguaje.

Para más información detallada relativa a los archivos aquí mencionados, vea: `MDaemon\WorldClient\CustomCategories.txt`.

Listas Blancas y Negras 353

Ahora puede ocultar las carpetas de Listas Blancas y Negras a los usuarios de WorldClient por omisión. Para hacerlo, abra el archivo `MDaemon\WorldClient\Domains.ini`, y en la sección `[Default:UserDefaults]` modifique el valor "`HideWhiteListFolder=`" o "`HideBlackListFolder=`" de "`No`" a "`Yes`". Puede ocultar o mostrar estas carpetas para usuarios específicos editando esas mismas llaves en el archivo `User.ini` en la sección `[User]`.

Verificación de Adjuntos

En los temas LookOut y WorldClient ahora existe la opción de verificar si un mensaje lleva archivos adjuntos antes de enviarlo, cuando los adjuntos se mencionan en el asunto o el cuerpo del mensaje. Esto puede ayudar a evitar que se envíen accidentalmente mensajes sin adjuntos cuando se supone que los incluyen.

Autenticación de Dos Factores 720

Ahora puede controlar si se permite o no a la cuenta utilizar o requerir el uso de la Autenticación de Dos Factores (Two Factor Authentication - 2FA). Estas dos nuevas opciones se encuentran en la plantilla Cuentas Nuevas 798 para controlar los valores por omisión de las cuentas nuevas y existen opciones correspondientes en la pantalla Servicios Web 720 para controlar 2FA para cuentas individuales.

Lo nuevo en MDaemon Private Cloud 4.0

- MDaemon Private Cloud 4.0 incluye MDaemon 16.0.3 y Outlook Connector 3.5.2.
- Se actualizó a una nueva versión del motor de Outbreak Protection.
- Se actualizó el motor de ClamAV a la versión 0.99.2.

Para una lista de las modificaciones a MDaemon vea las Notas de la Versión de MDaemon 16.0.

Para una lista de las modificaciones a Outlook Connector vea las Notas de la Versión de Outlook Connector 3.5.2.

Lo nuevo en MDaemon 16.0

Actualización de la Interface de MDaemon Administración Remota (MDaemon Remote Administration - MDRA)

La interface de usuario de MDRA ya no utiliza marcos y ha sido actualizada para utilizar un diseño responsivo móvil. El soporte a navegadores se limita a IE10+, la última versión de Chrome, de Firefox y de Safari en iOS y Mac. Se sabe que los navegadores Android genéricos tienen problemas con el desplazamiento, pero Chrome en dispositivos Android funciona bien.

Este diseño se basa por completo en el tamaño de la ventana en uso. Ya sea que el usuario utilice un teléfono, tableta o PC, la apariencia es la misma para el mismo tamaño de ventana. Los cambios más importantes se encuentran en el menú. En resolución de 1024 pixeles y menor, el menú se oculta en el extremo izquierdo del navegador. Se pueden utilizar dos métodos para desplegar el menú. Si se utiliza un dispositivo touch, deslizar con el dedo hacia la derecha mostrará el menú secundario. Ya sea que el dispositivo esté en uso o no, también existe un botón "menú" en la esquina superior izquierda que desplegará el menú secundario. Dando un toque o clic en el título del menú en la flecha izquierda en la parte superior del menú se desplegará el menú principal. Las secciones Ayuda, Acerca de y Salir en la esquina superior derecha cambian también con base en el ancho de la pantalla. De 768 pixeles hacia arriba se despliegan las palabras Ayuda, Acerca de y Salir. De 481 a 767 pixeles, solo se despliegan los íconos. De 480 pixeles hacia abajo se despliega solo un ícono de "rondana", al darle clic o un toque desplegará un menú desplegable con las opciones Ayuda, Acerca de y Salir. Las vistas de Listas con más de una columna tienen botones para habilitar/deshabilitar las columnas, a los que se puede accesar dando clic o un toque en el botón de flecha gris hacia la derecha que se encuentra en el extremo derecho del contenedor de la barra de herramientas. Las páginas de ajustes ya no se diseñaron para ser copias exactas de la interface de usuario de MDaemon, sino que están diseñadas para reposicionarse y ajustarse con base en el ancho/altura del navegador.

Detección de Spambot

Una nueva funcionalidad denominada Detección de Spambot rastrea las direcciones IP que utiliza todo valor SMTP MAIL (return-path) durante un periodo de tiempo dado. Si se utiliza el mismo return-path en un número inusual de direcciones IP en un periodo de tiempo corto, esto puede indicar una red de spambot. Aunque podría ser un uso legítimo de un sistema de correo, las pruebas experimentales han mostrado que esta funcionalidad puede ser efectiva en casos limitados para detectar redes distribuidas de spambot en tanto utilicen el mismo valor return-path. Si se detecta un spambot, la conexión se cierra inmediatamente y el valor return-path opcionalmente se coloca en lista negra por un rango de tiempo que usted determine. También opcionalmente puede poner en lista negra todas las IPs spambot conocidas por un periodo de tiempo definido por el usuario.

CardDAV

MDaemon ahora soporta la sincronización de contactos vía el protocolo CardDAV. El servidor CardDAV de MDaemon permite a un cliente autentificado CardDAV tener acceso a la información de contactos almacenada en MDaemon. Los más notables clientes CardDAV son Apple Contacts (incluido en Mac OS X), Apple iOS (iPhone) y Mozilla Thunderbird vía el complemento SOGO. Para más información sobre CardDAV y configurar clientes CardDAV vea: CalDAV & CardDAV.

Autentificación de Dos Factores para WorldClient y Administración Remota

MDaemon ahora soporta la Autentificación de Dos Factores (i.e. Verificación de Dos Pasos) para usuarios que ingresan a través de las interfaces web WorldClient y MDaemon Administración Remota. Cualquier usuario que abre sesión en WorldClient vía HTTPS puede activar la Autentificación de Dos Factores para la cuenta en la pantalla **Opciones » Seguridad.** A partir de ese momento el usuario debe ingresar un código de verificación al ingresar a WorldClient o Administración Remota. El código se obtiene de una app de autentificación instalada en el dispositivo móvil o tableta del usuario. Esta funcionalidad está diseñada para cualquier cliente que soporta el Autenticado de Google.

Cliente de Migración del protocolo ActiveSync

MDaemon ahora incluye un Cliente de Migración basado en el protocolo ActiveSync (`ASMC.exe`). Permite migrar correo, calendarios, tareas, notas y contactos desde servidores ActiveSync que soporten el protocolo versión 14.1. Se puede encontrar documentación al respecto en la carpeta `\MDaemon\Docs`.

API XML para Tareas Administrativas

MDaemon ahora incluye una API basada en XML sobre http(s). El resultado es que es posible crear clientes de Administración para MDaemon utilizando cualquier lenguaje o plataforma que pueda hacer peticiones post sobre http(s):// en el servidor. En MDaemon, esto solo está disponible para Administradores Globales autentificados, pero en MDaemon Private Cloud los administradores del dominio pueden acceder a un subconjunto de las operaciones disponibles. La API también produce un sitio web con documentación sobre la especificación API. La instalación por omisión es en la ruta `http://servername:RemoteAdminPort/MdMgmtWS/`, sin embargo, puede apuntar a cualquier url por motivos de mayor seguridad.

Las operaciones disponibles incluyen:

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

En este momento, se han escrito/probado clientes de administración de línea de comando en JavaScript, PowerShell, VBScript, C, C++ y Visual Basic. Se ha utilizado un sitio de prueba simple con HTML y JavaScript como prueba de concepto para una consola de administración basada en web que opera sobre varios de los navegadores más populares. Aunque no se ha probado, se espera que esta API trabaje en servidores web utilizando PHP, Perl y otras plataformas de desarrollo.

Ver:

Introducción 12
Actualizando a MDaemon Private Cloud 12.0.0 71
Pantalla principal de MDaemon 80

1.4 Actualizando a MDaemon Private Cloud 12.0.0

A continuación, se presenta una lista de consideraciones especiales y notas que debe tomar en cuenta al actualizar a MDaemon versión 24.0.0 desde una versión anterior. Para una lista completa de las adiciones, cambios y correcciones incluidas en MDaemon 24.0.0, ver las Notas de la Versión.

Versión 24.0.0

- La API XML ahora por omisión niega el acceso desde IPs que no están permitidas específicamente. Esto se puede modificar en la interface de la aplicación en: Inicio | Servicio XML API | Restricciones de Dirección 487.

Versión 23.5.0

- No hay consideraciones especiales únicas para MDaemon 23.5.0 al actualizar de la versión anterior. Si está actualizando desde una versión previa, por favor revise las notas especiales abajo para todas las versiones liberadas desde la que usted va a actualizar.

Versión 23.0.2

- Outbreak Protection ha sido restaurado a MDaemon 23.0.2.

Versión 23.0.1

- Cyren Anti-Virus ha sido reemplazado con IKARUS Antivirus. Cyren anunció recientemente sus planes para descontinuar operaciones, sin aviso previo. Esto nos obligó a encontrar un nuevo socio antivirus. Después de una profunda evaluación, IKARUS se destacó por su excelente tasa de detección y su velocidad. IKARUS Antivirus actualiza automáticamente sus definiciones cada 10 minutos. El escaneo con IKARUS se deshabilita si la licencia de AntiVirus ha expirado
- Cyren Outbreak Protection ha sido eliminado. Cyren anunció recientemente sin previo aviso sus planes de descontinuar operaciones. Estamos investigando y evaluando activamente opciones viables de tecnología antispam como adiciones adecuadas a los mecanismos antispam actuales disponibles en nuestros productos de software.
- El soporte a etiquetas IMAP de palabras clave (keyword flags) ahora se puede habilitar o deshabilitar vía el ajuste [Special] IMAPKeywordFlags=Yes/No en \MDaemon\App\MDaemon.ini. Las etiquetas IMAP de palabras clave se encuentran deshabilitadas por omisión al actualizar MDaemon desde alguna versión anterior a la 23, para evitar la pérdida potencial de etiquetas en los clientes de correo Thunderbird. Cuando Thunderbird se conecta a un servidor IMAP que soporta etiquetas de palabras clave, sobrescribe sus etiquetas de mensajes locales con etiquetas leídas del servidor, que inicialmente están en blanco. Las etiquetas IMAP de palabras clave se habilitar por omisión para instalaciones nuevas y al actualizar desde la versión 23.0.0.

Versión 22.0.0

- MDaemon de 32-bit ha sido descontinuado. Si está utilizando actualmente la versión de 32 bits en un sistema operativo que soporta 64 bits, simplemente puede instalar la versión de 64 bits sobre la instalación existente.
- La longitud mínima para contraseñas fuertes 855 ahora debe ser de al menos 8 caracteres. Si su longitud mínima estaba configurada a menos de 8 caracteres antes de actualizar a MDaemon 22, será modificada a 8. La longitud mínima por omisión para contraseñas fuertes en instalaciones nuevas es ahora de 10.
- MDaemon deja de utilizar los términos "lista blanca" y "lista negra". En muchos casos, ahora son "lista de permitidos" y "lista de bloqueados". Funcionalidades que temían una "lista blanca" para exentar IPs, direcciones, etc., ahora tienen una "lista de exentos". Las carpetas de contactos por usuario del filtro de spam ahora se denominan "Remitentes Permitidos" y "Remitentes Bloqueados". Las carpetas para todas las cuentas serán renombradas cuando MDaemon 22 inicie por primera vez.

Versión 21.5.0

- El encabezado `X-MDOrigin-Country`, que el Monitoreo de Localizaciones 572 puede agregar a los mensajes, ahora contendrá las dos letras de código ISO 3166 de país y continente en lugar de los nombres de los países y continentes. Asegúrese de actualizar cualquier filtro que tenga que utilice valores particulares en este encabezado.
- Al renombrar el tema "Mobile" de Webmail a "Pro", hay un posible efecto secundario para usuarios que están utilizando el tema Mobile y tienen habilitada la opción Recuérdame. Estos usuarios pueden encontrar que no pueden abrir archivos adjuntos. Para corregir esto, simplemente deben salir de sesión y volver a entrar en Webmail.

Versión 21.0.2

- Los ajustes en Configuración » Preferencias » Misceláneos para copiar a los administradores globales y de dominio todas las notificaciones generadas por el sistema dirigidas al postmaster, ahora aplican a más notificaciones, tales como Cuentas Congeladas y Deshabilitadas, Usuario Inexistente, Error de Disco, Bajo espacio en Disco y expiración de licencias Beta y AV. Si no considera apropiado que sus administradores reciban estas notificaciones, debe deshabilitar este ajuste.

Versión 20.0.3

- MDaemon comentará la línea "`AlertExceedsMax yes`" en el archivo `clamd.conf` de ClamAV, porque genera demasiados fallos de escaneo de tipo "`Heuristics.Limits.Exceeded`".

Versión 20.0.1

- Los ajustes de acceso a recursos de la red en Configuración | Preferencias | Servicio de Windows ahora configura el Servicio MDaemon (y los servicios Administración Remota y Servidor XMPP) para ejecutarse con la cuenta especificada, en lugar de que MDaemon se ejecute como SYSTEM y luego distintos procesos e hilos como esa cuenta. El instalable actualizará los

servicios para ejecutarse con la cuenta especificada al actualizar esta versión.

- Debido a cambios y a obsolescencia de muchos ajustes en clamd.conf, el instalable ahora sobrescribe el archivo clamd.conf existente. Si lo ha personalizado, puede requerir revisarlo y hacer sus cambios al archivo clamd.conf luego de la instalación.

Versión 20.0.0

- Por favor lea cuidadosamente la sección en las notas completas de la versión marcada como tarea [8930] ya que involucra cambios al sistema de integración con Active Directory y puede encontrar que algunas cosas que no funcionaban en el pasado empiezan ahora a funcionar. Por favor considere todos los cambios hechos en esa área y lea cuidadosamente esa sección de las notas de la versión.
- MDaemon 20.0 requiere Windows 7, Server 2008 R2, o superior.
- Preferencias » Misceláneos 503 cuenta con dos nuevas casillas de verificación que controlan si los correos de notificación generados por el sistema, que se envían periódicamente al alias del Postmaster, deben ser enviados a los administradores a nivel Global y de Dominio. Por omisión, ambas opciones están deshabilitada. Los Administradores del Dominio están restringidos para recibir solo los correos dirigidos a su dominio y las Notas de la Versión. Los Administradores Globales reciben todo incluyendo el reporte Resumen de Colas, Reporte de Estadísticas, Notas de la Versión, usuario 'No encontrado' (para todos los dominios), notificaciones de Error de Disco, notificaciones de cuentas Congeladas y Deshabilitadas para todos los dominios (que, como los Administradores del Dominio, pueden descongelar y rehabilitar), advertencias sobre licencias y versiones beta por expirar, reportes Resumen de Spam y quizá otros también. Si cree que no es adecuado que sus administradores reciban estas notificaciones, puede deshabilitar estos ajustes.
- Se modificó la manera en que se almacenan las autorespuestas. El texto de la autorespuesta de una cuenta ahora se almacena en el archivo `OOF.MRK` dentro de la carpeta DATA de la cuenta que es una nueva subcarpeta dentro de la carpeta raíz de correo de la cuenta. Los archivos de script de autorespuestas ya no se mantienen en la carpeta APP y no se comparten entre cuentas. Cuando MDaemon inicie la primera vez migrará todos los archivos y ajustes de autorespuesta existentes a los lugares correctos para todas las cuentas. El archivo `AUTORESP.DAT` es obsoleto y será eliminado junto con cada archivo `.RSP` específico por cuenta (`OutOfOffice.RSP` y archivos específicos no pertenecientes a cuentas, permanecerán en su lugar para propósitos de referencia y ejemplos). Si desea asignar rápidamente una única configuración de autorespuesta para múltiples cuentas puede utilizar el nuevo botón Publicar que se encuentra en Ajustes de Cuentas » Autorespuestas 726. Este botón copiará el texto del script de autorespuesta existente y todos los ajustes de la cuenta hacia las otras cuentas que usted seleccione. También hay un botón para Editar archivo de autorespuesta 726 que le permite editar el script de autorespuesta por omisión (`OutOfOffice.rsp`). Este archivo por omisión se copia al archivo `OOF.MRK` si este no se encuentra o está vacío.
- Se ha modificado la manera en que se almacenan los archivos de firma de las cuentas. Los archivos de firma ahora se almacenan en `SIGNATURE.MRK` dentro de la carpeta DATA de la cuenta, que es una nueva subcarpeta

dentro de la carpeta raíz de correo de la cuenta. Cuando MDaemon inicie por primera vez, migrará todos los archivos de firma existentes a los lugares correctos para cada cuenta. La carpeta raíz MDaemon Signatures ya no contendrá archivos de firma específicos por cuenta, pero permanecerá en su lugar ya que puede contener elementos necesarios por MDaemon Administración Remota o el Filtro de Contenido. La carpeta original de Firmas se respalda en `\Backup\20.0.0\Signatures\` antes de la migración. Finalmente, el archivo `ADMINNOTES.MRK` de cada cuenta se ha movido a la carpeta raíz de correo de la cuenta en la nueva subcarpeta DATA.

- Filtro de Spam » Lista Blanca (automática) 688 se cambió el valor por omisión a des habilitado para la opción "*...solo agregar a lista blanca direcciones que se autentifican con DKIM*". Habilitar esto puede ser muy restrictivo para muchos e impide que funcione la lista blanca de direcciones para correo MultiPOP y DomainPOP. Habilite este ajuste si no esto no es de su agrado.
- La opción Preferencias » IU 491 para "*Centrar todos los diálogos en la IU*" se ha restablecido por omisión a "habilitada" para todos. Si lo prefiere, la puede deshabilitar. Esto impide que las pantallas se creen fuera de marco parcialmente, pero puede ocasionalmente generar que se encimen pantallas y se dificulte seleccionarlas.
- Administrador de Seguridad » Monitoreo » Monitor de Localizaciones 572 - El valor por omisión para esta funcionalidad se ha modificado de deshabilitado a habilitado. Cuando se habilita el Monitoreo de Localizaciones el país/región que se conecta siempre se registrará (si se conoce) aun cuando el país/región no esté siendo bloqueada activamente. De manera que aun cuando no desee bloquear ningún país, puede habilitar el Monitoreo de Localizaciones (sin seleccionar ningún país a bloquear) de manera que el país/región se muestre y sea registrado. Dado que el valor por omisión para esto se ha modificado, debe revisar si su configuración del Monitoreo de Localizaciones es correcta. MDaemon insertará en encabezado "`X-MDOrigin-Country`" que enlista el país y región para el filtro de contenido y otros propósitos.
- El límite de 2 MB para escaneos del filtro de Spam, estaba fijo en código y ha sido eliminado. Ahora no hay límite teórico del tamaño de un mensaje para que pueda ser escaneado. Sin embargo, aún es posible configurar su propio límite en caso de que esto sea un problema, sin embargo, utilizar la opción "0" ahora significa sin límite. Debe revisar la pantalla Filtro de Spam » Ajustes 698 para asegurarse de que esta opción está configurada con el valor que usted prefiera.
- Se agregaron las columnas 'Dominio del Remitente' y 'Dominio del Destinatario' en la pantalla de Colas en la IU principal. Como resultado de esto se tiene que hacer por única ocasión un restablecimiento del ancho de columnas grabado. Una vez que ha configurado el ancho de columnas a su gusto, esta configuración será recordada.
- Por omisión el Monitoreo de Host ahora se aplica a conexiones MSA. Esta opción se localiza en: Administrador de Seguridad » Monitoreo » Monitoreo de Host 564.
- Por omisión los servidores IMAP, Webmail y ActiveSync de MDaemon ya no dan acceso a las carpetas compartidas de las cuentas deshabilitadas. Puede modificar esto con un ajuste nuevo en Ajustes de Servidor » Carpetas Pública & Compartidas 128.

Versión 19.5.2

- La opción "*Max comandos RSET permitidos*" en la pantalla Ajustes de Servidor » Servidores 100 se ha eliminado dado que es esencialmente una opción menos flexible de la misma funcionalidad que se encuentra en Monitoreo SMTP 566. El Monitoreo SMTP es parte del sistema de Monitoreo Dinámico que toma en consideración otros factores (ej. cuenta con una lista blanca, considera estatus de autentificación, etc.). Sus valores anteriores se han movido a la pantalla Monitoreo SMTP. Por favor verifíquelos para asegurarse que están como usted lo desea. Los valores correctos por omisión (recomendados) para las opciones son: *Bloquear IPs que envían este número de RSETs* definida como "**20**" y la opción *Cerrar sesión SMTP luego de bloquear la IP* se configura a **habilitada/verificada**.

Versión 19.5.1

- La funcionalidad de LetsEncrypt 594 se ha actualizado para utilizar ACME v2. Esta actualización se requiere porque LetsEncrypt va a descontinuar el soporte para ACME v1. Ahora se requieren PowerShell 5.1 y .Net Framework 4.7.2 para poder utilizar LetsEncrypt.

Versión 19.5.0

- Algunos ajustes, tal como las llaves de registro, se han movido desde `\MDaemon\App\MDaemon.ini` a `\MDaemon\LocalData\LocalData.ini`. Si necesita regresar a una versión previa de MDaemon, los instalables anteriores no encontrarán los ajustes en las nuevas ubicaciones y por consiguiente le solicitarán que ingrese la llave de registro. Esto se puede evitar copiando los ajustes a `MDaemon.ini` o restaurando primero un respaldo de `MDaemon.ini`.

Versión 19.0.0

- La interface web de MDaemon Administración Remota (MDRA) ha sido expandida para incluir acceso a funcionalidades que previamente solo podrían ser administradas utilizando la sesión de Configuración (esto es, la interface de escritorio de MDaemon) y ahora se cuenta con varias opciones que a las que solo se puede acceder vía MDRA. En consecuencia, para las nuevas instalaciones de MDaemon, el acceso directo "Iniciar MDaemon" ahora abrirá por omisión MDaemon Administración Remota en el navegador en lugar de abrir una sesión de Configuración de MDaemon. Si desea modificar esto, edite el archivo `\MDaemon\App\MDaemon.ini` y defina `[MDLaunch] OpenConfigSession=Yes/No` y `OpenRemoteAdmin=Yes/No`. Defina la *URL de Administración Remota* en Configurar » Web & Servicios IM » Administración Remota » Servidor Web 356 si la URL autogenerada no funciona o si MDRA se ejecuta en un servidor web externo. Si no es posible determinar un URL funcional, se abrirá una sesión de Configuración. Finalmente, bajo el Menú de Inicio de Windows, el grupo de programas de MDaemon ahora presenta accesos directos a *Abrir Sesión de Configuración de MDaemon* y *Abrir Administración Remota de MDaemon*.
- SyncML se ha descontinuado y ha sido eliminado.
- Los cálculos de espacio en disco de MDaemon se hacían de manera inconsistente en varias ubicaciones (por ejemplo, algunas veces utilizaba 1000, en otras ocasiones utilizaba 1024 bytes para los cálculos de

kilobytes). Esto se ha corregido para utilizar 1024 consistentemente. Como resultado, los valores de cuota de espacio en disco de sus usuarios pueden ser ligeramente diferentes que con las versiones anteriores. Por favor revise y haga los ajustes que considere necesarios.

- La opción "Solo enviar notificaciones de actualización de antivirus cuando hay fallo 665" ahora se habilita por omisión. Al actualizar a MDaemon 19, esta opción se habilitará cuando MDaemon inicie por primera vez.

Ver:

Introducción 12
Lo nuevo en MDaemon Private Cloud 12.0 15
Pantalla principal de MDaemon 80

1.5 Obtener ayuda

Opciones de Soporte

El soporte es una parte vital de la experiencia del consumidor en MDaemon Technologies. Queremos que obtenga los mejores resultados de nuestros productos después de una compra inicial e instalación, y estamos dedicados a asegurarnos que sus conflictos se resuelvan con satisfacción por su parte. Para la información más actualizada de Servicio al Consumidor, Opciones de Soporte Técnico, Recursos de Autosoporte, Información de Producto, y más, visite la página de soporte de MDaemon Technologies en: www.altn.com/support/

MDaemon Pruebas Beta

MDaemon Technologies mantiene equipos activos para hacer pruebas beta de nuestros productos. Si desea información sobre cómo unirse a los equipos de pruebas beta de MDaemon, envíe un mensaje a MDaemonBeta@altn.com.

El Equipo Beta es para aquellos que deseen obtener software de MDaemon antes de su distribución global y ayudar en su fase de pruebas; no es una alternativa al soporte. El soporte técnico de MDaemon sólo se proveerá a través de los métodos indicados en: www.mdaemon.com/support/.

Contáctenos

Horario de Oficina
L-V 8:30 am - 5:30 pm Central Standard Time
Se excluyen fines de semana y días festivos en los Estados Unidos
Servicio al Consumidor o Ventas
Teléfono gratuito para EEUU: 866-601-ALTN (2586)
Internacional: 817-601-3222
sales@helpdesk.mdaemon.com

Soporte Técnico
www.mdaemon.com/support/

Capacitación
training@mdaemon.com

Desarrollo de Negocios/Alianzas
alliance@mdaemon.com

Medios/Analistas
press@mdaemon.com

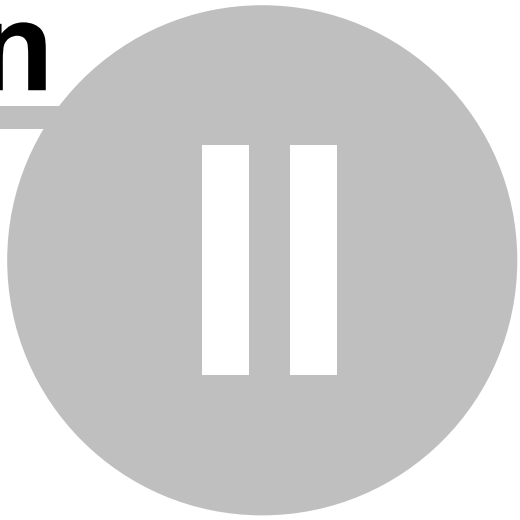
Consultas para Revendedores/Distribuidores
Por favor, consulte la página del Canal de Partners para información adicional.

Sede Corporativa

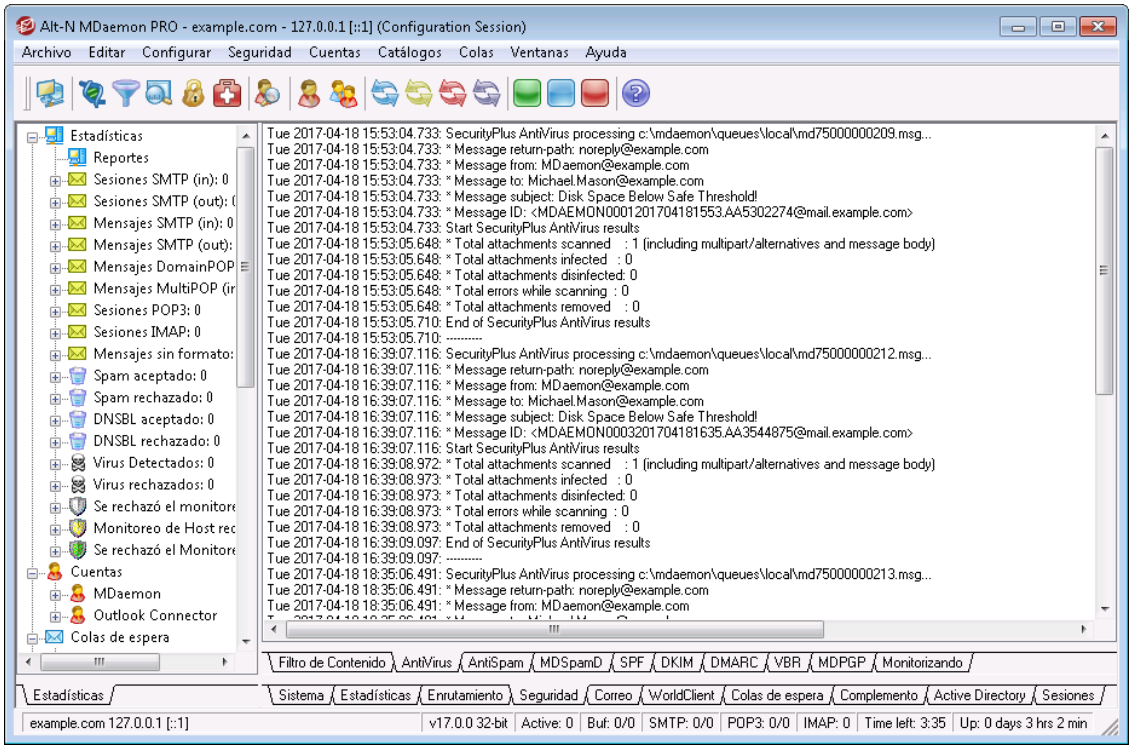
MDaemon Technologies
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
U.S. Llamada sin costo: 866-601-ALTN (2586)
Internacional: 817-601-3222
Fax: 817-601-3223

Marcas Registradas

Sección



2 Pantalla Principal de MDaemon



La interfaz gráfica principal de usuario (GUI) proporciona información importante acerca de los recursos de MDaemon, estadísticas, sesiones activas y el correo en cola esperando a ser procesado. También contiene opciones para activar/desactivar fácilmente varios de los servidores de MDaemon. Los paneles en las pestañas de la GUI le mantienen al día de cómo actúan el servidor y sus conexiones entrantes y salientes.

Estadísticas

El panel de Estadísticas es el panel izquierdo por defecto de la interfaz principal de MDaemon. Este panel contiene cuatro secciones: Estadísticas, Cuentas, Colas y Servidores.

La sección *Estadísticas* contiene estadísticas sobre el número de mensajes enviados y recibidos por MDaemon, así como de las sesiones POP3 e IMAP, el SPAM aceptado y rechazado, virus y más. Las estadísticas se calculan desde el momento que MDaemon inicia y con clic derecho se puede accesar un menú para reiniciar los contadores.

Cuando haga clic en la opción "restablecer contadores del nodo raíz", todos los contadores se restablecerán, no solamente el que se esté apuntando. Además, existe una opción en Configurar » Preferencias » GUI que se puede usar para "*Preservar los contadores de nodo raíz en los*

> *reinicios*." Sin esta opción, los contadores se restablecerán siempre que el servidor se reinicie.

La sección *Cuentas* contiene registros para MDaemon, MDaemon Connector y ActiveSync. Cada opción enlista el número de cuentas utilizadas y el número de cuentas restantes, dependiendo de su licenciamiento.

La sección *Colas* contiene una entrada para cada cola de mensaje y el número de mensajes (si los hay) que contiene cada cola. Puede hacer clic derecho en cada entrada de cola para abrir un menú de acceso directo que contenta una o más de las siguientes opciones, dependiendo de la cola que haya seleccionado:

Ver Cola — esta opción cambia el panel principal a la pestaña de Colas y muestra la cola seleccionada. Se desplegará una lista de todos los mensajes que contiene la cola y se puede dar clic derecho a cualquier mensaje para abrir un menú de acceso rápido conteniendo numerosas opciones similares a las que están disponibles en el Administrador de Colas & Estadísticas, tales como Copiar, Mover, Editar y demás.

Administrador de colas y estadísticas — abre el Administrador de Colas y Estadísticas por la Página de Cola mostrando la información para la cola seleccionada.

Procesar Ahora — esta opción "reencola" todos los mensajes contenidos en la cola e intenta procesarlos normalmente para envío. Si intenta procesar mensajes contenidos en la Cola de Espera, Cola incorrecta, o similar, entonces es posible que los mensajes encuentren los mismos errores que originaron que se les colocara ahí en primer lugar y vuelvan a la misma cola.

Inmovilizar / liberar cola — pausa temporalmente el procesamiento para la cola seleccionada, o continua el procesamiento si actualmente se encuentra pausada.

Liberar — libera mensajes de la Cola de Espera. MDaemon intentará enviar los mensajes aun y cuando se encuentren errores — no serán devueltos a la cola de Espera, aunque vuelvan a encontrar los mismos errores que inicialmente los colocaron allí.

Volver a poner en la cola — Esta opción está disponible para la Cola de Espera, y tiene el mismo efecto que la opción anterior de *Procesar Ahora*.

Habilitar/deshabilitar cola — activa o desactiva la Cola de Espera. Cuando de deshabilita, los mensajes no se moverán a la cola de Espera aun y cuando se encuentren errores.

La sección *Servidores* contiene una entrada para cada servidor contenido en MDaemon, y cada entrada lista el estado actual del servidor: "Activo" o "Inactivo". A continuación de cada entrada de servidor existe una entrada para cada dominio (cuando aplique) y el puerto e IP actualmente en uso por dicho dominio. El menú de acceso directo provee control para alternar el estado de cada servidor entre Activo e Inactivo. Cuando un servidor esté inactivo su ícono se volverá rojo.

Registro de Eventos y logueo

El panel derecho por defecto de la interfaz principal contiene un grupo de pestañas que muestran las acciones actuales de MDaemon y el estatus de varios servidores y recursos, y se actualizan constantemente para reflejar las condiciones actuales del servidor. Cada sesión activa y acción del servidor se registra en la pestaña

apropiada cuando se completa. La información que se muestra en estas pestañas se copia a los archivos de bitácora que se guardan en el directorio Logs, si se ha solicitado que se registre tal actividad.

El panel principal de la GUI de MDaemon contiene las siguientes pestañas:

Sistema — en el inicio del programa, la pestaña de Sistema muestra un registro del Proceso de Inicialización, que puede alertarle de posibles problemas con la configuración o el estatus de MDaemon. También muestra actividad tal como los diversos servidores de MDaemon habilitados/deshabilitados.

Estadísticas — esta pestaña mostrará un informe de las estadísticas del servidor correspondientes a la información contenida en los diversos contadores de nodos raíz en la pestaña Estadísticas en el panel de Estadísticas del panel de Herramientas y Estadísticas. Si desea cambiar la fuente o el tamaño de fuente utilizado para dicho informe, puede hacerlo editando las siguientes claves del archivo `MDaemon.ini`:

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

Además, cada día a medianoche, el Postmaster y todas las direcciones listadas en la pantalla Destinatarios 665 en el Filtro de Contenido recibirán una copia del informe vía correo. Este es el mismo informe que se genera cuando se usa el comando de correo "Estatus" listado en Control Remoto del Servidor 899. Si no desea que se envíe dicho informe, puede deshabilitar la opción *"Enviar reporte estadístico al Postmaster a medianoche"* localizada en la pantalla Misceláneos 503, bajo Preferencias.

Enrutamiento — muestra la formación de enrutado (Destinatario, Origen, ID de Mensaje, y demás) para cada mensaje procesado por MDaemon.

Seguridad — haga clic en esta pestaña y otras pestañas relacionadas con la seguridad aparecerán por encima de ésta.

Filtro de Contenido — Las operaciones de Filtro de Contenido 645 de MDaemon se listan en esta pestaña. Cuando un mensaje coincide con el criterio de alguna regla de mensaje del Filtro de Contenido, la información relacionada con dicho mensaje y las acciones tomadas se registran aquí.

Antivirus — Las operaciones del AntiVirus 645 se enlistan en esta pestaña. Cuando un mensaje sea escaneado para virus, la información relevante relacionada con dicho mensaje y la acción realizada serán registradas aquí.

AntiSpam — muestra todas las actividades de prevención del Filtro de Correo Basura 675 de MDaemon.

MDSpamD — lista todas las actividades del MDaemon Spam Daemon 686.

SPF — muestra todas las actividades de Sender Policy Framework 526.

DKIM — lista todas las actividades de DomainKeys Identified Mail 529.

DMARC — lista todas las actividades DMARC 538.

VBR — esta pestaña muestra las actividades de Certificación VBR 553.

MDPGP — esta pestaña despliega las actividades MDPGP 629.

Monitoreo — esta pestaña muestra las actividades de Tarpitting[602] y Monitoreo Dinámico[566].

Fallos Auth — Esta pestaña (y el archivo de registro correspondiente) contiene registros detallados para cada intento de inicio de sesión SMTP, IMAP y POP que falla. La información incluye el Protocolo utilizado, el valor Session ID (para que pueda buscar en otros archivos de registro) y la IP del ofensor, el valor de Inicio de sesión que intentaron utilizar (en ocasiones es un alias) y la Cuenta que coincide con el inicio de sesión (o 'ninguno' si ninguna cuenta coincide. Puede dar clic derecho en la línea de esta pestaña y agregar la dirección IP del ofensor a la lista de bloqueados.

MTA-STS — Despliega toda la actividad relacionada con SMTP MTA: Strict Transport Security (MTA-STS).

Correo — haga clic en esta pestaña y otras pestañas relacionadas con el correo aparecerán encima de ésta.

SMTP (entrante) — toda la actividad de sesiones entrantes que utilicen el protocolo SMTP se muestra en esta pestaña.

SMTP (saliente) — toda la actividad de sesiones salientes que utilicen el protocolo SMTP se muestra en esta pestaña.

IMAP — las sesiones de correo que utilicen el protocolo IMAP serán registradas en esta pestaña.

POP3 — cuando un usuario recoge correo de MDaemon utilizando protocolo POP3, la actividad se registra aquí.

MultiPOP — esta pestaña muestra la actividad de recogida de correo a través de MultiPOP de MDaemon.

DomainPOP — esta pestaña muestra la actividad de DomainPOP de MDaemon.

LDAP — muestra la actividad del servidor LDAP.

Minger — muestra la actividad del servidor Minger[863].

RAW — Los mensajes RAW o generados por sistema se registran en esta pestaña.

MDaemon Connector — muestra todas las actividades de MDaemon Connector[387].

Webmail

Webmail — despliega las actividades de correo de Webmail.

ActiveSync — esta pestaña despliega la actividad ActiveSync.

Colas de espera — esta pestaña da acceso a otra fila de pestañas por encima, cada una de las cuales corresponde cada cola de mensaje, tal como: Local, Remota, En Espera, Cuarentena, Correo basura bayesiano, y demás.

Complementos — despliega todas las actividades relacionadas a cualquiera de los complementos de MDaemon.

Active Directory — despliega toda la actividad relacionada a Active Directory.

Complemento — muestra todas las actividades relacionadas con cualquiera de los complementos de MDaemon.

Sesiones — haga clic en esta pestaña y otras pestañas aparecerán por encima de ésta. Estas pestañas muestran una entrada para cada conexión activa de MDaemon. Siempre que una conexión SMTP entre o salga, POP entre o

salga, IMAP, Webmail o ActiveSync, la información de cada una de las sesiones activas se mostrará aquí. Hacer doble clic en una sesión activa muestra la Ventana de Sesión 95, que muestra la transcripción de la sesión SMTP mientras ésta progresa.

La información que se muestra en estas pestañas no afecta a la cantidad de datos que se guarda en los ficheros de registro. Sin embargo, MDaemon tiene una amplia flexibilidad con respecto a la cantidad de información que se registra en dichos archivos. Vea el diálogo de logueo 175 para más información.

Menú de Acceso Directo de la Ventana de Registro de Eventos

Si hace clic derecho en cualquiera de las pestañas del panel de Registro de Eventos, se abrirá un menú de acceso directo. Se ofrecen varias opciones en este menú que se pueden usar para seleccionar, copiar, borrar o guardar los contenidos de una pestaña concreta. La opción de menú *Imprimir/Copiar* abrirá cualquier texto seleccionado en el bloc de notas, que puede ser usado para imprimir los datos o para guardarlos en un archivo. La opción *Borrar* borrará el texto seleccionado. La opción *Buscar* abrirá una ventana en la que podrá especificar una palabra o frase que buscar en los archivos de registro. MDaemon buscará en todos los archivos de registro dicha cadena y luego todas las transcripciones de sesiones que la contengan se confinarán en un solo archivo y se abrirán en Bloc de Notas para su revisión. Un uso práctico de esta funcionalidad seria buscar un ID de Mensaje concreto, que podría facilitar una compilación de todos los registros de todas las transcripciones de sesión que contengan dicho ID de Mensaje. En algunas pestañas existen opciones para reportar mensajes a MDaemon.com que han sido clasificados erróneamente como spam o como que contienen virus o que deberían haber sido clasificados como tales (ej. falsos positivos o falsos negativos). Los mensajes reportados serán analizados y se pasarán a los proveedores para que tomen acciones correctivas.

La disposición de la GUI de MDaemon no está limitada a las posiciones descritas anteriormente. Puede intercambiar la posición haciendo clic en Ventanas » Cambiar Paneles en la barra de menús.

Vista de Registro Compuesto

Localizado en el menú Ventanas de la barra de menús de MDaemon se encuentra la opción Vista de Registro Compuesto. Haciendo clic en esta opción se agrega una ventana a la GUI que combinará la información mostrada en una o más de las pestañas del panel principal. Utilice las opciones en la pantalla Registro Compuesto 177 de la opción logueo para definir la información que aparecerá en esa ventana.

Contadores de Rendimiento

MDaemon soporta los Contadores de Rendimiento de Windows, que permiten que programas de monitoreo rastreen el estatus de MDaemon en tiempo real. Existen contadores para el número de sesiones activas para varios protocolos, número de mensajes en las colas, estados de actividad/inactividad del servidor, tiempo en línea de MDaemon y estadísticas de sesión y mensajes.

Para utilizar los contadores de rendimiento, inicie el Monitor de Sistema en Panel de Control | Herramientas Administrativas | Rendimiento o ejecutando "perfmon". Dé clic en Agregar Contadores, seleccione el objeto MDaemon, luego seleccione y agregue los contadores que desea ver. Para ver los contadores de rendimiento de MDaemon corriendo en otro equipo debe tener habilitado el servicio "Registro Remoto" y tener acceso a través de sus firewall.

Ver:

Ventana de Sesión 95
Iconos de Bandeja 93
Menú de Accesos Directos 94
Registro Compuesto 177

2. .1 AutoDiscovery Service

MDaemon soporta el servicio AutoDiscovery, que permite a los usuarios configurar sus clientes de correo para conectar sus cuentas proporcionando solamente la dirección de correo y la contraseña en lugar de tener que conocer otros detalles de configuración tales como los nombres de los servidores de correo y los puertos. La mayoría de los clientes soportan el servicio, aunque algunos solo tienen soporte limitado. El servicio AutoDiscovery se habilita por omisión, pero lo puede deshabilitar/habilitar manualmente desde la interface principal de MDaemon. Bajo **Servidores** en el panel de Estadísticas, dé clic en **Servicio AutoDiscovery** y clic en **Habilitar/Deshabilitar AutoDiscovery.**

Los clientes que soportan totalmente el servicio AutoDiscovery utilizarán el nombre de dominio en la cuenta de correo del usuario para hacer una consulta del registro de servicio en el DNS (SRV) buscando el Tipo de Servicio _autodiscover._tcp y se conectarán a ese servidor para obtener información adicional. De manera que para soportar AutoDiscovery se deben crear registros DNS SRV para AutoDiscovery y los servicios que soporta. La implementación del servicio AutoDiscovery de MDaemon soporta: ActiveSync 416 (airsync), IMAP, POP, SMTP, DAV y XMPP.

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

Nota: algunos clientes siempre buscarán primero en `autodiscover.{domain}.{tld}`. A ese respecto puede ayudar hacer que el registro del servicio

AutoDiscovery apunte a un servidor llamado `autodiscover.{domain}.{tld}`. En el ejemplo siguiente, sin embargo, el servicio AutoDiscovery es `adsc.example.com`.

Ejemplo:

Nombre de Dominio: example.com

El admin debe configurar un registro de servicio_tcp para el tipo de servicio _autodiscover

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

En este caso, apunta a `adsc.example.com`, que tiene un registro A apuntando a `192.168.0.101`

Entonces el cliente se conectará a ese servidor y solicitará información del punto de conexión para algunos protocolos específicos: ActiveSync, IMAP, XMPP, SMTP, DAV, etc...

Luego el servicio AutoDiscovery consulta los protocolos solicitados y devuelve los nombre de servidor adecuados para esos protocolos. Ej. para ActiveSync, devolverá el nombre de servidor definido en el registro de servicio _tcp _airsync, que, en este ejemplo, sería eas.{domain}.{tld}

Si Outlook estuviera llamando a AutoDiscovery, devolvería los servidores IMAP y SMTP, representados por los registros de servicio _tcp de _imap y _msa, resultando en que los servidores que se devolverán serán imap4.example.com y msa.example.com.

Aquí un ejemplo para configurar correctamente los servicios AutoDiscovery. Se asume que se desea utilizar nombres únicos para cada protocolo pero se puede adaptar fácilmente para utilizar digamos un nombre común, tal y como mail.example.com.

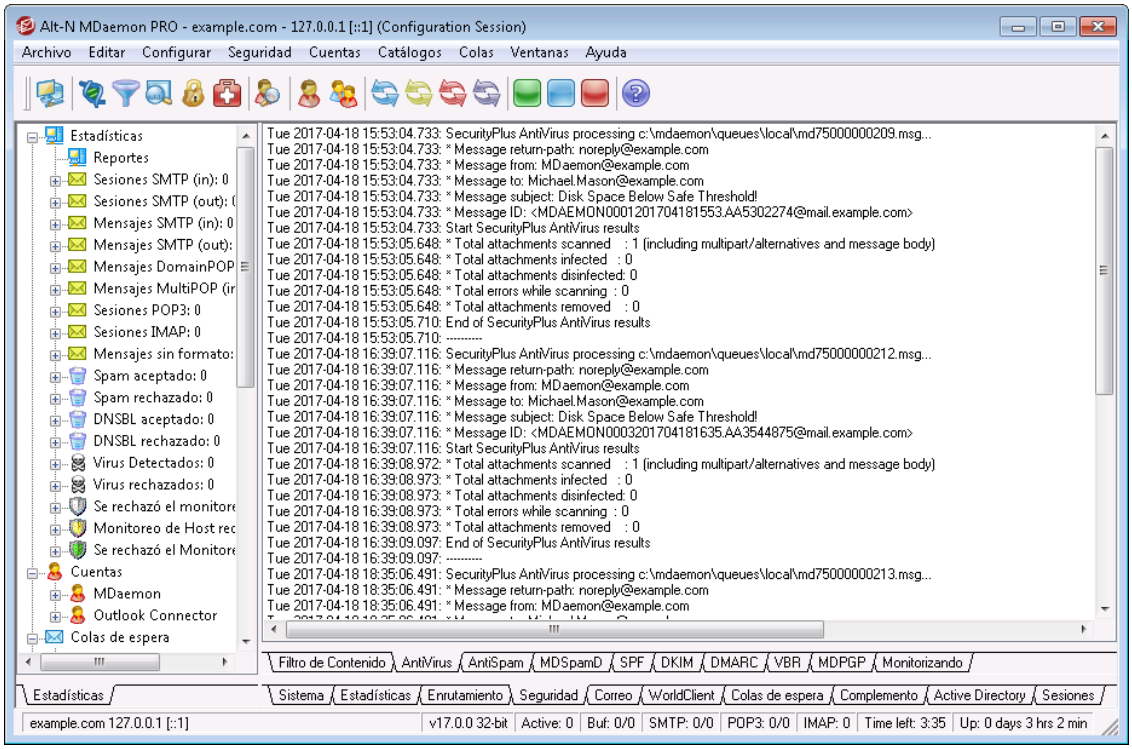
```
;
;  Archivo de base de datos example.com.dns para example.com zone.
;

@ IN  SOA dns.mydnsprovider.org. hostmaster.mydnsprovider.org. (
        4            ; serial number
        900          ; refresh
        600          ; retry
        86400        ; expire
        3600       ) ; default TTL

;
;  Zone NS records
;

@       NS dns.mydnsprovider.org

;
;  Zone records
;

@             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.example.com.
;
;  Service records
;

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

Ver:

Para información más general sobre AutoDiscover, vea el documento de Microsoft: Autodiscover for Exchange.

2.2 Registro de Eventos y Loggeo



La interfaz gráfica principal de usuario (GUI) proporciona información importante acerca de los recursos de MDaemon, estadísticas, sesiones activas y el correo en cola esperando a ser procesado. También contiene opciones para activar/desactivar fácilmente varios de los servidores de MDaemon. Los paneles en las pestañas de la GUI le mantienen al día de cómo actúan el servidor y sus conexiones entrantes y salientes.

Estadísticas

El panel de Estadísticas es el panel izquierdo por defecto de la interfaz principal de MDaemon. Este panel contiene cuatro secciones: Estadísticas, Cuentas, Colas y Servidores.

La sección *Estadísticas* contiene estadísticas sobre el número de mensajes enviados y recibidos por MDaemon, así como de las sesiones POP3 e IMAP, el SPAM aceptado y rechazado, virus y más. Las estadísticas se calculan desde el momento que MDaemon inicia y con clic derecho se puede accesar un menú para reiniciar los contadores.

Cuando haga clic en la opción "restablecer contadores del nodo raíz", todos los contadores se restablecerán, no solamente el que se esté apuntando. Además, existe una opción en Configurar » Preferencias » GUI que se puede usar para "*Preservar los contadores de nodo raíz en los reinicios*." Sin esta opción, los contadores se restablecerán siempre que el servidor se reinicie.

La sección *Cuentas* contiene registros para MDaemon, MDaemon Connector y ActiveSync. Cada opción enlista el número de cuentas utilizadas y el número de cuentas restantes, dependiendo de su licenciamiento.

La sección *Colas* contiene una entrada para cada cola de mensaje y el número de mensajes (si los hay) que contiene cada cola. Puede hacer clic derecho en cada entrada de cola para abrir un menú de acceso directo que contenta una o más de las siguientes opciones, dependiendo de la cola que haya seleccionado:

Ver Cola — esta opción cambia el panel principal a la pestaña de Colas y muestra la cola seleccionada. Se desplegará una lista de todos los mensajes que contiene la cola y se puede dar clic derecho a cualquier mensaje para abrir un menú de acceso rápido conteniendo numerosas opciones similares a las que están disponibles en el Administrador de Colas & Estadísticas, tales como Copiar, Mover, Editar y demás.

Administrador de colas y estadísticas — abre el Administrador de Colas y Estadísticas por la Página de Cola mostrando la información para la cola seleccionada.

Procesar Ahora — esta opción "reencola" todos los mensajes contenidos en la cola e intenta procesarlos normalmente para envío. Si intenta procesar mensajes contenidos en la Cola de Espera, Cola incorrecta, o similar, entonces es posible que los mensajes encuentren los mismos errores que originaron que se les colocara ahí en primer lugar y vuelvan a la misma cola.

Inmovilizar / liberar cola — pausa temporalmente el procesamiento para la cola seleccionada, o continua el procesamiento si actualmente se encuentra pausada.

Liberar — libera mensajes de la Cola de Espera. MDaemon intentará enviar los mensajes aun y cuando se encuentren errores — no serán devueltos a la cola de Espera, aunque vuelvan a encontrar los mismos errores que inicialmente los colocaron allí.

Volver a poner en la cola — Esta opción está disponible para la Cola de Espera, y tiene el mismo efecto que la opción anterior de *Procesar Ahora*.

Habilitar/deshabilitar cola — activa o desactiva la Cola de Espera. Cuando de deshabilita, los mensajes no se moverán a la cola de Espera aun y cuando se encuentren errores.

La sección *Servidores* contiene una entrada para cada servidor contenido en MDaemon, y cada entrada lista el estado actual del servidor: "Activo" o "Inactivo". A continuación de cada entrada de servidor existe una entrada para cada dominio (cuando aplique) y el puerto e IP actualmente en uso por dicho dominio. El menú de acceso directo provee control para alternar el estado de cada servidor entre Activo e Inactivo. Cuando un servidor esté inactivo su ícono se volverá rojo.

Registro de Eventos y logueo

El panel derecho por defecto de la interfaz principal contiene un grupo de pestañas que muestran las acciones actuales de MDaemon y el estatus de varios servidores y recursos, y se actualizan constantemente para reflejar las condiciones actuales del servidor. Cada sesión activa y acción del servidor se registra en la pestaña apropiada cuando se completa. La información que se muestra en estas pestañas se copia a los archivos de bitácora que se guardan en el directorio Logs, si se ha solicitado que se registre tal actividad.

El panel principal de la GUI de MDaemon contiene las siguientes pestañas:

Sistema — en el inicio del programa, la pestaña de Sistema muestra un registro del Proceso de Inicialización, que puede alertarle de posibles problemas con

la configuración o el estatus de MDaemon. También muestra actividad tal como los diversos servidores de MDaemon habilitados/deshabilitados.

Estadísticas — esta pestaña mostrará un informe de las estadísticas del servidor correspondientes a la información contenida en los diversos contadores de nodos raíz en la pestaña Estadísticas en el panel de Estadísticas del panel de Herramientas y Estadísticas. Si desea cambiar la fuente o el tamaño de fuente utilizado para dicho informe, puede hacerlo editando las siguientes claves del archivo `MDaemon.ini`:

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

Además, cada día a medianoche, el Postmaster y todas las direcciones listadas en la pantalla Destinatarios 665 en el Filtro de Contenido recibirán una copia del informe vía correo. Este es el mismo informe que se genera cuando se usa el comando de correo "Estatus" listado en Control Remoto del Servidor 899. Si no desea que se envíe dicho informe, puede deshabilitar la opción *"Enviar reporte estadístico al Postmaster a medianoche"* localizada en la pantalla Misceláneos 503, bajo Preferencias.

Enrutamiento — muestra la formación de enrutado (Destinatario, Origen, ID de Mensaje, y demás) para cada mensaje procesado por MDaemon.

Seguridad — haga clic en esta pestaña y otras pestañas relacionadas con la seguridad aparecerán por encima de ésta.

Filtro de Contenido — Las operaciones de Filtro de Contenido 645 de MDaemon se listan en esta pestaña. Cuando un mensaje coincide con el criterio de alguna regla de mensaje del Filtro de Contenido, la información relacionada con dicho mensaje y las acciones tomadas se registran aquí.

Antivirus — Las operaciones del AntiVirus 645 se enlistan en esta pestaña. Cuando un mensaje sea escaneado para virus, la información relevante relacionada con dicho mensaje y la acción realizada serán registradas aquí.

AntiSpam — muestra todas las actividades de prevención del Filtro de Correo Basura 675 de MDaemon.

MDSpamD — lista todas las actividades del MDaemon Spam Daemon 686.

SPF — muestra todas las actividades de Sender Policy Framework 526.

DKIM — lista todas las actividades de DomainKeys Identified Mail 529.

DMARC — lista todas las actividades DMARC 538.

VBR — esta pestaña muestra las actividades de Certificación VBR 553.

MDPGP — esta pestaña despliega las actividades MDPGP 629.

Monitoreo — esta pestaña muestra las actividades de Tarpitting 602 y Monitoreo Dinámico 566.

Fallos Auth — Esta pestaña (y el archivo de registro correspondiente) contiene registros detallados para cada intento de inicio de sesión SMTP, IMAP y POP que falla. La información incluye el Protocolo utilizado, el valor Session ID (para que pueda buscar en otros archivos de registro) y la IP del ofensor, el valor de Inicio de sesión que intentaron utilizar (en

ocasiones es un alias) y la Cuenta que coincide con el inicio de sesión (o 'ninguno' si ninguna cuenta coincide. Puede dar clic derecho en la línea de esta pestaña y agregar la dirección IP del ofensor a la lista de bloqueados.

MTA-STS — Despliega toda la actividad relacionada con SMTP MTA: Strict Transport Security (MTA-STS).

Correo — haga clic en esta pestaña y otras pestañas relacionadas con el correo aparecerán encima de ésta.

SMTP (entrante) — toda la actividad de sesiones entrantes que utilicen el protocolo SMTP se muestra en esta pestaña.

SMTP (saliente) — toda la actividad de sesiones salientes que utilicen el protocolo SMTP se muestra en esta pestaña.

IMAP — las sesiones de correo que utilicen el protocolo IMAP serán registradas en esta pestaña.

POP3 — cuando un usuario recoge correo de MDaemon utilizando protocolo POP3, la actividad se registra aquí.

MultiPOP — esta pestaña muestra la actividad de recogida de correo a través de MultiPOP de MDaemon.

DomainPOP — esta pestaña muestra la actividad de DomainPOP de MDaemon.

LDAP — muestra la actividad del servidor LDAP.

Minger — muestra la actividad del servidor Minger 863.

RAW — Los mensajes RAW o generados por sistema se registran en esta pestaña.

MDaemon Connector — muestra todas las actividades de MDaemon Connector 387.

Webmail

Webmail — despliega las actividades de correo de Webmail.

ActiveSync — esta pestaña despliega la actividad ActiveSync.

Colas de espera — esta pestaña da acceso a otra fila de pestañas por encima, cada una de las cuales corresponde cada cola de mensaje, tal como: Local, Remota, En Espera, Cuarentena, Correo basura bayesiano, y demás.

Complementos — despliega todas las actividades relacionadas a cualquiera de los complementos de MDaemon.

Active Directory — despliega toda la actividad relacionada a Active Directory.

Complemento — muestra todas las actividades relacionadas con cualquiera de los complementos de MDaemon.

Sesiones — haga clic en esta pestaña y otras pestañas aparecerán por encima de ésta. Estas pestañas muestran una entrada para cada conexión activa de MDaemon. Siempre que una conexión SMTP entre o salga, POP entre o salga, IMAP, Webmail o ActiveSync, la información de cada una de las sesiones activas se mostrará aquí. Hacer doble clic en una sesión activa muestra la Ventana de Sesión 95, que muestra la transcripción de la sesión SMTP mientras ésta progresa.

La información que se muestra en estas pestañas no afecta a la cantidad de datos que se guarda en los ficheros de registro. Sin embargo, MDaemon tiene una amplia flexibilidad con respecto a la cantidad de información que se registra en dichos archivos. Vea el diálogo de logueo 175 para más información.

Menú de Acceso Directo de la Ventana de Registro de Eventos

Si hace clic derecho en cualquiera de las pestañas del panel de Registro de Eventos, se abrirá un menú de acceso directo. Se ofrecen varias opciones en este menú que se pueden usar para seleccionar, copiar, borrar o guardar los contenidos de una pestaña concreta. La opción de menú *Imprimir/Copiar* abrirá cualquier texto seleccionado en el bloc de notas, que puede ser usado para imprimir los datos o para guardarlos en un archivo. La opción *Borrar* borrará el texto seleccionado. La opción *Buscar* abrirá una ventana en la que podrá especificar una palabra o frase que buscar en los archivos de registro. MDaemon buscará en todos los archivos de registro dicha cadena y luego todas las transcripciones de sesiones que la contengan se confinarán en un solo archivo y se abrirán en Bloc de Notas para su revisión. Un uso práctico de esta funcionalidad seria buscar un ID de Mensaje concreto, que podría facilitar una compilación de todos los registros de todas las transcripciones de sesión que contengan dicho ID de Mensaje. En algunas pestañas existen opciones para reportar mensajes a MDaemon.com que han sido clasificados erróneamente como spam o como que contienen virus o que deberían haber sido clasificados como tales (ej. falsos positivos o falsos negativos). Los mensajes reportados serán analizados y se pasarán a los proveedores para que tomen acciones correctivas.

La disposición de la GUI de MDaemon no está limitada a las posiciones descritas anteriormente. Puede intercambiar la posición haciendo clic en Ventanas » Cambiar Paneles en la barra de menús.

Vista de Registro Compuesto

Localizado en el menú Ventanas de la barra de menús de MDaemon se encuentra la opción Vista de Registro Compuesto. Haciendo clic en esta opción se agrega una ventana a la GUI que combinará la información mostrada en una o más de las pestañas del panel principal. Utilice las opciones en la pantalla Registro Compuesto 177 de la opción logueo para definir la información que aparecerá en esa ventana.

Contadores de Rendimiento

MDaemon soporta los Contadores de Rendimiento de Windows, que permiten que programas de monitoreo rastreen el estatus de MDaemon en tiempo real. Existen contadores para el número de sesiones activas para varios protocolos, número de mensajes en las colas, estados de actividad/inactividad del servidor, tiempo en línea de MDaemon y estadísticas de sesión y mensajes.

Para utilizar los contadores de rendimiento, inicie el Monitor de Sistema en Panel de Control | Herramientas Administrativas | Rendimiento o ejecutando "perfmon". Dé clic en Agregar Contadores, seleccione el objeto MDaemon, luego seleccione y agregue los contadores que desea ver. Para ver los contadores de rendimiento de

MDaemon corriendo en otro equipo debe tener habilitado el servicio "Registro Remoto" y tener acceso a través de sus firewall.

Ver:

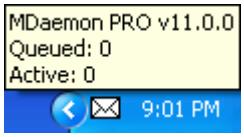
Ventana de Sesión 95
Iconos de Bandeja 93
Menú de Accesos Directos 94
Registro Compuesto 177

2.4 Icono de Bandeja

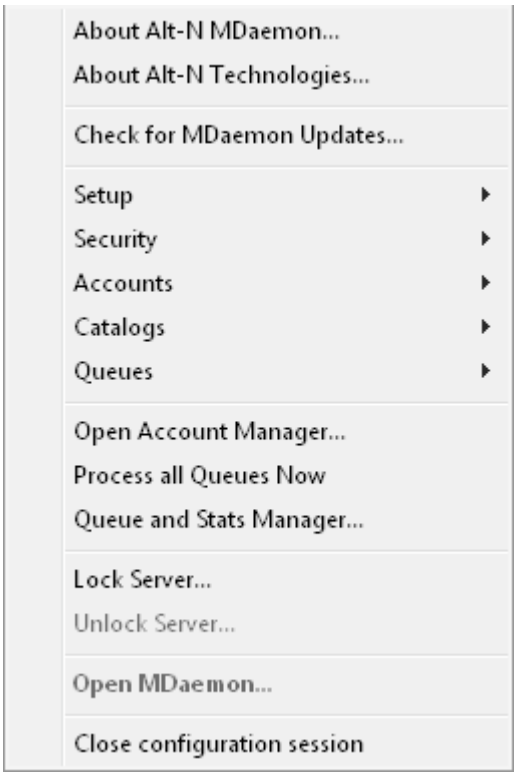
Siempre que el servidor de MDaemon se está ejecutando, este icono será visible en la bandeja del sistema. Además de permitirle saber cuándo el servidor se está ejecutando, el icono también es dinámico y cambiará los colores en función del estado actual del servidor. La siguiente es una lista de los indicadores de icono:

	Todo correcto. No hay colas locales o remotas.
	Todo correcto. Hay colas locales o remotas.
	Espacio en disco disponible por debajo del umbral (ver Configurar » Preferencias » Disco 496).
	La red está caída, la marcación telefónica ha fallado, o el disco está lleno.
Icono Parpadea	Una nueva versión de MDaemon se encuentra disponible.

Hay información adicional sobre el servidor disponible a través de la ayuda contextual del icono. Pause el puntero del ratón encima de éste y la ayuda contextual aparecerá, mostrando el número de los mensajes en cola actuales y las sesiones activas.



Menú de Acceso Directo



Haga clic derecho en el icono de bandeja de MDaemon para mostrar el menú de acceso directo. Este menú le da acceso rápido a virtualmente todos los menús de MDaemon sin tener que abrir la interfaz de usuario principal.

Haga Clic en la opción "Acerca de MDaemon..." en la sección superior del menú de acceso directo para averiguar más acerca de MDaemon o MDaemon Technologies.

En la siguiente sección, haga clic en "Buscar actualizaciones de MDaemon..." para ver si existe una versión más nueva de MDaemon para descarga.

En la tercera sección puede acceder a los siguientes menús de MDaemon: Configurar, Seguridad, Cuentas y Colas. Cada uno de estos menús en cascada es idéntico al menú del mismo nombre ubicado en la barra de menús de la interfaz principal.

La cuarta sección tiene opciones para abrir el Gestor de Cuentas y el Gestor de Colas y Estadísticas, y uno que hará que todas las colas de correo de MDaemon se procesen.

A continuación, existen comandos para bloquear y desbloquear la interfaz de MDaemon (Vea la sección "Bloquear/Desbloquear la Interfaz Principal de MDaemon" a continuación) seguido por la opción de menú "Abrir MDaemon...", se utiliza para abrir/restaurar la interfaz de MDaemon cuando esta ha sido minimizada a la bandeja de sistema.

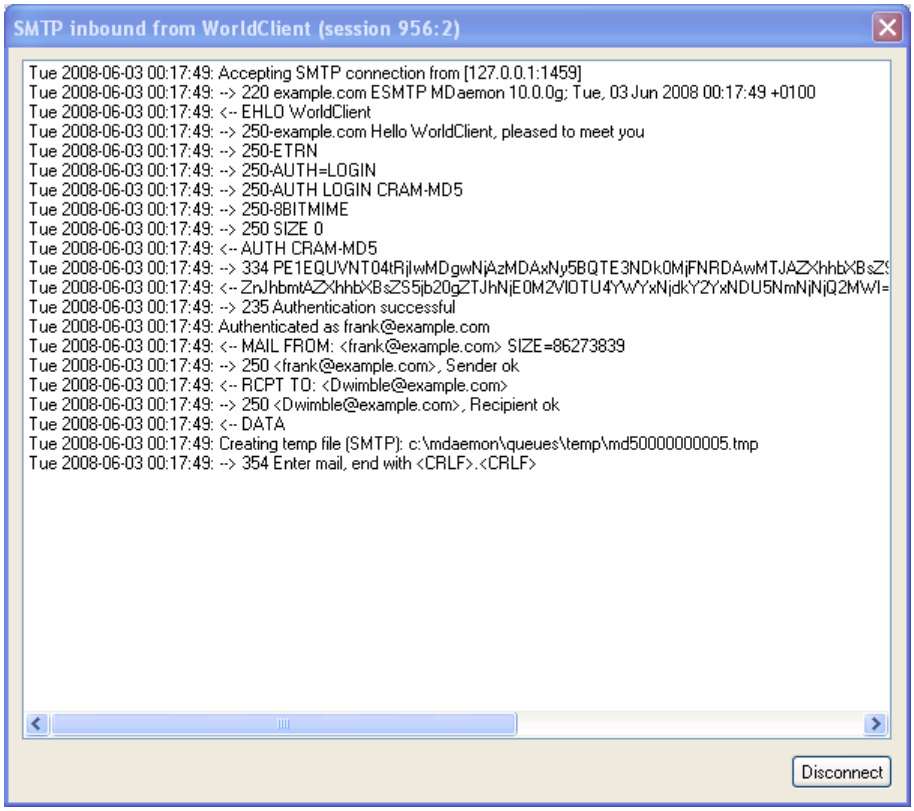
La última opción es "Cerrar la sesión de Configuración" que cierra la interface de MDaemon. Si se cierra la sesión de Configuración, no se detiene el servicio MDaemon.

Bloquear/Desbloquear la Interfaz Principal de MDaemon

Para bloquear la interfaz de usuario, minimice MDaemon, haga clic en la opción de menú "Bloquear servidor..." y luego entre una contraseña en el campo que se abre. Después de confirmarlo entrándolo una segunda vez, la interfaz de usuario de MDaemon se bloqueará. No puede ser abierta o visualizada, pero MDaemon seguirá funcionando normalmente. Seguirá pudiendo, sin embargo, usar la opción de "Procesar todas las colas ahora..." para procesar manualmente las colas. Para desbloquear MDaemon, abra el diálogo de "Desbloquear MDaemon" haciendo doble clic en el icono de bandeja, o haciendo clic derecho y escogiendo la opción "Desbloquear Servidor..." Luego, entre la contraseña que se introdujo cuando se bloqueó.

2.5 Ventana de Sesión

Cuando se hace doble-clic en una sesión activa de una de las Pestañas de Sesión 81 de la interfaz principal, ello hará que se abra la ventana de sesión que corresponda a dicha entrada. La ventana de sesión mostrará la transcripción SMTP de dicha sesión según progresa. Puede hacer clic en Desconectar en esta ventana si desea interrumpir y desconectar dicha sesión en progreso.

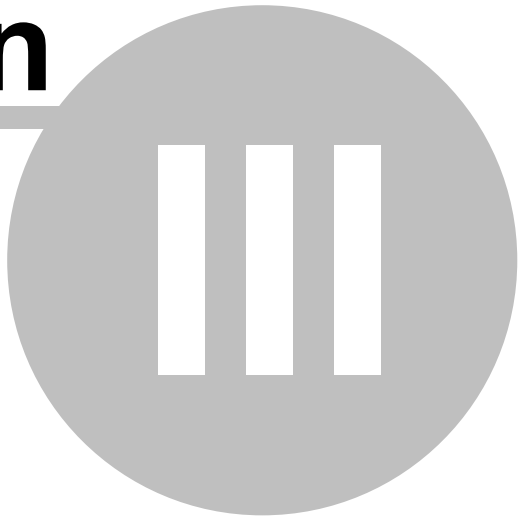


2.6 Flujo de Trabajo del SMTP en MDaemon

Cuando se realiza una conexión SMTP entrante, MDaemon pasa por una serie de complejos pasos de proceso para determinar si debe o no aceptar el mensaje para entrega, y qué hacer con él una vez se acepte. La siguiente es una representación gráfica de este proceso de trabajo para los mensajes SMTP entrantes.

La medida en la que se ejecutan estos pasos va en función de su configuración particular. Uno o más pasos pueden ser saltados si una de las funcionalidades se desactiva en su configuración.

Sección

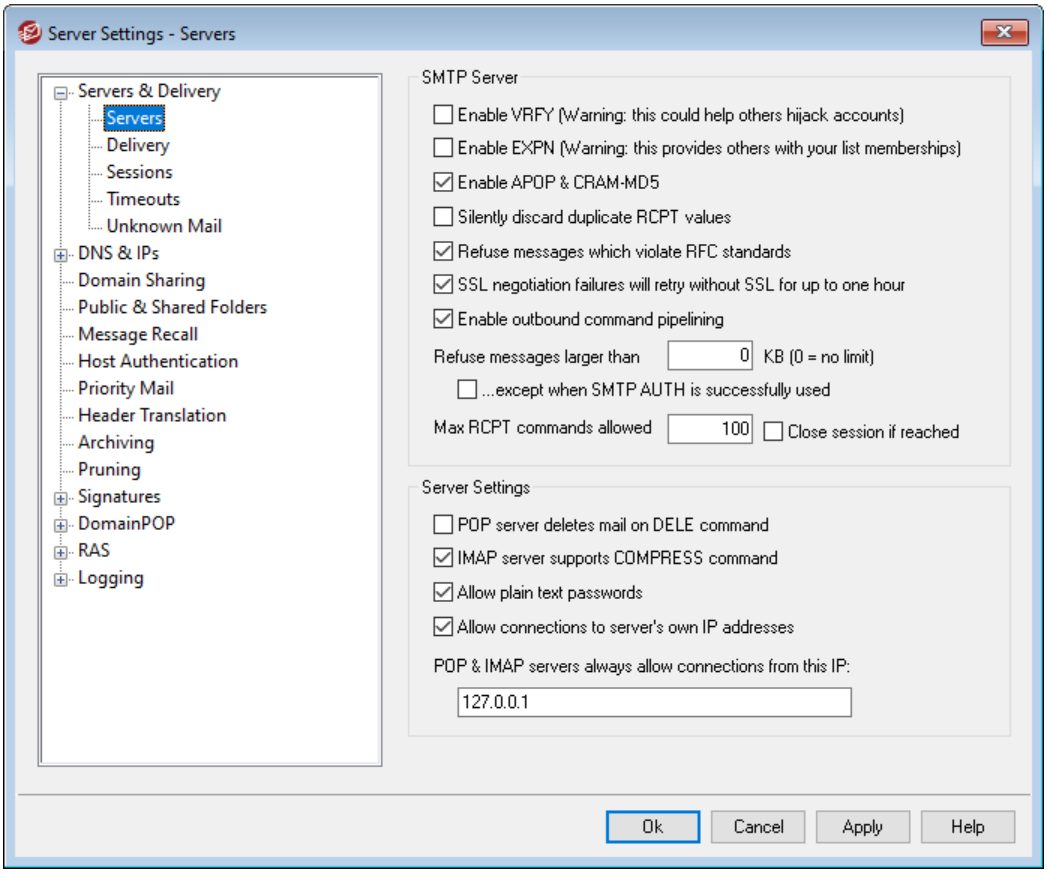


3 Menú Configuración

3.1 Configuración del Servidor

3.1.1 Servidores & Entrega

3.1.1.1 Servidores



Servidor SMTP

Habilitar VRFY
Haga clic en esta opción si desea responder a los comandos SMTP VRFY. Este comando se utiliza a veces por servidores que usan la función call forward o call back de SMTP para intentar confirmar la validez de las direcciones de correo en su servidor. Está deshabilitado por defecto.

Habilitar EXPN
Haga clic en esta casilla de verificación si desea que MDaemon responda a comandos EXPN.

Habilitar APOP & CRAM-MD5
Por omisión los servidores de MDaemon (POP, IMAP y demás) no respetan los métodos de autentificación APOP y CRAM-MD5. Este tipo de autentificación requiere que se almacenen contraseñas utilizando encripción reversible, que no se recomienda por motivos de seguridad, con el fin de impedir que las contraseñas sean desencriptadas por MDaemon, el administrador o algún posible

atacante. En consecuencia, esta opción no se compatible con la Opción de Contraseñas 855 "*Almacenar contraseñas de buzones utilizando encriptación no reversible*", ni con la autentificación vía Active Directory. No obstante, si usted no utiliza SSL/TLS, entonces APOP y CRAM-MD5 le pueden proporcionar seguridad extra posibilitando que los usuarios se autentifiquen sin enviar las contraseñas en texto limpio.

responden a los métodos de autenticación APOP y CRAM-MD5. Estos métodos proveen de seguridad extra haciendo posible para los usuarios autenticarse sin enviar las contraseñas en texto plano. Deshabilite esta casilla si no desea permitir APOP o CRAM-MD5.

Ignora silenciosamente valores RCPT duplicados
Habilite esta opción si desea que el servidor SMTP ignore los destinatarios duplicados en la misma sesión SMTP. MDaemon aceptará y descartará los destinatarios duplicados. Esta opción se encuentra deshabilitada por omisión.

Rechazar mensajes que violan los estándares RFC
Habilite esta opción si desea rechazar mensajes durante el proceso SMTP que no cumplan con los estándares RFC de Internet. Para que los mensajes pasen la prueba de cumplimiento deben:

1. Tener un tamaño mayor a 32 bytes (el tamaño mínimo requerido para incluir todos los elementos requeridos).

2. Tener un encabezado FROM: o SENDER: (remitente o destinatario).

3. No tener más de un encabezado FROM:.

4. No tener más de un encabezado SUBJECT:, aunque no es requerido tener el encabezado asunto.

Los mensajes que utilizan sesiones autentificadas o que provienen de dominios o direcciones IP confiables estarán exentos de estos requerimientos.

Fallos de negociación SSL reintentarán sin SSL hasta por una hora
Esta opción le permite reintentar temporalmente IPs de host sin SSL cuando se encuentra un error SSL durante una sesión SMTP saliente. Se restablece cada hora.

Rechazar mensajes mayores de [xx] KB (0=sin límite)
Establecer un valor aquí impide que MDaemon acepte o procese correo que exceda cierto tamaño fijo. Cuando se habilita esta opción MDaemon intentará utilizar el comando ESMTP SIZE especificado en el RFC-1870. Si el agente remitente soporta esta extensión SMTP entonces MDaemon determinará el tamaño del mensaje antes de su entrega y rechazará el mensaje inmediatamente. Si el agente remitente no soporta esta extensión SMTP entonces MDaemon tendrá que iniciar la aceptación del mensaje, rastrear su tamaño periódicamente durante la transferencia y finalmente rechazar la entrega del mensaje una vez que la transacción se haya completado. Utilice "0" en esta opción si no desea establecer un tamaño límite. Si desea exentar a las sesiones autentificadas de la verificación SIZE, utilice la opción siguiente "*...excepto cuando SMTP AUTH se utiliza exitosamente*".

...excepto cuando SMTP AUTH se utiliza exitosamente
Marque esta caja si desea exentar los mensajes de la verificación de tamaño cuando la sesión SMTP haya sido autentificada.

Max comandos RCPT permitidos
Utilice esta opción si desea limitar el número de comandos RCPT que se pueden enviar por mensaje. Utilice "0" si no desea establecer un límite.

Cerrar la sesión si se alcanza
Marque esta caja si desea cerrar la sesión inmediatamente cuando se alcanza el número máximo de comandos RCPT.

Ajustes de Servidor

El servidor POP elimina el correo con el comando DELE
Haga clic en esta opción si desea que MDaemon borre inmediatamente los mensajes que se han recuperado y se reciba el comando DELE aun y cuando la sesión POP no se haya completado correctamente.

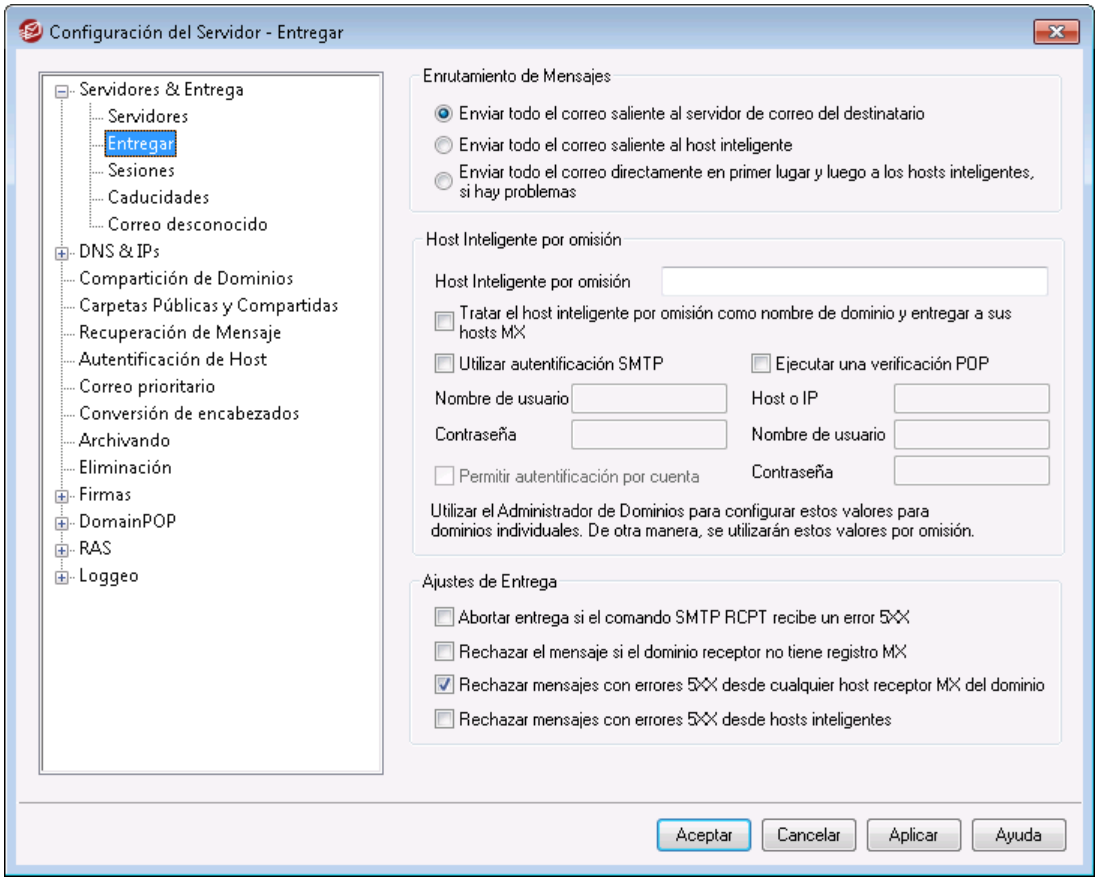
El servidor IMAP soporta el comando COMPRESS
Dé clic en esta opción si desea habilitar el soporte a la extensión IMAP COMPRESS (RFC 4978), que comprime todos los datos enviados y recibidos del cliente. COMPRESS incrementará el uso de memoria y procesador por cada sesión IMAP.

Permitir contraseñas en texto plano
Esta opción controla si MDaemon acepta o no contraseñas enviadas en texto plano a los servidores SMTP, IMAP, o POP3. Si se deshabilita, los comandos `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN` y `SMTP AUTH LOGIN` devolverán un error a menos que la conexión esté utilizando SSL.

Permitir conexiones a las direcciones IP del servidor
Cuando se habilita esta opción, MDaemon se puede conectar consigo mismo.

Los servidores POP & IMAP siempre permiten conexiones desde esta IP
Los servidores POP e IMAP siempre aceptarán conexiones desde la dirección IP registrada en este campo sin importar los ajustes de monitoreo y protección IP.

3.1.1.2 Entrega



Enrutamiento de Mensajes

Enviar todo el correo saliente al servidor de correo del destinatario
Cuando se escoge esta opción, MDaemon intentará enviar el correo directamente en lugar de pasarlo a otro host. MDaemon colocará los mensajes que no fue posible enviar en el sistema de reintentos y continuará intentando el envío de acuerdo con los parámetros y los intervalos de tiempo que se establezcan en la pantalla Cola de Reintentos 872 del diálogo de Colas de Correo.

Enviar todo el correo saliente a un host inteligente
Seleccione esta opción si quiere que todo el correo saliente, independientemente del dominio de destino, sea entregado en cola hacia otro host para enrutamiento de envío. Si se selecciona, el correo saliente será enviado al *Host Inteligente por Omisión* especificado abajo. Típicamente, esta funcionalidad es útil durante períodos de alto volumen cuando el envío directo de mensajes pudiera resultar en un excesivo uso de los recursos del servidor. Si un mensaje no puede ser enviado al servidor designado será movido al sistema de reintentos y MDaemon seguirá intentando enviarlo según los parámetros e intervalos de tiempo que se establezcan en la pantalla Cola de Reintentos 872 del diálogo Colas de Correo.

Enviar primero todo el correo directamente y luego al host inteligente si hay problemas
Esta opción es una combinación de las dos opciones de entrega previas. Primero MDaemon intentará entregar el correo saliente directamente al servidor, pero si no puede hacerlo, intentará enviar el mensaje al *Host Inteligente por omisión especificado abajo.* El correo que no se puede entregar es aquel destinado a hosts para los que no pudo resolverse una dirección IP (tal como una Puerta de enlace no registrada hacia una red remota) o correo dirigido a un host cuya

dirección se resolvió correctamente, pero al que no se pudo conectar directamente o que está rechazando las conexiones directas. En lugar de devolver ese mensaje al remitente, esta opción hace que MDaemon pase el mensaje a un MTA más poderoso. Algunas veces el sistema de correo administrado por su ISP puede tener métodos de ruteo para la entrega de correo a los que no tiene acceso directo su servidor de correo local. Sin embargo, si un mensaje no puede ser entregado al host inteligente definido entonces pasará al sistema de reintentos y MDaemon continuará intentando entregarlo de acuerdo con los parámetros e intervalos de tiempo configurados en la pantalla Cola de Reintentos 872 de la opción Colas de Correo. En cada intento de entrega subsecuente, MDaemon otra vez intentará entregar primero al destinatario y luego al host inteligente definido.

Host Inteligente por Omisión

Host inteligente por Omisión
Especifique aquí el nombre o dirección IP del host de correo. Este es generalmente el servidor SMTP de su ISP.

No introduzca aquí el nombre del Dominio por Defecto o la dirección IP de su servidor MDaemon. Esta entrada debe ser un ISP u otro servidor de correo que pueda enrutar correo procedente de usted.

Tratar el host inteligente por omisión como nombre de dominio y entregar a su host MX
Habilite esta opción si desea que MDaemon trate el *Host Inteligente por Omisión* como nombre de dominio, consultando su registro DNS y entregando a sus hosts MX.

Utilizar autentificación SMTP
Dé clic en esta casilla y registre sus credenciales de acceso si el *Host Inteligente por Omisión* requiere autentificación. Estas credenciales de ingreso serán utilizadas para todos los mensajes SMTP salientes enviados al host inteligente. Sin embargo, si selecciona utilizar la opción *Permitir autentificación por cuenta* que se encuentra abajo, MDaemon se autentificará ante el host inteligente de manera separada para cada mensaje, utilizando las credenciales definidas para cada cuenta en la pantalla Servicios de Correo 719 del Editor de Cuentas.

Nombre de usuario
Introduzca aquí su nombre de usuario o nombre de acceso.

Contraseña
Utilice esta opción para especificar la contraseña de host inteligente.

Ejecute primero una validación POP
Si su host inteligente requiere comprobación POP3 antes de aceptar mensajes procedentes de usted, entonces seleccione esta casilla de verificación e introduzca las credenciales requeridas a continuación.

Host o IP
Introduzca la dirección IP o el host al cual desea conectarse.

Nombre de usuario
Este es el nombre de acceso o nombre de usuario de la cuenta POP.

Contraseña
Esta es la contraseña de la cuenta POP.

Permitir autenticación por cuenta
Haga clic en esta casilla de verificación si desea utilizar autenticación por cuenta para los mensajes SMTP salientes enviados al *Host Inteligente* especificado arriba. En lugar de utilizar las credenciales de *Nombre de Usuario* y *Contraseña* aquí especificadas, se utilizarán las credenciales de cada cuenta para *Acceso Host Inteligente*, definidas en la pantalla Servicios de Correo 719. Si no se han definido credenciales para el host inteligente para una cuenta dada, se utilizarán las credenciales generales por omisión.

Si desea configurar la *autenticación por cuenta* para que utilice la contraseña de cada correo en lugar de la *Contraseña de host inteligente* opcional, entonces puede hacerlo editando la siguiente clave en el archivo `MDaemon.ini`:

```
[AUTH]
ISPAUTHUsePasswords=Yes (Default No)
```

Establecer la opción `ISPAUTHUsePasswords=Yes` comunicará a lo largo de un tiempo las contraseñas de las cuentas de usuario de correo locales al smart host. Esto podría ser un riesgo para la seguridad en el correo, puesto que se está facilitando información sensible a otro servidor. Debería no utilizar dicha opción salvo que esté usando un smart host en el que confíe plenamente y crea que es necesario hacerlo. Además, debería tener en cuenta que esta opción da a los usuarios permiso para cambiar su *Contraseña de* vía Webmail o por otros métodos, y entonces también estarían cambiando la *Contraseña de Smart Host.* Eso podría causar que la autenticación del smart host fallara para una cuenta cuando la *Contraseña de Correo* no se haya cambiado en el smart host.

Abortar entrega si el comando SMTP RCPT recibe un error 5xx
Habilite esta opción si desea que MDaemon aborte el intento de enviar un mensaje cuando reciba un error fatal 5xx en respuesta al comentado SMTP RCPT. Esta opción está deshabilitada por defecto.

Rechazar el mensaje si el dominio remitente no tiene registro MX
Normalmente cuando MDaemon verifica los registros DNS del dominio remitente, busca los registros MX y luego busca un registro A cuando no encuentra los primeros. Si no se encuentra ninguno de los dos, rechazará el mensaje indicando al remitente que no fue entregable. Habilite esta opción si desea que MDaemon rechace inmediatamente el mensaje si no encuentra registros MX, en lugar de permitirle buscar el registro A. Esta opción se encuentra deshabilitada por omisión.

Haga clic en esta opción para hacer que MDaemon devuelva inmediatamente el mensaje cuando la búsqueda de DNS muestre que no existe un registro MX ni un registro A para el dominio del destinatario. Esto previene que ese tipo de

mensajes entren innecesariamente en el ciclo de intento de envío. Esta opción está habilitada por defecto.

Rebotar mensajes con el primer error 5XX de algún dominio de HOST de destinatario
Cuando esta casilla de verificación está habilitada, MDaemon devolverá/rebotará el mensaje cuando reciba un error fatal 5xx como respuesta de un host MX. Consecuentemente, no continuará intentando el envío a ningún host MX siguiente que puedan estar designados para el dominio del destinatario. Si esta opción se deshabilita, MDaemon no rebotará los mensajes mientras al menos uno de los hosts MX devuelva un error no fatal 4xx como respuesta. Esta opción está habilitada por defecto.

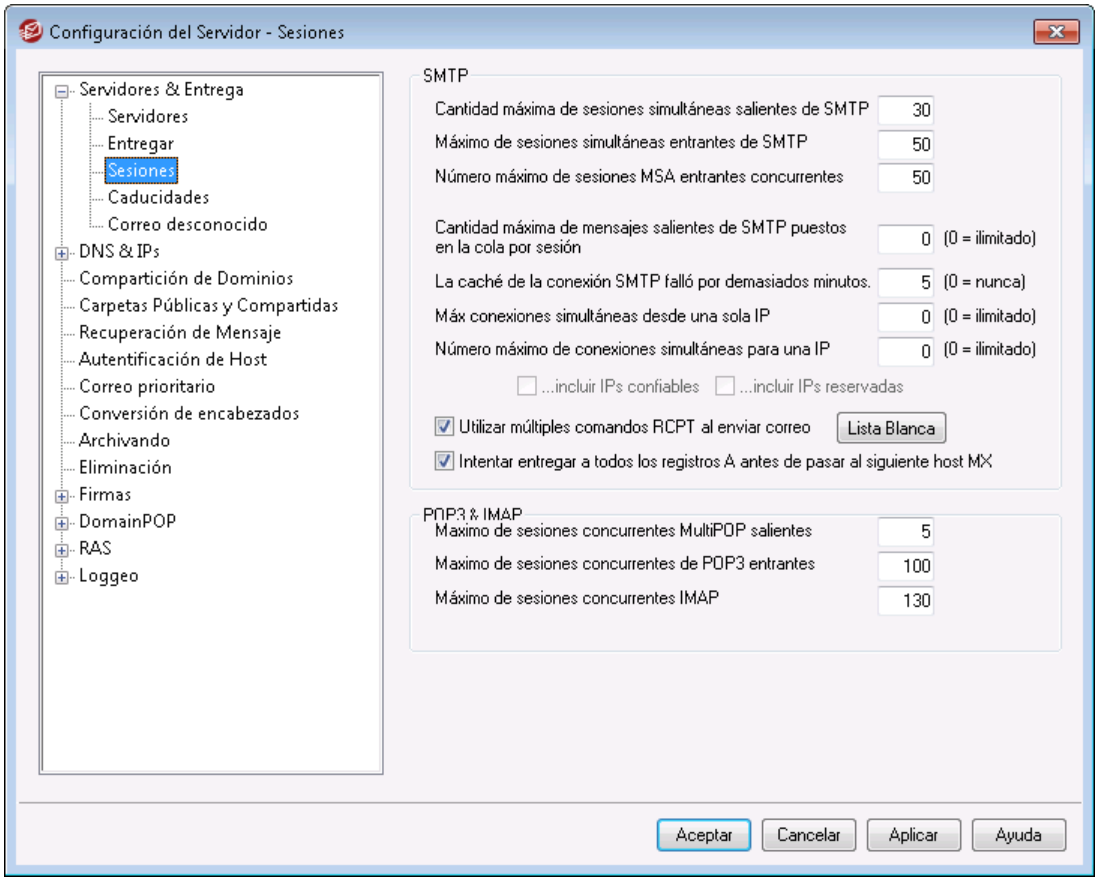
Rebotar mensajes al encontrar errores 5XX de hosts inteligentes

Utilice esta opción si desea devolver/rebotar un mensaje cuando recibe una respuesta de error fatal 5XX por parte del host inteligente.

Ver:

Cola de Reintentos 872
Servicios de Correo 719

3.1.1.3 Sesiones



SMTP

Cantidad máxima de sesiones concurrentes salientes de SMTP
El valor aquí introducido representa el máximo de sesiones SMTP salientes que se crearán cuando se envíe correo saliente. Cada sesión enviará mensajes salientes hasta que la cola esté vacía o la configuración *Cantidad máxima de mensajes salientes de SMTP puestos en la cola por sesión* haya sido alcanzada. Por ejemplo, si el correo saliente tiene veinte mensajes esperando, entonces cuando sea momento de enviar correo y el valor de esta configuración sea cinco, cinco sesiones se crearán de manera simultánea y enviarán consecutivamente cuatro mensajes cada una.

Esta opción está configurada a 30 por defecto, pero puede que desee experimentar con el número de sesiones para poder encontrar la configuración que le resultará mejor para el rendimiento de su ancho de banda. Es posible especificar tantas sesiones que su ancho de banda esté sobrecargado o que su sistema Windows se quede sin recursos y pierda eficacia de envío. Recuerde, cada sesión SMTP creada por MDaemon enviará los mensajes de manera consecutiva y así pues cuatro sesiones enviando dos mensajes cada una puede que ofrezcan mejor y más rápido rendimiento que ocho hilos de envío con sólo un mensaje cada uno. Un buen punto para empezar es de cinco a diez hilos cuando se use un módem de 56k y de veinte a treinta para banda ancha.

Máximo de sesiones simultáneas entrantes de SMTP
Este valor controla el número de sesiones SMTP entrantes concurrentes que el servidor acepta antes de empezar a responder con el mensaje "Servidor demasiado ocupado". El valor por defecto es 50.

Máximo de sesiones simultáneas entrantes MSA
Utilice esta opción para definir el número máximo permitido de sesiones concurrentes de un agente de envío de correo (Mail Submission Agent - MSA).

Cantidad máxima de mensajes salientes de SMTP colocados en la cola por sesión
Esta configuración establece un límite en el número de mensajes individuales que enviará cada sesión antes de empezar a enviar correo y liberar su memoria. Normalmente, debe tener este control puesto a cero, lo que causará que en cada sesión se envíen continuamente los mensajes hasta que la cola se quede vacía.

Colocar en caché los fallos de conexión SMTP durante estos minutos (0 = nunca)
Cuando una conexión SMTP de un host concreto provoca fallos, MDaemon dejará de intentar conectar a ese host durante el número de minutos especificados en esta opción. Esto puede prevenir que MDaemon esté inútilmente intentando conectarse a un host con problemas de conexión cuando, por ejemplo, tiene múltiples mensajes designados para dicho host y descubre que está caído cuando intenta el primer envío. La configuración por defecto es "5" minutos. Utilice "0" si no desea guardar en caché los fallos SMTP.

Máx. conexiones simultáneas por IP (0 = sin límite)
Este es el número máximo de conexiones simultáneas permitidas desde una IP antes de que sea bloqueada. Utilice "0" si no desea establecer un límite.

Máx. conexiones simultáneas hacia una misma IP (0 = sin límite)
Use esta opción para limitar el número de conexiones simultáneas permitidas a una sola dirección IP durante el envío de correo. Utilice "0" si no desea limitar las conexiones simultáneas.

Esta opción es útil para prevenir demasiadas conexiones a una o varias direcciones IP. Durante el envío, si un mensaje requiriera una conexión a una IP que excediera el límite de conexión, dicha conexión saltaría al siguiente host MX (o smart host). Si no existen hosts adicionales disponibles el mensaje se encolará para el siguiente ciclo de envío. Por defecto esta opción está deshabilitada, lo cual preserva el comportamiento existente.

...incluir IPs confiables
Por omisión, las conexiones a direcciones IPs confiables están exentas de la opción *Max conexiones simultáneas hacia una misma IP*. Marque esta casilla si desea habilitarla para IPs confiables también.

...incluir IPs reservadas
También por omisión, las conexiones a direcciones IP reservadas para uso de intranet están exentas de esta funcionalidad. Éstas son `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, y `172.16.0.0/12`. Marque esta casilla si desea habilitar esta opción para direcciones IP reservadas.

Utilice múltiples comandos RCPT al enviar correo
Por omisión MDaemon utiliza encolado inteligente, esto es, utilizará múltiples comandos RCPT en una sesión al enviar correo. Deshabilite esta opción si desea utilizar solo un comando RCPT por sesión.

Lista de Exentos
Este botón abre la Lista de Exentos de Encolado Inteligente. Cuando MDaemon envía mensajes a dominios en esta lista, NO utilizará el encolado inteligente, solo se utilizará un comando RCPT por sesión.

Intentar entregar a todos los registros A antes de pasar al siguiente host
Cuando ocurren errores o fallos de entrega, por omisión MDaemon intentará entregar a todos los registros A de un host MX antes de pasar al siguiente host MX. Deshabilite esta opción si desea que MDaemon pase al siguiente host MX inmediatamente luego de encontrar un error en lugar de intentar primero con todos los registros A.

POP3 & IMAP

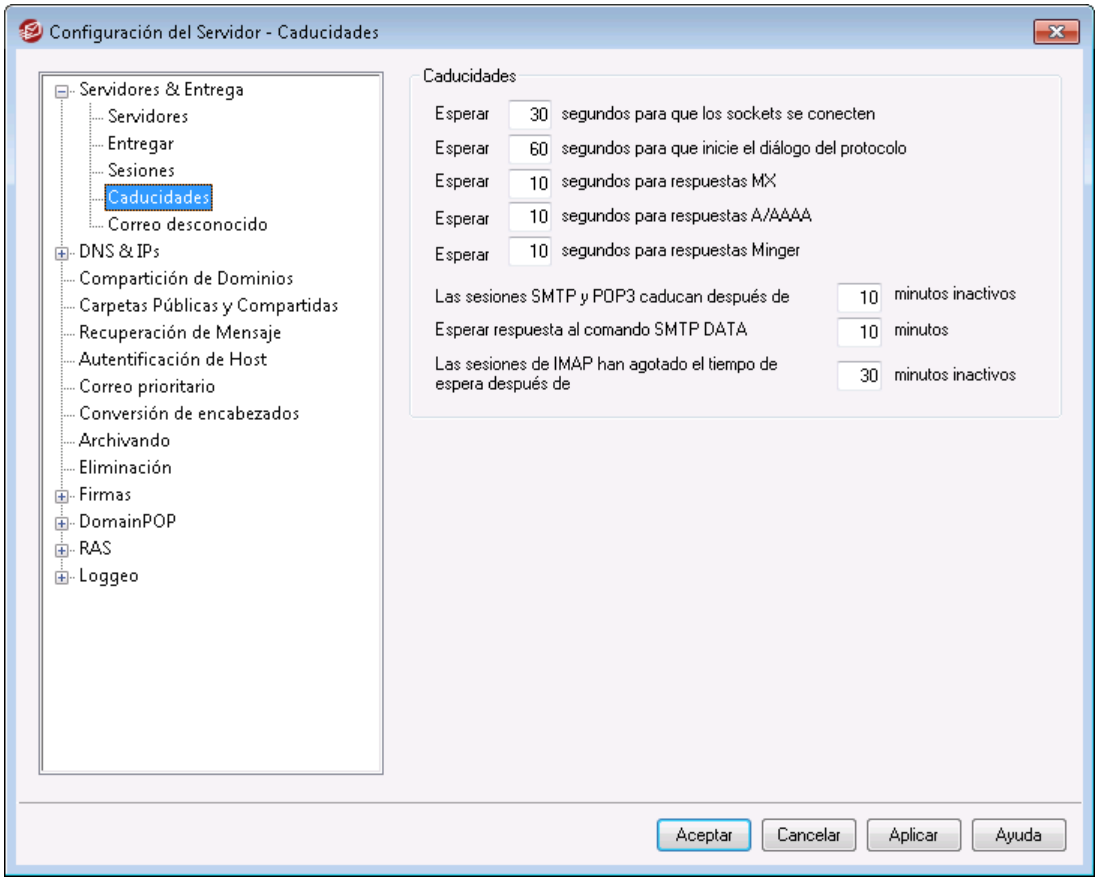
Máximas sesiones concurrentes salientes MultiPOP
El valor introducido aquí representa el máximo posible de sesiones POP salientes que se crearán cuando sea momento de recolectar correo MultiPOP. Cada sesión recolectará el correo hasta que los servidores MultiPOP hayan sido procesados, y todo el correo recolectado. Por ejemplo, si hay quince sesiones MultiPOP entre todos sus usuarios y el valor de esta configuración se establece en tres, cada sesión recolectará correo de cinco fuentes MultiPOP.

Debería experimentar con el número de sesiones para determinar qué número ofrecerá el mejor rendimiento para su ancho de banda. Es posible especificar tantas sesiones que el ancho de banda se sobrecargue, o su sistema Windows se quede sin recursos y se pierda eficiencia en los procesos. Recuerde que cada sesión POP creada por MDaemon recolectará correo hasta que todas las fuentes estén agotadas. Así pues, cuatro sesiones recolectando correo de 20 fuentes puede que rindan mejor y más rápido que veinte sesiones recolectando de una sola fuente.

Máximo de sesiones entrantes concurrentes de POP3
Este valor controla el número máximo de sesiones de correo entrantes POP que el servidor aceptará antes de empezar a responder con el mensaje "Servidor demasiado ocupado".

Máximo de sesiones simultáneas de IMAP
Este valor controla el número máximo de sesiones IMAP concurrentes que el servidor aceptará antes de empezar a responder "Servidor demasiado ocupado".

3.1.1.4 Caducidades



Caducidades

Esperar xx segs. para que los sockets se conecten
Después de iniciar una petición de conexión, MDaemon esperará estos segundos a que el sistema remoto acepte la conexión Si el sistema remoto no responde dentro de este espacio de tiempo, MDaemon enviará el mensaje a un *Host inteligente* especificado o lo colocará en el sistema de reintentos, dependiendo de qué opción se haya escogido en la pantalla Entrega 102 del Editor del Dominio por Defecto.

Esperar xx segs. para que el diálogo del protocolo inicie
Una vez la conexión se haya establecido con un host remoto, este es el número de segundos que MDaemon esperará a que el host remoto empiece un diálogo de protocolo SMTP o POP3. Si el host remoto no empieza la sesión de protocolo dentro de este tiempo, MDaemon enviará el mensaje al *Host inteligente* especificado o lo colocará en el sistema de reintentos, dependiendo de qué opción se haya escogido en la pantalla Entrega 102 del Editor de Dominio por Defecto.

Esperar XX segs. para obtener respuestas MX
Cuando se utilicen servicios de DNS para resolver hosts MX para dominios remotos, MDaemon esperará la respuesta a las consultas MX esta cantidad de segundos. Si el servidor DNS no responde dentro de este periodo de tiempo, MDaemon intentará enviar el mensaje a la dirección IP especificada en el registro A del servidor DNS. Si éste intento falla, MDaemon enviará el mensaje al *Host inteligente* especificado o lo colocará en el sistema de reintentos, dependiendo

de qué opción se haya escogido en la pantalla Entrega 102 del Editor de Dominio por Defecto.

Esperar XX segs. para obtener respuestas A/AAAA
Este temporizador gobierna cuánto tiempo MDaemon esperará mientras se intenta resolver la dirección IP remota del host. Si el intento falla, MDaemon enviará el mensaje al *Host inteligente* especificado o lo colocará en el sistema de reintentos, dependiendo de qué opción se haya escogido en la pantalla Entrega 102 del Editor de Dominio por Defecto.

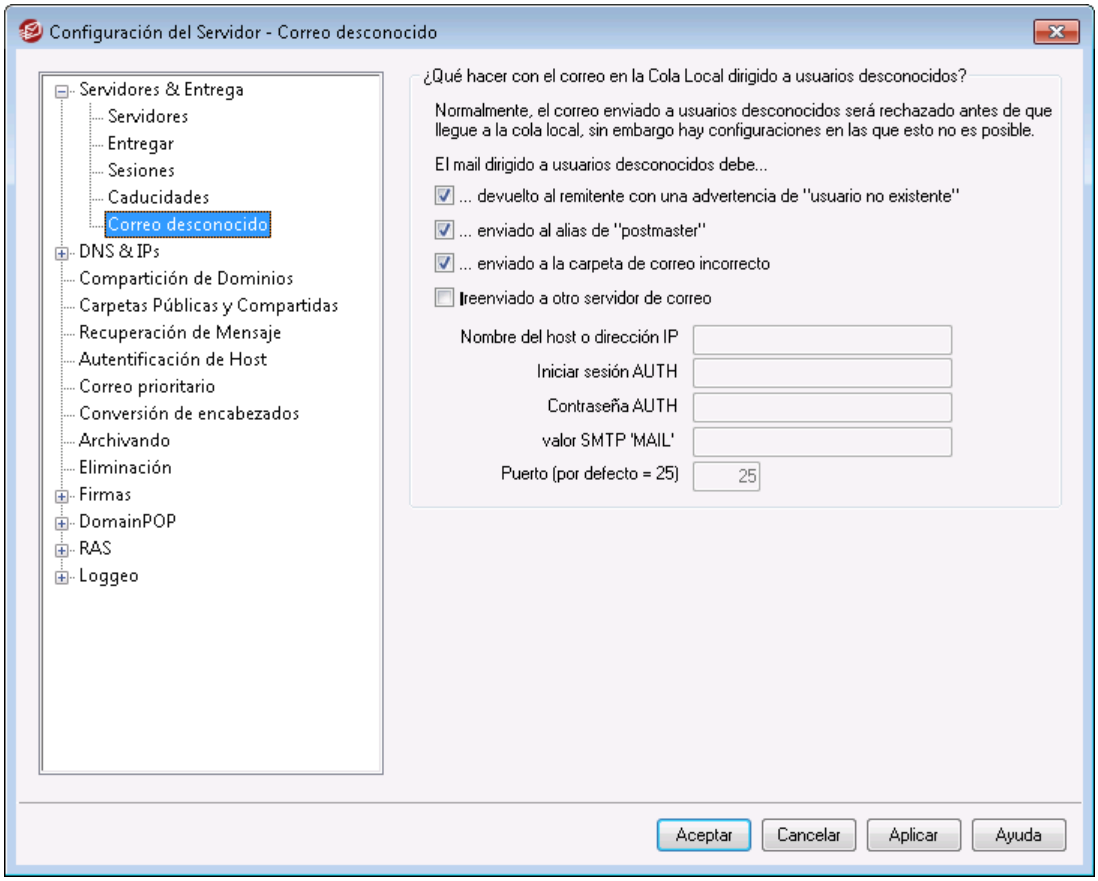
Esperar XX segs. para respuestas Minger
Este es la cantidad de segundos que MDaemon esperará para obtener una respuesta de un servidor Minger 863.

Las sesiones SMTP y POP3 caducan después de XX minutos inactivos
Si una sesión conectada correctamente permanece inactiva (sin entradas/salidas) durante este periodo de tiempo, MDaemon abortará la transacción. MDaemon volverá a intentarlo durante el siguiente intervalo de procesamiento.

Esperar la respuesta al comando SMTP DATA XX minutos
Esta opción gobierna cuánto tiempo MDaemon esperará para la respuesta "250 OK" después de enviar el comando DATA durante el proceso SMTP. Puesto que algunos servidores destinatarios ejecutan operaciones muy largas de antispam, antivirus u otras, esta opción se puede usar para darles tiempo a completar dichas tareas. El valor por defecto es 10 minutos.

Las sesiones IMAP agotan el tiempo de espera después de xx minutos inactivos
Si una sesión IMAP no tiene actividad durante este número de minutos, MDaemon cerrará la sesión.

3.1.1.5 Correo desconocido



Correo encolado para usuarios desconocidos debe ser...

...devuelto al remitente con una advertencia de "usuario no existente"
Cuando se activa esta opción, los mensajes que lleguen al servidor destinados para usuarios supuestamente locales pero desconocidos se devolverán al remitente del mensaje.

...enviado al alias de "Postmaster"
Por defecto, los mensajes que lleguen al servidor destinados a usuarios desconocidos, pero supuestamente locales serán reenviados al usuario al que se le haya asignado el alias de Postmaster. Deshabilite esta opción si no desea que los mensajes se envíen al Postmaster.

...enviado a la carpeta de correo erróneo
Por defecto, los mensajes que lleguen al servidor destinados para usuarios desconocidos, pero supuestamente locales serán enrutados a la cola de mensajes erróneos. Desactive esta casilla de verificación si no desea enviar dichos mensajes a la cola de mensajes erróneos.

...reenviado a otro servidor de correo
Utilice esta opción si desea reenviar mensajes a otro servidor de correo cuando vengan dirigidos a usuarios locales desconocidos.

Nombre de Host o IP
Especifique el nombre de host o dirección IP a la que desea reenviar los mensajes.

Lo siguiente aplica globalmente en cualquier lugar de MDaemon en el que se permita especificar en host para reenvío, copia o envío de correo. Si indica el host entre corchetes (p. ej. `[ejemplo.com]`), MDaemon se saltará las búsquedas de registros MX cuando envíe hacia dicho host. Por ejemplo, si esta opción contiene "`ejemplo.com`" entonces las búsquedas MX se efectuarán normalmente. Si, sin embargo, la opción contuviera "`[ejemplo.com]`" entonces sólo se ejecutará la búsqueda de Registros-A.

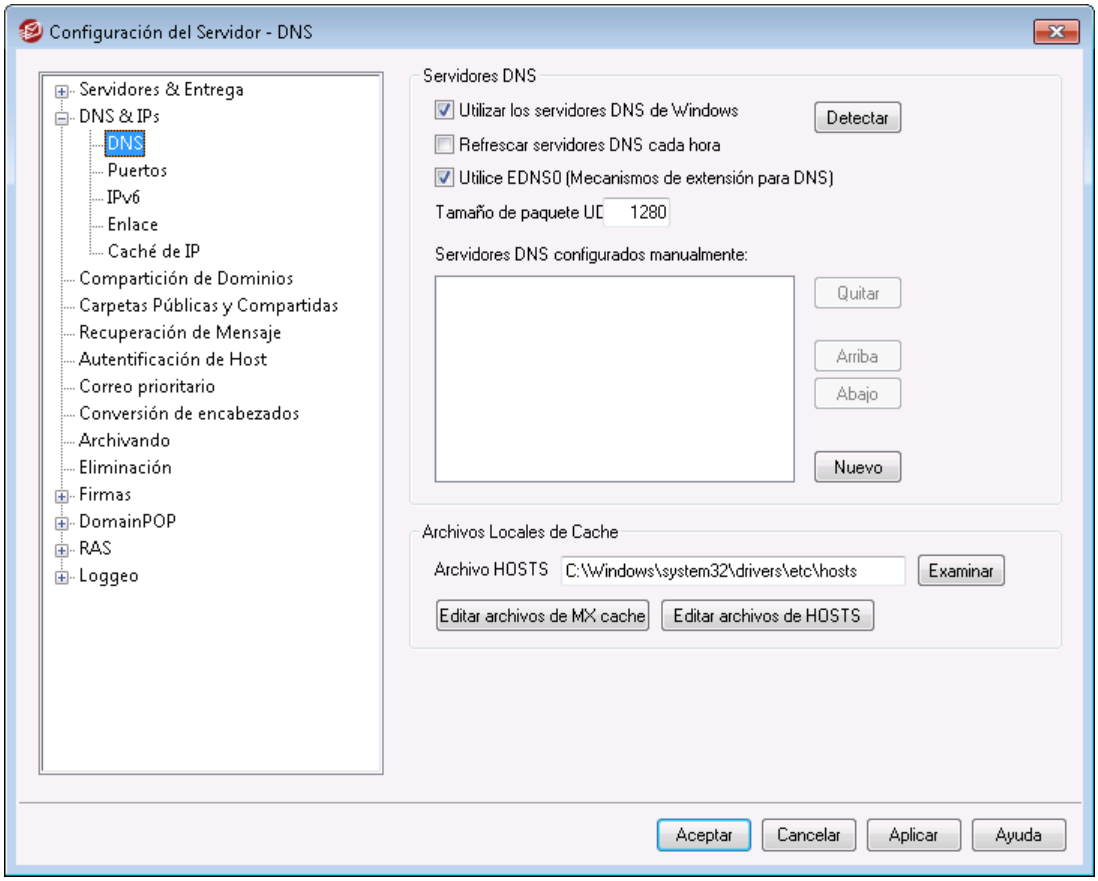
Inicio de sesión/contraseña AUTH
Registre las credenciales de inicio de sesión/contraseña que sean necesarias para el servidor de correo al que está reenviando los mensajes dirigidos a usuarios desconocidos.

Valor SMTP 'MAIL'
Esta dirección se usará en la declaración SMTP "`Mail From:`" que se usa durante la sesión de presentación con el host destino. Normalmente el remitente del mensaje se utiliza en esta porción del sobre SMTP. Si requiere un comando vacío (`MAIL FROM <>`) entonces introduzca "`[trash]`" en este control.

Puerto (por defecto = 25)
Este es el puerto TCP que MDaemon utiliza para enviar mensajes. El valor por omisión es el puerto 25.

3.1.2 DNS & IPs

3.1.2.1 DNS



Servidores DNS

Utilizar los servidores DNS de Windows
Cuando se selecciona esta opción, MDaemon utilizará los servidores DNS que encuentre en la configuración TCP/IP de Windows. MDaemon probará cada servidor DNS una vez por operación de búsqueda y en secuencia hasta que agote la lista de servidores DNS o encuentre el primero que responda. Si incluye servidores DNS adicionales en la opción *Servidores DNS configurados manualmente* abajo, MDaemon probará con esos servidores también. Finalmente, al arranque del sistema, la bitácora desplegará cada servidor DNS e indicará su origen (i.e. configurado manualmente o tomado de Windows).

Recargar el servidor DNS cada hora
Marque esta caja si desea recargar el servidor DNS cada hora. Está deshabilitada por omisión.

Utilizar EDNS0 (Mecanismos de Extensión para DNS)
Por omisión, MDaemon soporta Mecanismos de Extensión para DNS (ver RFC 2671). Deshabilite esta casilla si no desea que lo soporte.

Tamaño de paquete UDP
Esta opción controla el tamaño de paquete UDP. El valor por omisión es de 1280 bytes.

Servidores DNS configurados manualmente
MDaemon utilizará todos los servidores DNS especificados aquí al realizar búsquedas DNS (separe múltiples direcciones IP con un espacio). MDaemon

probará una vez y en secuencia cada servidor, por cada operación de búsqueda, hasta que agote la lista o encuentre el primero que le responda. Si habilita la opción *Utilizar los servidores DNS de Windows* de arriba, MDaemon también consultará todos los servidores DNS que encuentre en la configuración TCP/IP de Windows. Finalmente, al inicio del sistema, se registrarán en bitácora los servidores DNS a utilizar, así como su origen (i.e. configurados manualmente o tomados de Windows).

Archivos locales de Cache

Archivo HOSTS...
Antes de consultar a los servidores DNS, MDaemon primero intentará resolver la dirección procesando el archivo HOSTS de Windows. Si este archivo contiene la dirección IP del dominio en cuestión, MDaemon no necesitará consultar al servidor DNS.

Debe introducir la ruta completa y nombre de archivo y no solamente el nombre de archivo. MDaemon intentará utilizar la siguiente ubicación por defecto para este archivo:

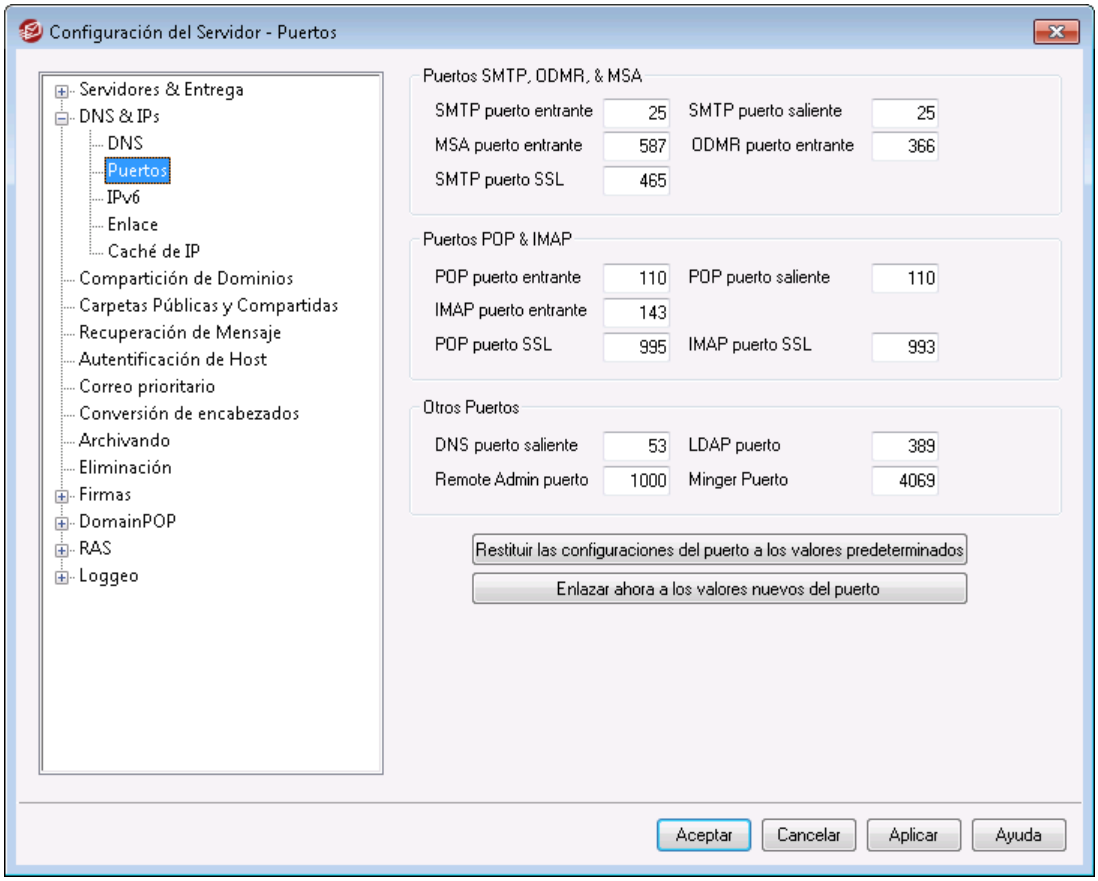
[unidad]:\windows\system32\drivers\etc\hosts

El archivo HOSTS es un archivo de Windows que contiene el registro A o la dirección de IP primaria para nombres de dominio. MDaemon también permite la especificación de registros MX y direcciones IP dentro de un archivo llamado MXCACHE.DAT. Este archivo se puede encontrar dentro del subdirectorio MDaemon\APP. Dé clic en **Editar archivo de caché MX** abajo y lea los comentarios en la sección superior para más información.

Editar archivo de caché MX
Haga clic en este botón para ver o editar el archivo MXCACHE.DAT.

Editar archivo HOSTS
Haga clic en este botón para ver o editar el archivo HOSTS.

3.1.2.2 Puertos



Puertos SMTP / ODMR / MSA

SMTP Puerto Entrante

MDaemon monitoreará este puerto TCP para conexiones entrantes de clientes SMTP. Este es el puerto SMTP principal, que en la mayoría de los casos debería dejarse configurado por defecto como el puerto 25.

SMTP Puerto Saliente

Este puerto se usará cuando el correo se envíe a otros servidores SMTP.

MSA Puerto Entrante

Este es el puerto del Agente de Envío de Mensajes (Message Submission Agent - MSA) que puede ser usado por los usuarios como alternativo al puerto *SMTP entrante* especificado anteriormente. La transmisión en este puerto requiere AUTH, así pues, los usuarios que envíen a dicho puerto deben configurar sus clientes de correo adecuadamente para asegurarse que sus conexiones son autenticadas. Además, dado que algunos ISP bloquean el puerto 25, sus usuarios remotos puede que resuelvan dicha restricción utilizando en su lugar el puerto MSA. Si no desea designar un puerto MSA puede establecerlo al valor "0" para desactivarlo.

Las conexiones al puerto MSA están exentas de búsquedas inversas y de PTR, monitorización de Host y de IP, Protección IP y Tarpitting. Las conexiones al puerto MSA continuarán utilizando limitación de conexiones de ataque de diccionario.

ODMR Puerto entrante
MDaemon monitoreará este puerto para las conexiones ODMR (On-Demand Mail Relay - Transmisión de Correo bajo demanda), tales como `ATRN` desde los Dominios de Puerta de Enlace.

Puerto SMTP SSL
Este es el puerto dedicado a las sesiones SMTP que utilicen conexiones Secure Sockets Layer (SSL). Ver SSL & Certificados 575 para más información.

Puertos POP/ IMAP

Puerto Entrante POP
MDaemon monitoreará este puerto para conexiones entrantes de clientes POP remotos.

Puerto Saliente POP
Este puerto se utilizará cuando MDaemon recoja correo de servidores POP.

Puerto entrante IMAP
MDaemon monitoreará este puerto para peticiones IMAP entrantes.

Puerto POP SSL
Este es el puerto dedicado a los clientes de correo POP que utilicen conexión Secure Sockets Layer (SSL). Ver SSL & Certificados 575 para más información.

Puerto IMAP SSL
Este es el puerto dedicado a los clientes IMAP de correo que utilicen conexión Secure Sockets Layer (SSL). Ver SSL & Certificados 575 para más información.

Otros puertos

Puerto saliente DNS
Introduzca el puerto que quiere que MDaemon utilice para enviar y recibir datagramas al servidor DNS.

Puerto LDAP
MDaemon publicará la información de libreta de direcciones y bases de datos en el servidor LDAP a través de este puerto.

Ver: Soporte a Libreta de Direcciones LDAP 831

Puerto de Administración Remota
Este es el puerto que MDaemon monitoreará para las conexiones de la Administración Remota 354.

Puerto Minger
Este es el puerto que el servidor Minger 863 monitoreará para conexiones.

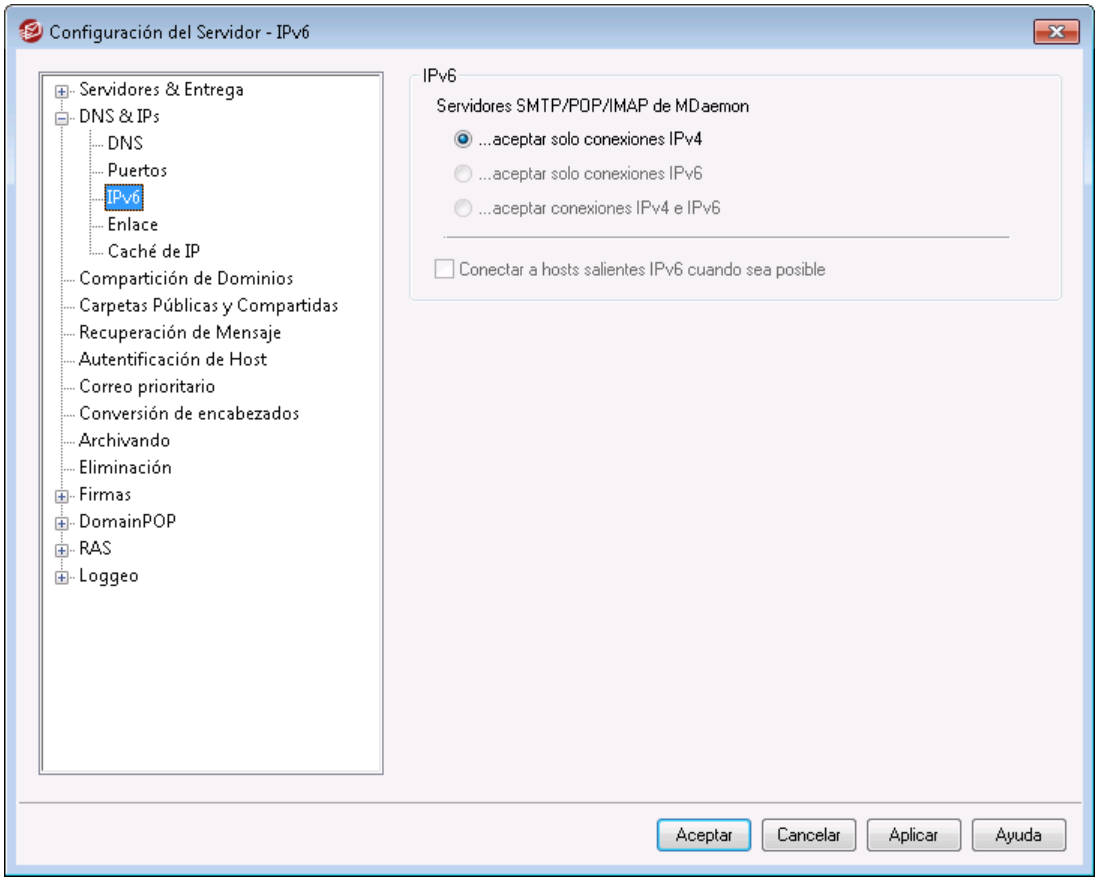
Restituir las configuraciones del puerto a los valores predeterminados
Este botón restablece todas las configuraciones de puerto a sus valores estándar.

Enlazar ahora a los valores nuevos del puerto
Cuando se alteran los valores de cualquiera de las configuraciones de puertos necesitará pulsar este botón para que los cambios sean inmediatos. Si no, los cambios no se aplicarán hasta la siguiente vez que el servidor sea iniciado.

Las configuraciones de puerto anteriores son críticas para la correcta operatividad del servidor y no deben ser alteradas a menos que se esté seguro de que debe hacerse. Poder cambiar los puertos que utiliza MDaemon permite configurar el servidor para que opere con sistemas proxy u otros servicios de software que requieren algunos puertos concretos.

Una dirección IP (una máquina) sólo dispone de un puerto disponible de cada. Si un programa intenta acceder a un puerto que está siendo utilizado por otro programa, un mensaje de error le informará que la dirección solicitada ya se encuentra en uso (IP: PUERTO).

3.1.2.3 IPv6



Por omisión MDaemon detecta el nivel de capacidad IPv6 que soporta su sistema operativo y hace un stack dual cuando es posible. De otra manera, MDaemon monitorea IPv4 e IPv6 de manera independiente.

IPv6

Servidores SMTP/POP3/IMAP de MDaemon ...

...aceptar solo conexiones IPv4
Elija esta opción si solo desea aceptar conexiones IPv4.

...aceptar solo conexiones IPv6
Elija esta opción si solo desea aceptar conexiones IPv6.

...aceptar conexiones IPv4 o IPv6
Elija esta opción si desea aceptar conexiones IPv6 e Ipv6. Este es el ajuste por omisión y MDaemon le dará precedencia a conexiones IPv6 sobre IPv4 siempre que sea posible.

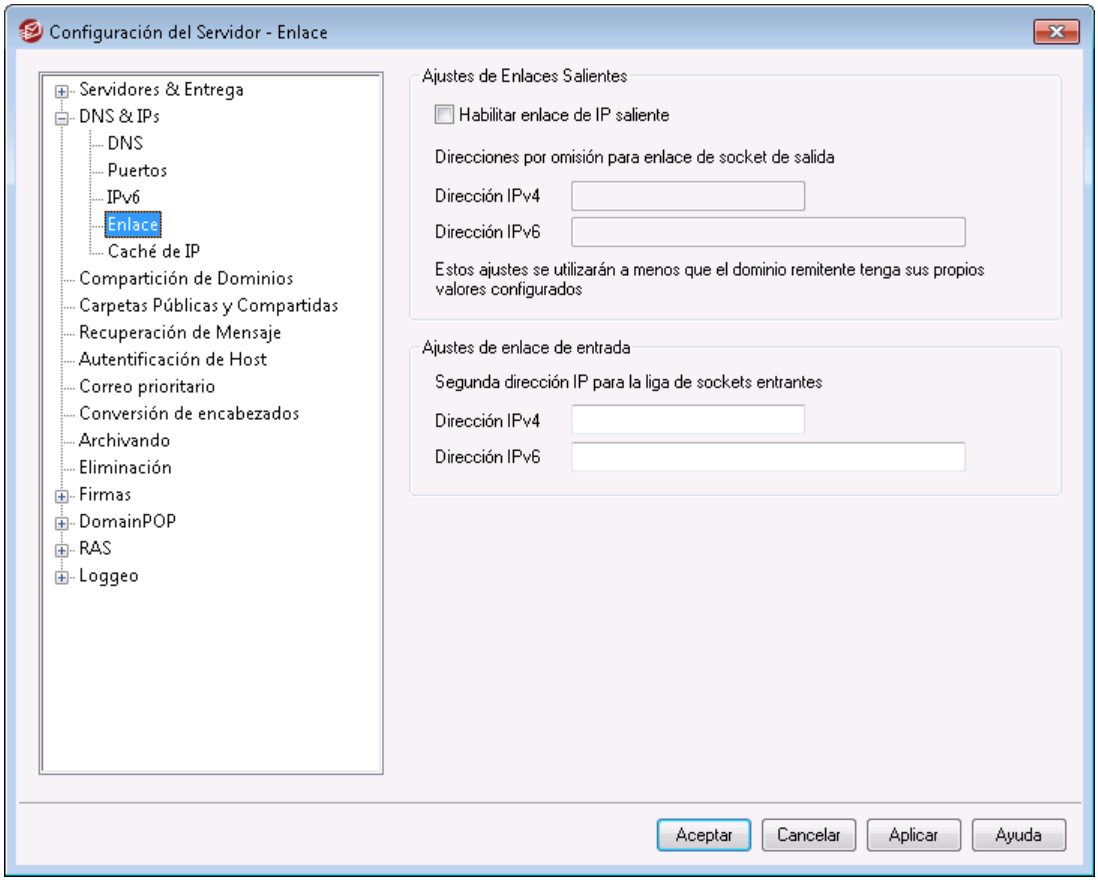
Conectarse a servidores salientes IPv6 siempre que sea posible
Habilite esta opción si desea que MDaemon se conecte a hosts salientes IPv6 siempre que sea posible.

Cuando MDaemon se conecta a un servidor IPv6, debe utilizar una dirección local IPv6 propia. La dirección IPv6 se define en la pantalla Administrador de Dominios » Nombre de Host & IP 192. Si es necesario, se puede especificar una dirección para enlace del socket saliente en la pantalla Enlace 120.

Ver:

Enlace 120
Administrador de Dominios » Nombre de Host & IP 192

3.1.2.4 Enlace



Ajustes de Enlace Saliente

Habilitar enlace de IP saliente
Cuando se habilita esta opción, MDaemon siempre liga los sockets salientes. Para dominios que tienen habilitada la opción *Teste dominio reconoce solo conexiones hechas a estas IPs* 192 en la pantalla Nombre d & IP de Servidor 192, MDaemon utiliza la IP configurada para el dominio. De otra forma utiliza el valor especificado abajo en *Dirección(es) por omisión para enlace de sockets salientes.*

Dirección(es) por omisión para enlace de sockets salientes: direcciones IPv4/IPv6
Estas son las direcciones IP que serán utilizadas para enlace de sockets salientes para dominios que no están enlazados a una dirección IP específica en la pantalla Nombre &IP del Host 192 del Administrador de Dominios.

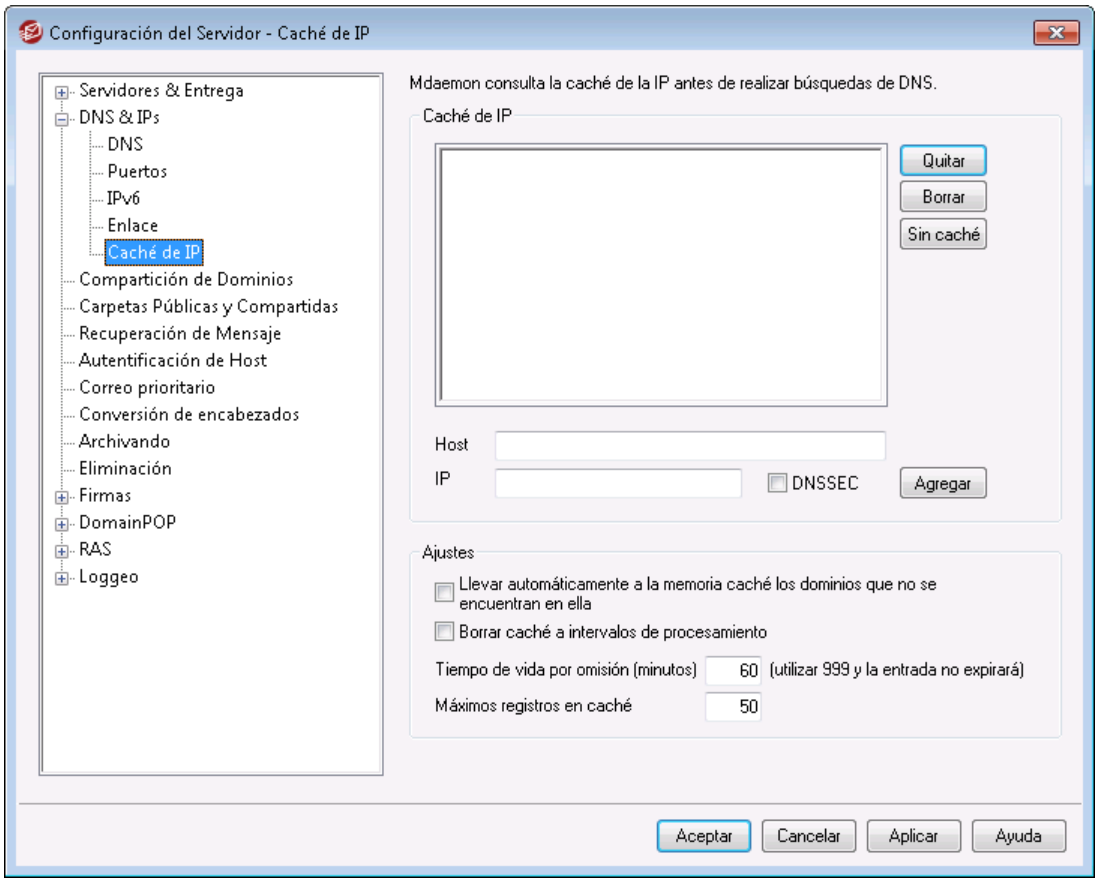
Ajuste de Enlaces Entrantes

Segunda dirección IP para enlace de sockets entrantes: direcciones IPv4/IPv6
Utilice esta opción si desea designar un segundo conjunto de direcciones IP para el enlace de sockets entrantes 192.

Ver:

Administrador de Dominios » Nombre & IP del Host 192
IPv6 119

3.1.2.5 Caché de IP



Para poder acelerar el envío de mensajes y acortar el tiempo de proceso del correo, MDaemon guarda en caché las direcciones IP de todos los hosts con los que establece contacto. Estas IPs se guardan y la caché se comprueba cada vez que MDaemon requiere una resolución de DNS en un nombre de dominio. Si el nombre de dominio que necesita resolución se encuentra en la caché IP, entonces se salta el proceso de búsqueda DNS, lo cual puede ahorrar una cantidad increíble de tiempo de proceso. Las configuraciones en esta ventana permiten manipular los parámetros bajo los cuales operará la caché. También puede añadir y quitar entradas manualmente, definir si se utilizará DNSSEC, establecer el tamaño máximo de la

caché y designar cuánto tiempo se mantienen las entradas en caché. La Caché de IP puede accederse a través de la selección de menú "Configurar » Configuración de Servidor » Caché de IP".

Caché de IP

Host
Introduzca el nombre del host que desea añadir al Caché de IP.

IP
Introduzca la dirección IP que desea añadir a la Caché de IP.

DNSSEC
Marque esta casilla para DNSSEC.

Agregar
Una vez haya agregado manualmente un host o dirección IP, haga clic en este botón para agregarlo a la caché.

Quitar
Si desea eliminar una dirección IP en caché de la lista, seleccione la entrada y luego haga clic en este botón.

Borrar
Este botón borrará todas las entradas en la caché.

Sin caché
Haga clic en este botón para establecer una lista de nombres de dominio/direcciones IP que no quiere que nunca se añadan a la Caché de IP.

Ajustes

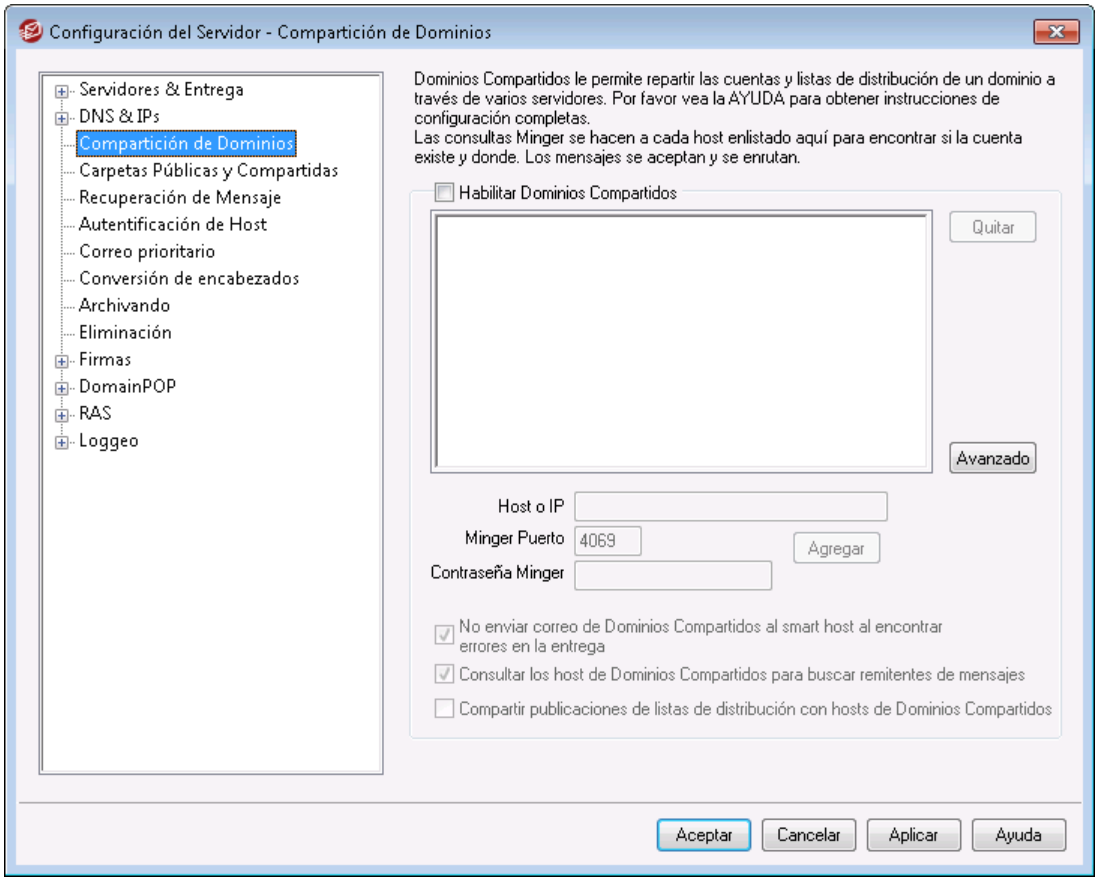
Llevar automáticamente a la memoria caché los dominios que no se encuentren en ella
Esta opción gobierna el motor interno de auto caché. Si quiere que MDaemon guarde en caché dominios de manera automática entonces active esta opción. Si quiere construir usted mismo una Caché de IP, entonces desactive esta casilla.

Borrar caché a intervalos de procesamiento
Si se selecciona, todos los contenidos de la caché se borrarán al inicio de cada sesión de correo. Eso permite a la caché refrescarse a cada intervalo de procesamiento de correo.

Tiempo de vida predeterminado (minutos)
Este es el valor por defecto en minutos que una entrada permanecerá en la Caché de IP. Una vez cada entrada haya estado en la Caché de IP durante este número de minutos, MDaemon la borrará. Si desea establecer una entrada permanente en la Caché de IP entonces establezca el *Tiempo predeterminado de vida* en 9999.

Cantidad máxima de entradas en caché
Este valor determinar cuán grande puede ser la caché. Cuando se alcance este número, la siguiente entrada de caché desplazará de la primera entrada.

3.1.3 Dominios Compartidos



La funcionalidad de Dominios Compartidos permite separar usuarios de un mismo dominio entre múltiples servidores. Ello hace posible tener servidores MDaemon ejecutándose en diferentes ubicaciones, todos utilizando los mismos nombres de dominio, pero diferentes cuentas de usuario. Una porción de las cuentas de usuario de su dominio se almacenarán en un servidor mientras que otra porción de ellas serán almacenadas en uno o más servidores adicionales. El diálogo de Dominios Compartidos se utiliza para especificar donde se ubica cada uno de esos servidores. Luego, cuando un mensaje entrante llega para un usuario local que no tiene un buzón local, la funcionalidad de Dominios Compartidos utilizará Minger para consultar a los otros servidores y poder descubrir si el usuario tiene o no una cuenta local en alguno de ellos. Si la dirección resulta ser válida, MDaemon aceptará el mensaje y lo enrutará al servidor donde se ubique la cuenta.

Por ejemplo, puede tener oficinas en múltiples ciudades y escoger utilizar Dominios Compartidos para permitir que cada empleado tenga una dirección terminada en "`@ejemplo.com`." Cada MDaemon de cada oficina almacenará una porción del correo de `ejemplo.com`, teniendo cuentas solamente para los usuarios locales que trabajan en cada oficina. Entonces, cada oficina será configurada para utilizar Dominios

Compartidos, para que todos los mensajes de cualquier empleado sean enrutados correctamente a la oficina correspondiente.

Dado que Dominios Compartidos utiliza Minger 863 para verificar las direcciones, Minger debe estar activado y debidamente configurado para cada servidor para poder utilizar la función de consultas. Si, aun así, ocurriera un error durante la consulta Minger, tal como que uno de los servidores estuviera temporalmente no disponible, MDaemon responderá con un código de error temporal "451" para que el servidor remitente intente enviar el mensaje nuevamente más tarde. Además, una vez que la dirección haya sido verificada, será guardada en caché durante cinco días para que MDaemon pueda inmediatamente aceptar futuros mensajes para esa dirección y pueda intentar el enrutado de los mensajes al host correcto.

Finalmente, para evitar problemas potenciales que podrían ocurrir si la misma cuenta fuera creada en múltiples servidores, MDaemon consultará todos los Servidores en Dominios Compartidos antes de crear cuentas nuevas.

Existe una opción llamada "*Las búsquedas de verificación Minger también provocan búsquedas en Dominios Compartidos*," ubicada en la pantalla Ajustes 273 del editor de Puerta de Enlace. Esta opción se puede usar para hacer que MDaemon también verifique los hosts de Dominios Compartidos siempre que la Verificación Minger 264 sea usada por una Puerta de Enlace.

Habilitar Dominios Compartidos
Haga clic en esta casilla de verificación para activar los Dominios Compartidos. Después de que se haya activado esta funcionalidad y añadido todos los hosts o direcciones IP de Dominios Compartidos a la lista, asegúrese que también ha habilitado y configurado Minger 863 para que pueda responder a las consultas de dichos hosts cuando intenten verificar direcciones locales.

Eliminar
Para eliminar una de las entradas de Dominios Compartidos, seleccione de la lista y haga clic en este botón.

Avanzado
Este botón abre un archivo donde puede configurar nombres de dominios a los que se les permite utilizar Dominios Compartidos. Cuando el archivo está vacío (la condición por omisión) entonces todos sus dominios pueden utilizar Dominios Compartidos. Vea las instrucciones en la parte superior del archivo para más información.

Host o IP
Utilice este cuadro para introducir el host o dirección IP que comparte uno o más de sus dominios. Puede agregar dos puntos y el puerto (i.e. correo.ejemplo.com:2525) si desea utilizar un puerto específico distinto al predeterminado, al enviar mensajes SMTP al servidor (este no es el mismo que el puerto Minger que se describe en el punto siguiente).

Puerto Minger
Este es el puerto que Minger utilizará cuando se consulte a este host. El puerto por defecto es 4069.

Contraseña Minger (opcional)
Si el host que está añadiendo requiere contraseña de Minger, introdúzcala aquí. Configurar Minger para que requiera contraseña es opcional, pero recomendable.

Agregar
Después de introducir el host o IP, puerto, y contraseña, haga clic en este botón para añadir la nueva entrada de Dominios Compartidos a la lista.

No enviar correo de Dominios Compartidos al host inteligente cuando ocurren errores en la entrega
Cuando se habilita esta opción, si MDaemon encuentra un error al intentar entregar correo de Dominios Compartidos (por ejemplo cuando alguno de los servidores que comparten el dominio está fuera de línea), el mensaje se mantendrá en la cola 872 en lugar de ser enviado al host inteligente 102. Si se envían estos correos al host inteligente, es posible que se ciclen los correos. Esta opción está habilitada por omisión.

Consultar los Hosts de Dominios Compartidos para verificar remitentes de mensajes
Por omisión, MDaemon aceptará correo de cuentas que existen en otros host de Dominios Compartidos. Si no desea que se ejecuten consultas del remitente en SMTP MAIL en Dominios Compartidos, deshabilite esta opción.

Compartir posteos de listas de distribución con hosts de Dominios Compartidos
Habilite esta opción s desea compartir listas de distribución con hosts de Dominios Compartidos. Cuando llega un mensaje para una lista de distribución, se crea una copia para cada host de Dominios Compartidos que también mantiene una versión de esa lista (se hace una consulta para verificar). Cuando estos hosts reciben sus copias, entregarán el mensaje a todos los miembros de la lista que hospedan. De esta manera, las listas de distribución se pueden dividir entre varios servidores sin perder funcionalidad. Para que esto funcione, cada host de Dominios Compartidos debe incluir las IPs de los otros hosts en su configuración de IPs Confiables 520. De otra manera los mensajes para la lista serán rechazados con el error 'El Remitente no es miembro de la lista'.

Ver:

Minger 863
Administrador de Dominios 190

3.1.4 Carpetas Públicas y Compartidas

MDaemon soporta carpetas Públicas e IMAP de Usuario. Las carpetas Públicas (que se manejan desde el Administrador de Carpetas Públicas 314) son carpetas adicionales que no pertenecen a ninguna cuenta en concreto pero que pueden ponerse disponibles para múltiples usuarios IMAP. Las carpetas de usuario son carpetas IMAP que pertenecen a cuentas de MDaemon individuales. Cada carpeta compartida, bien sea pública o de usuario, debe tener una lista de usuarios de MDaemon asociada a ella, y sólo los miembros de dicha lista de acceso podrán acceder a ella vía MDaemon Webmail o un cliente de correo IMAP.

Cuando los usuarios IMAP acceden a su lista de carpetas personales, podrán ver las carpetas públicas y las carpetas compartidas a las cuales se les ha dado acceso. De esta manera algunas carpetas de correo pueden compartirse con múltiples usuarios, pero pueden seguir requiriendo a cada usuario las credenciales de inicio de sesión. Además, tener acceso a una carpeta no significa necesariamente tener permisos completos de lectura/escritura o acceso administrativo a ella. Pueden asignarse derechos de acceso específicos a usuarios individuales, así pues, permitiendo establecer diferentes niveles de acceso para cada uno. Por ejemplo, puede permitir que algunos usuarios borren mensajes mientras restringe a otros de hacerlo.

Una vez creada una carpeta pública o de usuario IMAP puede utilizar el Filtro de Contenido para definir criterios con los cuales algunos mensajes se muevan a dicha carpeta. Por ejemplo, puede ser útil hacer una regla de filtro que haga que los mensajes que contengan `soporte@ejemplo.com` en el encabezado `TO:` se muevan a la carpeta pública `Soporte`. Las Acciones del Filtro de Contenido 648 "`Move Message to Public Folders...`" y "`Copy Message to Folder...`" lo hacen posible. Para carpetas de usuario compartidas, puede usar los filtros de IMAP personales 737 para enrutar mensajes específicos a ellas. Además de utilizar los filtros IMAP y el Filtro de Contenido, puede asociar una carpeta compartida con una cuenta específica para que los mensajes destinados a dicha "Cuenta de Envío" sean automáticamente enrutados a la carpeta compartida. Aun así, sólo los usuarios que tengan concedidos permisos de publicación en la carpeta podrán enviar a dicha dirección.

Para mayor comodidad, el editor de Listas de Distribución también contiene una pantalla de Carpetas Públicas 304 que hace posible que se configure una carpeta pública para una lista particular. Si activa dicha funcionalidad entonces una copia de cada mensaje de lista se colocará en la carpeta pública especificada. Todas las carpetas públicas se almacenan en el directorio `\Public Folders\` dentro de la jerarquía de directorios de MDaemon.

Carpetas de Documentos de Webmail

Los temas de Webmail permiten compartir documentos utilizando carpetas de documentos. Estas carpetas de documentos soportan Listas de Control de Acceso (ACL) 316 como el resto de carpetas compartidas, que pueden utilizarse para definir permisos y cualquier tipo de archivo se puede compartir a través de este sistema. Los usuarios de Webmail pueden subir archivos a sus carpetas de documentos utilizando las herramientas integradas. Si se utiliza el tema LookOut, los navegadores que soportan la funcionalidad la API de Arrastrar & Pegar de HTML5, tales como Chrome y Firefox, también pueden subir archivos arrastrándolos desde el escritorio hacia la ventana del navegador. Se pueden hacer búsquedas por nombre de archivo y éstos se pueden renombrar, así mismo se pueden adjuntar archivos a mensajes nuevos al momento de redactarlos.

Se puede habilitar/deshabilitar las carpetas de documentos (y otras carpetas compartidas) en base a dominio o usuario editando el archivo `\WorldClient\Domains.ini` y los archivos individuales `\Users\..\WC\user.ini` respectivamente. Es posible configurar ambos valores por omisión y configuraciones personalizadas que tendrán prioridad sobre los valores por omisión. Por ejemplo:

```
[Default:UserDefaults]
DocumentsFolderName=Documents
EnableDocuments=Yes

[example.com:UserDefaults]
DocumentsFolderName=Example Documents
EnableDocuments=Yes
```

```
[superControllingDomain.gov:UserDefaults]
EnableDocuments=No
EnableCalendar=No
EnableNotes=No
EnableTasks=No
```

Configurar un Tamaño Máximo de Archivo

Puede limitar el tamaño de los archivos individuales que se pueden cargar a las carpetas de documentos, agregando esta llave en el archivo `domains.ini`: `MaxAttachmentSize=<valor en KB>` El valor por omisión es `0`, lo que significa que no hay límite.

Bloquear o permitir Tipos de Archivo

Para impedir que se carguen ciertos tipos de archivo a la carpeta de documentos, agregue la llave `BlockFileTypes=` al archivo `domains.ini`, enlistando los tipos de archivo que desee bloquear, separados por espacio o coma. Por ejemplo, "`BlockFileTypes=exe dll js`".

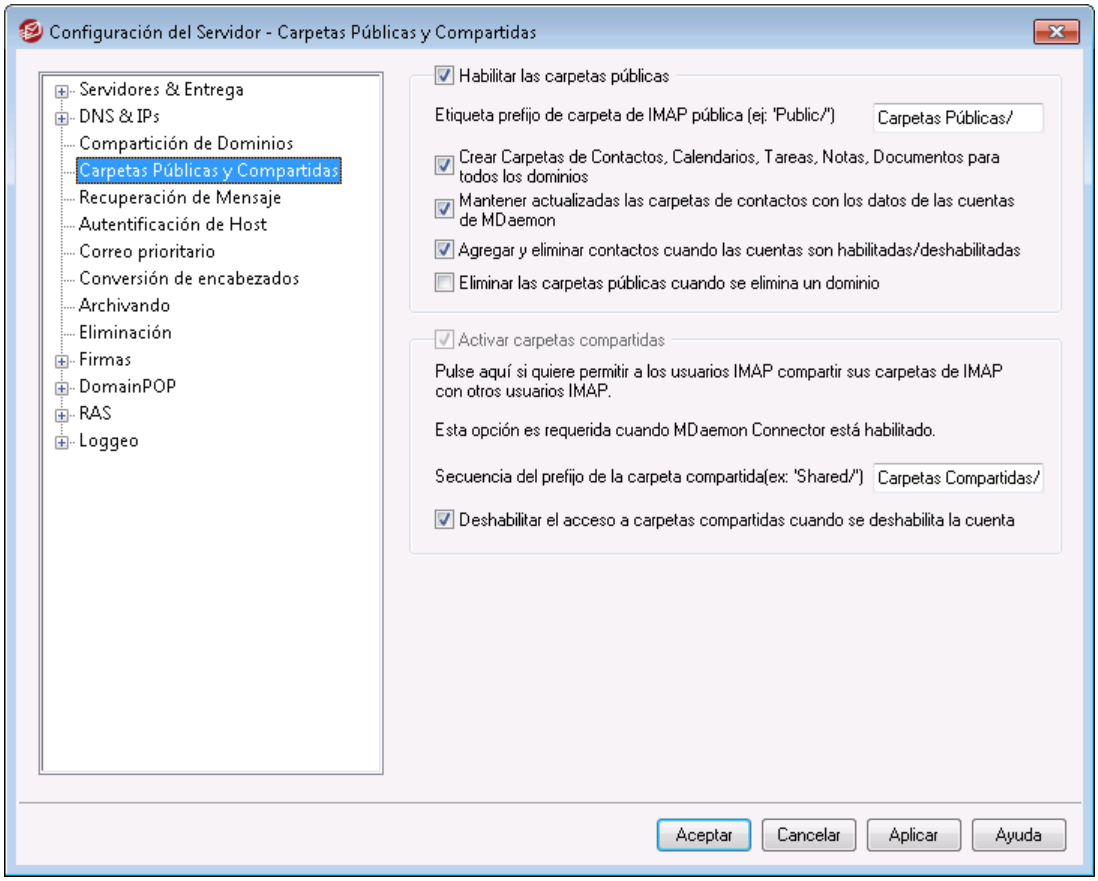
Para permitir que solo se carguen ciertos tipos de archivo a la carpeta de documentos, agregue la llave `AllowFileTypes=` al archivo `domains.ini`, enlistando los tipos de archivo que desea permitir, separados por espacio o coma. Por ejemplo, "`AllowFileTypes=jpg png doc docx xls xlsx`".

Cuando se utilizan ambas llaves, se da prioridad a los archivos bloqueados, cuando exista conflicto; si una extensión se encuentra en ambas listas, será bloqueada. Si se utiliza una llave sin valor (ej.: sin lista de extensiones), entonces esa llave no será utilizada. Las extensiones de archivo incluyen un "." (ej.: .exe .dll), Pero no es requerido.

Ver:

Carpetas Públicas y Compartidas 128
Administrador de Carpetas Públicas 314
Lista de Control de Acceso 316
Editor de Cuentas » Carpetas Compartidas 743
Listas de Distribución » Carpetas Públicas 304

3.1.4.1 Carpetas Públicas y Compartidas



Para tener acceso a la pantalla de Carpetas Públicas y Compartidas, haga clic en "Configurar » Configuración de Servidor » Carpetas Públicas y Compartidas".

Habilitar Carpetas Públicas

Haga clic en esta casilla si desea permitir que los usuarios tengan acceso a las carpetas públicas. Los usuarios que pueden acceder a ellas y el nivel de acceso para cada carpeta se establecen en la pantalla Administrador de Carpetas Públicas 314. Desactive esta casilla si desea esconder las carpetas públicas de todos los usuarios.

Etiqueta prefijo de carpeta IMAP pública (ej.: 'Public/')
Las carpetas Públicas se prefijan con una secuencia de hasta 20 caracteres, tales como "#" o "Carpetas Publicas/". Ello ayuda a los usuarios a distinguir las carpetas públicas de las privadas dentro de su cliente de correo. Utilice este cuadro para especificar los caracteres que desea que se usen para denotar las carpetas públicas.

Crear Carpetas de Contactos, Calendario, Tareas, Diario y Notas para todos los dominios
Haga clic en esta casilla de verificación si desea asegurarse que estas carpetas existen para todos los dominios. Siempre que un Dominio 190 se añade a MDaemon, estas carpetas se crearán.

Mantener actualizada la carpeta de contactos con los datos de las cuentas de MDaemon
Si se habilita esta opción, MDaemon mantendrá sincronizada la información de cuentas con su lista de contactos.

Agregar y eliminar contactos cuando las cuentas se habilitan/deshabilitan
Por omisión, cuando deshabilita una cuenta, esta será eliminada de la carpeta pública de contactos del dominio. Entonces, si rehabilita la cuenta, será agregada de nuevo a los contactos. Esta opción se habilita por omisión para impedir que las cuentas deshabilitadas se muestren en el sistema de autocompletar de Webmail.

Eliminar las Carpetas Públicas del Dominio cuando éste se elimina.
Dé clic en esta casilla si desea eliminar las carpetas públicas del dominio cuando el dominio mismo es eliminado.

Habilitar Carpetas Compartidas

Haga clic en esta casilla si desea permitir a los usuarios IMAP tener acceso a sus carpetas IMAP. Los usuarios que puedan tener acceso a ellas y el nivel de acceso asignado para cada carpeta se definen en la pantalla Carpetas Compartidas 743 en el Editor de Cuentas. (Cuentas » Gestión de Cuentas » [Cuenta de Usuario] » Carpetas Compartidas). Desactive esta casilla de verificación para evitar que los usuarios puedan compartir el acceso a sus carpetas, y evitar que la antes mencionada pantalla de Carpetas Compartidas aparezca en el Editor de Cuentas.

Cuando se utilice Outlook Connector para MDaemon, esta opción no estará disponible. No será posible desactivarla porque la funcionalidad de carpetas compartidas se requiere para que Outlook Connector funcione adecuadamente.

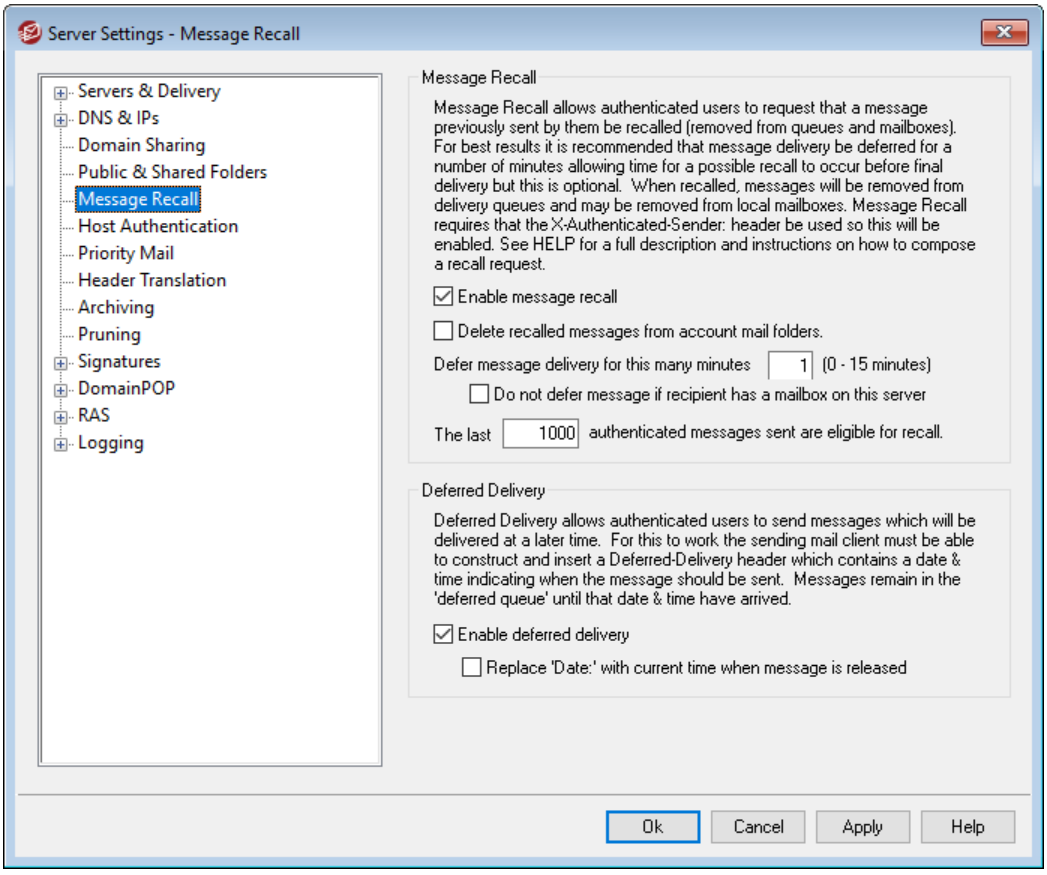
Secuencia del prefijo de la carpeta compartida (ej.: 'Shared/')
Las carpetas compartidas de usuario se marcan en una secuencia de hasta 20 caracteres, tales como "`Carpetas Compartidas/`". Esto es para ayudar a los usuarios a distinguir fácilmente las carpetas compartidas de las carpetas privadas dentro de su cliente de correo. Use este cuadro de texto para especificar la serie de caracteres que desea que se use para marcar las carpetas compartidas de usuario.

Deshabilitar acceso a carpetas compartidas cuando la cuenta está deshabilitada
Por omisión, los servidores IMAP, Webmail y ActiveSync de MDaemon no permiten acceso a las carpetas compartidas para las cuentas deshabilitadas. Deshabilite esta casilla si desea permitir el acceso a las carpetas compartidas de las cuentas aun cuando la cuenta está deshabilitada.

Ver:

Descripción General de Carpetas Públicas 125
Administración de Carpetas Públicas 314
Lista de Control de Acceso 316
Editor de Cuentas » Carpetas Compartidas 743
Listas de Distribución » Carpetas Compartidas 304

3.1.5 Recuperación de Mensajes



Sistema de Recuperación de Mensajes

MDaemon cuenta con un sistema de recuperación de mensajes que puede utilizar para retrasar mensajes entrantes enviados a usuarios locales autentificados durante 0 a 15 minutos, lo cual da a los usuarios un breve periodo de tiempo durante el cual pueden intentar detener la entrega de un mensaje. Durante el periodo de retraso los mensajes se colocan en una cola dedicada para esto (Cola de Diferidos) en lugar de ir directamente a la cola de mensajes Entrantes—los mensajes en la Cola de Diferidos tienen la fecha en que deben enviarse codificada en el nombre del archivo. MDaemon verifica la cola una vez por minuto y cuando es momento de que el

mensaje deje la cola, lo mueve a la cola Entrante y es sujeto al procesamiento y entrega normales. La actividad se registra en la pestaña de Enrutamiento y en el archivo de registro.

Puede configurar el tiempo de retraso a "0" si lo desea, pero esto incrementa la posibilidad de que el mensaje que un usuario desea recuperar ya haya sido enviado. Por esto, se recomienda un retraso de 1 o 2 minutos para dar tiempo a sus usuarios de darse cuenta de que quieren recuperar un mensaje, enviar la petición de recuperación y contar con tiempo para que MDaemon procese la petición. Sin embargo, dado que MDaemon puede eliminar de la(s) cola(s) Remota(s) los mensajes recuperados, donde puede haber algún retraso, algunos administradores pueden encontrar innecesario este temporizador de diferimiento de la entrega.

Recuperación de un Mensaje

Hay varias maneras en las que los usuarios pueden recuperar un mensaje.

1. En MDaemon Webmail, dé clic en el botón de Recuperación que se despliega al visualizar un mensaje enviado recientemente en la carpeta de Enviados. Si se da clic antes de que expire el límite de tiempo de recuperación, Webmail enviará un mensaje RECALL a MDaemon.
2. Enviar un mensaje a la cuenta de sistema mdaemon@example.com, con la palabra "RECALL" (sin comillas) como Asunto del mensaje. Esto recuperará el último mensaje que haya enviado. Solo recuperará el último mensaje.
3. En la carpeta de Enviados, localice el mensaje que desea recuperar, elija la opción "Reenviar como Adjunto" y envíe el mensaje a la cuenta del sistema mdaemon@example.com, utilizando "RECALL" como Asunto del sistema.
4. Visualice los encabezados del mensaje, copie el encabezado "Message-ID: <message-ID value>" y genere un mensaje nuevo con el asunto "RECALL Message-ID: <message-ID value>" (sin comillas).

Sin importar el método de recuperación seleccionado, MDaemon enviará el mensaje de regreso al usuario, diciendo si la recuperación fue exitosa o no. Cuando un mensaje se recupera exitosamente, MDaemon, lo elimina de la cola como si nunca hubiera sido enviado. Opcionalmente, si está habilitada la opción *Eliminar mensajes recuperados de las carpetas de correo de la cuenta*, MDaemon también intentará eliminar el mensaje recuperado de la carpeta local del usuario ha donde haya sido entregado. Los mensajes enviados a múltiples destinatarios serán recuperados con una sola petición. Finalmente, el sistema de Recuperación de Mensajes no funciona sin el encabezado `X-Authenticated-Sender` para dar seguridad y evitar que otras personas recuperen mensajes que no generaron. Por esto, la opción para deshabilitar ese encabezado 499 será omitida si se habilita la Recuperación de Mensajes.

Recuperación de Mensajes

Habilitar recuperación de mensajes
Dé clic en esta casilla de verificación para activar el sistema de recuperación de mensajes. La opción está deshabilitada por omisión.

Eliminar mensajes recuperados de las carpetas de correo de las cuentas
Dé clic en esta caja si también desea eliminar los mensajes recuperados de las carpetas de correo de sus cuentas locales de MDaemon si el mensaje ya ha sido entregado antes de que haya sido recuperado. Esto puede hacer que desaparezcan mensajes de las carpetas de correo y teléfonos de los usuarios locales. La opción está deshabilitada por omisión.

Diferir la entrega de mensajes durante estos minutos XX (0-15 minutos)
Este es el número de minutos que MDaemon retendrá mensajes entrantes provenientes de usuarios locales autentificados. Si se recibió el comando RECALL durante el periodo de retraso entonces MDaemon eliminará dicho mensaje antes de que se ejecute ningún intento de entrega. Esta opción se puede configurar entre 0-15 minutos. 1 minuto es el ajuste por omisión.

No diferir mensajes si el destinatario tiene un buzón en este servidor
Marque esta casilla si no desea diferir mensajes cuando el buzón del destinatario se encuentra en el mismo servidor MDaemon que el remitente. Nota: al utilizar la opción descrita arriba "*Eliminar mensajes recuperados de las carpetas de correo de la cuenta*", aun mensajes que ya fueron entregados se pueden recuperar y eliminar del buzón del usuario.

Los últimos [xx] mensajes autentificados enviados son elegibles para recuperación
MDaemon recuerda los IDs de los mensajes y sus ubicaciones para un número específico de correos más recientes enviados por usuarios autentificados. Los intentos de recuperación fallarán si el mensaje a recuperar no se encuentra en ese grupo de mensajes. Por esto al utilizar la opción descrita arriba "*Eliminar mensajes recuperados de las carpetas de correo de la cuenta*" se posibilita recuperar mensajes directamente de los buzones de los usuarios aun cuando ya hayan sido entregados. Por omisión esta opción se define en 1000 mensajes.

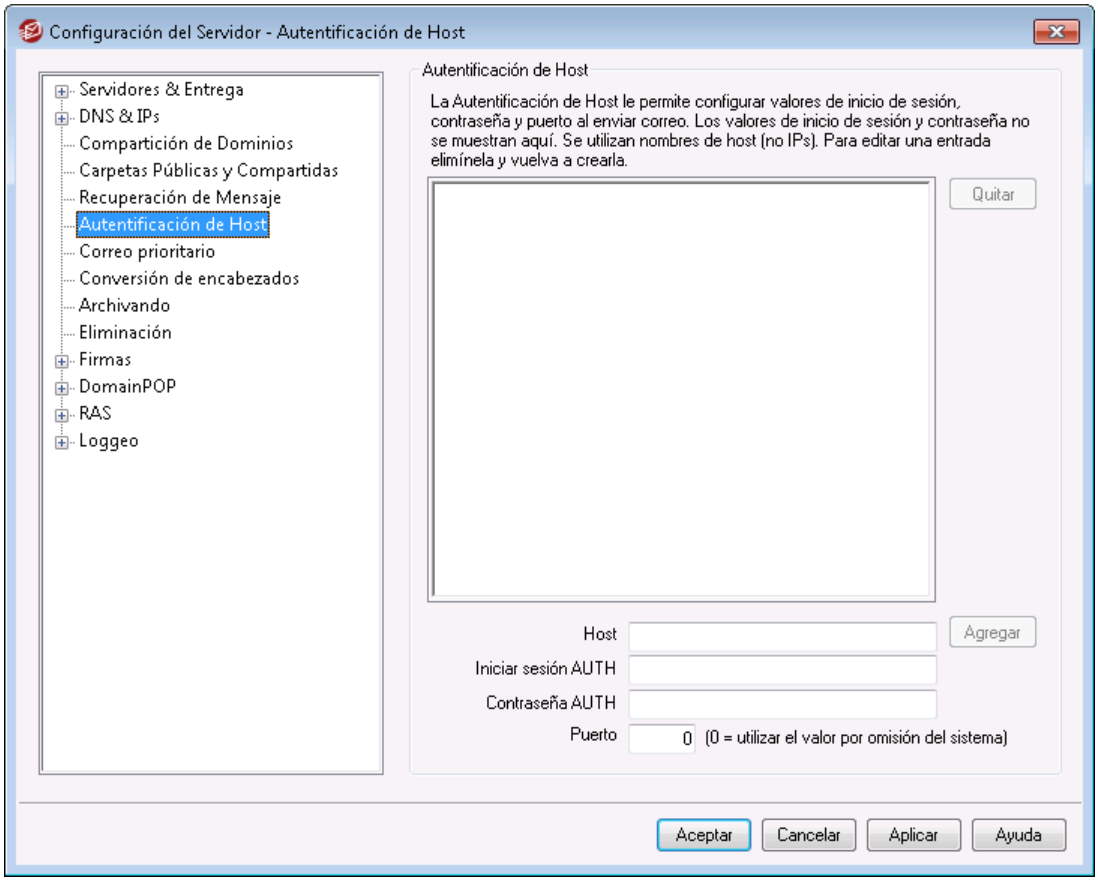
Entrega Diferida

La opción Entrega Diferida permite a clientes autentificados enviar mensajes en una fecha y hora programados. Webmail incluye esta opción, permitiendo a los usuarios dar clic en "Enviar Después" y especificar la fecha y hora para enviar el mensaje. El mensaje incluye el encabezado `Deferred-Delivery` conteniendo la fecha y hora para intentar entregarlo. Si está habilitada la Recuperación de Mensajes y se recibe una petición de recuperación para un mensaje programado para entrega diferida, MDaemon intentará eliminar el mensaje recuperado.

Habilitar entrega diferida
Habilite esta opción si desea permitir que clientes autentificados utilicen el encabezado `Deferred-Delivery` para programar la entrega diferida de mensajes. Cuando se habilita esta opción, los usuarios de Webmail tendrán disponible la opción **Enviar Después**, en los temas WorldClient y Lookout. La opción está deshabilitada por omisión.

Reemplazar 'Fecha:' con la fecha/hora actual en que se libera el mensaje
Habilite esta opción si desea reemplazar el encabezado 'Fecha:' con la fecha/hora actual en que el mensaje es liberado de la Cola de Diferidos. Se encuentra deshabilitado por omisión.

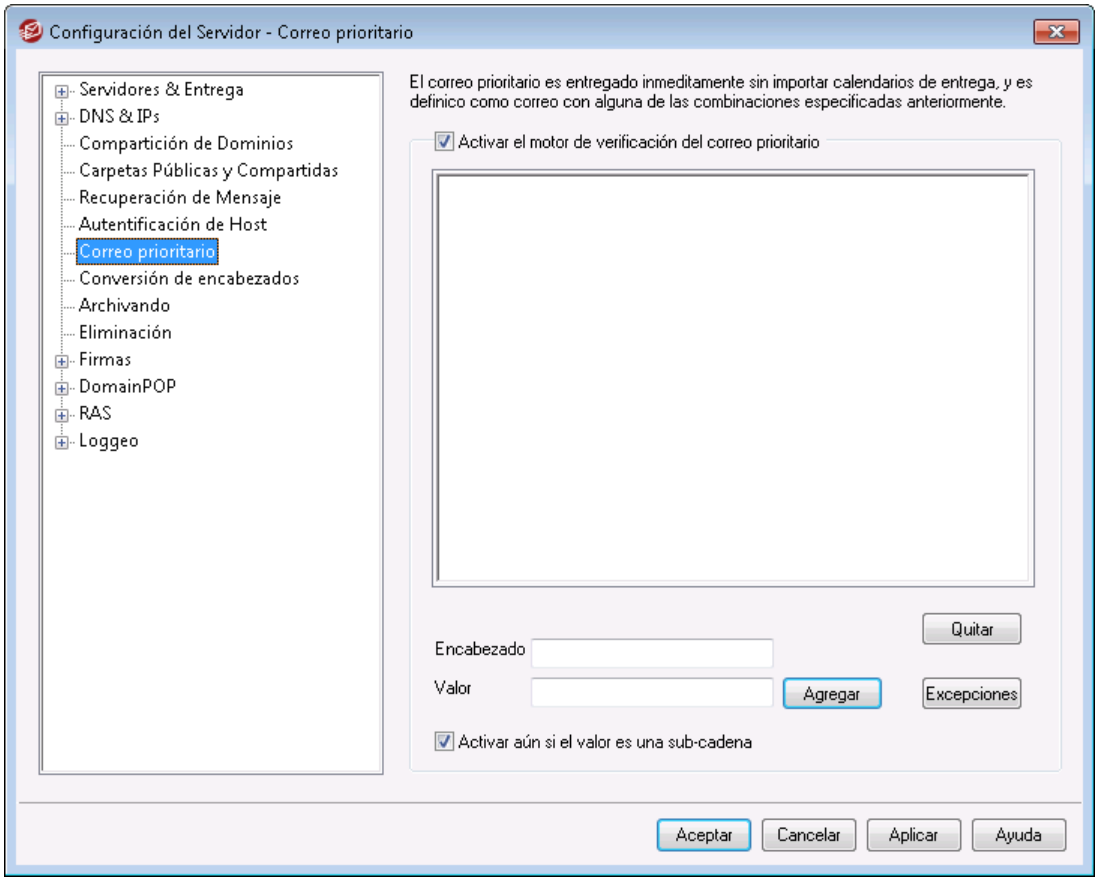
3.1.6 Autentificación de Host



Autentificación de Host

Utilice esta pantalla para configurar el inicio de sesión, contraseña y puerto para cualquier host. Cuando MDaemon envía correo SMTP a ese host, se utilizarán las credenciales asociadas que se encuentran aquí. Por favor note que esas credenciales son una segunda opción y solo se usan cuando no están disponibles otras credenciales específicas para ciertas tareas. Por ejemplo, si configura inicio de sesión y contraseña para las opciones de reenvío del Editor de Cuentas o la opción de Desencolamiento del Administrador de Puertas de Enlace, o cualquiera de muchos otros ajustes específicos a ciertas tareas, entonces esas credenciales se utilizan y reemplazan las configuradas aquí. Esta funcionalidad trabaja solamente con nombres de host (no direcciones IP).

3.1.7 Correo Prioritario



A la pantalla de Correo Prioritario se accede a través de la selección de menú "Configurar » Configuración de Servidor » Correo Prioritario". Se usa para definir qué constituye Correo Prioritario en nuestro Sistema de correo. El correo prioritario se envía directamente independientemente de los intervalos de proceso de correo definidos por MDaemon. Cuando un mensaje nuevo llega, MDaemon inspecciona sus encabezados para una combinación de valores/encabezados que se especifique en este diálogo. Si lo encuentra, lo considera un mensaje de alta prioridad e intenta el envío de manera inmediata.

Motor de Correo Prioritario

Activar el motor de verificación del correo prioritario
Marque esta casilla para activar la funcionalidad de Correo Prioritario. MDaemon inspeccionará todos los mensajes entrantes para un estatus de prioridad.

Encabezado
Introduzca el encabezado de mensaje en este campo. No incluya el carácter final de ":".

Valor
Introduzca el valor que se debe encontrar en el encabezado especificado para que el mensaje se considere de alta prioridad.

Activar aun si el valor es una sub-cadena
Cuando se introduce una nueva configuración de Correo Prioritario esta funcionalidad permite activar la priorización de una porción coincidente (sub-

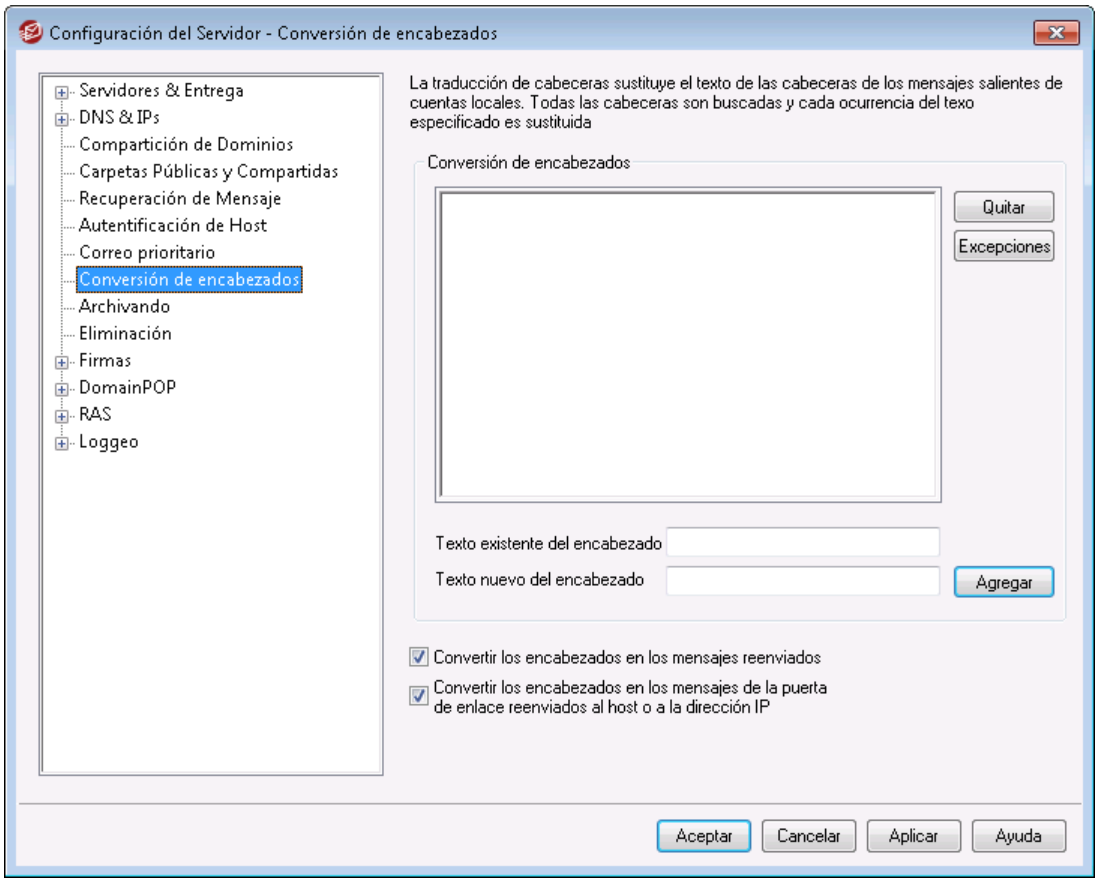
cadena) del valor de encabezado. Por ejemplo, puede crear una configuración de Correo Prioritario para el encabezado "`To`" con el valor "`Jefe`". Entonces, cualquier mensaje que contenga "`Jefe@loquesea`" en dicho encabezado será considerado correo prioritario. Si se crea una entrada sin esta funcionalidad activada, el encabezado debe coincidir exactamente; si coincide sólo una porción no será suficiente.

Agregar
Después de introducir información de Encabezado/Valor en los cuadros de texto especificados, y después de especificar si a esta entrada se aplicarán o no sub-cadenas, haga clic en el botón *Agregar* para crear la nueva entrada de Correo Prioritario.

Quitar
Haga clic en este botón para quitar una entrada seleccionada de la ventana *Configuración Actual de Correo Prioritario*.

Excepciones
Esto te permite definir combinaciones de campo/valor que harán que el mensaje se considere una excepción a las configuraciones de prioridad de correo. Esto da cierto control flexible sobre esta funcionalidad.

3.1.8 Conversión de encabezados



La funcionalidad de Conversión de Encabezados puede cambiar cualquier porción del texto encontrado en un encabezado a cualquier valor siempre que un mensaje se detecte que abandonará el dominio para dirigirse a un host remoto. Se especifica el texto que se quiere buscar y su valor de reemplazo correspondiente. MDaemon buscará en todos los encabezados del mensaje y realizará las sustituciones. Puede especificar también encabezados que MDaemon **no** deba modificar (tal como los encabezados "Subject:" o "Received:") haciendo clic en el botón *Excepciones* en este diálogo.

Esta funcionalidad es necesaria para algunas configuraciones de MDaemon en las cuales el dominio local es ficticio o diferente del nombre de dominio que debe aparecer en el correo saliente. En dicha situación, la Conversión de Encabezados puede utilizarse para cambiar cualquier ocurrencia de "`@dominiolocal`" a "`@DominioRemoto`".

Conversión de encabezados

Esta lista contiene las porciones de texto que MDaemon escaneará para los encabezados de mensajes salientes, y el texto que se sustituirá cuando se encuentre una igualdad.

Quitar
Seleccione una entrada en la lista de Conversiones de Encabezado Actuales y luego haga clic en este botón para eliminarlo de la lista.

Excepciones
Haga clic en este botón para abrir el diálogo Excepciones de la conversión de encabezados 137. Este diálogo se usa para especificar cualquier Encabezado que desee que se omita del proceso de Conversión de Encabezados.

Texto del encabezado existente
Escriba el texto que desea que sea reemplazado cuando se encuentre dentro de los encabezados de cualquier mensaje saliente.

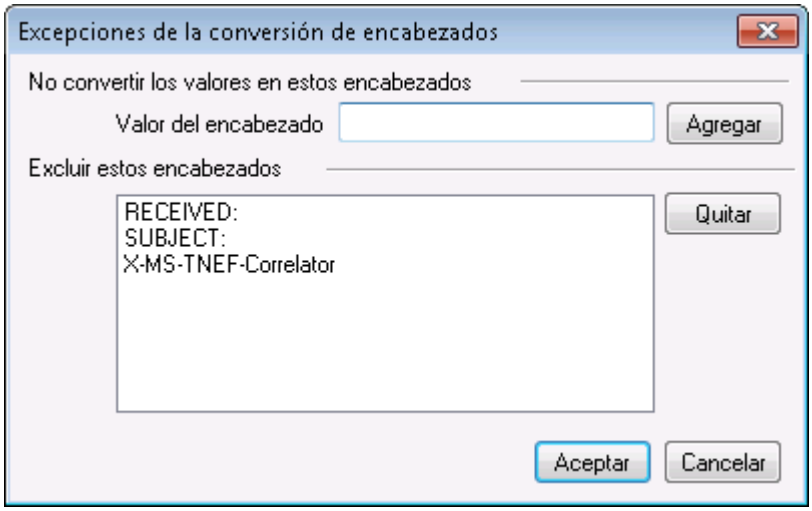
Nuevo texto del encabezado
Este texto será sustituido por aquel que se especifique en el campo *Texto del encabezado existente*.

Agregar
Haga clic en este botón para añadir los parámetros de texto a la lista *Conversión de Encabezados.*

Convertir los encabezados en los mensajes enviados
Haga clic en esta casilla de verificación para hacer que la conversión de encabezados se aplique solamente a los mensajes reenviados automáticamente de un dominio local a un dominio no-local.

Convertir los encabezados en los mensajes de la puerta de enlace reenviados al host o a la dirección IP
Haga clic en esta casilla de verificación si desea que los encabezados sean convertidos en el correo de los dominios reenviados de puerta de enlace. Vea la pantalla Reenvío 268 del Editor de Puerta de Enlace para más información.

3.1.8.1 Excepciones de la conversión de encabezados



No convertir los valores en estos encabezados

Valor del encabezado
Introduzca aquí cualquier encabezado que desea que se omita del proceso Conversión de Encabezados 135.

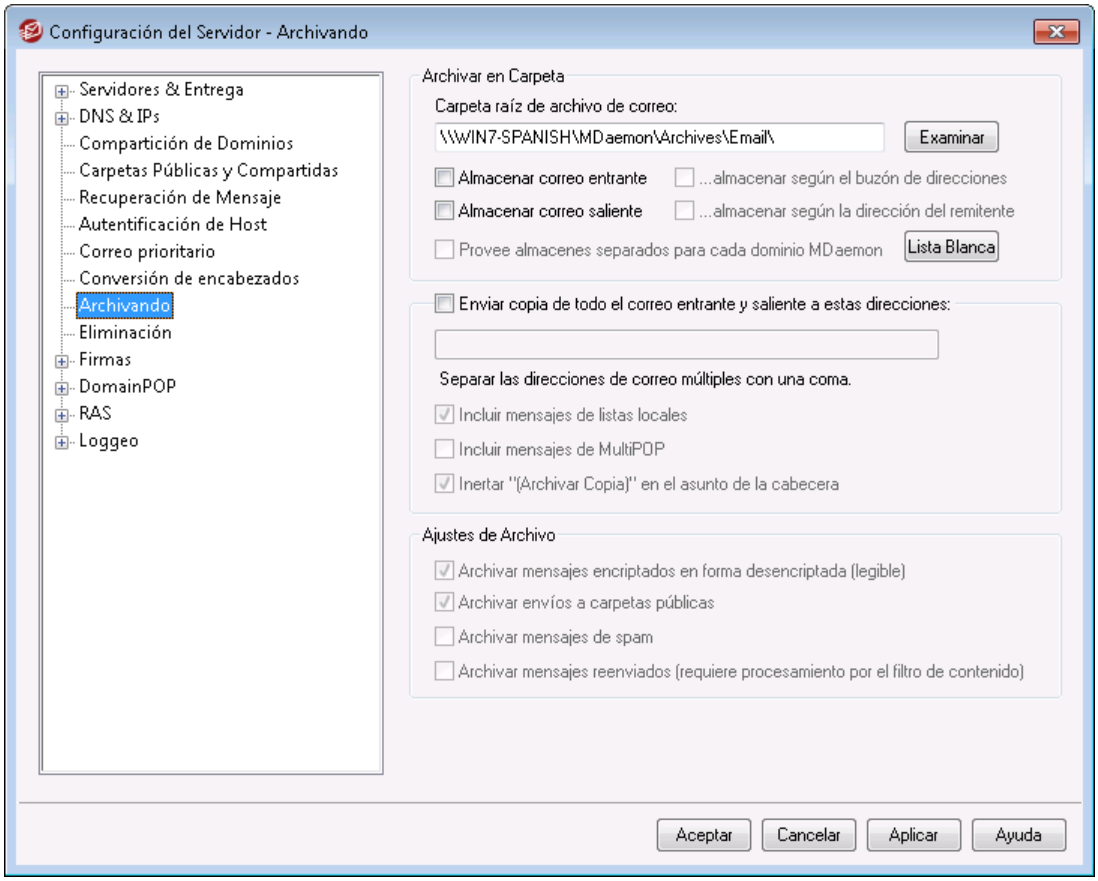
Agregar
Haga clic en este botón para añadir un nuevo encabezado a la lista.

Excluir estos encabezados

MDaemon no escaneará estos encabezados cuando se sustituya texto de encabezado.

Quitar
Seleccione un encabezado en la lista y haga clic en este botón para eliminarlo.

3.1.9 Archivar



Utilice esta funcionalidad para archivar todos los mensajes entrantes y salientes en una carpeta. La ubicación por omisión de esta carpeta es `C:\MDaemon\Archives\Email\`, pero puede configurarla hacia cualquier carpeta que seleccione. Puede elegir archivar mensajes entrantes dirigidos a sus usuarios locales, mensajes salientes de sus usuarios locales o ambos. Los mensajes de listas de distribución, los mensajes reenviados, mensajes del sistema y autorespuestas, nunca se archivan. Ni los mensajes de spam o mensajes con virus.

Los mensajes entrantes y salientes serán almacenados en las subcarpetas `\In\` y `\Out\`, respectivamente. Se pueden subdividir aún más utilizando las opciones *...archivar con base en la dirección del destinatario* y *...archivar con base en la dirección del remitente*. Así mismo, se puede mantener archivos separados por cada dominio utilizando la opción *Proporcionar archivos separados para cada dominio de MDaemon.*

Los mensajes archivados se graban en el estado final en el que aparecen en la carpeta de correo del usuario local, o en el estado "listo para ser entregado" para los mensajes salientes. Esto significa que si usted, por ejemplo, hace que el filtro de contenido aplique algún cambio a un mensaje, tal como agregar un encabezado, entonces el mensaje archivado contendrá esa modificación.

Para visualizar la carpeta de archivo utilice una de sus cuentas de correo (o genere una nueva) y apunte su Carpeta de Correo 718 a la misma carpeta utilizada para archivar. Si varias personas necesitan tener acceso al archivo, entonces ingrese a la cuenta de archivo y comparta 743 las carpetas deseadas utilizando la Lista de Control de Acceso 316.

Existe una cola del sistema, oculta, localizada en: "\MDaemon\Queues\ToArchive\". Esta cola se verifica a intervalos regulares buscando mensajes que han sido colocados ahí manualmente, por un complemento o de otra manera. Cuando se encuentra un mensaje ahí, inmediatamente se archiva y elimina. Si se encuentran mensajes ahí que no son elegibles para archivo, simplemente se borran. La pantalla/registro de Enrutamiento mostrarán detalles siempre que un mensaje sea archivado exitosamente.

Archivar a una carpeta

Defina su carpeta de archivo de correo aquí. Por omisión se configura en C:\MDaemon\Archives\Email\, pero la puede apuntar a cualquier carpeta que desee.

Archivar correo entrante
Dé clic en esta casilla de verificación para grabar una copia de todos los mensajes destinados a los usuarios locales. Los mensajes de listas de distribución y que contengan virus no se archivan.

...archivar con base en la dirección del destinatario
Dé clic en esta opción si desea que el correo entrante se archive con base en la dirección del destinatario.

Archivar correo saliente
Dé clic en esta casilla para grabar una copia de todos los mensajes enviados por los usuarios locales. Los mensajes de listas de distribución y mensajes conteniendo virus no se archivan.

...archivar con base en la dirección del remitente
Dé clic en esta opción si desea archivar el correo saliente en categorías con base en la dirección del remitente.

Proporcione archivos separados para cada dominio de MDaemon
Dé clic en esta opción si desea mantener un archivo por separado para cada dominio.

Lista de Exentos
Dé clic en este botón para abrir la Lista Exentos del Archivo. Aquí puede enlistar las direcciones "para" y "de" que desea estén exentas de archivo.

Enviar copias de todos los mensajes entrantes y salientes a estas direcciones

Registre una o más direcciones a las que desea que se envíen los mensajes de archivo. Múltiples direcciones deben separarse con coma. Puede especificar direcciones locales y remotas y alias de direcciones.

Incluir mensajes de listas de distribución locales
Cuando se habilite esta opción, se enviarán copias de los mensajes de listas de distribución locales a estas direcciones.

Incluir mensajes recolectados por MultiPOP
Habilite esta opción si desea enviar mensajes recolectados a través de la funcionalidad MultiPOP 739 de MDaemon.

Insertar "(Archive Copy)" en el encabezado Asunto del mensaje
Cuando se habilita esta opción, se insertará "(Archive Copy)" en el encabezado `Subject:` de los mensajes enviados.

Ajustes de Archivo

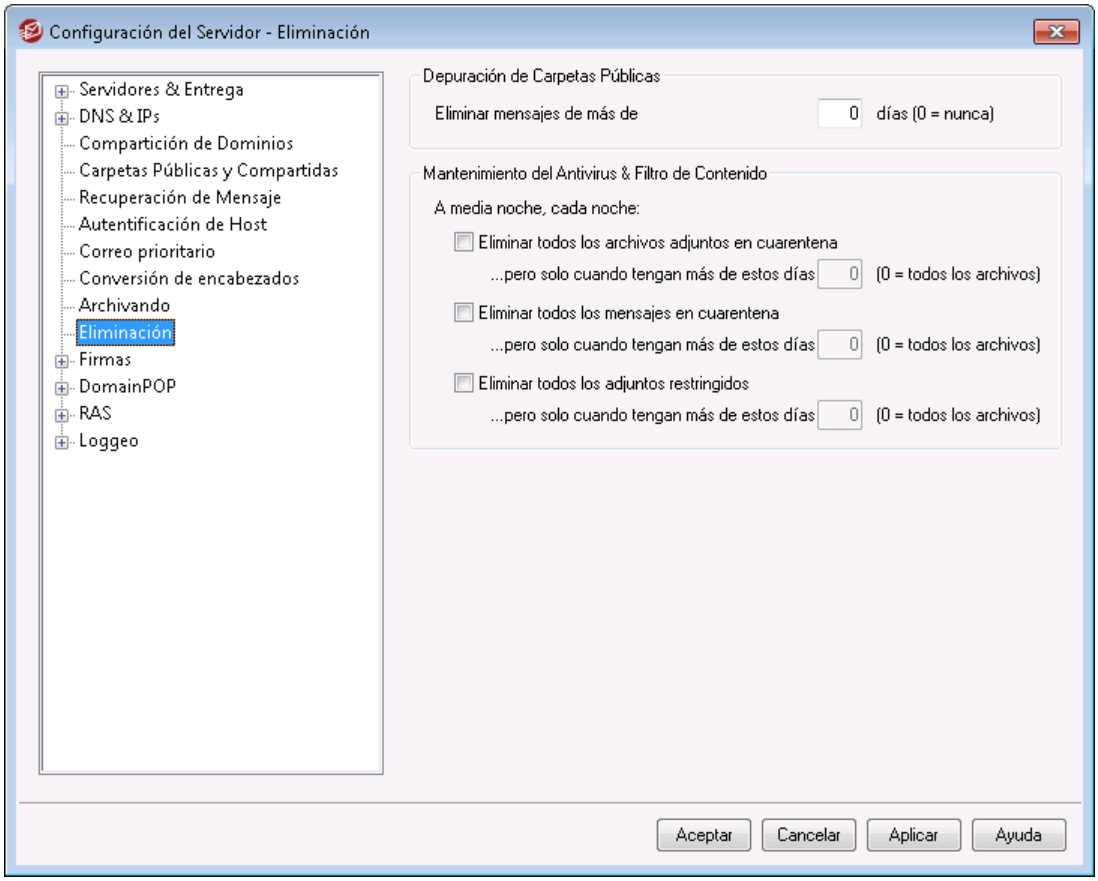
Archivar mensajes encriptados en forma desencriptada (legible)
Por omisión, las copias desencriptadas de mensajes encriptados se almacenan en el archivo. Si, sin embargo, un mensaje no se puede desencriptar, se almacenará la forma encriptada en su lugar. Deshabilite esta opción si prefiere almacenar versiones encriptadas cuando la desencripción está disponible.

Archivar envíos a carpetas públicas
Por omisión, los mensajes enviados a carpetas públicas son archivados. Deshabilite esta opción si no desea archivar esos mensajes.

Archivar mensajes de spam
Habilite esta opción si desea que el archivo y copias enviadas incluyan mensajes marcados como spam.

Archivar mensajes reenviados (requiere procesamiento del filtro de contenido)
Habilite esta opción si desea que los mensajes archivados y enviados incluyan los mensajes reenviados. Por omisión estos no se archivan.

3.1.10 Eliminación



Depuración de Carpetas Públicas

Eliminar los mensajes mayores de XX días (0=nunca)
Especifique un número de días en esta opción si desea que los mensajes antiguos sean eliminados de las Carpetas Públicas 125.

Antivirus/Depuración del Filtro de Contenido

Borrar todos los archivos en cuarentena
Haga clic en esta opción si desea que todos los archivos en cuarentena sean borrados cada noche.

...pero solo cuando son mayores de este número de días [xx] (0 = todos los archivos)
Por omisión todos los archivos en cuarentena serán eliminados. Especifique un número de días en esta opción si desea que se eliminen solo los archivos mayores del valor definido.

Borrar todos los mensajes en cuarentena
Haga clic en esta opción si desea que todos los mensajes en cuarentena sean borrados cada noche.

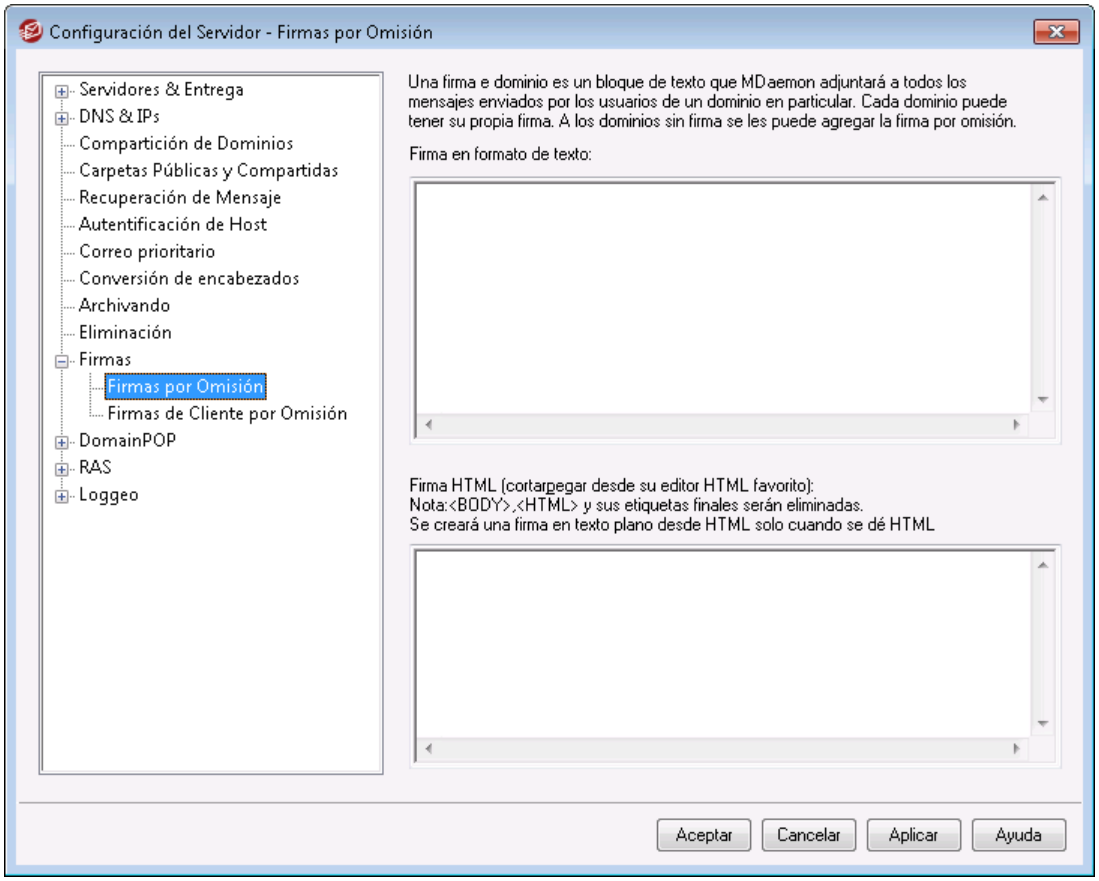
...pero solo cuando son mayores de este número de días [xx] (0 = todos los archivos)
Por omisión todos los mensajes en cuarentena serán eliminados. Especifique un número de días en esta opción si desea que se eliminen solo los mensajes mayores del valor definido.

Borrar todos los adjuntos restringidos
Haga clic en esta opción si desea que todos los adjuntos restringidos sean borrados cada noche.

...pero solo cuando son mayores de este número de días [xx] (0 = todos los archivos)
Por omisión todos los adjuntos restringidos serán eliminados. Especifique un número de días en esta opción si desea que se eliminen solo los adjuntos restringidos mayores del valor definido.

3.1.11 Firmas

3.1.11.1 Firmas por Omisión



Utilice esta pantalla para agregar una firma a todos los mensajes enviados por sus usuarios de MDaemon. Utilice la pantalla Firmas 210 en el Administrador de Dominios si desea utilizar firmas diferentes para usuarios de dominios específicos—cuando existe una firma específica para un dominio, ésta será utilizada en lugar de la Firma por Omisión. Las firmas se agregar al final de los mensajes, excepto en los mensajes de listas que utilizan pies de página, en cuyo caso el pie se agrega abajo de la firma.

También puede utilizar la funcionalidad Firma[753] del Editor de Cuentas para agregar firmas individuales a cada Cuenta. Las firmas de cuentas se agregan justo antes de la firma por Omisión o la firma del Dominio.

Firma en texto plano

Esta área es para insertar una firma en texto plano. Si desea designar una firma HTML a ser utilizada en el segmento texto/HTML de mensajes multiparte, utilice el área *Firma HTML* abajo. Si se incluye una firma en ambos lugares, entonces MDaemon utilizará la adecuada para cada parte del mensaje multiparte. Si no se especifica firma HTML, entonces se utilizará la firma en texto plano en ambas partes.

Firma HTML (Puede cortar&pegar desde su editor HTML favorito)

Esta área es para insertar una firma HTML a utilizar en el segmento texto/HTML de mensajes multiparte. Si se incluye una firma tanto aquí como en el área *Firma en Texto Plano* arriba, MDaemon utilizará la firma adecuada para cada segmento del mensaje multiparte. Si no se especifica firma de texto entonces se utilizará la firma HTML.

Para crear una firma HTML, puede teclear aquí el código HTML o cortar&pegar directamente desde su editor HTML favorito. Si desea incluir imágenes incrustadas en su firma HTML, lo puede hacer utilizando `$ATTACH_INLINE:path_to_image_file$` macro.

Por ejemplo:

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

Existen varias maneras de insertar imágenes incrustadas en las firmas desde la interface web de la Administración Remota[354] de MDaemon:

- En la pantalla Firmas por Omisión en la Administración Remota, dé clic en el botón "Imagen" de la barra de herramientas en el editor HTML y seleccione la pestaña para cargar archivo.
- En la pantalla Firmas por Omisión en la Administración Remota, dé clic en el botón "Agregar Imagen" de la barra de herramientas en el editor HTML.
- Arrastre y pegue la imagen en la pantalla Firmas por Omisión del editor HTML utilizando Chrome, Firefox, Safari o MSIE 10+.
- Copie y pegue la imagen desde el Portapapeles en la pantalla Firmas por Omisión n el editor HTML utilizando Chrome, Firefox o MSIE 11+

Las etiquetas <body></body> y <html></html> no se permiten en firmas y serán eliminadas cuando se detecten.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto

del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje siempre que quieran que aparezca la firma,

Signature Selector	
$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.
$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**

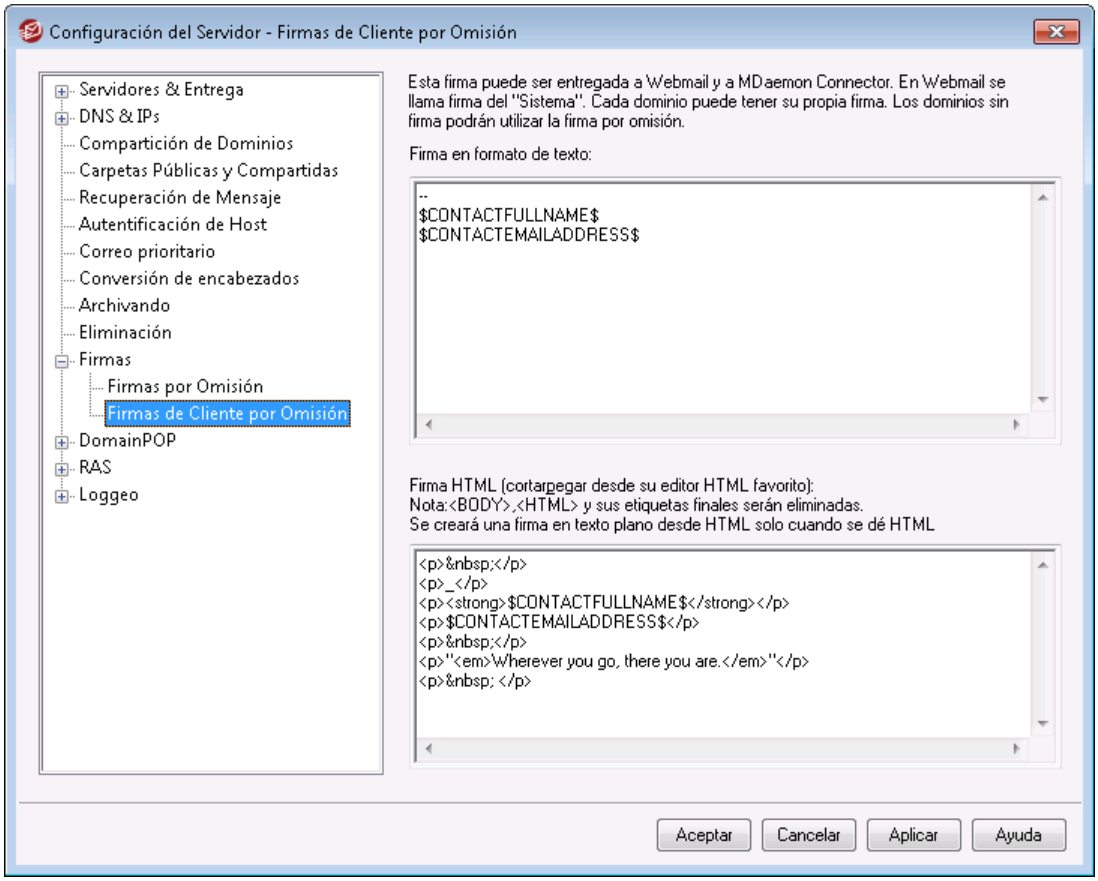
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**
Gerencia	**$CONTACTBUSINESSMANAGER$**
Asistente	**$CONTACTBUSINESSASSISTANT$**

Teléfono Asistente	$CONTACTBUSINESSASSISTANTPHONE$
Teléfono directo en la Empresa	$CONTACTBUSINESSMAINPHONE$
Teléfono de la Empresa	$CONTACTBUSINESSPHONE$
Teléfono 2 de la Empresa	$CONTACTBUSINESSPHONE2$
Teléfono IP de la Empresa	$CONTACTBUSINESSIPPHONE$
Fax de la Empresa	$CONTACTBUSINESSFAX$
Pager de la Empresa	$CONTACTBUSINESSPAGER$
Radio de la Empresa	$CONTACTBUSINESSRADIO$
Dirección de la Empresa	$CONTACTBUSINESSADDRESS$
Ciudad de la Empresa	$CONTACTBUSINESSCITY$
Estado de la Empresa	$CONTACTBUSINESSSTATE$
Código Postal de la Empresa	$CONTACTBUSINESSZIPCODE$
País de la Empresa	$CONTACTBUSINESSCOUNTRY$
Sitio web de la Empresa	$CONTACTBUSINESSWEBADDRESS$
Otros	
Esposo(a)	$CONTACTSPOUSE$
Hijos	$CONTACTCHILDREN$
Categorías	$CONTACTCATEGORIES$
Comentario	$CONTACTCOMMENT$

Ver:

Administrador de Dominios » Firmas 210
Editor de Cuentas » Firma 753

3.1.11.2 Firmas de Cliente por Omisión



Utilice esta pantalla para crear una firma de cliente por omisión que puede entregar a MDaemon Webmail 345 y a MDaemon Connector 404, para ser utilizada por sus usuarios al redactar mensajes de correo. Puede utilizar las macros 148 enlistadas abajo para personalizar la firma, de manera que será única para cada usuario, incluyendo elementos como el nombre del usuario, dirección de correo, número de teléfono y demás. Utilice la pantalla Firmas de Cliente 215 en el Administrador de Dominios si desea utilizar una firma distinta para usuarios de dominios específicos. Cuando existe una firma específica por dominio, se utilizará en lugar de la Firma de Cliente por Omisión. Utilice la opción *Entregar Firma de Cliente* 345 si desea entregar la firma de cliente a Webmail y la opción *Entregar firma de Cliente a Outlook* 404 si desea entregarla a MDaemon Connector. En las opciones de Redacción de Webmail, la firma entregada al cliente se denomina "Sistema". Para MDaemon Connector puede definir un nombre para la firma que aparecerá en Outlook.

Firma en Texto Plano

Esta área es para insertar una firma en texto plano. Si desea definir una firma html correspondiente para ser utilizada en la sección texto/html de mensajes multiparte, utilice el área *Firma HTML* que se menciona abajo. Si una firma se incluye en ambos lugares, MDaemon utilizará la apropiada para cada parte de un mensaje multiparte. Si no se especifica firma html, se utilizará la firma en texto plano en ambas partes.

Firma HTML (cortar y pegar desde su editor HTML favorito)

Esta área es para insertar una firma HTML para ser utilizada en la parte texto/html de mensajes multiparte. Si se incluye una firma tanto aquí como en el área *Firma en Texto Plano* mencionada arriba, MDaemon utilizará la firma apropiada para cada

parte del mensaje multiparte. Si no se define firma en texto plano, se utilizará la firma html para crear una.

Para crear su firma html, teclee aquí manualmente el código html o corte&pegue directamente desde su editor HTML favorito. Si desea incluir imágenes en línea en su firma HTML, lo puede hacer utilizando la macro `$ATTACH_INLINE:path_to_image_file$`.

Por ejemplo:

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

También hay varias maneras en las que se pueden insertar imágenes en línea en las firmas desde la interface web de la Administración Remota 354 de MDaemon:

- En la pantalla Firma de Cliente por Omisión en la Administración Remota, dé clic en el botón "Imagen" de la barra de herramientas, en el editor HTML y seleccione la pestaña para cargar.
- En la pantalla Firma de Cliente por Omisión en la Administración Remota, dé clic en el botón de la barra de herramientas "Agregar imagen" en el editor HTML.
- Arrastre y suelte la imagen en la pantalla del editor HTML de la Firma de Cliente por omisión, con Chrome, FireFox, Safari, o MSIE 10+
- Copie y pegue una imagen desde el portapapeles, en la pantalla del editor HTML de la Firma del Cliente por omisión, con Chrome, FireFox, MSIE 11+

Las etiquetas <body></body> y <html></html> no son permitidas en firmas y serán eliminadas cuando se encuentren.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje siempre que quieran que aparezca la firma,

Signature Selector

$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.
$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**

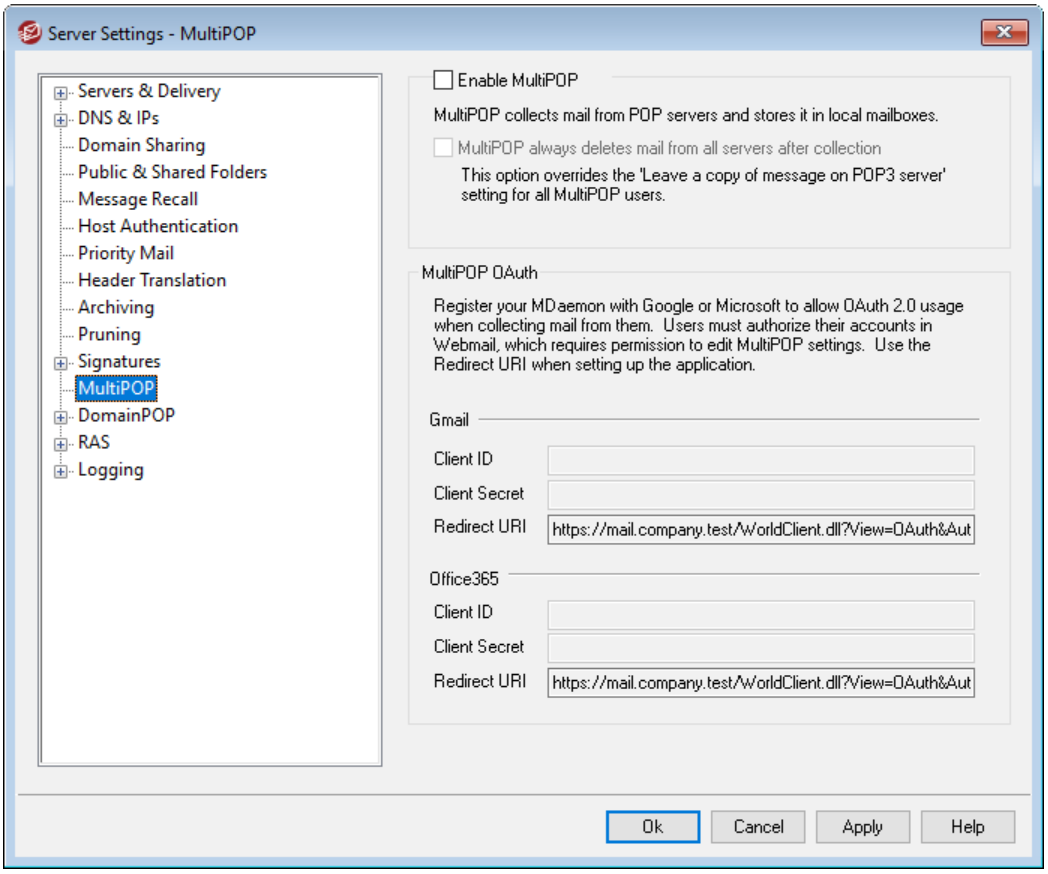
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**
Gerencia	**$CONTACTBUSINESSMANAGER$**
Asistente	**$CONTACTBUSINESSASSISTANT$**
Teléfono Asistente	**$CONTACTBUSINESSASSISTANTPHONE$**
Teléfono directo en la Empresa	**$CONTACTBUSINESSMAINPHONE$**
Teléfono de la Empresa	**$CONTACTBUSINESSPHONE$**
Teléfono 2 de la Empresa	**$CONTACTBUSINESSPHONE2$**
Teléfono IP de la Empresa	**$CONTACTBUSINESSIPPHONE$**
Fax de la Empresa	**$CONTACTBUSINESSFAX$**
Pager de la Empresa	**$CONTACTBUSINESSPAGER$**

Radio de la Empresa	$CONTACTBUSINESSRADIO$
Dirección de la Empresa	$CONTACTBUSINESSADDRESS$
Ciudad de la Empresa	$CONTACTBUSINESSCITY$
Estado de la Empresa	$CONTACTBUSINESSSTATE$
Código Postal de la Empresa	$CONTACTBUSINESSZIPCODE$
País de la Empresa	$CONTACTBUSINESSCOUNTRY$
Sitio web de la Empresa	$CONTACTBUSINESSWEBADDRESS$
Otros	
Esposo(a)	$CONTACTSPOUSE$
Hijos	$CONTACTCHILDREN$
Categorías	$CONTACTCATEGORIES$
Comentario	$CONTACTCOMMENT$

Ver:

Firmas por Omisión 142
Administrador de Dominios » Firmas 210
Administrador de Dominios » Firmas de Cliente 215
Editor de Cuentas » Firmas 753
Ajustes de Webmail 345
Ajustes del Cliente OC » Firma 404

3.1.12 MultiPOP



Habilitar MultiPOP

Marque esta casilla para habilitar el servidor MultiPOP; este recolecta correo de servidores POP de parte de sus usuarios y los almacena en sus buzones locales. La funcionalidad MultiPOP le permite crear un número ilimitado de combinaciones POP3 de servidor/usuario/contraseña para recolección de mensajes de correo desde múltiples fuentes. Esto es útil para usuarios que tienen cuentas de correo en múltiples servidores pero prefieren recolectar y recibir todo su correo junto en un solo lugar. Antes de ser colocado en el buzón del usuario, el correo recolectado por MultiPOP primero se coloca en la cola local para que pueda ser procesado como cualquier otro correo y se le aplican las Autorespuestas y el Filtro de Contenido. Las opciones de programación para MultiPOP se localizan en: Configuración » Programación de Eventos » Programación de Correo » Recolección MultiPOP 383.

MultiPOP siempre elimina correo de todos los servidores luego de la recolección
Dé clic en esta casilla si desea ignorar la opción *Dejar una copia del mensaje en el servidor POP* (localizada en la pantalla MultiPOP 739 del Editor de Cuentas) para todos los usuarios. Todos los mensajes se eliminarán de cada servidor MultiPOP luego de ser recolectados.

Enviar correo de notificación luego de este número de fallos
Por omisión, MDaemon envía un mensaje de notificación luego de múltiples fallos al verificar una cuenta MultiPOP. Dado que los fallos temporales son comunes, esta opción le permite especificar cuantos fallos consecutivos toma para detonar la notificación y la opción abajo le permite elegir cuantos días esperar entre esas notificaciones. El contenido y destinatarios de los mensajes de notificación se puede personalizar editando `\MDaemon\App\MPOPFailureNotice.dat`. Por

omisión, las notificaciones se envían al propietario de la cuenta MultiPOP luego de 5 fallos, no más de una vez cada 7 días.

No notificar de nuevo durante este número de días
Por omisión, las notificaciones de fallos MultiPOP se envían no más de una vez cada siete días. Use esta opción si desea ajustar el intervalo.

MultiPOP OAuth

OAuth 2.0 es un método moderno de autentificación que ahora requieren Gmail y Microsoft (Office) 365 (o pronto requerirán) conforme deshabiliten el soporte a la autentificación básica. A fin de que la funcionalidad MultiPOP de MDaemon utilice OAuth 2.0 para recolectar correo de Gmail u Office 365 por parte de sus usuarios, debe registrar su servidor de MDaemon con Google o Microsoft, respectivamente, creando una aplicación OAuth 2.0 utilizando la Consola de API de Google o Active Directory de Microsoft Azure. Esto es similar al procedimiento requerido para utilizar la Integración con Dropbox 337 de MDaemon para sus usuarios de Webmail.

Para configurar MultiPOP para recolectar correo desde Gmail o Microsoft (Office 365 para sus usuarios:

1. Vaya a la opción describa arriba **Habilitar MultiPOP**.
2. Siga las instrucciones siguientes para **Crear y vincular su App OAuth MultiPOP** 154 para Gmail o para Office 365.
3. En la página MultiPOP del Editor de Cuentas 739, **Habilite MultiPOP** para cada usuario al que desea permitir utilizar MultiPOP para recuperar correo desde Gmail o desde Office 365.
4. Agregue la cuenta de Gmail (`pop.gmail.com:995`) u Office 365 (`outlook.office365.com:995`) para cada uno de los usuarios y habilite la opción **Utilizar OAuth**. Opcionalmente puede hacer que sus usuarios ejecuten este paso por sí mismos víaWebmail 321. **Nota:** para cuentas Gmail, cada una debe ser agregada a los Usuarios de Prueba en su app Gmail OAuth (ver la nota **Estatus de Publicación** en las instrucciones siguiente *Crear y Vincular su App MultiPOP OAuth* 154.
5. En la página Servicios Web del Editor de Cuentas 720, habilite la opción "**...editar ajustes MultiPOP**" para cada uno de esos usuarios.
6. Cada usuario debe iniciar sesión en Webmail para ir a la página **Buzones** en Opciones, agregar su cuenta Gmail u Office 365 (si no lo ha hecho aún por ellos) y dar clic en **Autorizar** para iniciar sesión en su cuenta de Gmail u Office 365 y realizar los pasos para autorizar a MDaemon a recolectar su correo desde esa ubicación.

Gmail/Office 365

ID de Cliente
Este es un único ID de Cliente asignado a su app MultiPOP OAuth 2.0 cuando lo crea en la Consola Google API o en el portal de Active Directory de Microsoft Azure. Luego de crear su app, copie este ID de Cliente y péguelo aquí.

Secreto de Cliente
El Secreto de Cliente se asigna a su app MultiPOP OAuth 2.0 cuando lo crea en la Consola Google API o en el portal Active Directory de Microsoft Azure. Luego de crear su app, copie este Secreto de Cliente y péguelo aquí. **Nota:** al crear el

Secreto de Cliente para una app en Azure, debe copiarlo cuando crea la app porque después ya no será visible. Si no lo copia en ese momento deberá eliminarlo y crear uno nuevo.

URI de Redireccionamiento
Debe especificar una URI de Redireccionamiento al crear su app OAuth 2.0 para Gmail u Office 365. La URI de Redireccionamiento desplegada en la pantalla MultiPOP es un ejemplo construido con su Nombre de host SMTP del Dominio por Omisión 190, que deberá funcionar para los usuarios de ese dominio al iniciar sesión en Webmail. Deberá agregar URIs de Redireccionamiento a su app para cualquier dominio adicional de MDaemon a los que vayan sus usuarios al iniciar sesión en Webmail. Por ejemplo, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" funcionará para cualquiera de sus usuarios que vayan a mail.example.com al iniciar sesión en Webmail. Ver: **Crear y Vincular su App MultiPOP OAuth** abajo para más información.

Ejemplo de URI de Redireccionamiento:

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

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

Crear y Vincular su App MultiPOP OAuth

Instrucciones paso a paso para crear su App MultiPOP OAuth 2.0.

Para Google Gmail

Siga los pasos siguientes para crear una aplicación de Google para permitir a MultiPOP autentificarse utilizando OAuth 2.0 al recolectar correo desde Gmail para sus usuarios.

1. En su navegador, vaya a Consola de Google API.
2. Si está en la lista de Proyectos, dé clic en **PROYECTO NUEVO**, o si está en la página Administrar Recursos, dé clic en **(+) CREAR PROYECTO**.
3. Teclee un **Nombre de Proyecto,** luego clic en **Editar** si desea editar el ID de Proyecto o dejarlo configurado con el valor por omisión. **Nota:** el ID de Proyecto no se puede modificar luego de que el proyecto haya sido creado.
4. En el panel izquierdo, vaya a **APIs & Servicios | Pantalla de Consentimiento de OAuth**.
5. Seleccione **Externo** y dé clic en **Crear**.
6. Registre el **Nombre de App** (ej. MultiPOP OAuth 2.0 para Gmail), una **Dirección de correo de soporte** para que contacten los usuarios y una **Dirección de correo de Desarrollador** para que Google lo contacte sobre modificaciones a su proyecto. Esto es todo lo que se requiere en esta página como configuración, pero dependiendo de su organización particular o requerimientos de verificación, también puede registrar el logo de su empresa y vínculos a sus Términos de servicio 365 y Política de Privacidad. Los campos **Dominios Autorizados** se llenarán automáticamente cuando agregue las *URIs de Redireccionamiento* en el paso siguiente. **Nota:** Esta información se utiliza para la pantalla de Consentimiento que se presentará a los usuarios para autorizar que MultiPOP recolecte correo de Gmail.

7. Dé clic en **Grabar y Continuar.**
8. Dé clic en **AGREGAR O REMOVER ALCANCES** y bajo "Agregar alcances manualmente" registre **https://mail.google.com/**. Dé clic en **AGREGAR A TABLA**, luego clic en **Actualizar**.
9. Dé clic en **Grabar y Continuar**.
10. Bajo Usuarios de Prueba, dé clic en **AGREGAR USUARIOS**, registre cada cuenta de Gmail para la que recolectará correo y dé clic en **AGREGAR** (ver la nota abajo acerca del Estatus de Publicación de su App 155).
11. Dé clic en **Guardar y Continuar**.
12. En Resumen, dé clic en **VOLVER AL PANEL** en la parte inferior de la página.
13. Dé clic en **Credenciales** en el panel izquierdo, clic en **(+) Crear Credenciales** y seleccione **ID de cliente OAuth**.
14. En el menú desplegable "Tipo de Aplicación", seleccione **Aplicación Web** y bajo "URI de redireccionamiento autorizados" dé clic en **+ AGREGAR URIs**. Registre la URI de Redireccionamiento. La URI de Redireccionamiento desplegada en la pantalla MultiPOP es un ejemplo construido con Nombre de Host SMTP de su Dominio por Omisión 190, que deberá funcionar para los usuarios de ese dominio al iniciar sesión en Webmail. Deberá agregar URIs de Redireccionamiento a su app si sus usuarios utilizan dominios adicionales de MDaemon al iniciar sesión en Webmail. Por ejemplo, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Gmail" funcionará para cualquiera de sus usuarios que vayan a mail.example.com al iniciar sesión en Webmail.
15. Dé clic en **CREAR.**
16. Copie los valores en **Su ID de Cliente** y **Secreto de Cliente** en las casillas ID de Cliente Gmail y Secreto de Cliente en su página MultiPOP.

Estatus de Publicación — Estas instrucciones son para crear una app de Google con un Estatus de Publicación definido como "**Prueba**". Esto requiere que agregue cada cuenta específica de Google que estará utilizando la app para recolectar correo desde Gmail y se limita a 100 usuarios. Más aún, en Webmail cuando se pide a sus usuarios autorizar a MDaemon a recolectar el correo desde Gmail, se desplegará un mensaje de advertencia "para confirmar que el usuario tiene acceso de prueba a su proyecto pero deberá considerar los riesgos asociados con otorgar acceso a sus datos desde una app no verificada". Así mismo, la autorización expira luego de siete días, por lo que cada usuario deberá reautorizar la recolección desde Gmail cada semana.

Si desea eliminar esos requerimientos y limitaciones, debe modificar el estatus a "**En Producción",** lo que puede o no requerir que ejecute un proceso de verificación. Para más información sobre verificación de apps y estatus de publicación, vea los siguientes artículos de Google: Configurar su pantalla de consentimiento OAuth y FAQs de la API de verificación Auth.

Para Microsoft (Office) 365

Siga los pasos siguiente para crear una aplicación Microsoft Azure para permitir que MultiPOP se autentifique utilizando OAuth 2.0 al recolectar correo desde Office 365 para sus usuarios.

1. Vaya a la página Microsoft Azure Active Directory en el portal de Azure y dé clic en **Registros de aplicaciones** en el panel izquierdo (debe iniciar sesión por una cuenta gratuita o de paga en Azure, si aún no cuenta con una).
2. Dé clic en **+ Nuevo registro**.
3. Ingrese un nombre de aplicación en el campo **Nombre** (ej. "OAuth de buzón para Office 365").
4. Para "Tipos de cuenta compatibles" seleccione **Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)**.
5. Para "URI de Redirección" seleccione **web** y luego ingrese su **URI de Redirección** Office 365. La URI de Redirección desplegada en la pantalla MultiPOP es un ejemplo construido a partir de su Nombre de host SMTP para el Dominio por Omisión 190, que deberá funcionar para los usuarios de ese dominio cuando inician sesión en Webmail. Deberá agregar URIs de Redirección adicionales para su app si sus usuarios utilizan dominios adicionales de MDaemon al iniciar sesión en Webmail. Por ejemplo, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" deberá funcionar para cualquiera de sus usuarios que apuntan a mail.example.com al iniciar sesión en Webmail.
6. Dé Clic en **Registrar**.
7. Tome nota de la **Id. de aplicación (cliente)** (a un lado hay un botón para copiarla al portapapeles). Puede encontrar posteriormente este ID dando clic en **Información General** en el panel izquierdo.
8. Si necesita agregar URIs de redireccionamiento adicionales, dé clic en la liga **URI de redirección: 1 web** a la derecha. Dé clic en **Agregar un URI** y registre el URI, repita como sea necesario y dé clic en **Guardar**.
9. Dé clic en **Permisos de API** en el panel izquierdo.
10. Dé clic en **+Agregar un permiso.**
11. Dé clic en **Microsoft Graph**.
12. Dé clic en **Permisos Delegados**.
13. Desplácese hasta abajo hasta **POP** y seleccione **POP.AccessAsUser.All**, luego bajo **User** seleccione y **User.Read** (User.Read ya fue seleccionado por omisión).
14. Dé clic en **Agregar permisos**.
15. En el panel izquierdo, dé clic en **Certificados & Secretos**.
16. Dé clic en **+ Nuevo secreto de cliente**.
17. Escriba una descripción (ej. "Secreto de Cliente para Office 365 MultiPOP OAuth app").
18. Seleccione el tiempo para que el secreto de cliente expire.
19. Dé clic en **Agregar**.

20. Tome nota del secreto de cliente generado en el campo **Valor** (a un lado hay un botón para copiarla al portapapeles). **NOTA:** el secreto de cliente no será visible de nuevo en esta página—se presentará a un lado el ícono **Eliminar** de manera que lo pueda eliminar y crear un secreto de cliente nuevo cuando sea necesario.
21. Copie los valores del ID de Aplicación (cliente) y el Secreto de Cliente en los campos **Id de Cliente** y **Secreto de Cliente** bajo la sección Office 365 de la página MultiPOP de MDaemon bajo Ajustes del Servidor.

Ver:

Editor de Cuentas | MultiPOP 739
Programación de Correo | Recolección MultiPOP 383

3.1.13 DomainPOP

Utilice la recolección de correo DomainPOP ("Configurar » Configuración de Servidor » DomainPOP") para configurar MDaemon para que descargue correo de un buzón POP remoto para redistribución a sus usuarios. Esta funcionalidad trabaja utilizando el protocolo POP3 para descargar todo el correo que se encuentra en el buzón POP del ISP asociado a un acceso (usuario) específico. Una vez recolectado, los mensajes son procesados de acuerdo con las configuraciones establecidas en este diálogo y luego colocados en los buzones de los usuarios o en la cola remota para que MDaemon los envíe, igual que si los mensajes llegaran al servidor utilizando las transacciones SMTP convencionales.

Es importante hacer notar que los mensajes almacenados en buzones y recolectados utilizando el protocolo POP3 estarán faltos de información importante de enrutado (algunas veces llamada el "sobre" del mensaje) que normalmente se proporcionaría si los mensajes se hubieran enviado utilizando el protocolo SMTP, más potente. Sin esta información de enrutado, MDaemon se ve forzado a "leer" el mensaje y examinar las cabeceras que muchas veces estarán notablemente faltas de la suficiente información necesaria para determinar el supuesto destinatario. Esta falta de lo que serían características fundamentales de un mensaje de correo - el recipiente o destinatario - puede ser sorprendente, pero uno debe tener en cuenta que el mensaje nunca se orientó a ser enviado a su destinatario a través de protocolo POP. Con SMTP, los contenidos del mensaje son irrelevantes puesto que el protocolo en sí mismo dicta específicamente al servidor, durante la transacción de correo, el supuesto destinatario del mensaje.

Para poder permitir la recolección POP y enviar luego los mensajes de una manera consistente y confiable, MDaemon emplea un potente juego de opciones de procesamiento de encabezados. Cuando MDaemon descarga un mensaje de un recurso remoto POP inmediatamente procesa toda la información relevante de los encabezados dentro del mensaje y construye una colección de destinatarios potenciales. Cada dirección de correo encontrada en los encabezados que MDaemon inspecciona se incluye en la colección.

Cuando este proceso se completa, la colección de destinatarios de MDaemon se divide en conjuntos locales y remotos. Además, las direcciones que son procesadas e insertadas en la colección como destinatarios potenciales se procesan a través del traductor de Alias 834 antes de ser divididos en conjuntos locales y remotos. Cada miembro del conjunto local (direcciones con uno de los dominios locales de MDaemon) recibirá una copia del mensaje. Lo que pasa con el conjunto remoto se

controla a través de las configuraciones de este diálogo. Puede seleccionar simplemente ignorar dichas direcciones, remitir una lista sumario de éstas al Postmaster o autorizarlas — en cual caso MDaemon enviará una copia del mensaje al destinatario remoto. Sólo bajo raras circunstancias se podrá garantizar la necesidad el envío a recipientes remotos.

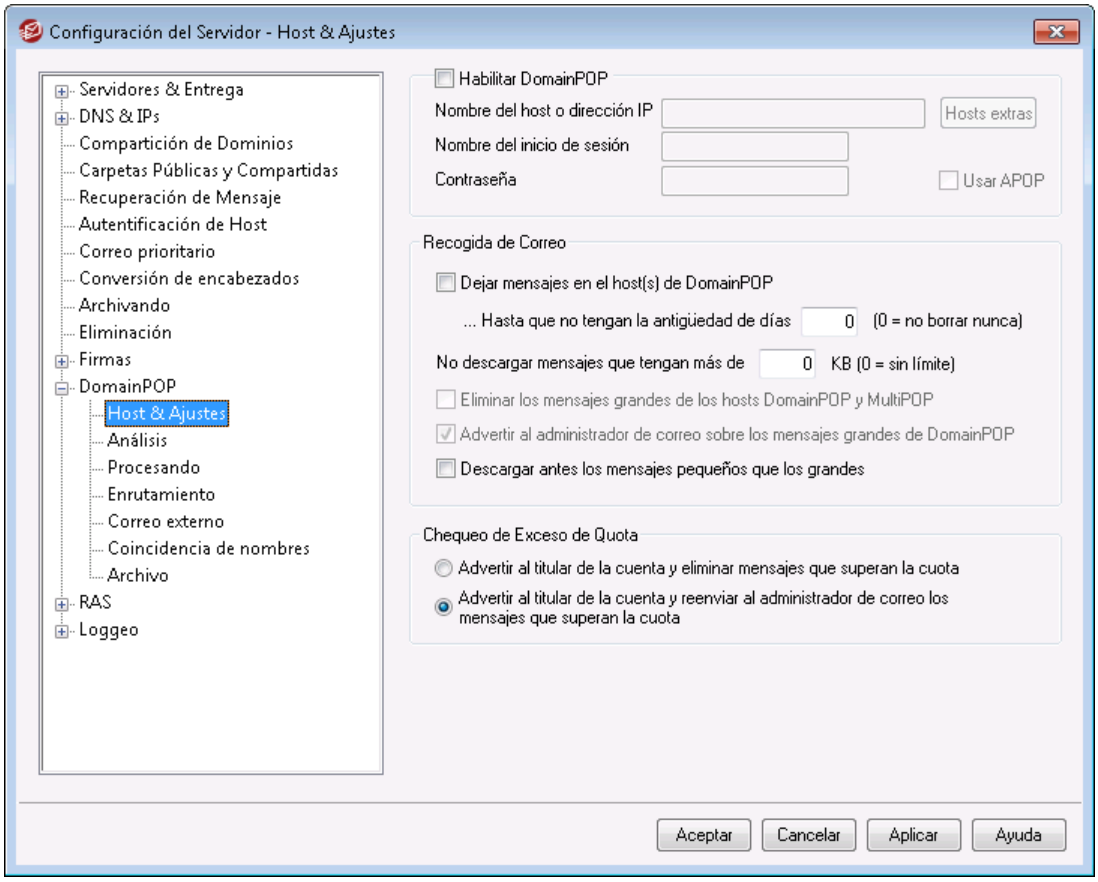
Se debe tener cuidado para prevenir mensajes duplicados o ciclos de envío en constantes bucles. Un problema común que resulta de la pérdida del sobre SMTP se manifiesta en sí mismo con la lista de correo. Típicamente, los mensajes distribuidos por una lista de correo no contienen dentro del cuerpo de mensaje ninguna referencia a las direcciones de los destinatarios. En su lugar, el motor de listas simplemente inserta el nombre de la lista de correo en el campo `TO:`. Esto representa un problema inmediato si el mensaje procesa el campo `TO:` (que contendrá el nombre de la lista de correo), y luego despacha los mensajes de vuelta a la misma lista de correo. Esto resultaría en el envío de otra copia del mismo mensaje nuevamente al buzón POP desde el cual MDaemon ha borrado el mensaje original — empezando pues el mismo ciclo repetidamente. Para afrontar con tales problemas los administradores deben tener cuidado de utilizar herramientas y configuraciones que provee MDaemon para o bien borrar el correo procedente de listas de distribución o probablemente alias de manera que sean enviados al correcto recipiente(s) local(es). También puede utilizar Reglas de Enrutado o Filtros de Contenido para enviar el mensaje a los destinatario(s) correcto(s).

Dudas adicionales cuando se emplea este tipo de esquema de recolección de correo giran en torno al hecho de la duplicación de mensajes no solicitados. Es muy sencillo para un correo que se ha enviado al buzón POP del ISP utilizando SMTP generar duplicados no solicitados, una vez ha sido recolectado utilizando DomainPOP. Por ejemplo, suponga que el mensaje se envía a alguien de su dominio y una copia se envía a otra persona del mismo dominio. En esta situación, SMTP enviará **dos** copias del mismo mensaje al buzón de su ISP — una para cada destinatario. Cada uno de los mensajes contendrán una referencia a los **dos** destinatarios, una en el campo `TO:` y otra en el campo `CC:`. MDaemon recolectará cada uno de estos dos mensajes idénticos y procesará las direcciones de correo contenidas en ellos. Ello resultará en que ambos destinatarios recibirán una copia adicional no solicitada del mensaje. Para protegerse contra este tipo de duplicaciones, MDaemon utiliza un control que le permite especificar un encabezado que MDaemon usará para comprobación de duplicación. El campo `Message-ID` es ideal para esto. En los ejemplos arriba mencionados, ambos mensajes son idénticos y por lo tanto tendrá el mismo valor en el campo `Message-ID`. MDaemon puede utilizar dicho valor para identificar y borrar el segundo mensaje durante la fase de descarga antes de que sea procesado para la información de direcciones.

Como medida final contra la duplicación de mensajes y los bucles de envío, MDaemon utiliza varios métodos para detectar cuantas vueltas o "saltos" ha hecho un mensaje a través del sistema de transporte. Cada vez que un servidor de correo SMTP procesa un mensaje, lo "estampa" con un encabezado "Received". MDaemon cuenta dichos encabezados cuando se encuentra por primera vez con un mensaje. Si el número total de servidores de correo excede el valor especificado, seguramente el mensaje está enganchado en un bucle de envío y debería ser sacado de la corriente de envío y movido al directorio de mensajes. Este valor se puede configurar a través de la Cola de Reintentos 872.

Filtros de Contenido 645
Listas de Distribución 274

3.1.13.1 Ajustes & Host



Propiedades del Host DomainPOP

Activar el motor de recolección de correo de DomainPOP
Si se selecciona, MDaemon usará las configuraciones proporcionadas en esta pantalla para recolectar correo de un host de correo DomainPOP para redistribución local.

Nombre del host o dirección IP
Introduzca el nombre de dominio de su host o dirección IP aquí.

Hosts extras
Haga clic en este botón para abrir el archivo `DpopXtra.dat`, donde puede designar hosts extras de los cuales recolectar correo DomainPOP. Vea el contenido de dicho archivo para más información.

Nombre del inicio de sesión
Introduzca sus credenciales de inicio de la cuenta POP usada por DomainPOP.

Contraseña
Introduzca la contraseña POP o APOP de la cuenta aquí.

Usar APOP
Haga clic en este cuadro si desea utilizar el comando APOP y autenticación CRAM-MD5 cuando solicite su correo. Esto posibilita autenticarse sin tener que enviar contraseñas en texto plano.

Recogida de Correo

Dejar mensaje en el host(s) de DomainPOP.
Si se selecciona, MDaemon descargará, pero no quitará, los mensajes de su host de correo DomainPOP.

...hasta que no tengan la antigüedad de días (0=no borrar nunca)
Este es el número de días que un mensaje puede estar en el host DomainPOP antes de ser borrado. Utilice "0" si no desea borrar los mensajes antiguos.

Algunos hosts pueden limitar el tiempo que está permitido almacenar los mensajes en su buzón.

No descargar mensajes que tengan más de [XX] KB (0 = sin límite)
Los mensajes mayores o iguales a este tamaño no se descargarán de su host de correo DomainPOP. Introduzca "0" si quiere que MDaemon descargue los mensajes independientemente del tamaño.

Eliminar los mensajes grandes de los hosts DomainPOP y MultiPOP
Activar esta opción hará que MDaemon borre los mensajes que excedan el tamaño designado en el cuadro anterior. Los mensajes simplemente se borrarán de los hosts de correo DomainPOP y MultiPOP y no serán descargados.

Advertir al administrador de correo sobre los mensajes grandes de DomainPOP
Seleccione esta opción si quiere que MDaemon envíe un aviso al Postmaster siempre que se descubran mensajes grandes en el buzón de DomainPOP.

Descargar antes los mensajes pequeños que los grandes
Active esta casilla de verificación si desea que el orden de la descarga de mensajes se base en el tamaño — empezando con el más pequeño y procediendo hasta el más grande.

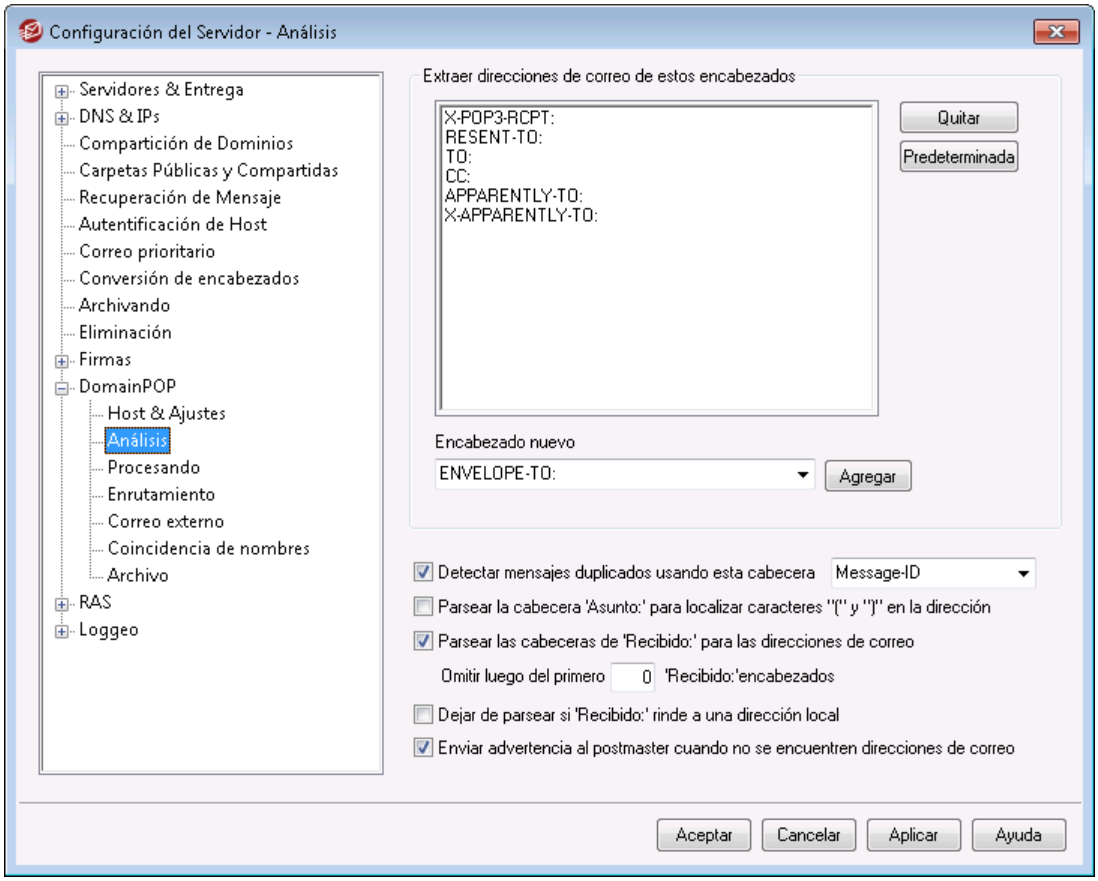
Esta opción recolecta antes los mensajes pequeños, pero requiere un mayor gasto interno de recursos para ordenación y procesamiento.

Chequeo de exceso de cuota

Advertir al titular de la cuenta y eliminar mensajes que superan la cuota
Cuando se escoge esta opción y un mensaje se recolecta de una cuenta que está por encima de la cuota (designada en la pantalla Cuotas 733 del editor de cuenta), MDaemon borrará el mensaje y luego enviará el mensaje al propietario de la cuenta indicando que la cuenta está por encima de su límite.

Advertir al titular de la cuenta y reenviar al administrador de correo los mensajes que superan la cuota
Cuando se escoge esta opción y el mensaje se recolecta de una cuenta que está por encima de su cuota, MDaemon remitirá el mensaje al Postmaster y enviará un aviso al usuario dejándole saber que su cuenta está por encima del límite.

3.1.13.2 Análisis



Analizar estos encabezados para las direcciones de correo electrónico
Esta área lista los encabezados que MDaemon analizará en un intento de extraer direcciones. Cada encabezado aquí listado se comprueba en busca de direcciones.

Quitar
Este botón quitará las entradas seleccionadas de la lista de encabezados.

Predeterminada
Este botón borrará los contenidos actuales de la lista de encabezados y añadirá la lista por defecto de MDaemon. Los encabezados por defecto son normalmente suficientes para extraer todas las direcciones del mensaje.

Nuevo encabezado
Introduzca el encabezado que desea añadir a la lista de encabezados.

Agregar
Después de especificar un encabezado en la opción *Nuevo Encabezado*, haga clic en este botón para añadirlo a la lista.

Detectar mensajes duplicados usando esta cabecera
Si esta opción se selecciona, MDaemon recordará el valor de los encabezados especificados y no procesará mensajes adicionales recogidos en el mismo ciclo de proceso que contengan un valor idéntico. El encabezado `Message-ID` es por defecto el encabezado usado en esta opción.

Parsear la cabecera 'Asunto:' para localizar caracteres "(" y ")"
Cuando se seleccione y MDaemon encuentre direcciones contenidas entre los caracteres "( )" en el encabezado "Subject:" del mensaje, esta dirección se añadirá a la lista de recipientes además de cualquier otra dirección descubierta.

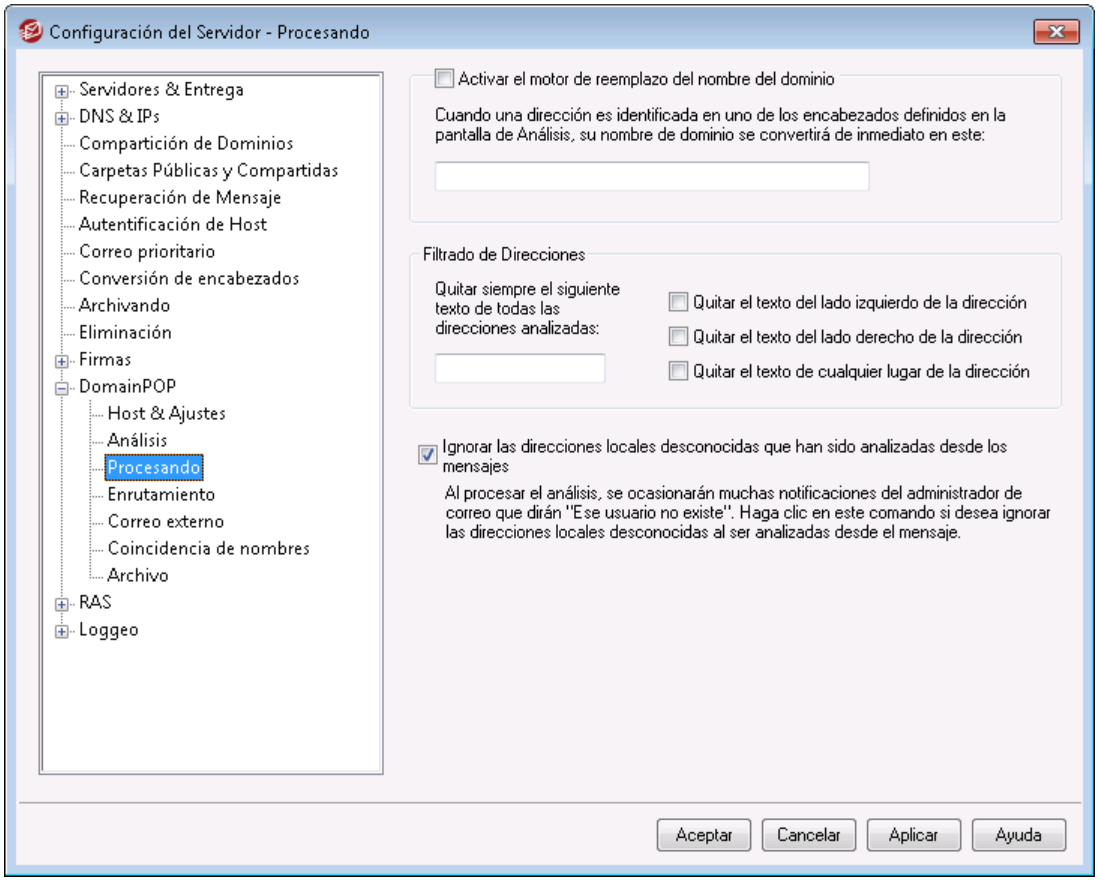
Parsear las cabeceras de "Recibido" para las direcciones de correo
Es posible guardar la información de los destinatarios encontrados normalmente sólo dentro del sobre mensaje en los encabezados de mensaje "Received". Esto hace posible que los analizadores del mensaje de correo puedan descubrir el destinatario real simplemente inspeccionando posteriormente los encabezados Received. Haga clic en esta casilla de verificación si desea analizar direcciones válidas de todos los encabezados "Received" encontradas dentro de un mensaje de correo.

Omitir el primero xx cabeceras "Recibido"
En algunas configuraciones puede que desee analizar los encabezados Received, pero necesite saltarse los primeros. Esta configuración le permite introducir el número de encabezados "Received" que MDaemon se saltará antes de empezar el análisis.

Dejar de parsear si 'Recibido' rinde a una dirección local
Si mientras se analiza el encabezado "Received" MDaemon detecta una dirección local válida, esta opción hará que los análisis subsiguientes paren y MDaemon no buscará en el mensaje más direcciones potenciales de destino.

Enviar aviso al postmaster cuando no se encuentren direcciones de correo
Por omisión, MDaemon envía un correo de advertencia al postmaster cuando no encuentra direcciones en el proceso de análisis. Deshabilite esta casilla si no desea que se envíe esta advertencia.

3.1.13.3 Procesando



Reemplazo de Nombre de Dominio

Activar el motor de reemplazo del nombre del dominio
Esta opción puede usarse para reducir el número de alias que su sitio pueda requerir. Cuando un mensaje se descargue, todos los nombres de dominio en todas las direcciones encontradas en dicho mensaje se convertirán a los nombres de dominio aquí especificados.

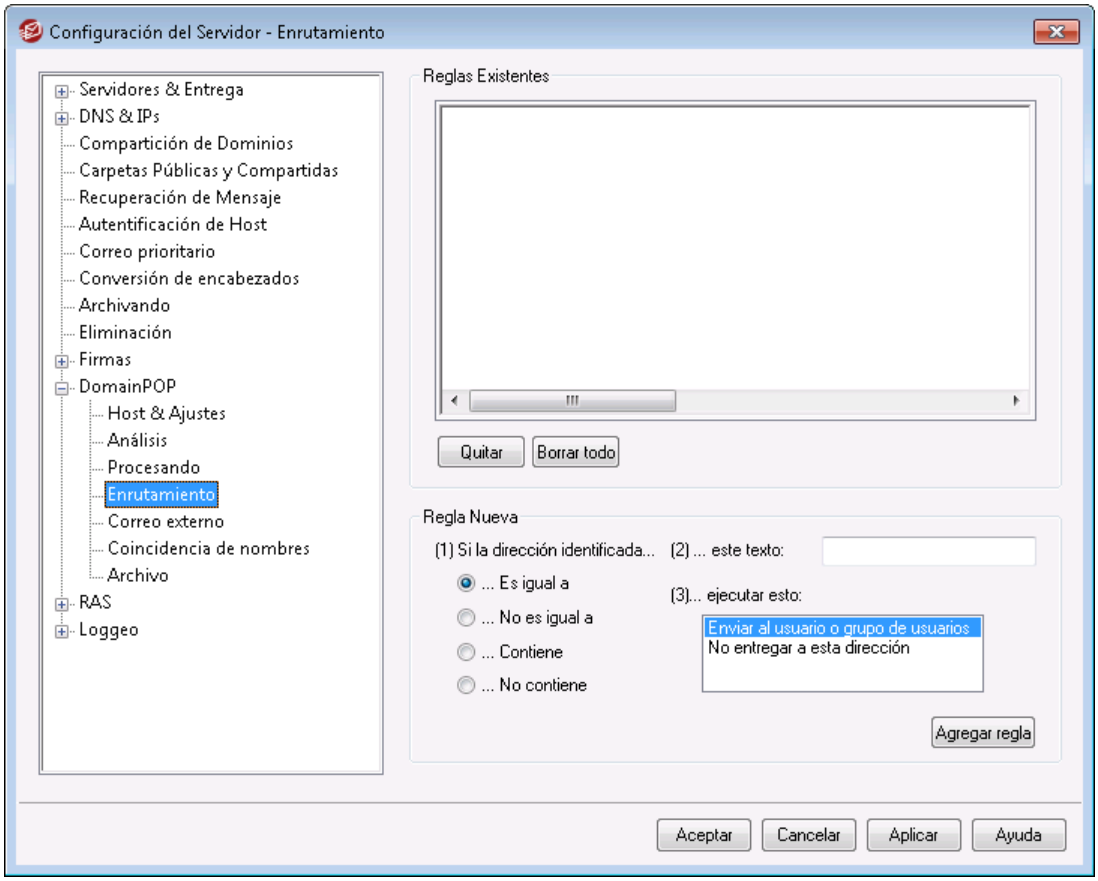
Filtrado de direcciones

Quitar siempre el siguiente texto de todas las direcciones analizadas
Algunos hosts estampan en cada mensaje una línea que indica quién debería ser el destinatario del mensaje, además de algo de información de enrutado agregada a la dirección bien en el lado izquierdo o derecho de ésta. Este sello sería perfecto para analizar la dirección de destino excepto que la información adicional de enrutado hace que sea imposible sin muchos alias de cuentas. En lugar de hacer eso, puede simplemente especificar el valor de este texto agregado y editar el control asociado con esta funcionalidad y MDaemon quitará cualquier aparición de dicho texto de todas las direcciones que analice.

Ignorar las direcciones locales desconocidas que han sido analizadas desde los mensajes
Como se menciona arriba, la funcionalidad de Reemplazo de Nombre de Dominio alterará el nombre de dominio en todas las direcciones de correo encontradas en

un mensaje, convirtiéndolas en el que se especifique en esta pantalla. Esto creará algunas direcciones que no tienen una cuenta correspondiente en su servidor. Dado que el dominio, pero no el buzón sería válido, MDaemon considerará dichas direcciones como usuarios locales desconocidos. Dichos mensajes típicamente generan un mensaje de "Usuario Inexistente". Marque esta casilla si desea prevenir que el Motor de Reemplazo de Nombres de dominio provoque que estos mensajes se generen.

3.1.13.4 Enrutamiento



Reglas Existentes

Esta lista muestra las reglas que se hayan creado y que serán aplicadas a sus mensajes.

Quitar

Selecciones una regla de la lista y luego haga clic en este botón para eliminarla.

Borrar todo

Este botón borra todas las reglas existentes.

Nueva regla

(1) Si la dirección parseada...

Es igual a, no es igual a, contiene, no contiene
Este es el tipo de comparación que se realizará cuando una dirección se compare con esta regla de enrutamiento. MDaemon buscará en cada dirección el texto contenido en el cuadro de opción *"...este texto*" y será luego procesado según la configuración escogida — ¿la dirección encaja completamente, no completamente, contiene el texto o no lo contiene en absoluto?

(2) ...Este texto:
Introduzca el texto que quiere que MDaemon busque cuando haga el escaneo de direcciones.

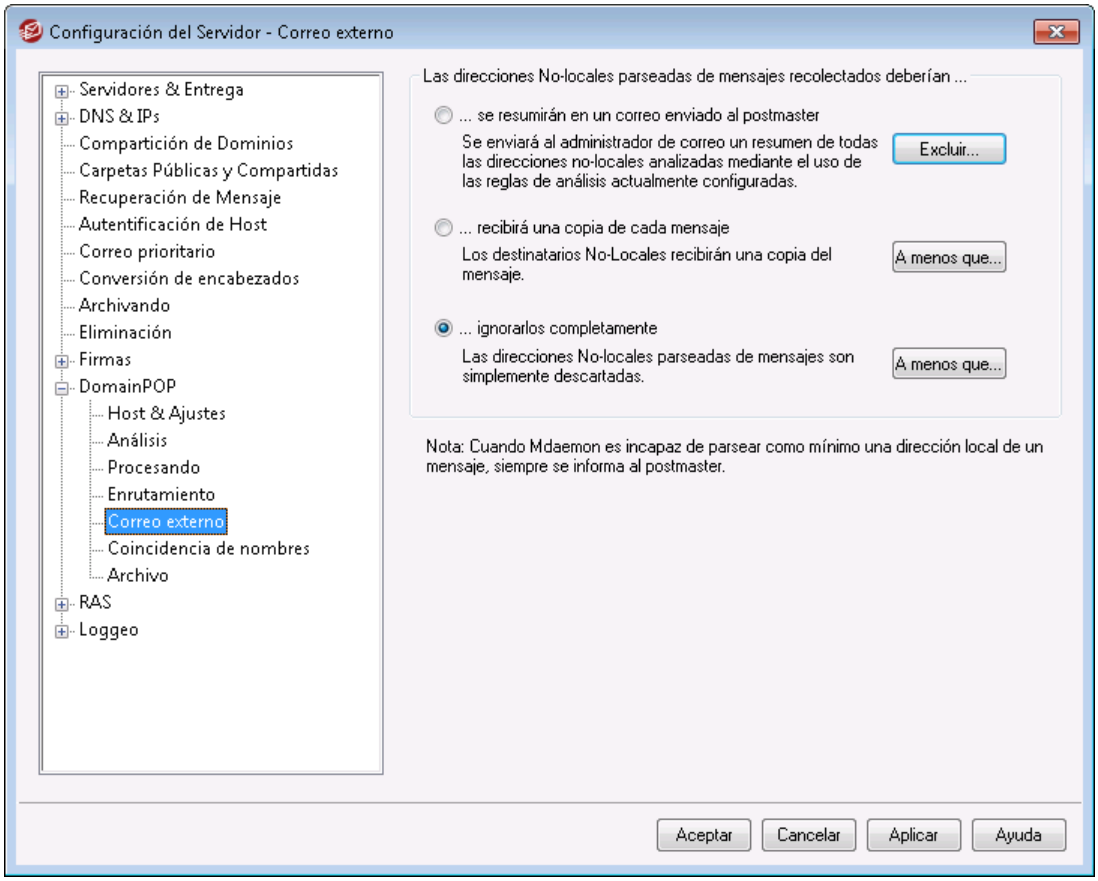
(3) ...Entonces hacer esto:
Esta opción muestra las acciones disponibles que se pueden ejecutar si el resultado es verdadero. Puede escoger de las siguientes acciones:

No entregar a esta dirección - Si selecciona esta opción se evitará que el mensaje sea enviado a la dirección especificada.

Enviar al usuario o grupo de usuarios - Si se selecciona esta acción se abrirá un diálogo en el cual se puede designar una lista de direcciones de correo que deben recibir una copia del mensaje que está siendo procesado.

Agregar regla
Después de establecer nuevos parámetros de reglas, haga clic en *Añadir regla* para añadirla a la lista de reglas.

3.1.13.5 Correo Externo



Las direcciones no-locales parseadas de mensajes recolectados deberían...

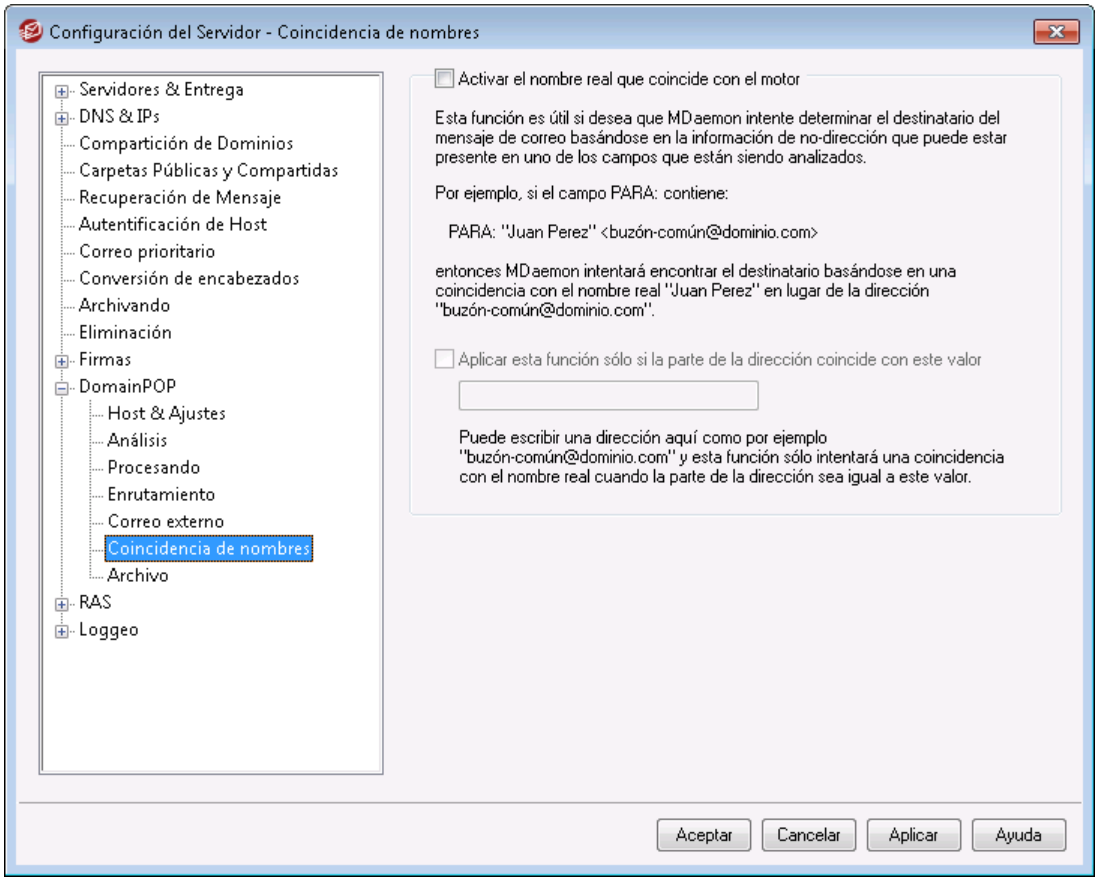
...se resumirán en un correo enviado al postmaster
Si se selecciona esta opción MDaemon enviará una única copia del mensaje al postmaster juntamente con un resumen de las direcciones no-locales que el motor de procesa ha extraído utilizando las reglas de análisis y encabezados actuales.

...recibirá una copia de cada mensaje
Si se selecciona esta opción MDaemon enviará una copia del mensaje a cualquier destinatario no-local que se encuentre en los encabezados inspeccionados.

...ignorarlos completamente
Si esta opción se selecciona MDaemon borrará de la lista de destinatarios cualquier dirección que no sea local. Será como si MDaemon nunca hubiera analizado las direcciones remotas del mensaje descargado original.

Los botones *Excluir...* y *A menos que...* le permiten definir direcciones que serán tratadas como excepciones para la opción seleccionada.

3.1.13.6 Coincidencia de Nombres



La funcionalidad de Coincidencia de Nombres sólo se activa junto con el motor de Recolección de Correo DomainPOP. Si desea utilizar esta funcionalidad, debe asegurarse que tiene DomainPOP activado. DomainPOP puede accederse a través de la selección de menú "Configurar » Configuración de Servidor » DomainPOP".

Motor de Coincidencia de Nombres Reales

Activar el nombre real que coincide con el motor
Esta funcionalidad permite que MDaemon determine quién debería recibir un mensaje recolectado de DomainPOP basándose no en la dirección de correo extraída sino en el texto incluido con la dirección. Normalmente suele ser el nombre real del destinatario.

Por ejemplo, un encabezado TO podría ser:

```
TO: "Michael Mason" <usuario01@ejemplo.com>
```

o

```
TO: Michael Mason <usuario01@ejemplo.com>
```

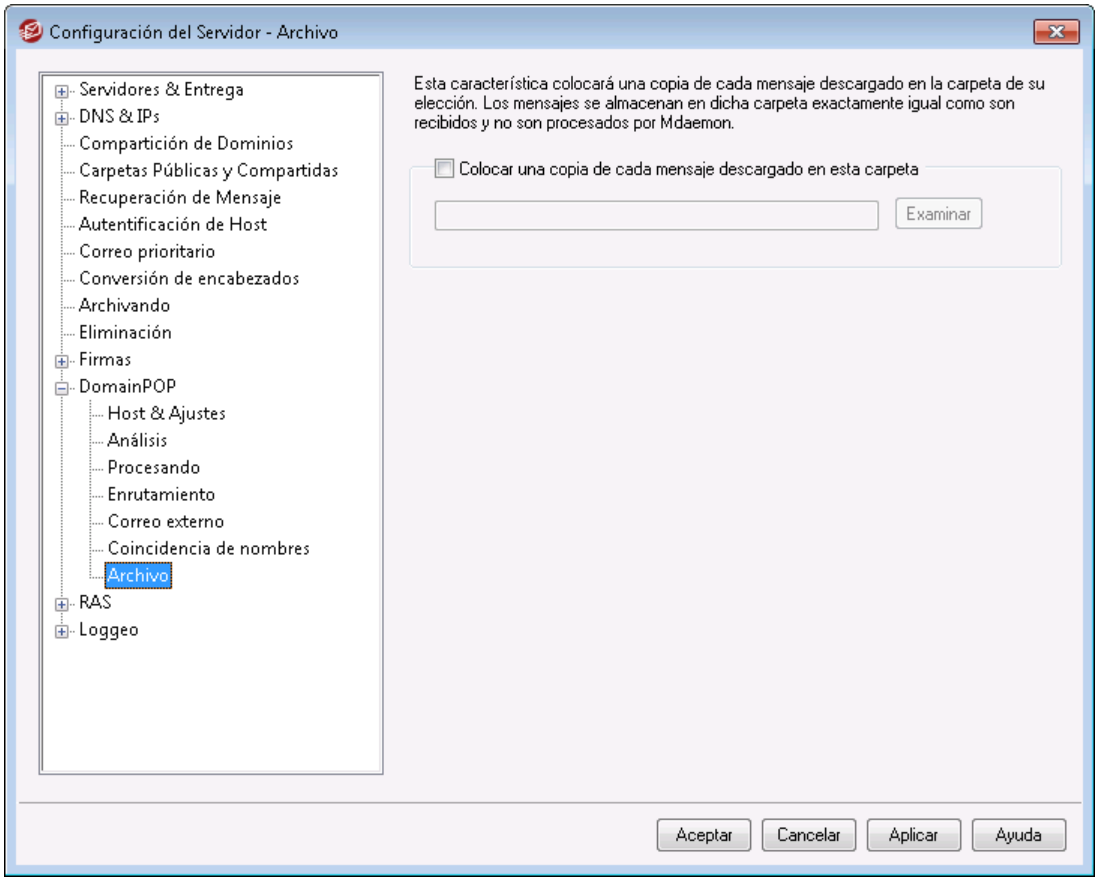
La coincidencia de nombres ignora la porción "usuario01@ejemplo.com" de la dirección. En su lugar extrae la porción "Michael Mason" y comprueba si es un usuario de MDaemon. Si se encuentra una coincidencia para el nombre real de una cuenta entonces dicha cuenta local se usa para propósitos de envío. Si no se encuentra coincidencia, entonces MDaemon vuelve a utilizar la opción de enviar el mensaje a la dirección extraída de los datos (usuario01@ejemplo.com en este ejemplo).

La porción de la dirección con el nombre real no debe contener comas, puntos o dos puntos.

Aplicar esta función solo si la parte de la dirección coincide con este valor
Esta opción permite especificar una dirección de correo que debe encontrarse presente en los datos extraídos para que el proceso de coincidencia de nombres proceda. Esto permite agregar una medida de control cuando se use la funcionalidad de Coincidencia de Nombres. Por ejemplo, puede especificar una dirección tal como "usuario01@ejemplo.com" y entonces solamente las direcciones que coincidan con dicho valor serán candidatos para la coincidencia de nombres.

Suponga que especifica "usuario01@ejemplo.com" en esta opción. Esto significa que "**`TO: 'Michael Mason' <usuario01@ejemplo.com>`**" será un candidato para la coincidencia de nombres mientras que "**`TO: 'Michael Mason' <usuario02@ejemplo.com>`** no lo será.

3.1.13.7 Archivo

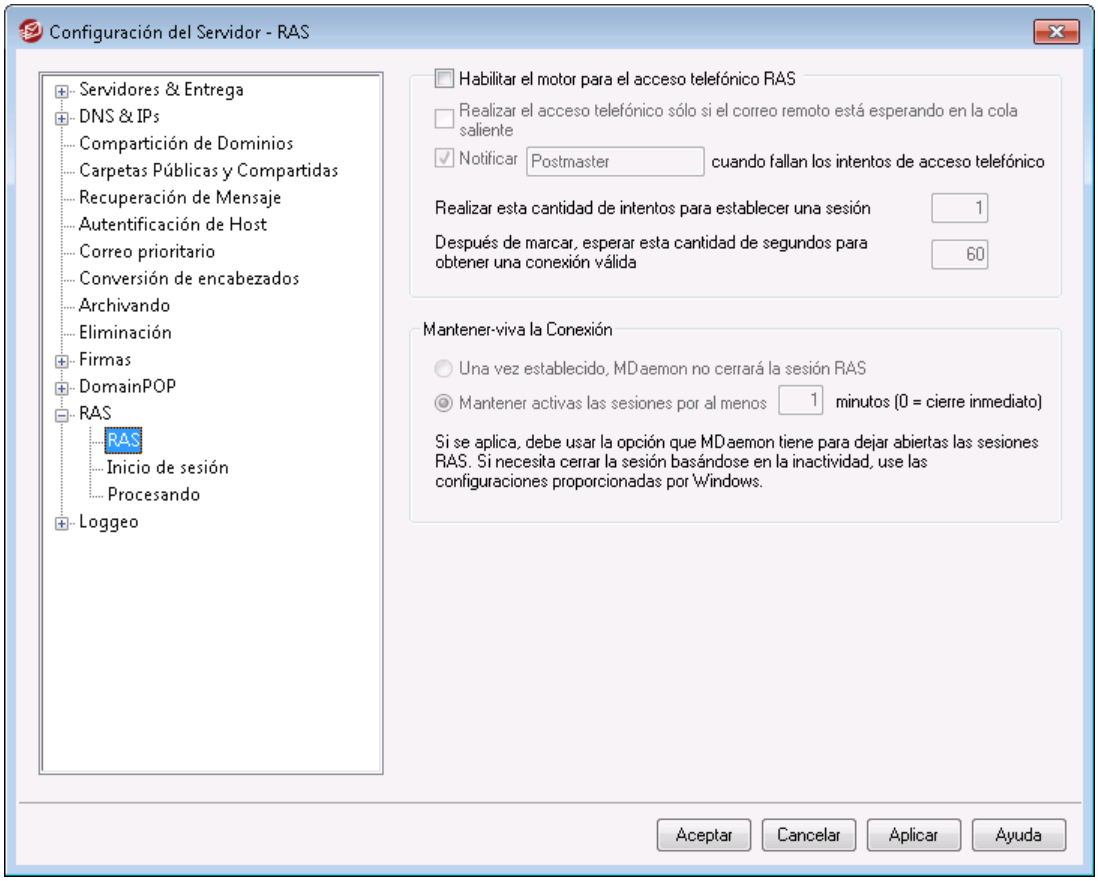


Archivo

Colocar una copia de cada mensaje descargado en esta carpeta
Esta es una medida de seguridad para asegurar que no se pierda ningún correo debido a direcciones no extraídas y que no se pierda ningún correo por otros errores que puedan ocurrir cuando se descarga correo en cantidades por bloque. Selecciones esta casilla si desea guardar una copia de cada mensaje descargado en la carpeta que se especifique. Estas copias se colocan en la carpeta exactamente como se reciben y no se procesan en absoluto por parte de MDaemon.

3.1.14 RAS

3.1.14.1 RAS



Dé clic en "Configurar » Configuración de Servidor » RAS" para configurar los parámetros de marcación RAS. Esta pantalla solo estará disponible si tiene instalados servicios RAS (Remote Access Services) en su sistema. Se utiliza por MDaemon cuando necesita marcar a su ISP antes de un evento de procesamiento de Correo Remoto.

Habilitar el motor para el acceso telefónico RAS
Cuando esta opción se encuentra habilitada, MDaemon usará las configuraciones especificadas aquí para realizar una conexión a un host remoto antes de enviar o recibir correo remoto.

Realizar el acceso telefónico sólo si el correo remoto está esperando en la cola saliente
Cuando esta casilla está marcada, MDaemon no marcará al ISP a menos que haya correo remoto esperando en la cola Remota. Esto puede ser beneficioso en algunas circunstancias, pero sea consciente que si MDaemon no marca entonces tampoco puede hacer ninguna **recolección** (a menos que se envíe a través de la LAN local).

Notificar [dirección] cuando fallan los intentos de acceso telefónico
Cuando se seleccione, MDaemon enviará un mensaje a la dirección especificada cuando un evento de marcación falle por causa de algún error.

Realizar esta cantidad de intentos para establecer una sesión
MDaemon intentará conectar al host remoto este número de veces antes de rendirse.

Después de marcar, esperar esta cantidad de segundos para obtener una conexión válida
Este valor determina cuánto tiempo esperará MDaemon para que el ordenador remoto complete la conexión RAS.

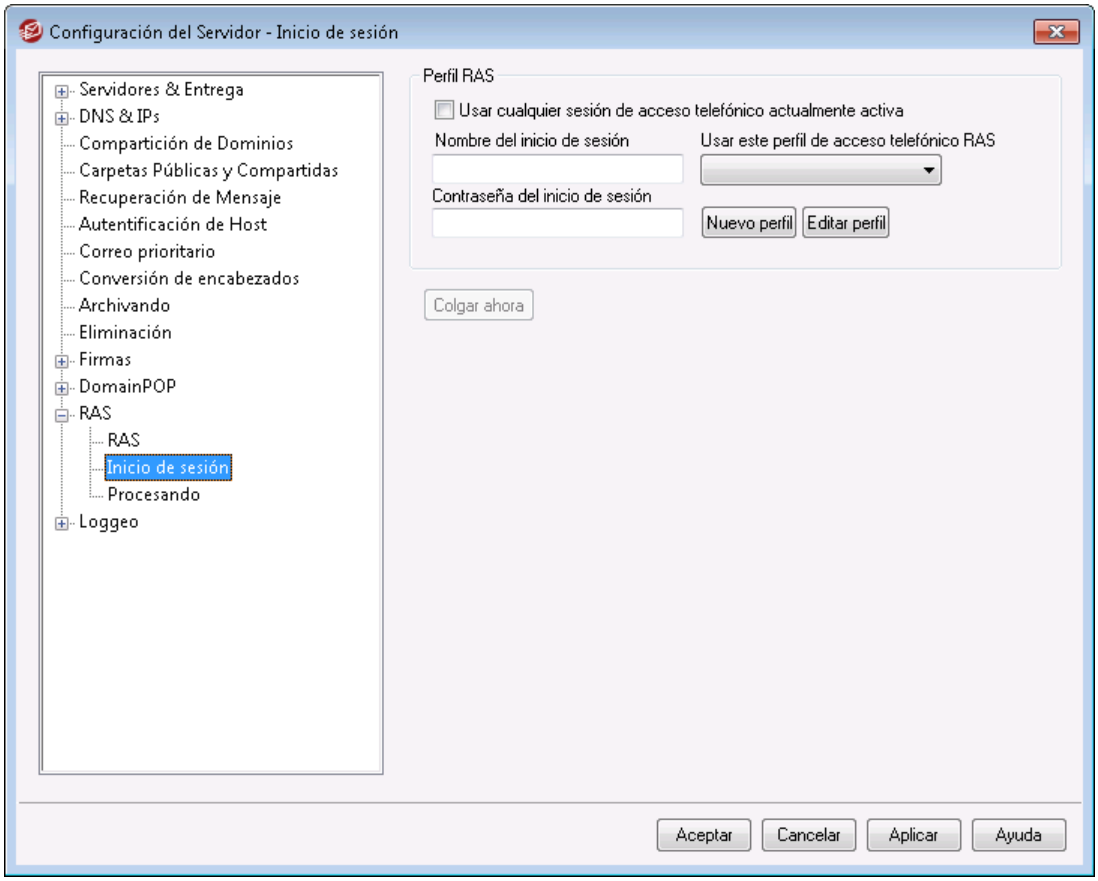
Mantener-viva la conexión

Una vez establecido, MDaemon no cerrará la sesión RAS
Por defecto, MDaemon cerrará la conexión creada inmediatamente después de haber completado todas las transacciones de correo y la sesión ya no esté en uso. Si se selecciona esta opción se causará que la conexión se mantenga abierta incluso después de que las transacciones hayan sido completadas.

MDaemon nunca cerrará una conexión que no haya sido creada por él.

Mantener activas las sesiones por al menos xx minutos
Si se activa, esta opción hará que una sesión RAS creada por MDaemon permanezca abierta al menos esta cantidad de minutos especificada o hasta que todas las transacciones de correo hayan sido completadas, lo que sea superior.

3.1.14.2 Inicio de sesión



Perfil RAS

Usar cualquier sesión de acceso telefónico actualmente activa
Haga clic en esta casilla si desea que MDaemon pueda utilizar otros perfiles de conexión cuando detecte que existe uno activo. Siempre que sea momento de marcar, MDaemon comprobará primero si existe una conexión activa que pueda utilizar en lugar de ejecutar una nueva marcación.

Nombre del inicio de sesión
El valor especificado aquí se usa para identificar el nombre de inicio de sesión que será pasado al host remoto durante el proceso de autenticación.

Contraseña de inicio de sesión
El valor aquí especificado es la contraseña que se le pasará al host remoto durante el proceso de autenticación.

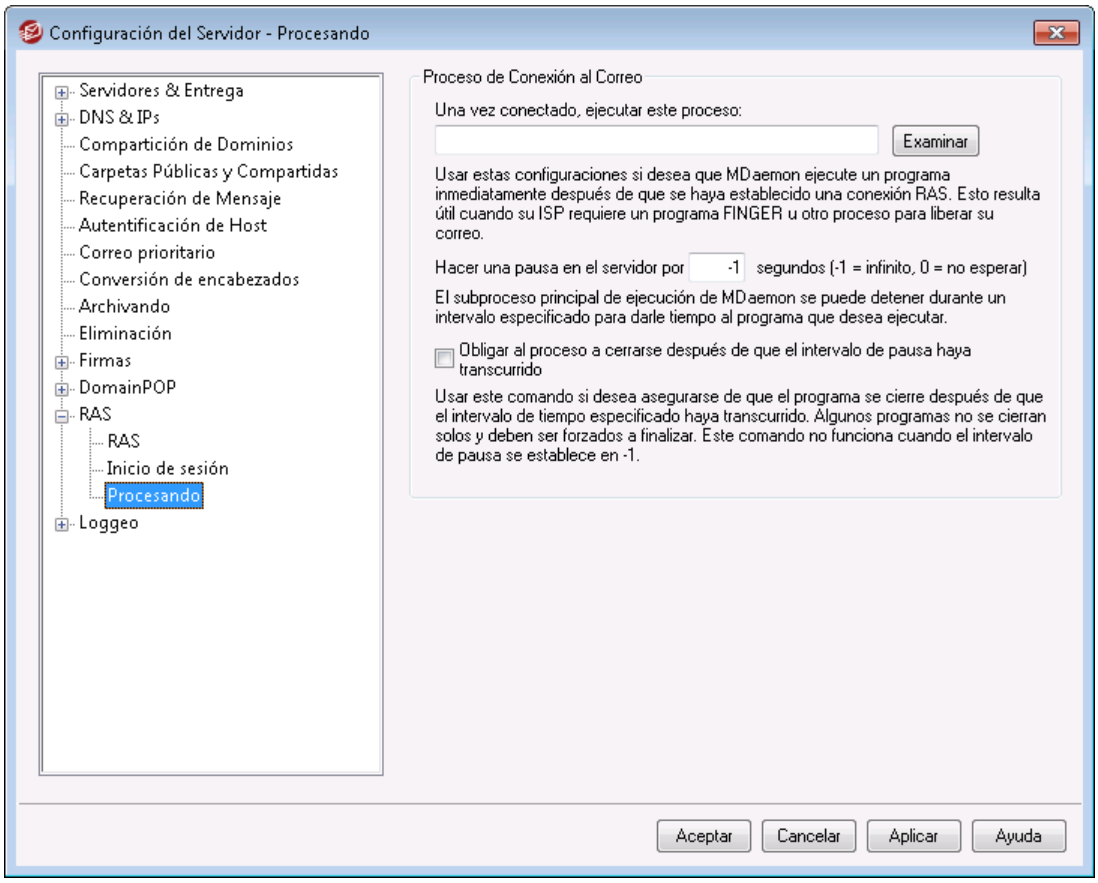
Usar este perfil de acceso telefónico RAS
Esta lista desplegable le permite seleccionar un perfil de sesión que se haya definido previamente a través de la Marcación de Red de Windows o la Configuración de Servicios de Acceso Remoto.

Nuevo perfil
Haga clic en este botón para crear un nuevo perfil de Marcación de Red de Windows o Configuración de Servicios de Acceso Remoto.

Editar perfil
Haga clic en este botón para editar el perfil actualmente seleccionado de Marcación de Red de Windows o la Configuración de Servicios de Acceso Remoto.

Colgar ahora
Este botón cerrará la conexión al ISP. Este botón sólo está activo cuando MDaemon ha iniciado una sesión RAS.

3.1.14.3 Procesando



Proceso de conexión al correo

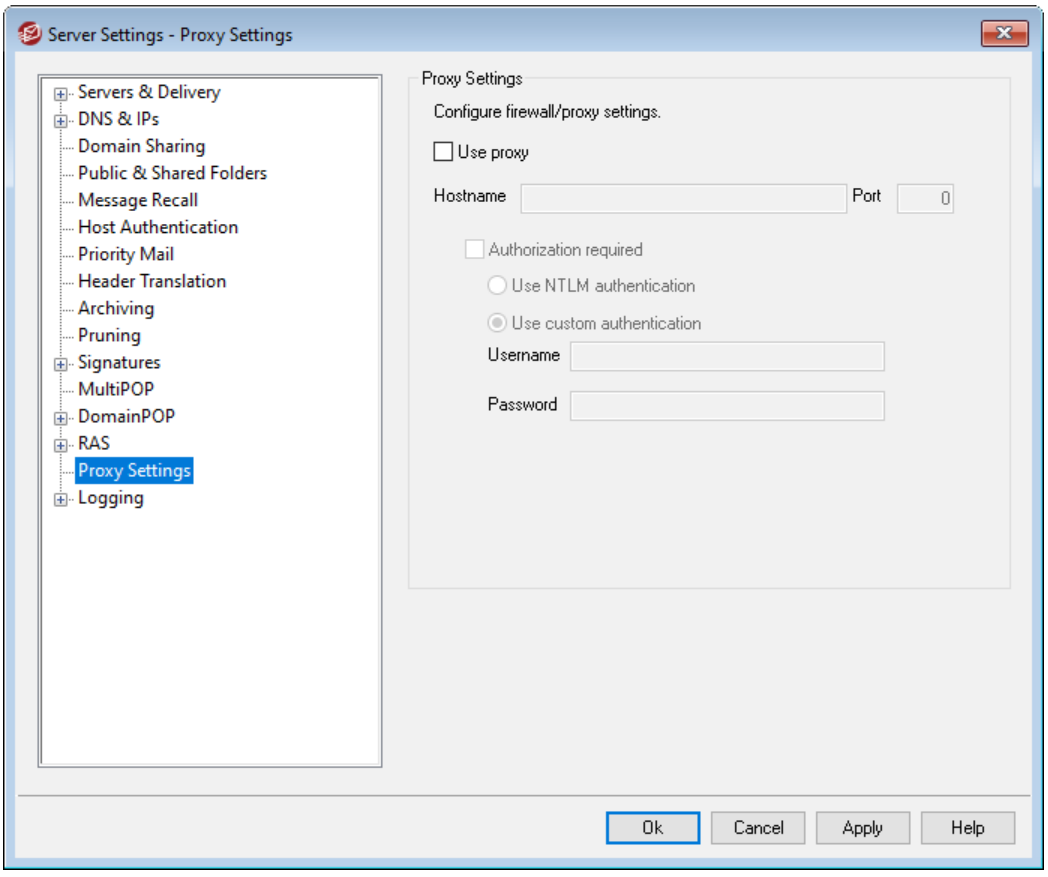
Una vez conectado, ejecutar este proceso:
Si se especifica aquí un programa, MDaemon creará un hilo y ejecutará el proceso. Esto es útil para aquellos que requieran el uso de `Finger` u otro programa para desbloquear el buzón del ISP.

Hacer una pausa en el servidor por xx segundos (-1 = infinito, 0=no esperar)
Si el control *Una vez conectado, ejecutar este proceso* contiene una entrada válida entonces el servidor pausará sus operaciones durante el número de minutos aquí especificado mientras espera al proceso que se esté ejecutando

retorne. Si introduce "-1" ello hará que el servidor espere indefinidamente a que el proceso retorne.

Obligar al proceso a cerrarse después de que el intervalo de pausa hay transcurrido
Algunas veces el programa que se necesita ejecutar puede que no finalice cuando haya completado su función; algunos programas requieren intervención del usuario para poder cerrarse. Ello no es aceptable cuando el software debe ejecutarse de modo desatendido. Si esta opción se selecciona, MDaemon forzará al hilo de proceso a terminar una vez haya pasado el número de segundos especificados en *Hacer una pausa en el servidor por xx segundos*. Esta función no funciona cuando el servidor se configura para esperar indefinidamente a que el proceso retorne.

3.1.15 Proxy Settings

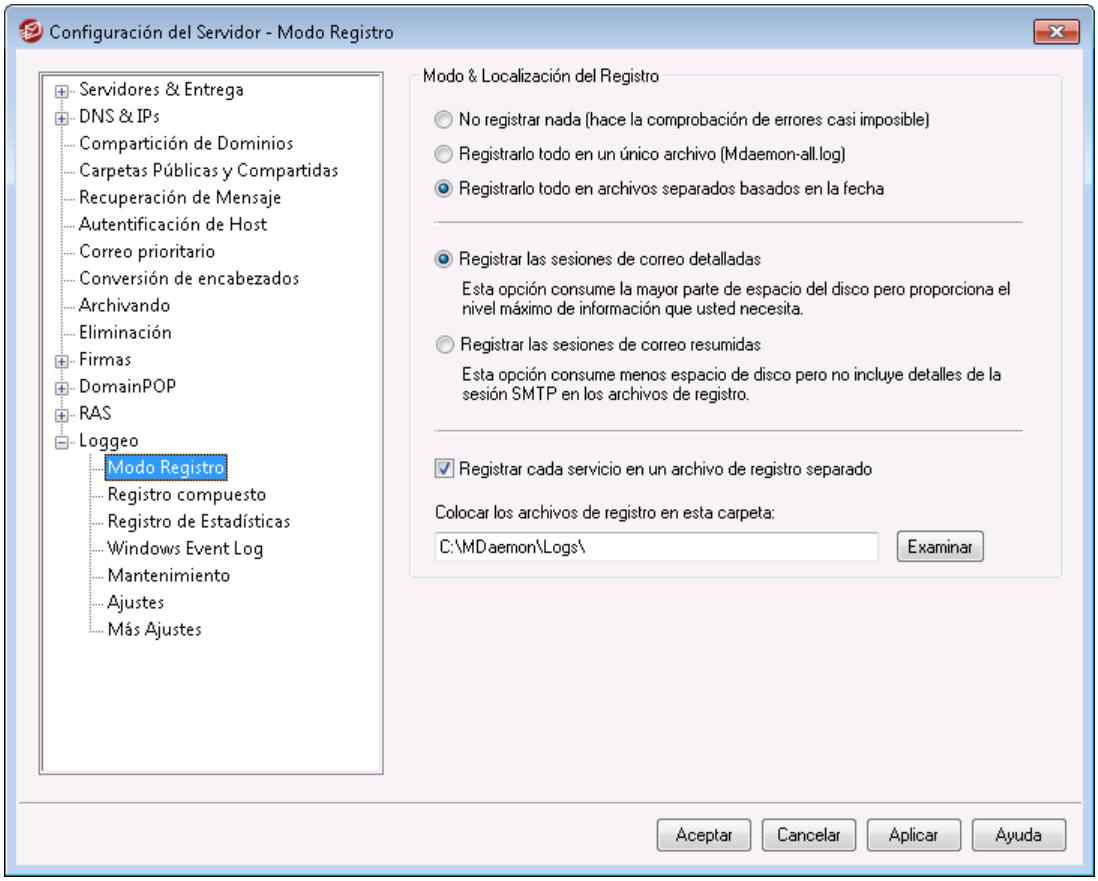


Ajustes de Proxy

Si está ejecutando MDaemon tras un cortafuegos o servidor proxy, puede utilizar este diálogo para configurar MDaemon para que utilice el proxy cuando sea necesario para hacer varias peticiones http, tales como cuando se verifican actualizaciones del Antivirus o se ejecutan otras tareas de mantenimiento normales. El diálogo de Ajustes de Proxy da opciones para registrar el nombre de host del servidor proxy y el puerto y si se requiere autenticación, puede elegir entre utilizar la autenticación NTLM de Windows o autenticación personalizada, ingresando el nombre de usuario y contraseña.

3.1.16 Loggeo

3.1.16.1 Modo Registro



Dé clic en "Configurar » Configuración de Servidor » logueo" para configurar los parámetros de registro. El registro en bitácoras es una herramienta útil para diagnosticar problemas y visualizar qué ha estado haciendo el servidor cuando no se le ha atendido.

Existen varias opciones en el diálogo de Preferencias que gobiernan la cantidad de datos de registro que se muestra en el panel de Registro de Eventos de la interfaz principal de MDaemon. Para más información, vea Preferencias » UI 491.

Modo & Localización del Registro

No registrar nada
Escoger esta opción desactivará todo el proceso de registro. Los archivos de registro se seguirán creando, pero no se escribirán datos en ellos.

No se recomienda esta opción. Sin registros puede ser extremadamente difícil, sino imposible, diagnosticar o

depurar cualquier problema potencial relacionado con el correo que usted pueda encontrarse.

Registrar todo en un archivo único (MDaemon-all.log)
Escoja esta opción si desea registrar todo en un único archivo separado llamado `MDaemon-all.log`.

Registrar todo en archivos separados basados en la fecha
Si se selecciona esta opción un archivo de registro separado se generará para cada día. El nombre del archivo corresponderá a la fecha en la que fue creado.

Registrar sesiones de correo detalladas
Cuando se active esta opción, se copiará una transcripción detallada de cada transacción en cada sesión, en el archivo de registro.

Registrar sesiones de correo resumidas
Esta opción hace que se copie en el archivo de registro una transcripción resumida de cada transacción de correo.

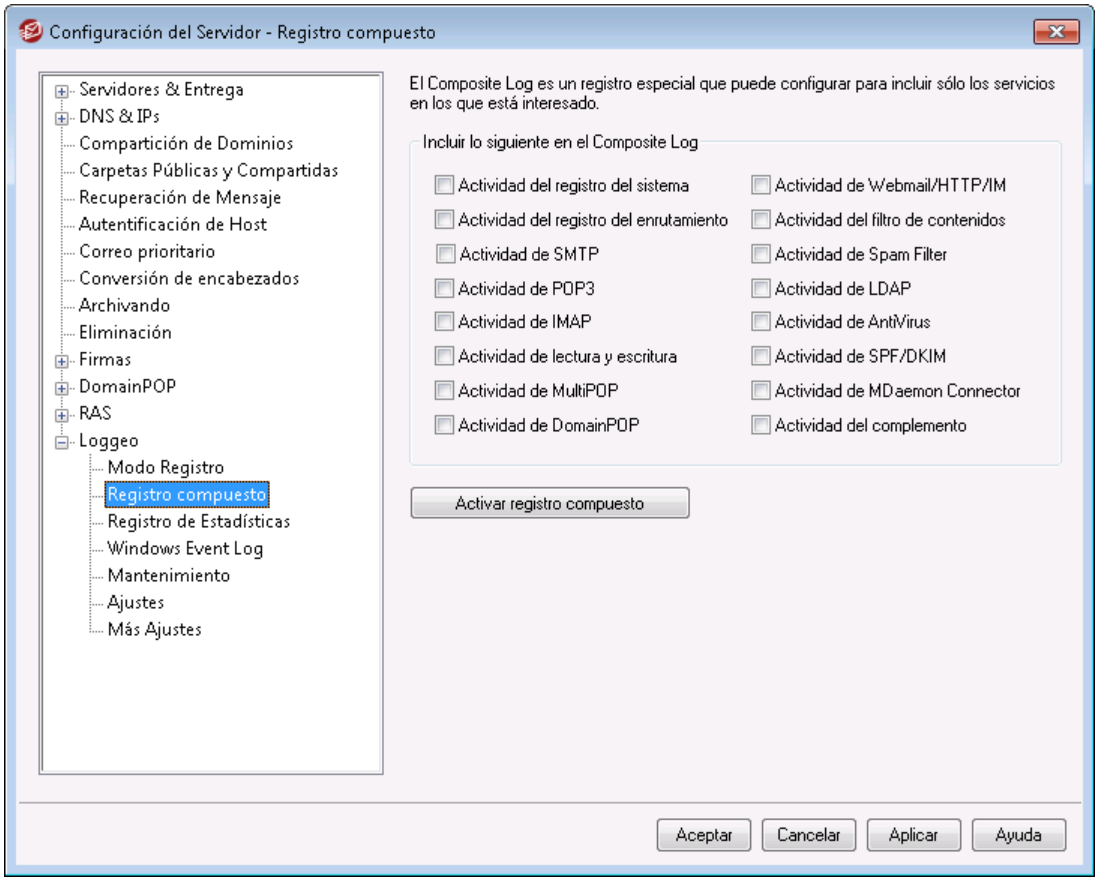
Registrar cada servicio en un archivo separado
Haga clic en esta casilla para hacer que MDaemon mantenga registros separados por servicio en lugar de en un sólo archivo. Por ejemplo, con este interruptor activado, MDaemon registrará la actividad SMTP en el archivo `MDaemon-SMTP.log` y la actividad IMAP en el archivo `MDaemon-IMAP.log`. Cuando se ejecute una instancia de Sesión de Configuración o Servicios de Terminal en la interfaz de MDaemon, esta opción debe estar seleccionada para que las pestañas de la interfaz muestren la información registrada.

Colocar los archivos de registro en esta carpeta:
Utilice esta opción si desea designar una carpeta específica para sus archivos de registro.

El archivo BadAddress.txt

Además de los archivos de registro, MDaemon mantiene el archivo `BadAddress.txt` en la carpeta de logs. Cuando la entrega hacia una dirección genera un error 5xx, la dirección se agregará a este archivo. Esto le puede ayudar, por ejemplo, a identificar más rápidamente direcciones erróneas en sus listas de distribución en lugar de buscar en los registros de SMTP saliente. Este archivo se elimina automáticamente en los procesos de depuración de media noche para impedir que crezca demasiado.

3.1.16.2 Registro Compuesto



Registro Compuesto

Incluir lo siguiente en el Registro Compuesto
Localizado en el menú Ventanas de la barra de menú de MDaemon se encuentra la opción Vista de Registro Compuesto. Si hace clic en dicha opción se añadirá a la pantalla principal de MDaemon una ventana que combinará la información mostrada en uno o más de las pestañas de Seguimiento de Eventos. Utilice los controles en esta sección para designar qué información de las pestañas se combinará en dicha ventana. La información contenida en las siguientes pestañas puede ser combinada:

Sistema—Muestra las actividades de sistema de MDaemon tales como la inicialización de servicios y si están habilitados/deshabilitados cualquiera de los diversos servidores de MDaemon.

Enrutamiento—Muestra la información de enrutado (De, Para, ID de Mensaje, y demás) para cada mensaje que sea procesado por MDaemon.

SMTP—Toda la actividad de envío/recepción de MDaemon que utilice el protocolo SMTP será mostrada.

POP3—Cuando los usuarios recolectan correo de MDaemon utilizando el protocolo POP3, dicha actividad será registrada.

IMAP—Las sesiones de correo que utilicen protocolo IMAP serán registradas.

RAW—La actividad de mensajes de sistema o RAW será registrada.

MultiPOP—Muestra las actividades de recolección de correo MultiPOP de MDaemon.

DomainPOP—Muestra la actividad de MultiPOP de MDaemon.

Webmail/HTTP/IM—Muestra toda la actividad de WorldClient y mensajería instantánea.

Filtro de Contenidos—Se listan las operaciones de Filtro de Contenidos de MDaemon.

Spam Filter—Muestra toda la actividad del Filtro de Spam.

LDAP—Muestra la actividad de LDAP.

Antivirus—Las operaciones de Antivirus se muestran en la vista compuesta.

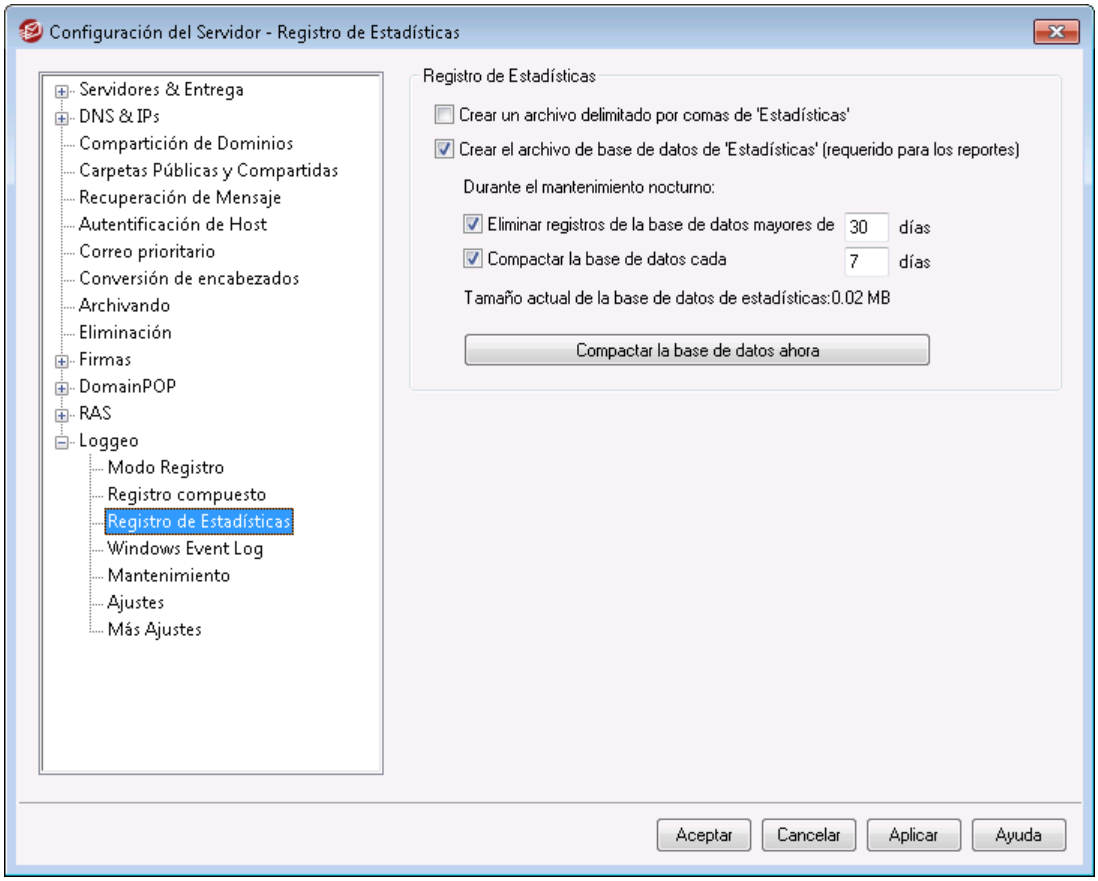
SPF/DKIM—Muestra toda la actividad de Sender Policy Framework y DKIM.

MDaemon Connector—Muestra toda la actividad de Outlook Connector.

Actividad de complementos—Registra todas las actividades de los complementos de MDaemon en el Registro Compuesto.

Activar registro compuesto
Haga clic en este botón para lanzar la ventana de registro compuesto en la pantalla principal de MDaemon. También se puede activar desde el menú Ventanas en la barra de menú de MDaemon.

3.1.16.3 Registro de Estadísticas



Registro de Estadísticas

Crear archivo de "Estadísticas" delimitado por comas
Utilice esta opción si desea mantener un archivo (delimitado por comas) de Estadísticas, conteniendo datos sobre el número de mensajes entrantes y salientes procesados, estadísticas de Spam, del antivirus y demás. Esta opción se encuentra deshabilitada por omisión.

Crear un archivo de base de datos de "Estadísticas" (requerido para los reportes)
Seleccione esta casilla si desea registrar información estadística sobre la actividad de MDaemon en un archivo de base de datos tipo SQLite. La base de datos contiene información sobre el uso de ancho de banda de MDaemon, número de mensajes entrantes y salientes, estadísticas de Spam y demás. Por omisión esta base de datos se encuentra almacenada en la carpeta "`MDaemon\StatsDB`" y se conservan 30 días de datos, pero es posible ajustar cuanta información desea conservar si quiere retener más o menos que los 30 días por omisión. Los datos mayores del límite designado serán eliminados durante los procesos nocturnos de mantenimiento. También puede especificar la frecuencia con la que MDaemon compactará la base de datos para conservar espacio.

La página de Reportes en la interface web de la Administración Remota de MDaemon utiliza esta base de datos para generar una variedad de reportes disponibles para los Administradores Globales. Para cada reporte, se pueden generar datos para varios rangos de fecha predeterminados o el administrador puede especificar un rango personalizado. Los Administradores pueden elegir entre los reportes siguientes:

- Reportes mejorados de ancho de banda
- Mensajes Entrantes y Salientes
- Mensajes correctos vs basura (porcentaje de correo que es Spam o algún virus)
- Mensajes entrantes procesados
- Principales destinatarios por número de mensajes
- Principales destinatarios por tamaño de mensajes
- Mensajes salientes procesados
- Principales fuentes de Spam (dominios)
- Principales receptores de Spam
- Virus bloqueados, por hora
- Virus bloqueados, por nombre

Durante el mantenimiento nocturno:
Las opciones siguientes controlan qué tareas relacionadas a la base de datos ejecutará MDaemon durante el proceso de mantenimiento nocturno.

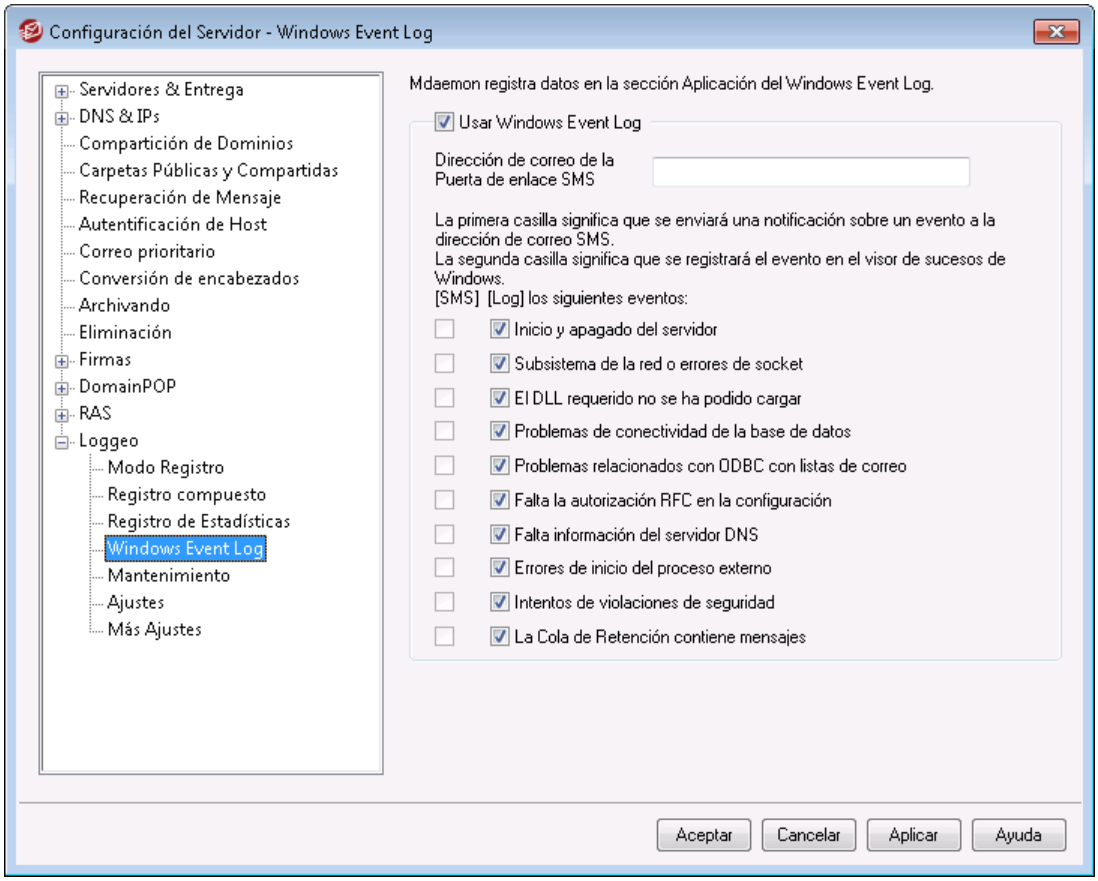
Eliminar registros de la base de datos mayores de [xx] días
Utilice esta opción para definir el número de días de registros en la base de datos de estadísticas que desea conservar. Por omisión esta opción está habilitada y configurada a 30 días.

Compactar la base de datos cada [xx] días
Utilice esta opción si desea compactar periódicamente la base de datos para conservar espacio. Por omisión esta opción está habilitada y configurada para compactar la base de datos cada 7 días.

Tamaño actual de la base de datos de estadísticas:
Aquí se muestra el tamaño actual de su base de datos de estadísticas.

Compactar la base de datos ahora
Dé clic en este botón para compactar inmediatamente la base de datos.

3.1.16.4 Registro de Eventos de Windows



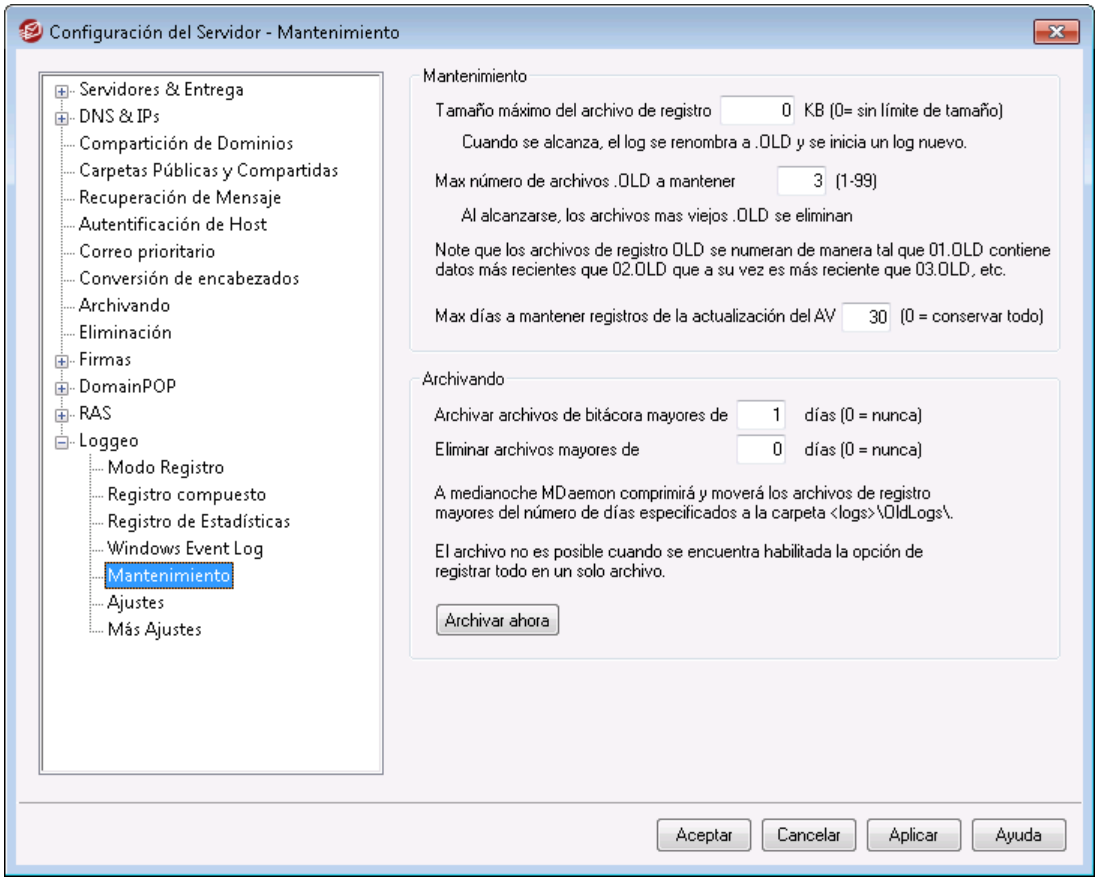
Usar el Registro de Eventos de Windows
Haga clic en esta casilla si desea registrar errores críticos de sistema, avisos y algunos otros eventos en la sección Aplicación del registro de Eventos de Windows.

Dirección de Correo de la puerta de Enlace SMS
Utilice esta opción si desea enviar dato de eventos para cualquier evento seleccionado abajo a algún dispositivo a través de un mensaje SMS (texto). Para hacerlo, especifique la dirección de correo del servicio de puerta de enlace de Correo a SMS de su carrier telefónico, tal como el de Verizon, que es `PhoneNumber@vtext.com` (ej. `8175551212@vtext.com`). Luego utilice las casillas de verificación en la columna SMS abajo para especificar los eventos que desea enviar al dispositivo.

SMS | Registrar los eventos siguientes:
Utilice las opciones SMS para definir los eventos que desea enviar a un dispositivo vía mensaje de texto. Utilice las opciones de registro para definir los eventos que desea registrar en la sección Aplicaciones del Visor de Sucesos de Windows. Para enviar mensajes SMS debe especificar la dirección de correo del servicio de puerta de enlace de Correo a SMS de su carrier telefónico en la opción anterior. Más aun, cualquier evento que detona un mensaje de notificación a la puerta de enlace SMS generará que se procese la cola remota; las notificaciones serán tratadas como correo "urgente".

La opción SMS para los eventos *Inicio y Apagado del Servidor* solo enviarán mensajes de correo a SMS para eventos de inicio, no de apagado.

3.1.16.5 Mantenimiento



Mantenimiento

Tamaño máximo del archivo de registro [xx] KB
Este es el tamaño máximo en kilobytes que puede alcanzar un archivo de registro. Una vez el tamaño haya sido alcanzado, el archivo de registro se copiará a "`LOGFILENAME.01.OLD`" y se iniciará un nuevo archivo. Si ya existe `LOGFILENAME.01.OLD, el archivo anterior se eliminará o renombrará a`" `LOGFILENAME.02.OLD`," dependiendo en el valor definido abajo en "*Máximo número de archivos .OLD a conservar*". Utilice "0" en esta opción si no desea limitar el tamaño de este archivo. Esta opción se configura en "0" por omisión.

Número máximo de archivos .OLD a conservar (1-99)
Cuando se utilice la opción anterior para limitar el tamaño del archivo de registro, esta opción administra cuantas iteraciones se mantendrán de un archivo de registro dado *.OLD* antes de que el más viejo sea eliminado. Estos archivos de

respaldo se denominan "LOGFILENAME.01.OLD," "LOGFILENAME.02.OLD," y así sucesivamente y el archivo más reciente se enlista primero. Por ejemplo, SMTP(out).log.01.old contiene datos más recientes que SMTP(out).log.02.old, etc. Cuando se alcanza el número máximo, el archivo más viejo se elimina al momento que se crea un archivo nuevo.

Máximo número de días del archivo de registro de actualizaciones de Antivirus (0=sin límite)
Esta opción controla el número máximo de días que se mantendrán los archivos de registro del Antivirus (i.e. avupdate.log). A medianoche, cada noche y también siempre que MDaemon reinicia después de una actualización, los datos más viejos serán eliminados del archivo. Utilice "0" en esta opción si no desea definir un límite temporal. Por omisión se mantienen los datos de los últimos 30 días.

El archivo de registro de actualizaciones de AV se mantiene por omisión y su tamaño está limitado a 5120 KB. Si desea modificar el tamaño de este límite o deshabilitar el registro de actualizaciones de AV, las opciones para hacerlo se localizan en el diálogo Configuración de Actualizaciones de AV 673, localizada en: **Seguridad » Antivirus » Actualizador de AV » Configurar Actualizador » Misc**.

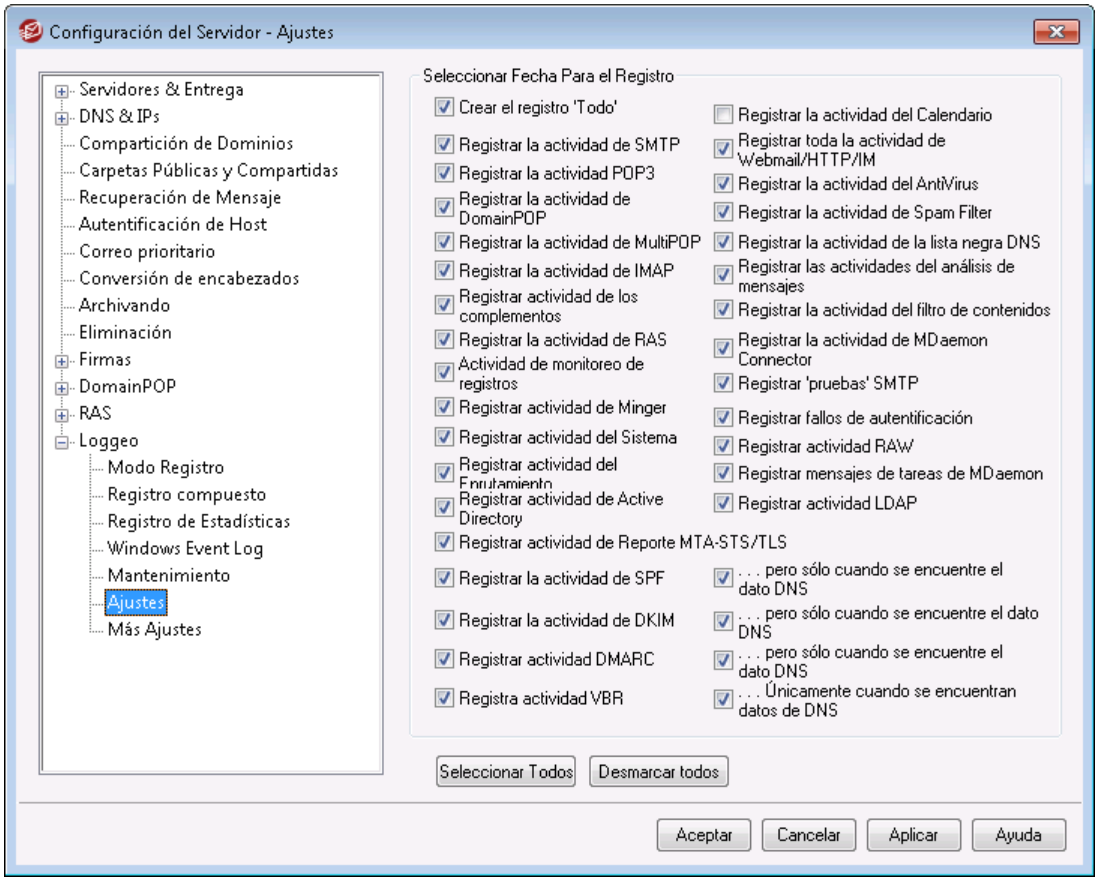
Archivando

Archivar archivos de registro mayores de [XX] días (0=nunca) Haga clic en esta opción si desea que MDaemon salve cada archivo de registro cuya edad exceda del número de días especificado. Cada día a medianoche, MDaemon crearán un ZIP con los archivos antiguos *.log y *.old y los moverá a la subcarpeta \Logs\OldLogs\ (borrando los archivos originales durante el proceso). Este proceso no archivará o borrará archivos que estén en uso, ni archivará cuando la opción "*Crear conjunto de archivos de registro estándar*" esté seleccionada en la pantalla de Modo de Registro.

Eliminar archivos mayores de [XX] días (0=nunca)
Utilice esta opción si desea que MDaemon elimine automáticamente los archivos de registro cuando su edad excede el número de días especificado aquí. Utilice "0" en esta opción si no desea eliminar archivos en automático. La eliminación de archivos ocurre durante el evento diario de reinicio de medianoche.

Archivar ahora
Haga clic en este botón para archivar los archivos de registro antiguos inmediatamente en lugar de esperar a que MDaemon los archive automáticamente a medianoche.

3.1.16.6 Ajustes



Seleccionar Datos a Registrar

Crear el registro 'All'
Haga clic en esta opción si desea que se genere el archivo "`*-all.log`", que contiene un registro compuesto de todas las actividades registradas.

Registrar actividad SMTP
Habilite esta opción si desea registrar toda la actividad SMTP de envío/recepción.

Registrar actividad POP3
Haga clic en esta casilla para registrar toda la actividad de correo POP. Esto registrara las sesiones de recolección POP de sus usuarios.

Registrar actividad de DomainPOP
Haga clic en esta casilla de verificación para registrar toda la actividad de correo DomainPOP.

Registrar actividad MultiPOP
Haga clic en esta casilla para registrar todas las actividades de recolección de correo MultiPOP de sus usuarios.

Registrar actividad IMAP
Activar esta opción causa que todas las sesiones IMAP de sus usuarios sean incluidas en los registros log.

Registrar actividad de complementos
Esta opción registra todas las actividades relativas a complementos.

Registrar actividad RAS
Haga clic en esta opción si desea que MDaemon copies la información de llamada/finalización de RAS en el archivo de registro. Esta información es útil para diagnosticar problemas de marcación.

Registrar actividad de Monitoreo
Dar clic en esta casilla si desea que se incluyan las actividades de Monitoreo de MDaemon en el archivo de registro de MDaemon.

Registrar actividad Minger
Haga clic en esta casilla para registrar las actividades del servidor Minger.

Registrar actividad del Sistema
Esta opción registra las actividades del sistema.

Registrar actividad de Enrutamiento
Esta opción registra todas las actividades de segmentación de colas Entrante, Local y Remota.

Registrar actividad Active Directory
Esta opción es para registrar todas las actividades de MDaemon relativas a Active Directory.

Registrar actividad de Reporteo MTA-STS/TLS
Registrar toda la actividad relacionada a SMTP MTA Strict Transport Security (MTA-STS).

Registrar la actividad del Programador
Habilite esta casilla si desea registrar toda la actividad del Programador de Eventos 380.

Registrar toda la actividad de Webmail/HTTP/IM
Haga clic en esta opción si desea registrar toda la actividad de WorldClient, HTTP y la WorldClient Mensajería Instantánea. Cuando se deshabilita, los registros de WorldClient y HTTP se seguirán creando, mostrando las inicializaciones y apagados de WorldClient, pero otras actividades WC/HTTP/IM no serán registradas.

Registrar actividad del Antivirus
Esta opción habilita el registro de las actividades del AntiVirus.

Registrar la actividad del Filtro de Spam
Registra toda la actividad del Filtro de Spam.

Registrar la actividad de la Lista de Bloqueados de DNS
Esta opción provoca que se registre toda la actividad de lista de bloqueados de DNS. Si utiliza esta opción podrá tener una referencia sencilla de sitios que se registraron bloqueados.

Registrar las actividades del análisis de mensajes
MDaemon realiza periódicamente una enorme cantidad de procesamiento de mensajes cuando determina a quién debería enviarse el mensaje. Active este control si desea que dicha información se incluya en el archivo de registro.

Registrar la actividad del filtro de contenidos
Haga clic en esta casilla si desea incluir la actividad del Filtro de Contenidos en el archivo de registro.

Registrar la actividad de MDaemon Connector
Esta opción gobierna si las actividades de Outlook Connector se deben o no registrar.

Registrar 'pruebas' SMTP
Haga clic en esta opción para registrar las sesiones SMTP cuando no hay datos de mensajes transmitidos por el servidor de envío (p.ej. cuando el servidor de envío no utiliza el comando DATA).

Registrar fallos de autentificación
Utilice esta opción si desea registrar fallos de autentificación.

Registrar actividad RAW
Registrar la actividad de mensajes RAW de MDaemon.

Registrar tareas de mensajes de MDaemon
Registrar tareas de mensajes.

Registrar actividad LDAP
Registrar toda la actividad LDAP.

Registrar actividad SPF
Haga clic en esta casilla de verificación si desea registrar todas las actividades de búsqueda de Sender Policy Framework

> **...pero sólo cuando se encuentren datos en DNS**
> Si está registrando las actividades SPF, haga clic en esta casilla si desea registrar solamente las búsquedas donde se localicen datos SPF en la búsqueda de DNS, en lugar de registrar todas las búsquedas SPF.

Registrar actividad DKIM
Haga clic en esta opción si desea registrar la actividad de DomainKeys (DK) y DomainKeys Identified Mail (DKIM).

> **...pero sólo cuando se encuentre el dato DNS**
> Haga clic en esta casilla de verificación si está registrando la actividad de DKIM pero desea registrar solamente aquellas instancias en las que se encuentren datos DNS en lugar de registrar toda la actividad.

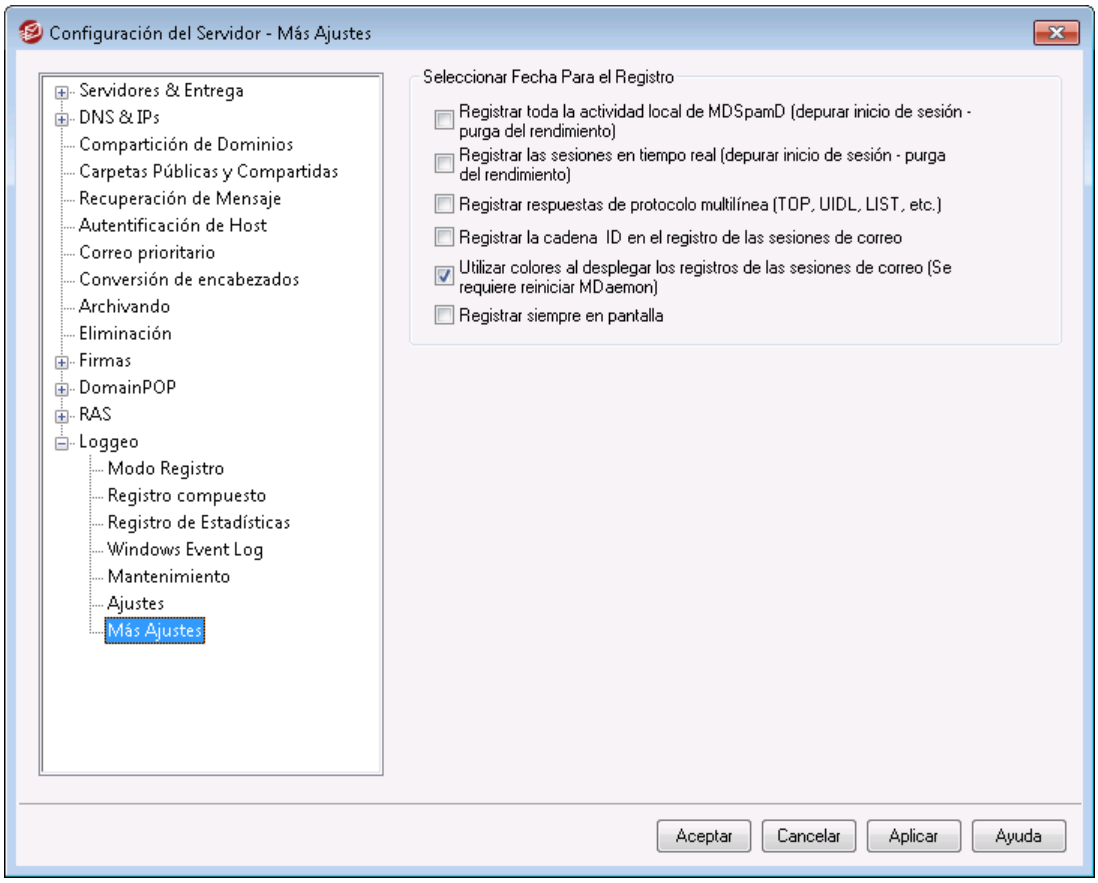
Registrar actividad DMARC
Dé clic en esta opción si desea registrar la actividad DMARC.

...pero solo cuando se encuentren datos DNS
Dé clic en esta casilla si está registrando actividad DMARC, pero solo desea los registros de aquellas instancias donde se encuentran datos de DNS en lugar de registrar toda la actividad.

Registrar actividad VBR
Utilice esta opción si desea registrar la certificación de mensajes[553].

...pero solo cuando se encuentran datos DNS
Si está registrando la actividad de certificación, dé clic en esta casilla si desea registrar solo cuando se encuentran datos de certificación durante la búsqueda DNS

3.1.16.7 Más Ajustes de Registro



Seleccionar Datos a Registrar

Registrar toda la actividad local de MDSpamD (depurar inicio de sesión - purga del rendimiento)
Utilice esta opción para registrar todas las actividades locales de MDSpamD (ver Advertencia a continuación).

Registrar las sesiones en tiempo real (depurar inicio de sesión - purga de rendimiento)
Normalmente, la información de sesión se registra después de que una sesión se haya finalizado para conservar recursos. Haga clic en esta opción si desea que la información de sesión se registre a medida que ocurra.

Cuando se utilice cualquier o alguna de las dos opciones previas para registrar, puede que vea disminuido el rendimiento de su sistema de correo, dependiendo del nivel de actividad del sistema. Generalmente debería utilizar estas opciones solamente con propósitos de depuración

Registrar las respuestas de protocolo multilínea (como UIDL y LIST)
Algunas veces las respuestas a peticiones de protocolo requieren más una línea de información. Haga clic en esta casilla si desea registrar dichas líneas adicionales.

Si activa esta opción puede incrementar potencialmente la cantidad de información registrada. Dado que el número de líneas en una respuesta no se puede determinar por adelantado, y dado que algunas respuestas tienen un enorme potencial de "llenar" el archivo de registro con posiblemente información innecesaria (por ejemplo, POP TOP, lista el contenido actual del mensaje), no recomendamos utilizar esta funcionalidad en si el tamaño del archivo de registro o la verbosidad tuvieran importancia para usted.

Registrar una cadena ID en los registros de sesión de correo
Haga clic en esta casilla si desea incluir unas cadenas de ID únicas `[%d:%d]` en los registros de sesión.

Utilizar colores al desplegar los registros de las sesiones de correo (requiere reiniciar MDaemon)
Habilite esta opción si desea dar colores al texto que se despliega en varias de las pestañas de Rastreo de Eventos y Registro 81 en la interface de usuario de MDaemon. La opción se encuentra deshabilitada por omisión y al habilitarla/deshabilitarla se requiere reiniciar MDaemon para que el cambio tenga efecto. Ver "Registros de Sesión a Color" abajo para más información.

Siempre desplegar en pantalla
Dé clic en esta opción si desea que los datos en registro se copien en la interface de usuario de MDaemon aun cuando esté minimizada o se esté ejecutando en la bandeja.

Cuando se deshabilita este control, los datos de registro no se copian al panel de Rastreo de Eventos cuando MDaemon se está ejecutando en la bandeja del sistema. En consecuencia, la actividad más reciente no se enlistará en ninguna de las pestañas del panel de Rastreo de Eventos cuando se abre MDaemon. Empezará a desplegar la información más reciente de ese momento en adelante.

Registros de Sesión a Color

En la Interface de usuario de MDaemon[81], las pestañas que despliegan la actividad de Enrutamiento, SMTP-entrante, SMTP-saliente, IMAP, POP, MultiPOP y DomainPOP pueden mostrarse a colores como una ayuda visual para separar eventos durante una sesión. Esta funcionalidad está deshabilitada por omisión pero se puede habilitar vía la opción "*Utilizar colores al desplegar las sesiones de registro de correo*" localizada en: Logueo » Más Ajustes[184] y Preferencias » UI[491]. Los colores por omisión se pueden modificar editando la sección `[Colors]` del archivo `LogColors.dat` en la carpeta `\APP\` de MDaemon. Vea la gráfica siguiente para una lista de los colores por omisión.

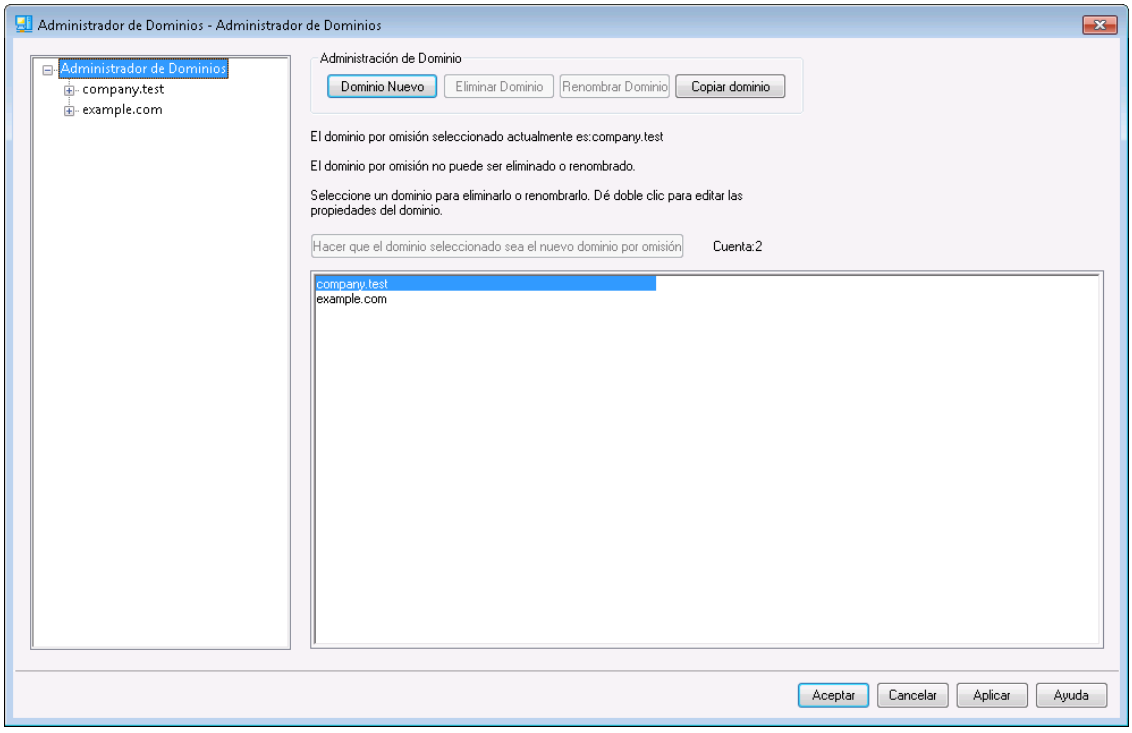
Si desea utilizar colores, pero no quiere colorear uno o más de los elementos enlistados, defina el valor de cada uno de esos elementos como cero (por ejemplo, `SpamFilter=0`). Con esto los elementos seleccionados utilizarán el color por omisión. Para `Background` y `SelectedBackground`, sin embargo, definir el valor en cero no funciona. Si requiere cambiar cualquiera de esos dos elementos tendrá que proporcionar un nuevo valor de color. Los valores de los colores se especifican en hexadecimal utilizando este formato: "`0xbbggrr`", donde "bb" es la intensidad relativa del azul, "gg" para verde y "rr" para rojo. Por ejemplo, "`Error=0x0000ff`" configura el texto de error en rojo. **Por favor note:** este es el inverso del orden tradicional de códigos de color, que típicamente es "`rrggbb`". Si hace cambios a los colores debe reiniciar MDaemon o crear un archivo denominado `COLORS.SEM` y colocarlo en la carpeta `\APP\` de MDaemon.

Colores por Omisión

Background=0x000000	Color de fondo; negro
SelectedBackground=0xff0000	Color de fondo Seleccionado; azul
Default=0xffffff	Color de texto por omisión; blanco
Processing=0x00ffff	Actividad interna de procesamiento; amarillo por omisión
DataIn=0x008040	Datos entrantes desde otro servidor; verde oscuro por omisión
DataOut=0x00ff00	Datos salientes hacia otro servidor; por omisión verde brillante
Error=0x0000ff	Mensajes de error; rojo por omisión
TCPIP=0xff8000	Actividad relacionada a TCP/UDP/DNS/PTR; azul claro por omisión
SpamFilter=0x0080ff	Filtrado de Spam; naranja por omisión
Antivirus=0xdda0dd	Procesamiento de Antivirus; ciruela por omisión
DKIM=0xff00ff	Actividad DomainKeys y DKIM; fucsia por omisión
VBR=0x40c0ff	Actividad VBR (Vouch by Reference); naranja claro por omisión

SPF=0x808080	Actividad SPF (Sender Policy Framework); gris por omisión
Plugins=0x0080c0	Cualquier mensaje de un componente adicional (plugin); café por omisión
Localq=0x00ffff	Enrutamiento de Cola Local; amarillo por omisión
Spam=0x0080ff	Enrutamiento de mensaje de Spam; naranja por omisión
Restricted=0x40c0ff	Enrutamiento de Mensajes restringidos; naranja claro por omisión
BlackList=0x808080	Enrutamiento de mensaje en lista negra; gris por omisión
Gateway=0x00ff00	Enrutamiento de Mensajes de Puertas de Enlace; verde claro por omisión
Inboundq=0xff8000	Enrutamiento de mensajes entrantes; azul claro por omisión
PublicFolder=0xdda0dd	Enrutamiento de mensajes a carpetas públicas; ciruela por omisión

3.2 Administrador de Dominios



MDaemon contiene soporte total para múltiples dominios, a través del Administrador de Dominios. Aquí puede definir nombres de dominio, direcciones IP, parámetros de depuración de cuentas y mensajes, configuración de Webmail y otras opciones específicas por dominio.

MDaemon soporta direcciones IP únicas y múltiples; las direcciones IP pueden ser únicas para dominios individuales o compartidas entre ellos. Más aun, hay varias opciones clave tales como Cuentas, Listas de Distribución y algunas configuraciones de Seguridad que ahora se manejan por dominio. Cuando se genera una cuenta nueva, por ejemplo, se debe especificar el dominio al que pertenece la cuenta. Lo mismo sucede con las Listas de Distribución. Esto significa que funcionalidades tales como el Monitoreo IP 562 y la Protección IP 521 están ligadas individualmente a los dominios.

Algunas funcionalidades, tales como la Coincidencia de Nombres 167 bajo DomainPOP 157, están ligadas exclusivamente al dominio principal. Este también es el que se despliega por omisión en varias opciones, como cuando se crean cuentas nuevas o listas de distribución. Más aun, para soportar el manejo del sistema de mensajes de MDaemon, los siguientes Alias 834 por omisión apuntan a varios nombres de buzón reservados para el dominio por omisión de MDaemon en lugar de para los dominios adicionales:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

Finalmente, a fin de soportar múltiples dominios, por omisión MDaemon requiere que los usuarios utilicen el nombre completo de la dirección de correo (ej.: "usuario01@ejemplo.com") para abrir sesión en lugar de solo la porción del buzón de la dirección (ej. "usuario01"). Algunos clientes de correo muy antiguos, sin embargo, no soportan el uso de '@' en el campo del inicio de sesión. Para soportar esos clientes, puede especificar un carácter alterno en la pantalla Sistema 494 bajo Preferencias. Adicionalmente, este valor puede ser de hasta 10 caracteres de longitud, lo que hace posible proporcionar una cadena de caracteres que sirva como delimitador en lugar de un solo carácter como podría ser '$'. Por ejemplo, el utilizar '**.at.**' le permitirá hacer que sus valores de inicio de sesión sean "usuario02.at.ejemplo.com". Puede deshabilitar el requerimiento de la dirección completa de correo permitiendo al usuario utilizar solo la porción del buzón de su dirección como valor para el inicio de sesión, pero no se recomienda y puede generar problemas si se cuenta con más de un dominio.

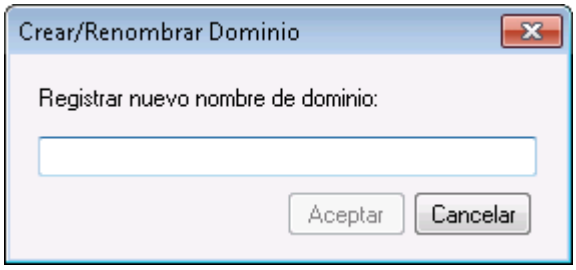
Listas de Dominios

El área a la izquierda de este diálogo contiene la lista de sus dominios, con ligas a cada pantalla utilizada para configurar los diversos parámetros específicos por dominio. El Dominio por Omisión se enlista primero y el resto se enlista alfabéticamente. La lista a la derecha se utiliza para eliminar y renombrar dominios y para designar el Dominio por Omisión. Puede dar doble clic a un dominio en esta lista para configurarlo.

Administración de Dominios

Dominio Nuevo

Para crear un dominio nuevo, dé clic en *Dominio Nuevo*, registre el nombre del dominio en el diálogo Crear/Actualizar y dé clic en *OK*.



Típicamente el valor registrado aquí será el nombre registrado en Internet al que resuelve el servidor DNS con la dirección IP de la máquina local donde corre el servidor o un alias calificado de ese nombre. Alternativamente, puede utilizar un nombre de dominio interno o algún otro nombre no-público (tal como "`company.mail`"). Al configurar su servidor de esta manera puede ser necesario utilizar la funcionalidad Conversión de Encabezados 135, y/o el Motor de Reemplazo de Nombres de Dominio 163 para habilitar la distribución correcta del correo.

Eliminar dominio
Para eliminar un dominio: seleccione el dominio de la lista y dé clic en *Eliminar dominio*, luego confirme su decisión de eliminarlo dando clic en *Sí*.

> No puede eliminar o renombrar el dominio por omisión. Si desea eliminar o renombrarlo debe primero seleccionar un dominio distinto para que sea el de omisión.

Renombrar dominio
Para modificar un nombre de dominio: seleccione el dominio de la lista, dé clic en *Renombrar dominio*, teclee el nuevo nombre en el diálogo Crear/Actualizar y dé clic en *OK*.

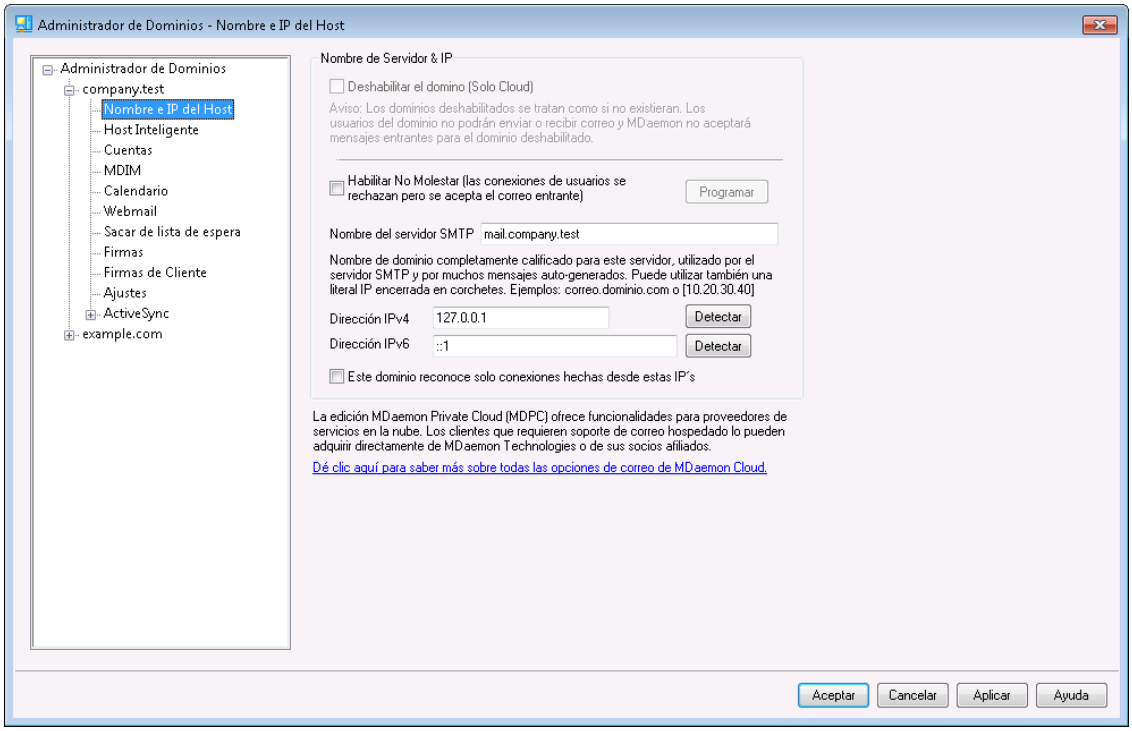
Copiar dominio
Si desea crear un dominio nuevo con ajustes similares a los de otro dominio, seleccione ese dominio de la lista, dé clic en este botón y especifique el nombre del nuevo dominio. No se copiarán las cuentas, listas y demás hacia el nuevo dominio.

Hacer que el dominio seleccionado sea el nuevo dominio por omisión
Si desea modificar el dominio por omisión de MDaemon, seleccione el dominio deseado en la lista y dé clic en este botón.

Ver:

Preferencias » Sistema 494

3.2.1 Nombre de Servidor & IP



Nombre de Host & IP

Deshabilitar dominio (solo Cloud)
Marque esta casilla si desea deshabilitar el dominio. Los dominios deshabilitados son tratados por MDaemon como si no existieran. Los usuarios del dominio no podrán enviar o recibir correo y MDaemon no aceptará mensajes entrantes para el dominio. Esta opción solo está disponible en MDaemon Private Cloud.

Habilitar No Molestar
Utilice esta opción para activar No Molestar para un dominio. Cuando se activa, el dominio rehusará conexiones para todos los usuarios y todos los servicios pero aceptará mensajes del mundo exterior.

Programación
Dé clic en este botón para programar cuando inicia y termina No Molestar. Por ejemplo, si configura Mayo 1, 2020 a Junio 30, 2020 de las 5:00 pm a 7:00 am, Lunes a Viernes, significa que no estarán disponibles los servicios de correo para los usuarios del dominio durante esos días, iniciando a las 5:00 pm y restableciéndose a las 7:01 am, en tanto la fecha se encuentre entre Mayo 1 y Junio 30, 2020. Si se elimina la fecha programada de inicio, se desactiva la programación y tiene el efecto de **dejar al dominio en 'No Molestar' para siempre**.

Nombre del host SMTP

Este valor es el Nombre de Dominio Totalmente Calificado (Fully Qualified Domain Name - FQDN) que se utilizará en la instrucción `SMTP HELO/EHLO` al enviar correo para este dominio. Para las conexiones entrantes, si la opción *Este dominio reconoce solo conexiones hechas a la dirección IP siguiente* está habilitada, el

dominio está ligado a su propia dirección IP y se utilizará el FQDN correcto para las conexiones hechas a ese dominio. Estrictamente, no se requiere utilizar esta opción para que esto funcione. Pero, si tiene dos o más dominios utilizando la misma dirección IP entonces el FQDN utilizado será el que se encuentre asociado con el dominio que está primero en la lista en orden alfabético.

En la mayoría de los casos el FQDN será ya sea el *Nombre de Dominio* o un subdominio del mismo (por ejemplo, "`mail.ejemplo.com`"), también puede utilizarse una sintaxis de IP literal como "`[192.0.2.0]`". Cuando no se especifica valor FQDN, MDaemon utilizará el FQDN del Dominio por Omisión.

Dirección IPv4/IPv6
Ingrese las direcciones IPv4 e IPv6 asociadas con este dominio. Si falta una dirección IP, MDaemon automáticamente tratará de detectar una dirección apropiada para utilizarla.

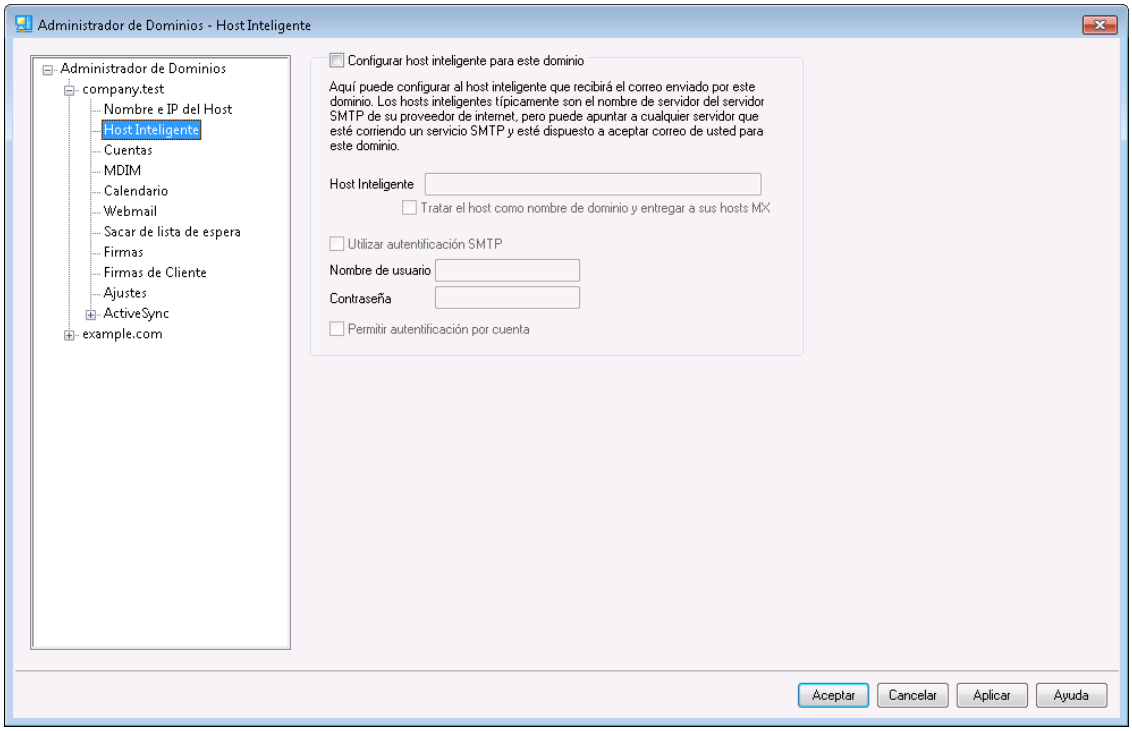
Detectar
Utilice estos botones para detectar las direcciones IPv4 e IPv6 elegibles para uso en las opciones correspondientes de direcciones IP. Puede seleccionar de las direcciones IP ahí listadas.

Este dominio reconoce solo las conexiones hechas a estas IPs
Dé clic en esta casilla si desea restringir las conexiones entrantes a este Dominio, a las direcciones IP especificadas arriba. Por omisión esto solo aplica a las conexiones entrantes. La liga de sockets salientes se administra en la opción bajo "Ajustes de Servidor » Enlace 120."

Ver:

Administrador de Dominios 190
Preferencias » Sistema 494
Enlace 120
IPv6 119

3.2.2 Host Inteligente



Configurar host inteligente para este dominio

Si desea enrutar el correo saliente de este dominio hacia un Host Inteligente específico en lugar de utilizar las opciones de Entrega 102 por omisión de MDaemon, habilite esta casilla y especifique el host inteligente. Todo el correo saliente del dominio será enrutado a ese host.

Host Inteligente
Especifique su ISP o el nombre de su servidor de correo o dirección IP aquí. Este es generalmente el servidor SMTP de su ISP.

No registre aquí el Dominio por Omisión de MDaemon o su dirección IP. Este registro debe ser un ISP u otro servidor de correo que pueda entregar correo por usted.

Tratar al host como nombre de dominio y entregar a su host MX
Marque esta casilla si desea tratar al host como un nombre de dominio en lugar de un servidor específico, haciendo que MDaemon recupere los hosts MX asociados con el dominio y se conecte a ellos.

Utilizar autentificación SMTP
Dé clic en esta casilla y registre las credenciales de acceso si el *Host inteligente* requiere autentificación. Estas credenciales serán utilizadas para todos los mensajes SMTP salientes enviados al host inteligente. Sin embargo, si decide utilizar la opción *Permitir autentificación por cuenta* que se muestra abajo, entonces MDaemon se autentificará con el host por separado para cada mensaje, utilizando las credenciales definidas en la pantalla *Acceso a Host Inteligente* en Servicios de Correo 719 en el Editor de Cuentas.

Nombre de usuario
Registre aquí su nombre de usuario o de inicio de sesión.

Contraseña
Utilice esta opción para especificar la contraseña de acceso a su host inteligente.

Permitir autentificación por cuenta
Dé clic en esta casilla si desea utilizar autentificación por cuenta para el correo saliente SMTP enviado al *Host Inteligente* especificado arriba. En lugar de utilizar el *Nombre de Usuario* y la *Contraseña* proporcionados aquí, se utilizarán las credenciales de acceso al *Host Inteligente*, definidas en la pantalla Servicios de Correo 719. Si no se han definido credenciales para el host inteligente para alguna cuenta, se utilizarán las credenciales definidas arriba.

Si desea configurar que la *autentificación por cuenta* utilice la contraseña de correo de cada cuenta, lo puede hacer editando la llave siguiente en el archivo `MDaemon.ini`:

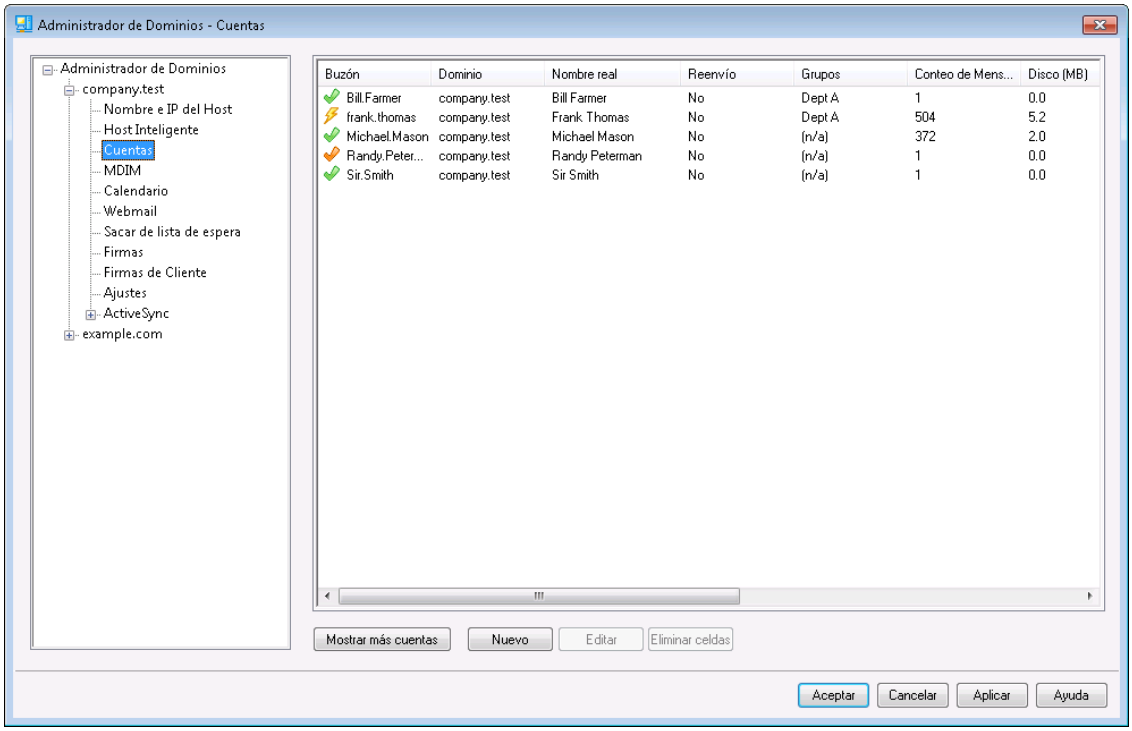
```
[AUTH]
ISPAUTHUsePasswords=Yes (Por defecto No)
```

El habilitar la opción `ISPAUTHUsePasswords=Yes` con el tiempo terminará comunicando todas las contraseñas de su correo local a su host inteligente. Esto puede convertirse en un riesgo para la seguridad de su correo, dado que se está proporcionando información sensible a otro servidor. No deberá utilizar esta opción a menos que su host inteligente sea absolutamente confiable y usted considere que es necesario hacerlo. Más aun, deberá notar que, si utiliza esta opción y le da a sus usuarios permiso de modificar su *Contraseña de Correo* vía Webmail o por algún otro medio, este cambio también se realizará en la *Contraseña del Host Inteligente*. Esto puede originar que la autentificación al host inteligente falle para una cuenta cuando su contraseña de correo se modifique localmente, pero la contraseña del host inteligente no sea actualizada.

Ver:

Administrador de Dominios 190
Configuración de Servidor » Entrega 102
Editor de Cuentas » Servicios de Correo 719

3.2.3 Cuentas



La página Cuentas despliega una lista de todas las cuentas de este dominio en MDaemon. Cada registro en la lista contiene íconos de Estatus de Cuenta (ver abajo), el buzón, el "nombre real" del propietario de la cuenta, los grupos a los que pertenece la cuenta, el conteo de mensajes y la cantidad de espacio en disco utilizado (en MB). Esta lista se puede ordenar de manera ascendente o descendente por cualquier columna que prefiera Dé clic en el encabezado de cualquier columna para sortear la lista en orden ascendente en base a esa columna. Dé clic de nuevo en la columna para sortear en orden descendente.

Íconos de Estatus de Cuentas

La cuenta es administrador global o de dominio.

Cuenta con acceso total. Tanto POP como IMAP están habilitados.

Cuenta con acceso restringido. POP, IMAP o ambos están deshabilitados.

Cuenta Congelada. MDaemon aun recibirá correo para la cuenta, pero el usuario no puede enviar o revisar su correo.

Cuenta deshabilitada. El acceso a la cuenta está completamente deshabilitado.

Nueva
Dé clic en este botón para abrir el Editor de Cuentas 715 a fin de crear una cuenta nueva.

Editar
Seleccione una cuenta de la lista y dé clic en este botón para abrirla en el Editor de Cuentas[715]. También puede dar doble clic en la cuenta para abrirla.

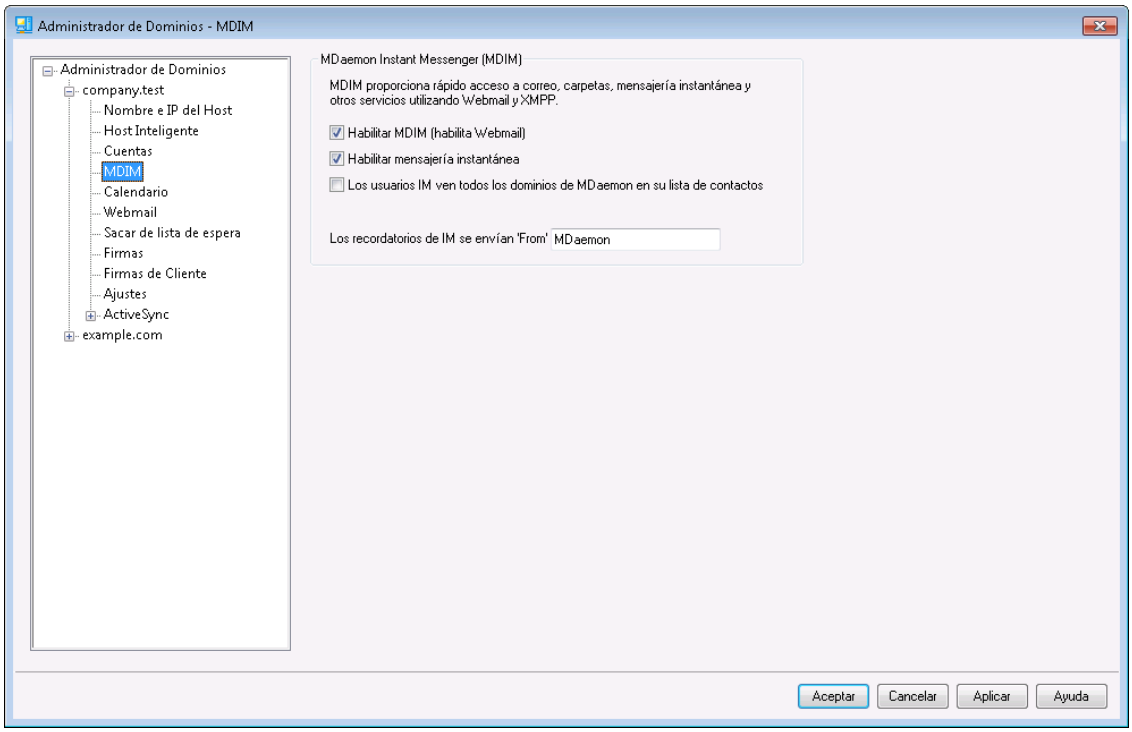
Eliminar
Seleccione una cuenta de la lista y dé clic en este botón para eliminarla. Se le solicitará confirmar su decisión de eliminar la cuenta antes de que MDaemon proceda.

Mostrar más cuentas
La lista de cuentas solo despliega 500 cuentas a la vez. Si el dominio cuenta con más de 500 cuentas dé clic en este botón para desplegar el segundo bloque de 500 cuentas.

Ver:

Administrador de Cuentas[712]
Editor de Cuentas[715]
Plantilla de Cuentas Nuevas[792]

3.2.4 MDIM



Esta pantalla controla varios aspectos de la Mensajería Instantánea de MDaemon (WCIM)[322] para este dominio. La configuración inicial en esta pantalla está determinada por la Configuración por Omisión de la Mensajería Instantánea de MDaemon[332] localizada en el diálogo Web & Servicios IM. MDIM se puede habilitar o deshabilitar para cuentas o grupos específicos vía las pantallas Servicios Web[720] y Propiedades de Grupo[783], respectivamente.

Mensajería Instantánea de MDaemon (MDIM)

Habilitar WCIM (habilita WorldClient)
Habilite esta opción si desea habilitar para descarga MDaemon Mensajería Instantánea, por omisión, desde Webmail, para los usuarios del dominio. Lo pueden descargar desde la página *Opciones » MDaemon Mensajería Instantánea.* El instalable se personalizará automáticamente para la cuenta de cada usuario a fin de facilitar la instalación y configuración. Esta opción también permite a MDIM utilizar la funcionalidad Mis Carpetas de Correo, que permite a los usuarios verificar si hay correo nuevo y abrir Webmail directamente desde el atajo de MDIM. MDIM se encuentra habilitado por omisión.

Habilitar Mensajería Instantánea
Dé clic en esta opción si desea activar la mensajería instantánea de WorldClient (MDIM) para los usuarios del dominio. Deshabilite la casilla se no desea que la mensajería instantánea esté disponible.

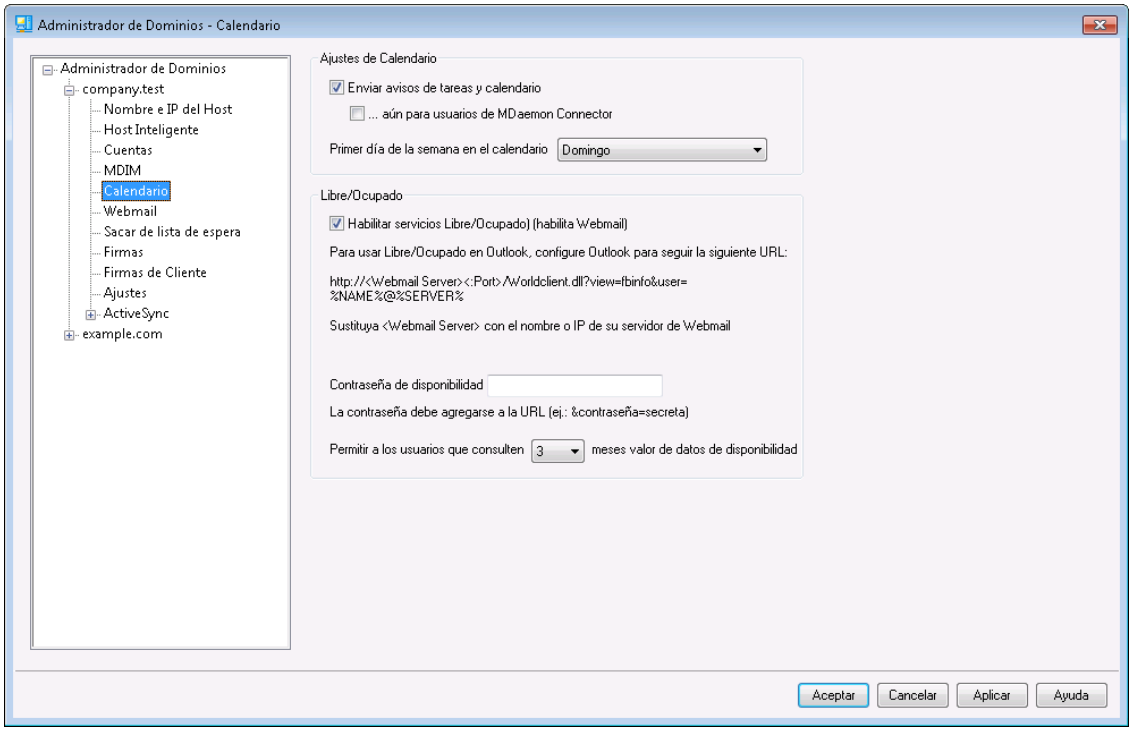
Los usuarios de IM ven todos los dominios de MDaemon en su lista de contactos
Dé clic en esta opción si desea que los usuarios de este dominio puedan agregar a su lista de contactos usuarios de todos sus dominios de MDaemon. Cuando la opción está deshabilitada, los contactos deben ser del mismo dominio. Por ejemplo, si su MDaemon está hospedando correo para example.com y example.org, al activar esta opción para example.com significa que los usuarios de ese dominio podrán agregar contactos de mensajería instantánea de ambos dominios. Al deshabilitar la opción los usuarios de example.com solo podrán agregar contactos de otros usuarios de example.com. Esta opción se encuentra deshabilitada por omisión.

Los recordatorios enviados a través del sistema IM son enviados 'De:' [*texto*]
Cuando una cita se programa en el calendario de Webmail de un usuario, el evento puede configurarse para enviar recordatorios al usuario en momentos específicos. Si el sistema de IM está activo para el dominio del usuario, entonces el recordatorio se enviará en un mensaje instantáneo para el usuario. Utilice esta casilla para especificar el nombre que desea que aparezca después de la palabra 'De' como remitente del mensaje.

Ver:

Administrador de Dominios 190
Webmail » MDaemon Mensajería Instantánea 332
Editor de Cuentas » Servicios Web 720
Propiedades de Grupo 783

3.2.5 Calendario



Esta pantalla controla las funcionalidades de Calendario de MDaemon para este dominio. La configuración inicial en esta pantalla está determinada por la pantalla Calendario 334 localizada en el menú Web y Servicios IM.

Ajustes de Calendario

Enviar recordatorios de calendario y tareas
Dé clic en esta casilla si desea permitir que los recordatorios de Calendario y Tareas se envíen a sus usuarios vía correo electrónico y a través de la MDaemon Mensajería Instantánea.

...también a usuarios de MDaemon Connector
Se ha habilitado la opción "*Enviar recordatorios de Calendario y Tareas*" mencionada previamente, dé clic en esta opción si también desea habilitar los recordatorios para usuarios de MDaemon Connector.

Primer día de la Semana
Seleccione un día de la lista desplegable. El día seleccionado aparecerá como primer día de la semana en los calendarios.

Libre/Ocupado

MDaemon incluye un servidor Libre/Ocupado, que permite a quién planea una reunión, visualizar la disponibilidad de participantes potenciales. Para tener acceso a esta funcionalidad, dé clic en Programación dentro de WorldClient al generar una nueva cita. Así se abre una ventana de Programación que contiene la lista de participantes y una cuadrícula de colores con una línea para cada uno de ellos. La línea de cada participante muestra en colores los horarios en los que pueden estar disponibles para la junta. Hay colores para Ocupado, Tentativo, Fuera de la Oficina y Sin Información. También hay un botón para AutoSeleccionar, que le permite consultar al servidor cual es el horario disponible

más cercano en el que todos los participantes pueden estar disponibles. Cuando termine de generar la reunión, se enviará una invitación a todos los participantes, que la pueden aceptar o declinar.

El servidor Libre/Ocupado de WorldClient también es compatible con Outlook de Microsoft. Para utilizarlo, configure Outlook para que consulte los datos de disponibilidad Libre/Ocupado en la URL listada a continuación. Por ejemplo, en Outlook 2002, las opciones Libre/ocupado se encuentran bajo "Herramientas » Opciones » Opciones de Calendario... » Opciones Libre/Ocupado..."

La URL Libre/Ocupado para Outlook es:

```
http://<WorldClient><:Puerto>/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Reemplace "<WorldClient>" con la dirección IP o el nombre de dominio de su servidor WorldClient; sustituya "<:Puerto>" con el número de Puerto (si no está utilizando el puerto Web por omisión). Por ejemplo:

```
http://ejemplo.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Para más información sobre cómo utilizar la funcionalidad Libre/Ocupado de WorldClient para programar sus citas, vea la Ayuda en línea incluida en WorldClient.

Habilitar servicios Libre/Ocupado (habilitado en Webmail)
Dé clic en esta opción si desea dar acceso a los usuarios a las funcionalidades del servidor Libre/Ocupado.

Contraseña Libre/Ocupado
Si desea que se solicite una contraseña cuando el usuario intente acceder a las funcionalidades del servidor Libre/Ocupado vía Outlook, registre la contraseña aquí. Esta debe agregarse a la URL mencionada previamente (con el formato "&password=FBServerPass") cuando los usuarios configuren sus parámetros de consulta Libre/Ocupado en Outlook. Por ejemplo:

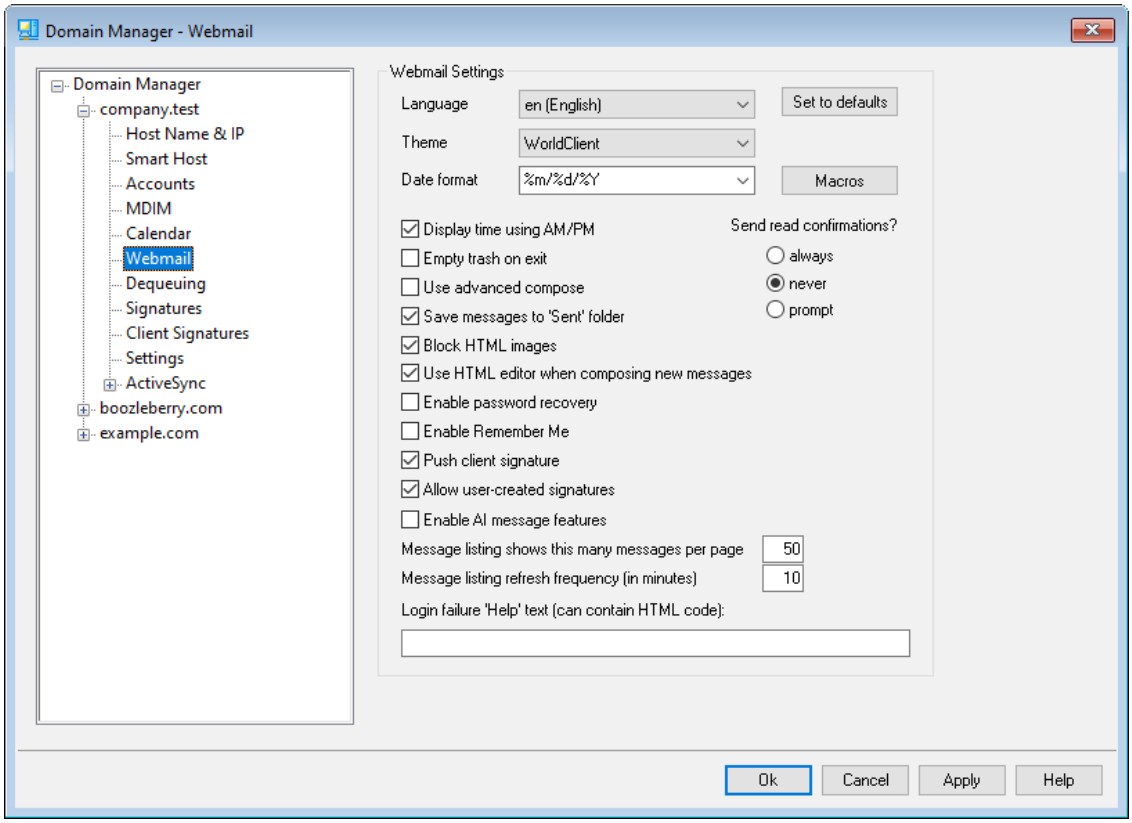
```
http://ejemplo.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%&password=MyFBServerPassword
```

Permitir que los usuarios consulten X meses de información Libre/Ocupado
Use esta opción para definir cuantos meses pueden consultar sus usuarios de la información Libre/Ocupado.

Ver:

Web mail » Calendario 334

3.2.6 Webmail



Esta pantalla controla varias opciones a nivel cliente de Webmail para este dominio. Cuando un usuario ingresa a Webmail, estas opciones definen como funcionará inicialmente Webmail para ese usuario. Muchos de estos parámetros se pueden personalizar por el usuario vía la página Opciones desde Webmail. La configuración por omisión de esta pantalla se define desde Webmail (correo web) » Ajustes 345 en el diálogo Web & Servicios IM.

Ajustes de Webmail

Restablecer a valores por omisión

Este botón restablece las opciones del dominio a los Ajustes por Omisión de Webmail 345.

Lenguaje

Utilice la lista desplegable para seleccionar el lenguaje por omisión con el que aparecerá la interface de WorldClient cuando los usuarios se firmen por primera vez al dominio seleccionado. Los usuarios pueden modificar el lenguaje de manera individual en la página de inicio de sesión de WorldClient, así como desde Opciones » Personalizar dentro de WorldClient.

Tema

Seleccione en esta lista desplegable el tema por omisión que utilizará WorldClient para los usuarios del dominio seleccionado siempre que ingresen al sistema por primera vez. Posteriormente, los usuarios pueden personalizar el tema desde Opciones » Personalizar desde WorldClient.

Formato de Fecha

Utilice esta caja de texto para definir el formato de fecha para el dominio seleccionado. Dé clic en el botón *Macros* para desplegar una lista de códigos de

macros que se pueden utilizar en esta caja de texto. Puede utilizar las macros siguientes en este control:

%A — Nombre completo del día de la semana

%B — Nombre completo del mes

%d — Día del mes (se despliega "01-31")

%m — Mes (se despliega como "01-12")

%y — Año en 2 dígitos

%Y — Año en 4 dígitos

Por ejemplo, "`%m/%d/%Y`" despliega la fecha en WorldClient como "`12/25/2011`".

Macros
Dé clic en este botón para desplegar la lista de códigos de macros que se pueden utilizar en el *Formato de Fecha*.

¿Enviar confirmaciones de lectura?
Esta opción controla como responderá Webmail a los mensajes entrantes que contienen una petición de confirmación de lectura.

siempre
Si se selecciona esta opción, MDaemon enviará un aviso al remitente indicando que el mensaje ha sido leído. El usuario de Webmail que recibió el mensaje no verá ninguna indicación de que la petición de confirmación se hizo o fue contestada.

nunca
Seleccione esta opción si desea que Webmail ignore las peticiones de confirmación de lectura.

preguntar
Seleccione esta opción si desea que Webmail pregunte a los usuarios si desean enviar o no la confirmación de lectura cada vez que un mensaje abierto lo solicite.

Desplegar la hora utilizando AM/PM
Dé clic en esta opción si desea que se utilice el reloj de 12 horas con AM/PM dentro de WorldClient para el horario desplegado en este dominio. Deshabilite la casilla si desea utilizar un reloj de 24 horas para el dominio. Los usuarios individualmente pueden modificar esta configuración vía la opción "*Desplegar la hora en formato AM/PM*" localizada en la página Opciones » Calendario desde Webmail.

Vaciar la papelera al salir
Esta opción hace que se vacíe la papelera del usuario cuando este cierre su sesión de Webmail. Los usuarios individualmente pueden modificar esta configuración en la página Opciones » Personalizar desde Webmail.

Utilizar composición avanzada
Marque esta casilla si desea que los usuarios del dominio vean por omisión la pantalla de Composición Avanzada en Webmail en lugar de la pantalla de

Composición Normal. Los usuarios pueden personalizar esta configuración desde Opciones » Composición desde Webmail.

Guardar mensajes en la carpeta de 'Enviados'
Dé clic en esta opción si desea que se guarde una copia de todos los mensajes enviados en la carpeta *Enviados*. Los usuarios pueden personalizar esta configuración desde Opciones » Composición desde Webmail.

Bloquear imágenes HTML
Habilite esta casilla si desea impedir que se desplieguen en automático imágenes remotas al visualizar mensajes de correo HTML en Webmail. A fin de visualizar las imágenes, el usuario debe dar clic en la barra que aparece sobre el mensaje en la ventana del navegador. Esta es una funcionalidad para prevenir el Spam, dado que muchos mensajes de correo no deseado contienen imágenes con URLs especiales que identifican la dirección de correo del usuario que las visualizó, confirmando así al spammer que es una dirección de correo válida. Esta opción se encuentra habilitada por omisión.

> **...excepto cuando el encabezado De coincide con un contacto en la lista de Remitentes Permitidos del dominio o del usuario**
> Marque esta casilla si desea permitir que se desplieguen en automático imágenes en mensajes cuando el encabezado De del mensaje contiene un contacto que se encuentra en la Lista de Remitentes Permitidos del usuario o del dominio. **Nota:** Esta opción solo está disponible en MDRA 354.

Deshabilitar hipervínculos en spam y mensajes que fallen la autenticación DMARC, DNSBL, o SPF
Por omisión, cuando un mensaje se marca como spam o falla la verificación DMARC 545, DNS-BL 701, o SPF 526, se deshabilitarán los hipervínculos contenidos en el mensaje. Deshabilite esta casilla si no desea deshabilitar los hipervínculos en esos mensajes. **Nota:** Esta opción solo está disponible en MDRA 354.

> **...excepto cuando el encabezado De coincide con un contacto en la lista de Remitentes Permitidos del dominio o del usuario**
> Marque esta casilla si desea exentar de que se deshabiliten los hipervínculos a mensajes marcados cuando el encabezado De coincida con un contacto en la Lista de Permitidos del usuario o el dominio.**Nota:** Esta opción solo está disponible en MDRA 354.

Utilizar el editor HTML al redactar mensajes nuevos
Marque esta casilla si desea que los usuarios del dominio vean el editor HTML por omisión en Webmail. Pueden controlar esta configuración desde Opciones » Composición desde **Webmail**.

Habilitar recuperación de contraseñas
Si se habilita, los usuarios del dominio que tengan permiso de editar su contraseña 720 podrán registrar una dirección de correo alterna en Webmail, a la que se puede enviar una liga para restablecer su contraseña si es que la olvidan. Para configurar esta funcionalidad, los usuarios deben registrar tanto la dirección de correo de recuperación de contraseña, así como su contraseña, en Webmail en la página Opciones » Seguridad. Una vez hecho esto, si el usuario intenta ingresar a Webmail con una contraseña incorrecta, aparecerá la liga "olvidó su contraseña?". Esta liga los lleva a una página que solicita confirmación de la cuenta de correo para recuperación de contraseña. Si se registra correctamente,

se enviará un mensaje con una liga hacia una página para modificar la contraseña. Esta funcionalidad se encuentra deshabilitada por omisión.

Puede habilitar/deshabilitar esta opción a nivel usuario agregando la llave siguiente en el archivo del usuario `user.ini` de Webmail (ej. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (o "=No" para deshabilitar la opción
para este usuario))
```

Permitir Recuérdame en Autentificación de Dos Factores (también aplica a la Administración Remota)
Cuando alguien utiliza Autentificación de Dos Factores (2FA) al iniciar sesión en Webmail o Administración Remota, normalmente está disponible una opción de Recuérdame para el usuario en la página de autentificación 2FA, que impedirá que el servidor solicite 2FA de nuevo de ese usuario durante un número definido de días (ver la opción "*Habilitar Recuérdame*" abajo). Deshabilite esta casilla si no desea desplegar la opción 2FA Recuérdame, lo que significa que todos los usuarios con 2FA habilitado deberán ingresar un código 2FA cada vez que inicien sesión. **Nota**: Esta opción solo está disponible en la interface web de MDaemon Administración Remota (MDRA) 354.

Habilitar Recuérdame
Marque esta casilla si desea que exista una casilla de verificación para habilitar *Recuérdame* en la página de inicio de MDaemon Webmail cuando los usuarios del dominio se conecten vía el puerto https 328. Si los usuarios habilitan esta caja al iniciar sesión, sus credenciales serán recordadas en ese dispositivo. Luego, cada vez que utilicen el dispositivo para conectarse a Webmail en el futuro, su sesión iniciará automáticamente, hasta el momento en que cierren la sesión de su cuenta manualmente o su token de Recuérdame expire.

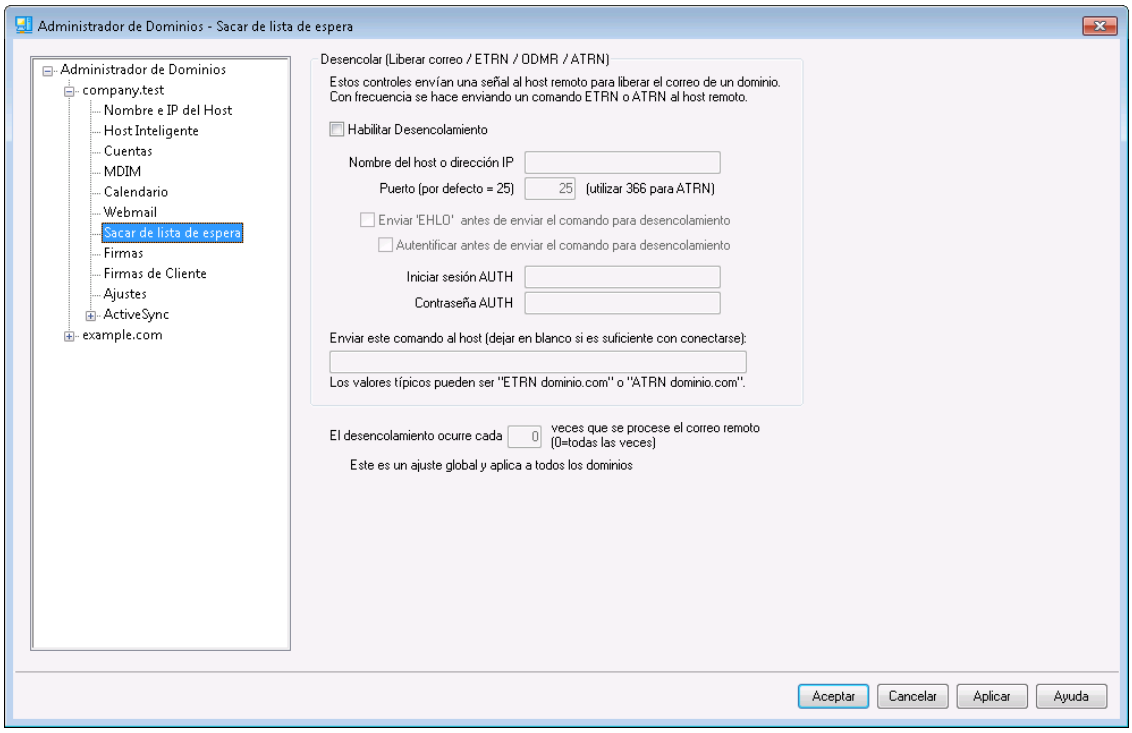
Por omisión, las credenciales del usuario se recuerdan durante un máximo de 30 días antes de que se obligue al usuario a iniciar sesión de nuevo. Si desea incrementar el tiempo de expiración, lo puede hacer modificando el valor en la opción *Expirar los tokens de Recuérdame dentro de estos días* en la interface web de MDaemon Administración Remota (MDRA) 354. También puede modificar este valor editando la llave `RememberUserExpiration=30` en el archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. El valor de expiración se puede establecer a un máximo de 365 días. **Nota:** La Autentificación de Dos Factores 720 (2FA) cuenta con su propia llave de expiración para Recuérdame (`TwoFactorAuthRememberUserExpiration=30`), localizada en la sección `[Default:Settings]` del archivo `Domains.ini` , que se encuentra en la carpeta `\MDaemon\WorldClient\`. Por esto 2FA requerirá un inicio de sesión cuando expire el token de Recuérdame, aun cuando el token regular aun sea válido.

La opción *Recuérdame* está deshabilitada por omisión aplica solo a su dominio. La opción global se encuentra en la pantalla de Ajustes 345 de Webmail.

Dado que *Recuérdame* permite a los usuarios tener un inicio de sesión persistente en múltiples dispositivos, los usuarios deberán ser advertidos de no utilizarlo en redes públicas. Más aun, si llega a sospechar que alguna cuenta haya sido comprometida, en MDRA existe el botón *Restablecer*

> *Recuérdame* que puede utilizar para restablecer los tokens de Recuérdame para todos los usuarios. Esto requerirá que todos los usuarios inicien sesión de nuevo.

3.2.7 Desencolamiento



Desencolamiento (Procesamiento de Correo/ ETRN/ODMR/ATRN)

Habilitar Desencolamiento
Cuando es momento de procesar el correo remoto, MDaemon se puede conectar a cualquier servidor en cualquier puerto y enviar cualquier cadena que usted desee enviar. Esto es útil cuando se desea enviar una señal a un servidor remoto para liberar correo enviándole alguna cadena. Por ejemplo, `ATRN`, `ETRN`, o `QSND`. También puede utilizar esta funcionalidad cuando se requiere brevemente una sesión `FINGER` o `TELNET` a fin de que su host remoto o ISP determine que usted está en línea.

Nombre del host o dirección IP
Éste es el host al que se le enviará la señal de liberación del correo.

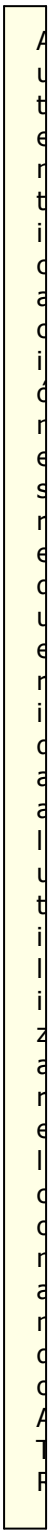
Puerto
Introduzca el puerto en el que desea hacer la conexión. Por defecto es 25 (el puerto SMTP), que es apropiado para los métodos de señal `ETRN` o `QSND`. El puerto 366 se utiliza típicamente para `ATRN`, y el puerto 79 se usa para `FINGER`.

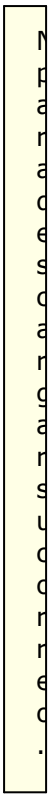
Enviar "EHLO" antes de enviar la cadena de texto

Si habilita esta casilla, deberá conectarse a un servidor SMTP para enviar una señal a fin de que su correo sea entregado. Esta opción origina que se inicie una

sesión SMTP con el servidor especificado y permite que la sesión avance justo hasta la etapa del SMTP "EHLO" antes de enviar la cadena de liberación.

Autentificar antes de enviar la cadena de texto (requerido para ATRN)
Como medida de seguridad, algunos servidores requieren que los clientes de autentifiquen utilizando ESMTP AUTH antes de liberar los mensajes en espera. Si este es el caso de su servidor de correo, dé clic en esta casilla y registre abajo las credenciales de autenticación requeridas.





Logon AUTH
Registre aquí el parámetro AUTH requerido por su servidor.

Contraseña AUTH
Registre aquí la contraseña AUTH.

Enviar este comando al host (dejar en blanco si es suficiente con conectar)
Este control sirve para especificar la cadena de texto que se necesita enviar para que su correo sea liberado. Por ejemplo, el método `ETRN` requiere el texto "`ETRN`" seguido por el nombre de dominio del sitio que está siendo desencolado. Otros métodos requieren el envío de diferentes textos. Consulte con su ISP si necesita más información sobre qué enviar para desbloquear su cola de correo. Si puede elegir el método a utilizar, recomendamos que use Transmisión bajo demanda (On-Demand Mail Relay - ODMR) 209 siempre que le resulte posible. ODMR requiere que se use el comando ATRN en esta opción.

Desencolar ocurre cada [xx] veces que se procese el correo remoto (0=siempre)
Por defecto la señal de desencolamiento se enviará cada vez que se procese el correo remoto. Si introduce un número en este control se impedirá que la señal se envíe siempre. Se enviará cada x veces según se defina. Por ejemplo, si se configura este valor a "3", la señal se enviará cada tercera vez que se procese el correo remoto.

Este es un ajuste global y aplica a todos los dominios.

Transmisión bajo demanda (ODMR - On-Demand Mail Relay)

Cuando necesite un método para colocar/quitar de cola a fin de almacenar y liberar su correo, recomendamos que use On-Demand Mail Relay (ODMR) siempre que le sea posible. Este método es superior a ETRN y otros métodos ya que requiere autenticación antes de que el correo sea liberado. Además, si utiliza un comando ESMTP llamado `ATRN`, no se requiere que el cliente tenga una dirección IP estática, porque inmediatamente establece el flujo de datos entre el cliente y el servidor y libera los mensajes sin tener que realizar una nueva conexión (a diferencia de ETRN).

MDaemon soporta ODMR plenamente en el lado del cliente utilizando el comando `ATRN` y los controles de autenticación en la pantalla de Entrega de correo 206, y en el lado del servidor utilizando las funcionalidades de Puertas de Enlace en la pantalla Sacar de lista de espera 269 del editor de Puertas de Enlace.

Algunos servidores de correo no tienen soporte para ODMR, así pues, debe comprobar con su proveedor antes de intentar utilizarlo.

Ver:

Entrega de Correo 206
Editor de Puerta de Enlace » Sacar de lista de espera 269

3.2.7.1 Transmisión bajo demanda

Cuando necesite un método para colocar/quitar de cola a fin de almacenar y liberar su correo, recomendamos que use On-Demand Mail Relay (ODMR) siempre que le sea posible. Este método es superior a ETRN y otros métodos ya que requiere autenticación antes de que el correo sea liberado. Además, si utiliza un comando ESMTP llamado `ATRN`, no se requiere que el cliente tenga una dirección IP estática, porque inmediatamente establece el flujo de datos entre el cliente y el servidor y libera los mensajes sin tener que realizar una nueva conexión (a diferencia de ETRN).

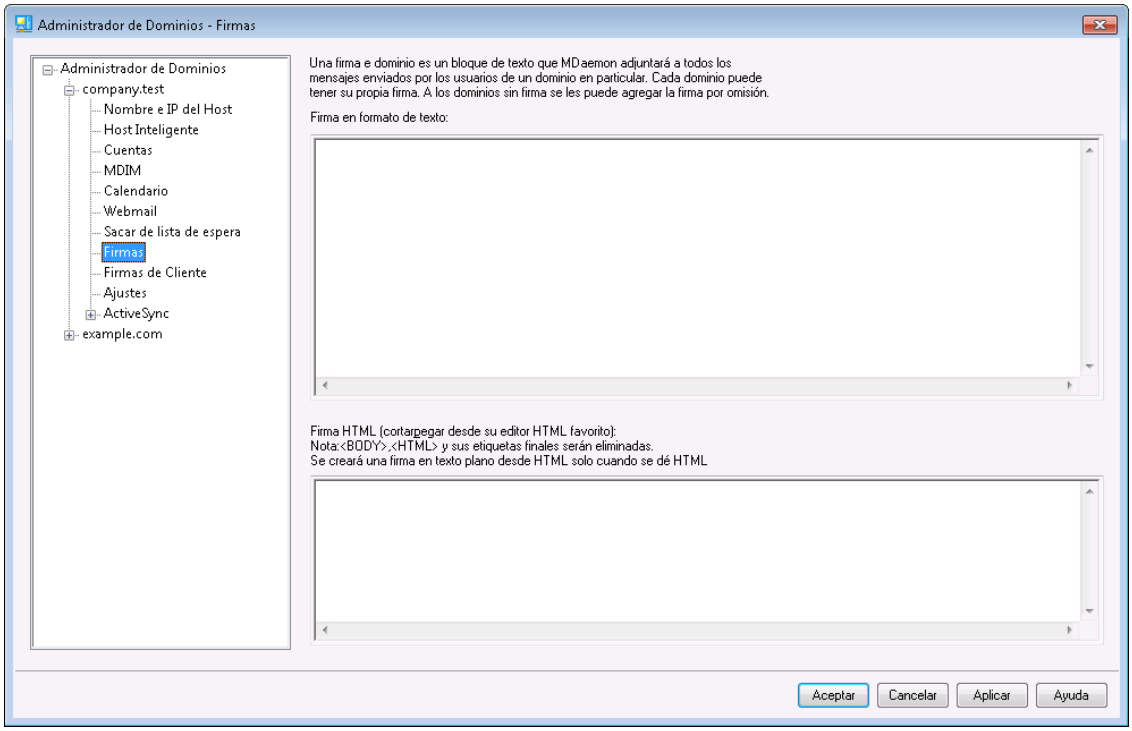
MDaemon soporta ODMR plenamente en el lado del cliente utilizando el comando `ATRN` y los controles de autenticación en la pantalla de Entrega de correo 206, y en el lado del servidor utilizando las funcionalidades de Puertas de Enlace en la pantalla Sacar de lista de espera 269 del editor de Puertas de Enlace.

Algunos servidores de correo no tienen soporte para ODMR, así pues, debe comprobar con su proveedor antes de intentar utilizarlo.

Ver:

Entrega de Correo 206
Editor de Puerta de Enlace » Sacar de lista de espera 269

3.2.8 Firmas



Utilice esta pantalla para agregar una firma a todos los mensajes enviados por los usuarios de este dominio. Si no se especifica firma aquí entonces se agregará la Firma por Omisión 142. Las firmas se agregan al final de los mensajes, excepto en mensajes de Listas que utilizan un pie de página 302, en cuyo caso éste se agrega abajo de la firma. También puede utilizar la funcionalidad de Firmas 753 en el Editor de Cuentas, para agregar firmas individuales a cada Cuenta. La firma de la cuenta se agrega antes de la Firma por Omisión o de la Firma del Dominio.

Firma en Texto Plano

Esta área es para insertar una firma en texto plano. Si desea definir una firma HTML para ser utilizada en el segmento texto/HTML de mensajes multiparte, utilice el área *Firma HTML* que aparece abajo. Si se incluye una firma en ambos lugares, entonces MDaemon utilizará la firma indicada para cada segmento, en el caso de mensajes multiparte. Si no se especifica firma HTML entonces se utilizará la firma en texto plano para ambos segmentos.

Firma HTML (cortar & pegar desde su editor HTML favorito)

Este espacio es para insertar una firma HTML, a ser utilizada en el segmento texto/HTML de mensajes multiparte. Si se incluye una firma tanto aquí como en el área *Firma en texto plano*, MDaemon utilizará la firma adecuada para cada

segmento del mensaje multiparte. Si no se especifica firma en texto plano entonces se utilizará la firma HTML.

Para crear una firma HTML, puede teclear directamente el código HTML o cortar&pegar desde su editor HTML favorito. Si desea incluir imágenes en línea en su firma HTML, lo puede hacer utilizando la macro `$ATTACH_INLINE:path_to_image_file$`.

Por ejemplo:

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

También existen varias maneras de insertar imágenes en línea desde la Administración Remota 354 de MDaemon:

- En la pantalla Firma/Pie en la Administración Remota, dé clic en el botón "Imagen" en la barra de herramientas del editor HTML y seleccione la pestaña para subir archivos.
- En la pantalla Firma/Pie en la Administración Remota, dé clic en el botón "Agregar Imagen" en la barra de herramientas del editor HTML.
- Arrastre y suelte una imagen en la pantalla Firma/Pie en el editor HTML desde Chrome, Firefox, Safari o MSIE 10+.
- Copie y pegue una imagen desde el portapapeles en la pantalla Firma/Pie en el editor HTML utilizando Chrome, Firefox o MSIE 11+

Las etiquetas <body></body> y <html></html> no se permiten en firmas y serán eliminadas si se encuentran.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje siempre que quieran que aparezca la firma,

Signature Selector	
$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.

$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**

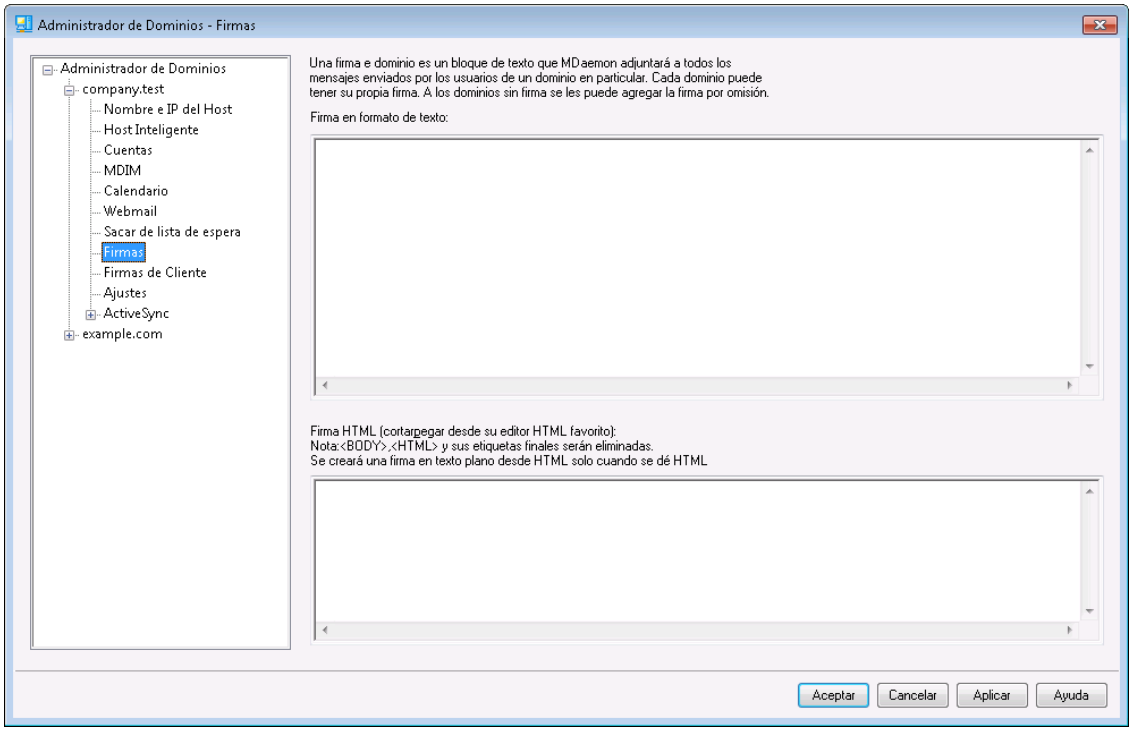
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**
Gerencia	**$CONTACTBUSINESSMANAGER$**
Asistente	**$CONTACTBUSINESSASSISTANT$**
Teléfono Asistente	**$CONTACTBUSINESSASSISTANTPHONE$**
Teléfono directo en la Empresa	**$CONTACTBUSINESSMAINPHONE$**
Teléfono de la Empresa	**$CONTACTBUSINESSPHONE$**
Teléfono 2 de la Empresa	**$CONTACTBUSINESSPHONE2$**
Teléfono IP de la Empresa	**$CONTACTBUSINESSIPPHONE$**
Fax de la Empresa	**$CONTACTBUSINESSFAX$**
Pager de la Empresa	**$CONTACTBUSINESSPAGER$**
Radio de la Empresa	**$CONTACTBUSINESSRADIO$**
Dirección de la Empresa	**$CONTACTBUSINESSADDRESS$**

Ciudad de la Empresa	**$CONTACTBUSINESSCITY$**
Estado de la Empresa	**$CONTACTBUSINESSSTATE$**
Código Postal de la Empresa	**$CONTACTBUSINESSZIPCODE$**
País de la Empresa	**$CONTACTBUSINESSCOUNTRY$**
Sitio web de la Empresa	**$CONTACTBUSINESSWEBADDRESS$**
Otros	
Esposo(a)	**$CONTACTSPOUSE$**
Hijos	**$CONTACTCHILDREN$**
Categorías	**$CONTACTCATEGORIES$**
Comentario	**$CONTACTCOMMENT$**

Ver:

Firmas por Omisión 142
Editor de Cuentas » Firmas 753

3.2.9 Firmas de Cliente



Utilice esta pantalla para crear una firma de cliente para este dominio, que pueda entregar a MDaemon Webmail 201 y a MDaemon Connector 404, para ser utilizada por sus usuarios al redactar mensajes de correo. Puede utilizar los macros 216 listados abajo para personalizar la firma, de manera que será única para cada usuario, incluyendo elementos como el nombre del usuario, la dirección de correo, número de teléfono y demás. Utilice la pantalla Firmas de Cliente por Omisión 147 si desea crear una firma diferente que sea utilizada cuando no exista firma de cliente específica para el dominio. Cuando existe una firma específica para el dominio, se utilizará en lugar de la Firma de Cliente por Omisión. Utilice la opción *Entregar firma de cliente* 201 si desea entregar la firma de cliente a Webmail y la opción *Entregar firma de cliente en Outlook* 404 si desea entregarla a MDaemon Connector. En las opciones de Redacción de Webmail, la firma de cliente entregada se denomina "Sistema." Para MDaemon Connector puede definir un nombre para la firma y este aparecerá en Outlook.

Firma en Texto Plano

Este espacio es para insertar una firma en texto plano. Si desea definir en correspondencia una firma html a ser utilizada en la sección text/html de mensajes multiparte, utilice el área abajo *firma HTML*. Si una firma se incluye en ambos lugares, MDaemon utilizará la apropiada para cada parte del mensaje multiparte. Si no se especifica firma html, entonces se utilizará la firma en texto plano en ambas partes.

Firma HTML (cortar &pegar desde su editor HTML favorito)

Esta área es para insertar una firma HTML a ser utilizada en la parte text/html de mensajes multiparte. Si se incluye una firma aquí y en el área *Firma en Texto Plano* arriba, MDaemon utilizará la apropiada para cada parte del mensaje multiparte. Si no se especifica firma en texto plano entonces se utilizará la firma html para crear una.

Para crear su firma html, teclee el código html aquí manualmente o copie & pegue directamente desde su editor HTML favorito. Si desea incluir imágenes en línea en su firma HTML, lo puede hacer utilizando la macro `$ATTACH_INLINE:path_to_image_file$`.

Por ejemplo:

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

También existen varias maneras en que puede insertar imágenes en línea en firmas desde la interface web de MDaemon Administración Remota 354:

- En la pantalla Firma de Cliente en Administración Remota, dé clic en el botón de la barra de herramientas "Imagen" en el editor HTML y seleccione la pestaña de carga.
- En la pantalla Firma de Cliente en Administración Remota, dé clic en el botón de la barra de herramientas "Agregar Imagen" en el editor HTML.
- Arrastre y suelte una imagen en la pantalla del editor HTML de la Firma de Cliente con Chrome, FireFox, Safari, o MSIE 10+
- Copie y pegue una imagen desde el portapapeles en la pantalla del editor HTML de la Firma de Cliente con Chrome, FireFox, MSIE 11+

Las etiquetas <body></body> y <html></html> no están permitidas en las firmas y serán eliminadas si se encuentran.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje siempre que quieran que aparezca la firma,

Signature Selector	
$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.

$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**

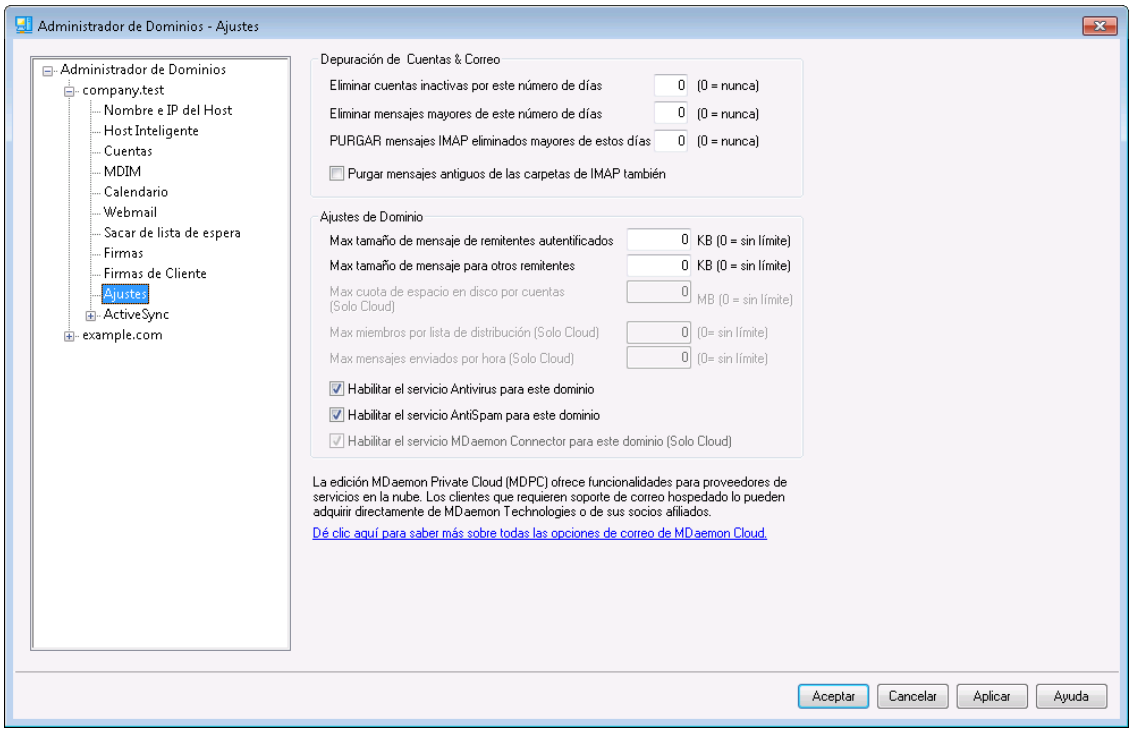
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**
Gerencia	**$CONTACTBUSINESSMANAGER$**
Asistente	**$CONTACTBUSINESSASSISTANT$**
Teléfono Asistente	**$CONTACTBUSINESSASSISTANTPHONE$**
Teléfono directo en la Empresa	**$CONTACTBUSINESSMAINPHONE$**
Teléfono de la Empresa	**$CONTACTBUSINESSPHONE$**
Teléfono 2 de la Empresa	**$CONTACTBUSINESSPHONE2$**
Teléfono IP de la Empresa	**$CONTACTBUSINESSIPPHONE$**
Fax de la Empresa	**$CONTACTBUSINESSFAX$**
Pager de la Empresa	**$CONTACTBUSINESSPAGER$**
Radio de la Empresa	**$CONTACTBUSINESSRADIO$**
Dirección de la Empresa	**$CONTACTBUSINESSADDRESS$**

Ciudad de la Empresa	**$CONTACTBUSINESSCITY$**
Estado de la Empresa	**$CONTACTBUSINESSSTATE$**
Código Postal de la Empresa	**$CONTACTBUSINESSZIPCODE$**
País de la Empresa	**$CONTACTBUSINESSCOUNTRY$**
Sitio web de la Empresa	**$CONTACTBUSINESSWEBADDRESS$**
Otros	
Esposo(a)	**$CONTACTSPOUSE$**
Hijos	**$CONTACTCHILDREN$**
Categorías	**$CONTACTCATEGORIES$**
Comentario	**$CONTACTCOMMENT$**

Ver:

Firmas de Cliente por Omisión 147
Firmas por Omisión 142
Administrador de Dominios » Firmas 210
Editor de Cuentas » Firma 753
Administrador de Dominios » Ajustes de Webmail 201
Ajustes de Cliente OC » Firma 404

3.2.10 Ajustes



Depuración de Cuentas & Correo

Estas opciones se utilizan para definir cuándo y si las cuentas inactivas o los mensajes antiguos, serán eliminados por MDaemon. Cada día a medianoche, MDaemon eliminará todos los mensajes y cuentas que hayan excedido los límites de tiempo establecidos aquí. Existen opciones similares en la pantalla Cuotas[733] del Editor de Cuentas, que se pueden utilizar para anular esta configuración para cuentas individuales.

Vea el archivo `AccountPrune.txt` en la carpeta "…`MDaemon\App\`" para obtener más información y opciones de línea de comandos.

Eliminar la cuenta si permaneció inactiva por este número de días (0 = nunca)
Especifique el número de días que desea permitir que una cuenta perteneciente al dominio permanezca inactiva antes de ser eliminada. Un valor de "0" en este control significa que las cuentas nunca serán eliminadas por inactividad.

Eliminar mensajes mayores de este número de días (0 = nunca)
El valor especificado en este control es el número de días que cualquier mensaje dado puede residir en el buzón del usuario antes de ser eliminado automáticamente por MDaemon. Un valor de "0" en este control significa que los mensajes nunca serán eliminados por su antigüedad. **Nota:** El ajuste de esta opción no aplica a mensajes contenidos en carpetas IMAP a menos que también habilite la opción siguiente "*PURGAR también mensajes antiguos de las carpetas IMAP*"

Depurar mensajes IMAP eliminados, mayores de este número de días (0 = nunca)
Utilice este control para especificar el número de días que desea permitir que los mensajes IMAP queden marcados para eliminación permanezcan en las carpetas de sus usuarios. De estos mensajes, los que tengan más días de los aquí determinados, serán borrados de los buzones. El valor de "0" significa que los mensajes marcados para eliminación nunca serán borrados debido a su edad.

PURGAR también mensajes antiguos de las carpetas IMAP
Dé clic en esta casilla si desea que el control "*Eliminar mensajes mayores de…*" se aplique también a los mensajes contenidos en carpetas IMAP. Cuando este control está deshabilitado, los mensajes contenidos en carpetas IMAP no serán borrados, sin importar su edad.

Ajustes de Dominio

Tamaño máximo de mensajes de remitentes autentificados [xx] KB (0=sin límite)
Utilice esta opción si desea limitar el tamaño de los mensajes que puede enviar al dominio un remitente autentificado. El valor está en Kilobytes y se define en "0" por omisión, lo que significa que no tiene límite. Si desea definir un tamaño límite de mensaje para remitentes no autentificados, utilice la opción que se describe abajo: "*...otros remitentes*".

Tamaño máximo de mensajes para otros remitentes [xx] KB (0=sin límite)
Utilice esta opción si desea limitar el tamaño de los mensajes que pueden enviar a su dominio remitentes no autentificados. El valor se define en Kilobytes y se establece en "0" por omisión, lo que significa sin límite. Si desea establecer un

límite al tamaño de mensajes para remitentes autentificados utilice la opción descrita previamente.

Cuota máxima de espacio en disco [xx] MB (0=sin límite) (Solo Cloud)
Utilice esta opción si desea establecer un límite sobre cuanto espacio en disco puede utilizar un dominio. Esta opción solo está disponible en MDaemon Private Cloud.

No. Max. de miembros por lista de correo [xx] (0=sin límite) (Solo Cloud)
Utilice esta opción si desea establecer un número máximo permitido de miembros para cada una de las listas de distribución del dominio. Existe una opción global correspondiente en la pantalla Ajustes 277 del Administrador de Listas de Distribución.

No. Max de mensajes enviados por hora [xx] (0=sin límite) (Solo Cloud)
Utilice esta opción si desea definir el número máximo de mensajes que puede enviar un dominio por hora. Una vez que se alcanza este límite, los mensajes subsecuentes quedan en la cola hasta que se restablece el conteo. El conteo de mensajes se restablece cada hora y cuando se reinicia el servidor Esta opción solo está disponible en MDaemon Private Cloud.

Habilitar el servicio de Antivirus para este dominio
Dé clic en esta casilla si desea que se apliquen los ajustes del AntiVirus 645 a este dominio.

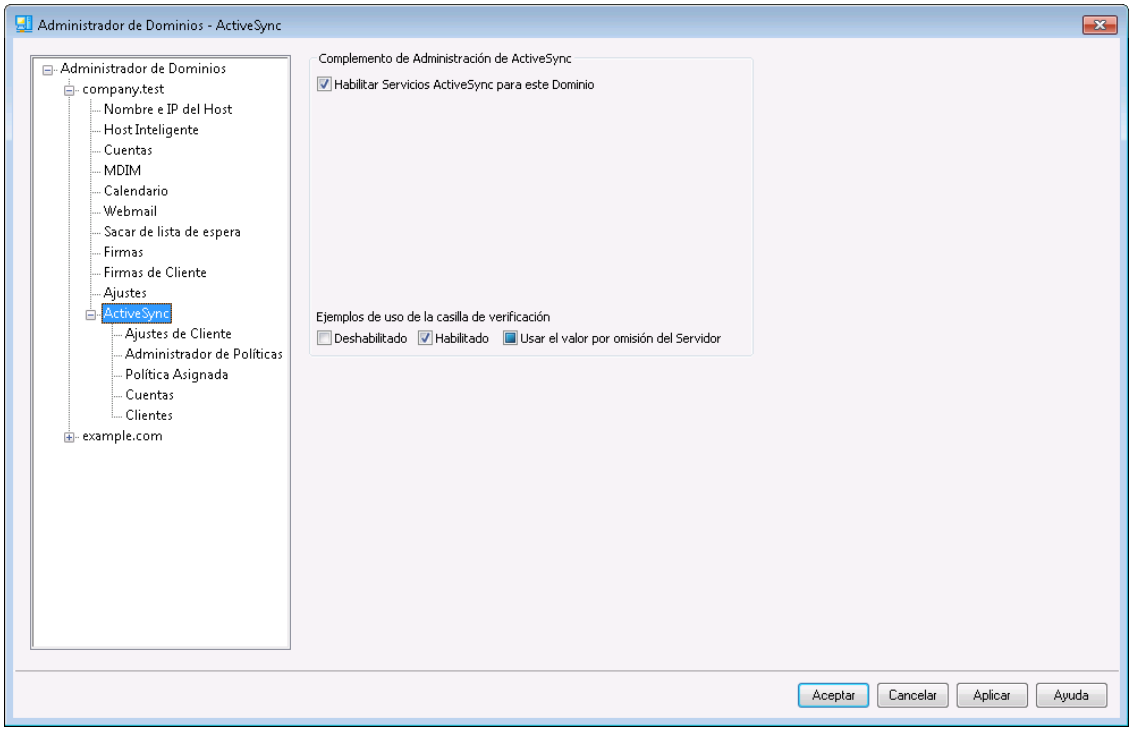
Habilitar el servicio de AntiSpam para este dominio
Dé clic en esta casilla si desea que la configuración del filtro de Spam de MDaemon se aplique a este dominio.

Habilitar MDaemon Connector para este dominio (Solo Cloud)
Marque esta casilla si desea habilitar el servicio MDaemon Connector 387 para este dominio.

Ver:

Editor de Cuentas » Cuotas 733

3.2.11 ActiveSync



Utilice esta sección de Administrador de Dominios para administrar los ajustes de ActiveSync 416 para cada dominio. Puede administrar todos los ajustes de ActiveSync y valores por omisión para todos los dominios desde la pantalla Dominios 434 en la Administración de ActiveSync.

Complemento de Administración de ActiveSync para MDaemon

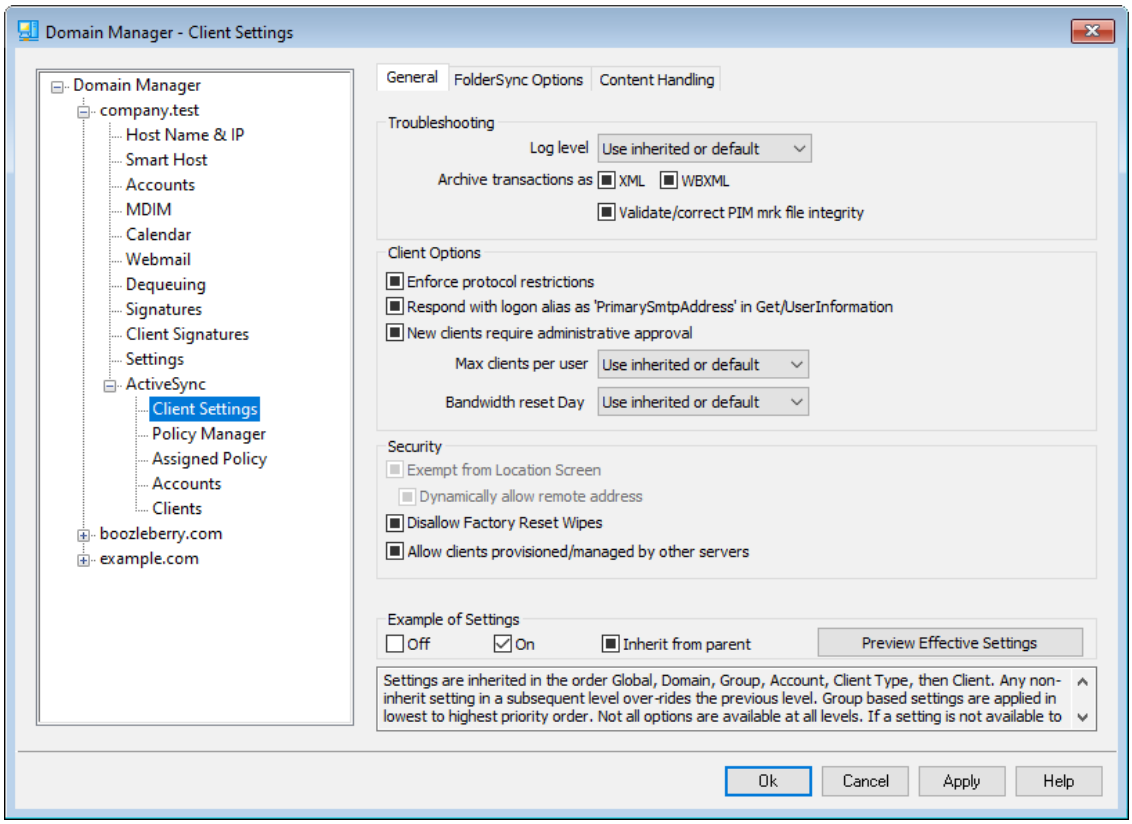
Habilitar el servicio ActiveSync para este Dominio
Esta opción controla si los usuarios del dominio pueden o no habilitar el uso de clientes ActiveSync para tener acceso a su correo y datos PIM. Por omisión este ajuste se hereda del Estado por Omisión de ActiveSync 434, pero puede invalidar este ajuste si selecciona el valor en la casilla a Habilitado o Deshabilitado. Este ajuste también se puede invalidar para cualesquiera cuentas 451 o clientes 460 que no desee que utilicen los ajustes por omisión del dominio. **NOTA:** Si deshabilita ActiveSync para este dominio, se abrirá una caja de confirmación para preguntarle si desea revocar el acceso vía ActiveSync a todos los usuarios del dominio. Seleccione **No** si desea permitir que cualquiera de los usuarios del dominio que actualmente utilizan ActiveSync, continúen utilizándolo. Si selecciona **Si**, ActiveSync será deshabilitado para todos los usuarios del dominio.

El ajuste a nivel dominio simplemente controla si las cuentas del dominio tendrán permiso de utilizar ActiveSync por omisión. La opción global para **Habilitar el Protocolo ActiveSync** 416 debe estar habilitada a fin de que ActiveSync sea accesible a cualquiera de los dominios o cuentas permitidos.

Ver:

ActiveSync » Dominios 434
ActiveSync » Cuentas 451
ActiveSync » Clientes 460

3.2.11.1 Ajustes de Cliente



Esta pantalla le permite administrar los ajustes por omisión para cuentas y clientes asociados con un dominio. Por omisión, todas las opciones en esta pantalla están configuradas para "Use el heredado o el de omisión", lo que significa que cada opción tomara su valor de la opción correspondiente en la pantalla Ajustes Globales de Cliente 421. Similarmente, las cuentas 197 de este dominio heredarán sus valores de esta pantalla, ya que es su pantalla padre. Cualquier modificación hecha a las opciones en esta pantalla se reflejará en esas pantallas de cuenta. Debajo de eso, los clientes 247 individuales también tienen pantallas de ajuste que heredan su configuración de los ajustes a nivel cuenta. Esta configuración le permite hacer modificaciones a todas las cuentas de un dominio y sus clientes simplemente haciendo modificaciones en esta pantalla y también posibilita que se omitan esos ajustes para cualquier cuenta o cliente como se requiera.

General

Resolución de problemas

Nivel de Registro

ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk

Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo

Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de*

Protocolo Permitidas definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que

pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync.

Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas[314] a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta[316] para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas[314] padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas[128] a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas[743] a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes[460] y tipos de clientes[475] que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura

para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

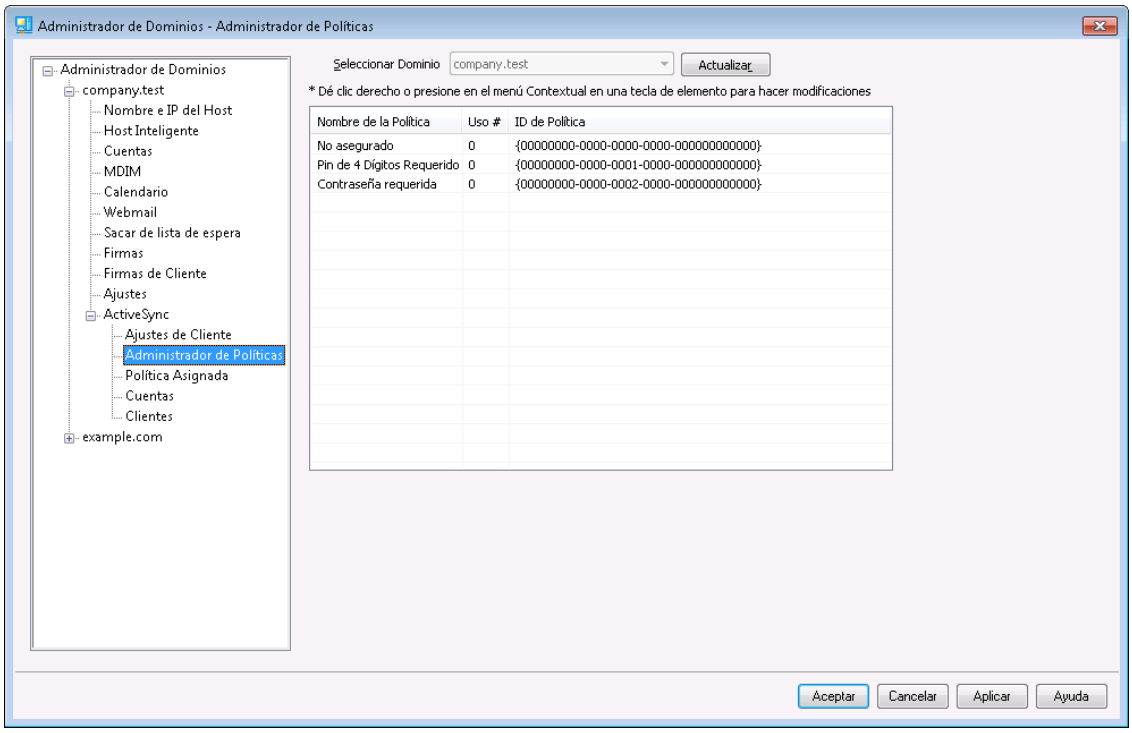
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Ajustes de Cliente 421
ActiveSync » Cuentas 451
ActiveSync » Clientes 460

3.2.11.2 Administrador de Políticas



Utilice esta pantalla para administrar las Políticas ActiveSync que pueden asignarse a dispositivos de usuario para controlar varias opciones. Se proporcionan políticas predefinidas y usted puede crear, editar y eliminar las que requiera. Es posible definir políticas por omisión al dominio y particulares para cada cuenta y cliente en sus pantallas respectivas de Políticas Asignadas.

No todos los dispositivos ActiveSync reconocen o aplican políticas consistentemente. Algunos pueden ignorar las políticas o ciertos elementos de política y otros pueden requerir un reinicio del dispositivo antes de que tengan efecto los cambios. Más aun, al intentar asignar una política nueva a un dispositivo, no se aplicará al mismo hasta la siguiente ocasión en que se conecte por sí mismo al servidor ActiveSync; las políticas no pueden "entregarse" a los dispositivos hasta que se conecten.

Políticas ActiveSync

Dé clic derecho en la lista para abrir un menú de acceso rápido a las opciones siguientes:

Crear Política
Dé clic en esta opción para abrir el Editor de Políticas ActiveSync, que se utiliza para crear y editar políticas.

Eliminar
Para eliminar una política, seleccione una política personalizada de la lista y de clic en **Eliminar**. Dé clic en **Sí** para confirmar la acción. Las políticas

predeterminadas no se pueden eliminar.

Editar Política
Para editar una política, dé clic derecho en una política personalizada en la lista y luego clic en **Editar Política**. Luego de hacer las modificaciones deseadas en el editor de políticas, dé clic en **OK**. Las políticas predeterminadas no se pueden editar.

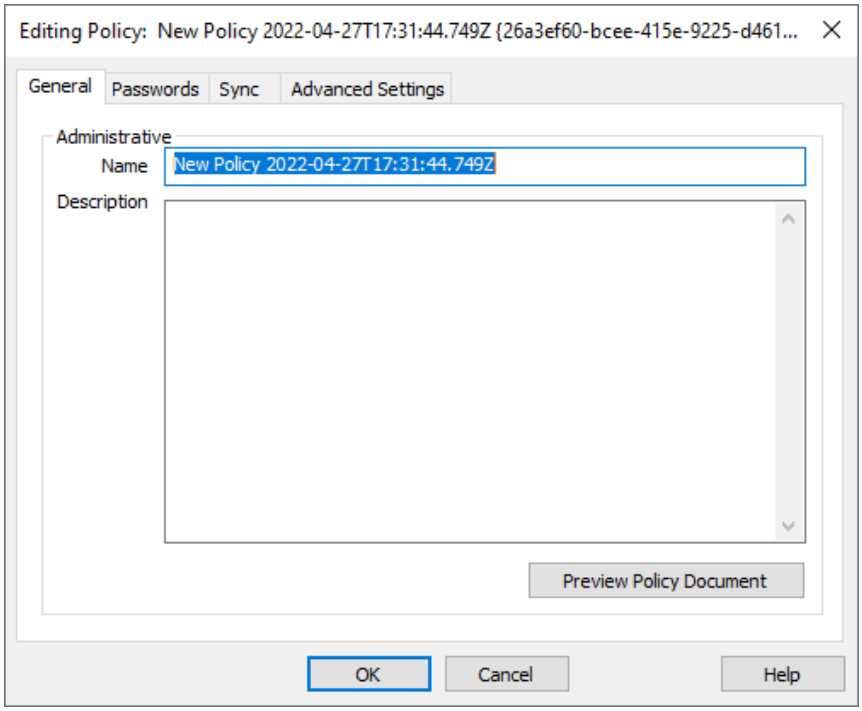
Visualizar Uso de Políticas
Dé clic derecho en una política y luego seleccione esta opción para visualizar una lista de todos los dominios, cuentas y clientes que están configurados para utilizar esta política.

Editor de Políticas ActiveSync

El Editor de Políticas ActiveSync cuenta con 4 pestañas: General, Contraseñas, Sync y Ajustes Avanzados. La pestaña de Ajustes Avanzados está oculta a menos que active *Habilitar la edición de opciones avanzadas de políticas*416, localizada en la pantalla ActiveSync Sistema.

General

Utilice esta pantalla para definir un nombre y descripción para su política. También puede tener una vista previa del documento XML de la política.



Administrativo

Nombre
Especifique aquí un nombre para su política personalizada.

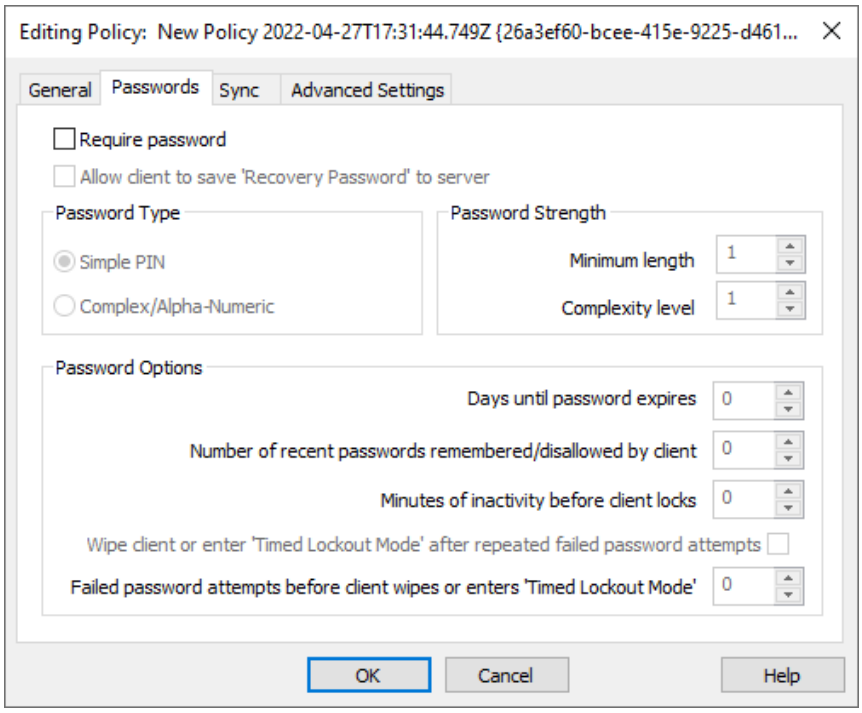
Descripción
Utilice esta área para describir su política personalizada. Esta descripción aparece en el diálogo Aplicar Política al seleccionar una política para aplicarla

a un dominio, cuenta o cliente.

Vista Previa del Documento de Política
Dé clic en este botón para una vista previa del documento XML de esta política.

Contraseñas

Las opciones de Contraseña y requerimientos para esta política se definen en esta pestaña.



Requerir contraseña
Marque esta caja si desea requerir contraseña en el dispositivo. Está deshabilitada por omisión.

Permitir al dispositivo grabar "Contraseña de Recuperación" en el servidor.
Habilite esta opción si desea permitir a los clientes utilizar la opción de Recuperación de Contraseña ActiveSync, que le permite al dispositivo grabar una contraseña temporal de recuperación en el servidor para desbloquear el dispositivo si la contraseña se olvida. El administrador puede encontrar esta contraseña de recuperación bajo los Detalles 460 del cliente. La mayoría de los dispositivos no soportan esta funcionalidad.

Tipo de Contraseña

PIN Simple
La manera en que se implementa es opción depende principalmente del dispositivo, pero seleccionar *PIN Simple PIN* como tipo de contraseña

generalmente significa que no hay restricciones o requerimientos de complejidad para la contraseña del dispositivo, más que la opción siguiente *Longitud Mínima de Contraseña.* Esta permite contraseñas simples tales como: "111," "aaa," "1234," "ABCD" y similares.

Compleja Alfa/Numérica
Utilice esta opción de política si desea requerir contraseñas más complejas y seguras en el dispositivo en lugar de la opción *PIN Simple*. Utilice la opción siguiente *Nivel de Complejidad* para definir exactamente qué tan compleja debe ser la contraseña. Esta es la selección por omisión cuando se requiere una contraseña con esta política.

Seguridad de la Contraseña

Longitud Mínima
Utilice esta opción para definir el número de caracteres mínimo que debe contener la contraseña del dispositivo, de 1 a 16. Esta opción está configurada como "1" por omisión.

Nivel de Complejidad
Utilice esta opción para establecer el requerimiento de nivel de complejidad de las contraseñas como *Compleja/Alfanumérica*. El nivel es el número de tipos diferentes de caracteres que debe contener la contraseña: mayúsculas, minúsculas, números y caracteres no-alfanuméricos (tales como signos de puntuación o caracteres especiales). Puede requerir de 1 a 4 tipos de caracteres. Por ejemplo, si esta opción se configura en "2", entonces la contraseña debe contener por lo menos dos de los cuatro tipos de caracteres: mayúsculas y números, mayúsculas y minúsculas, números y símbolos, etc. Esta opción se configura como "1" por omisión.

Opciones de Contraseña

Días para que expire la contraseña (0=nunca)
Este es el número de días permitido antes de que la contraseña del dispositivo deba ser modificada. La opción se encuentra deshabilitada por omisión (configurada en "0").

Número de contraseñas recientes a recordar/deshabilitar por dispositivo (0=ninguna)
Utilice esta opción si desea prevenir que el dispositivo reutilice un número específico de contraseñas anteriores. Por ejemplo, si esta opción se configura como "2" y usted modifica la contraseña del dispositivo, no podrá cambiarla a ninguna de las últimas dos contraseñas que haya utilizado. Esta opción está deshabilitada por omisión (configurada en "0").

Minutos de inactividad antes de que se bloquee el dispositivo (0=nunca)
Esta es la cantidad de minutos que puede funcionar un dispositivo sin interacción del usuario antes de que se bloquee. Esta opción de contraseña se encuentra deshabilitada por omisión (configurada en "0").

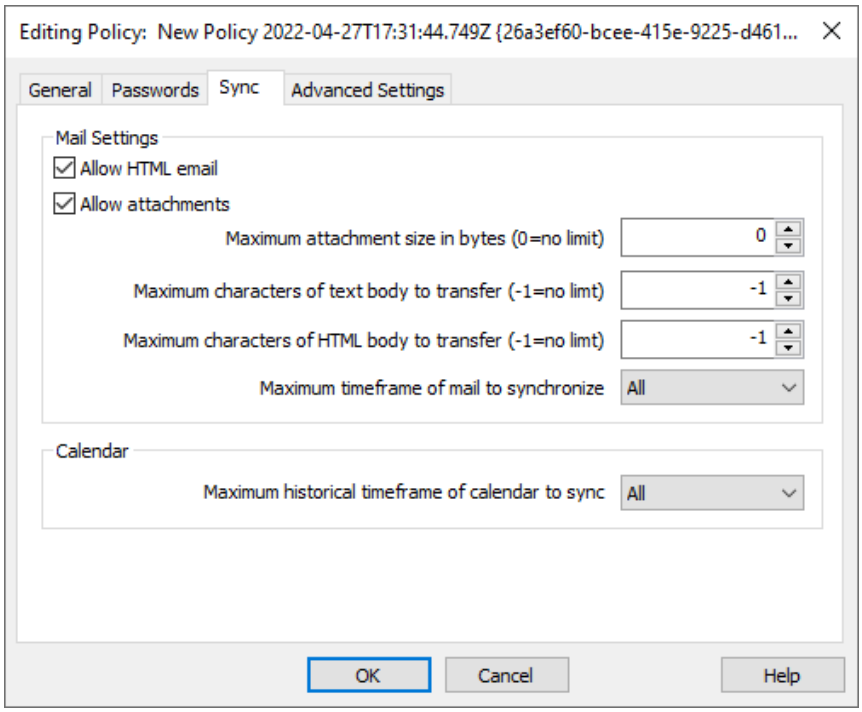
Borrar el dispositivo o pasarlo a 'Modo de Bloqueo' luego de intentos fallidos de contraseña
Cuando esta opción está habilitada y el usuario falla el número determinado de intentos de contraseña, el dispositivo se bloqueará durante cierto tiempo

o ejecutará un borrado de todos los datos, dependiendo del dispositivo. Esta opción está deshabilitada por omisión.

Intentos fallidos de contraseña antes de que el dispositivo se borre o entre en "Modo Bloqueo"
Cuando la opción "*Borrar el Dispositivo...*" descrita arriba está habilitada y el usuario falla este número de intentos de contraseña, el dispositivo será borrado o se detonará el 'Modo de Bloqueo' dependiendo del dispositivo.

Sync

Esta pantalla contiene varios ajustes que administran el correo HTML, permitiendo adjuntos, limitando el número de caracteres a transferir y el rango de tiempo máximo de correo y calendario a sincronizar.



Ajustes de Correo

Permitir correo HTML
Por omisión, se puede sincronizar/enviar correo con formato HTML a los clientes ActiveSync. Deshabilite esta caja si desea enviar solo texto plano.

Permitir adjuntos
Permite al dispositivo descargar archivos adjuntos. La opción está habilitada por omisión.

Max tamaño de adjuntos en bytes (0=sin límite)
Este es el tamaño máximo de adjunto que se puede descargar en automático al dispositivo. Por omisión el tamaño de adjunto no tiene

límite (configurado a "0").

Máximo de caracteres a transferir en el cuerpo del mensaje en texto plano (-1=sin límite)
Este es el número máximo de caracteres en el cuerpo de mensajes con formato en texto plano que se enviará al cliente. Si el cuerpo del mensaje contiene más caracteres de los permitidos, será truncado al límite especificado. Por omisión no está configurado ningún límite (la opción está configurada a "-1"). Si establece la opción a "0" solo se enviará el encabezado del mensaje.

Máximo de caracteres a transferir en el cuerpo del mensaje HTML (-1=sin límite)
Este es el número máximo de caracteres en el cuerpo de mensajes con formato HTML que se enviará al cliente. Si el cuerpo del mensaje contiene más caracteres de los permitidos, será truncado al límite especificado. Por omisión no está configurado ningún límite (la opción está configurada a "-1"). Si establece la opción a "0" solo se enviará el encabezado del mensaje.

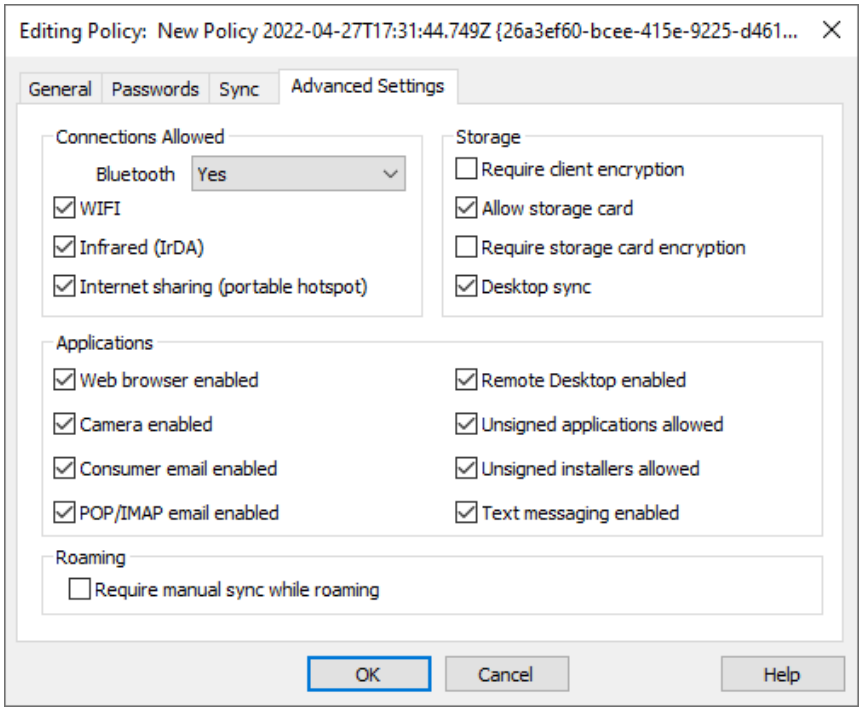
Máximo lapso para sincronizar correo
Esta es la cantidad de correo anterior por rango de fecha desde hoy, que puede sincronizarse al dispositivo. Por omisión está configurado a "Todo", lo que significa que todo el correo se puede sincronizar sin importar su antigüedad.

Calendario

Máximo lapso para sincronizar calendario
Esto es que tan atrás a partir de hoy se sincronizarán registros del calendario al dispositivo. Por omisión está configurado como "Todo", lo que significa que todos los registros pasados serán sincronizados sin importar su antigüedad.

Ajustes Avanzados

La pestaña de Ajustes Avanzados contiene opciones que controlan los tipos de conexiones permitidas y si ciertas aplicaciones pueden ser habilitadas, el almacenamiento, encripción y roaming.



Esta pestaña está oculta a menos que active *Habilitar la edición de políticas avanzadas* 416, localizada en la pantalla ActiveSync para MDaemon.

Conexiones Permitidas

Bluetooth
Utilice esta opción para definir si se permiten conexiones Bluetooth en el dispositivo. Puede seleccionar **Si** para permitir conexiones Bluetooth, **No** para impedirlas o **Manos Libres** para restringir Bluetooth solo a Manos Libres. Esta opción está configurada a **Si** por omisión.

WIFI
Permite conexiones WIFI. Habilitada por omisión.

Infrarrojo (IrDA)
Permite conexiones infrarrojas (IrDA). Habilitada por omisión.

Compartir Internet (Punto de acceso portátil)
Esta opción permite al dispositivo utilizar el Internet compartido (punto de acceso portátil). Se encuentra habilitada por omisión.

Almacenamiento

Requerir encripción del dispositivo
Dé clic en esta opción si desea requerir encripción en el dispositivo. No todos los dispositivos soportan la encripción. Está deshabilitada por omisión.

Permitir tarjeta de almacenamiento
Permite que el dispositivo utilice una tarjeta de almacenamiento. Se encuentra habilitada por omisión.

Requerir encripción en la tarjeta de almacenamiento
Utilice esta opción si desea requerir encripción en la tarjeta de almacenamiento. Está deshabilitada por omisión.

Sincronización con el Escritorio
Permite ActiveSync en el Escritorio en el dispositivo. Está habilidad por omisión.

Aplicaciones

Navegador habilitado
Permite el uso el navegador en el dispositivo. No todos los dispositivos soportan esta opción y puede no aplicar a navegadores de terceros. Está habilitada por omisión.

Cámara habilitada
Permite utilizar la cámara en el dispositivo. Esta opción se encuentra habilitada por omisión.

Correo del consumidor habilitado
El dispositivo permite al usuario configurar una cuenta de correo personal. Cuando se deshabilita, los tipos de cuentas de correo o servicios que están prohibidos dependen por entero del cliente ActiveSync en particular. Esta opción está habilitada por omisión.

Correo POP/IMAP habilitado
Permite el acceso a correo POP o IMAP. Se encuentra habilitada por omisión.

Escritorio Remoto habilitado
Permite al cliente utilizar el Escritorio Remoto. Está habilitada por omisión.

Permitir aplicaciones no firmadas
Esta opción permite que se utilicen aplicaciones no firmadas en el dispositivo. Está habilitada por omisión.

Permitir instaladores no firmados
Esta opción permite que se ejecuten instaladores no firmados en el dispositivo. Está habilitada por omisión.

Mensajería de texto habilitada
Esta opción permite la mensajería de texto en el dispositivo. Se encuentra habilitada por omisión.

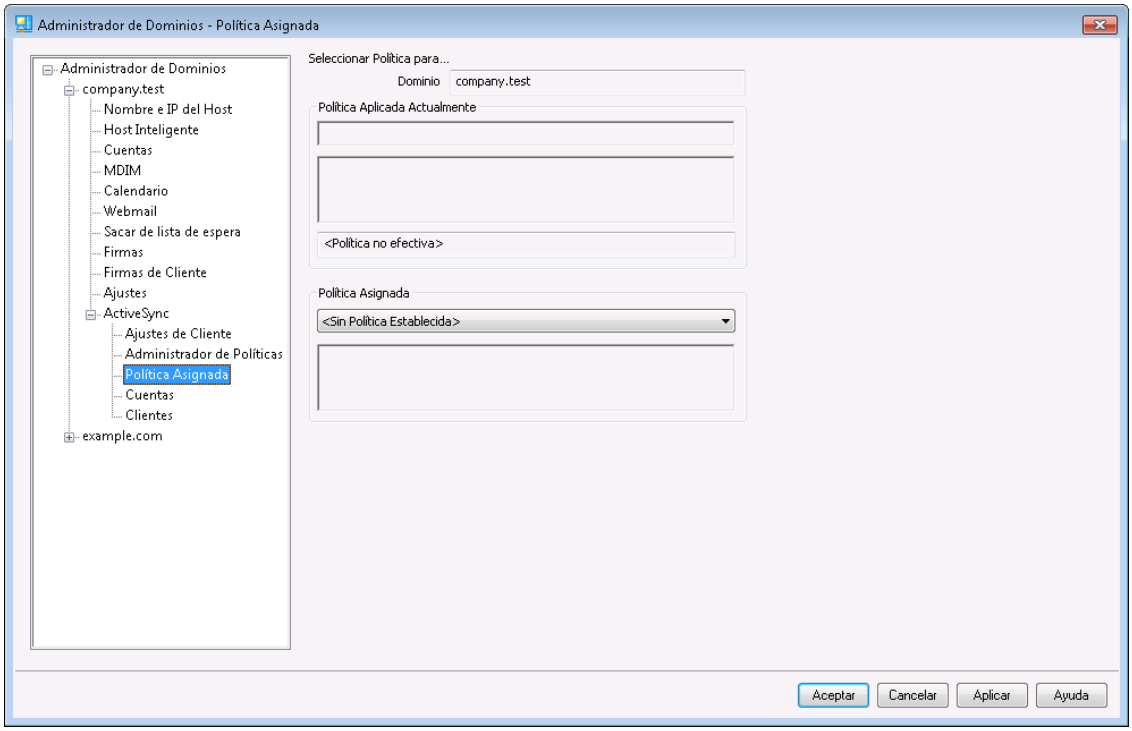
Roaming

Requerir sincronización manual cuando se encuentra en roaming
Utilice esta opción de política si desea requerir que el dispositivo se sincronice manualmente cuando se encuentra en roaming. El permitir la sincronización automática en roaming puede incrementar los costos de datos para el dispositivo, dependiendo de su carrier y su plan de datos. Esta opción está deshabilitada por omisión.

Ver:

[Administrador de Dominios » Políticas Asignadas](#) 237
[ActiveSync » Cuentas](#) 451
[ActiveSync » Clientes](#) 460

3.2.11.3 Políticas Asignadas



Utilice esta pantalla para asignar la Política ActiveSync 229 por omisión para el dominio. Cuando un cliente ActiveSync se conecta utilizando una de las cuentas del dominio, esta política se asignará al cliente, a menos que se haya configurado una política alterna específica para esa cuenta.

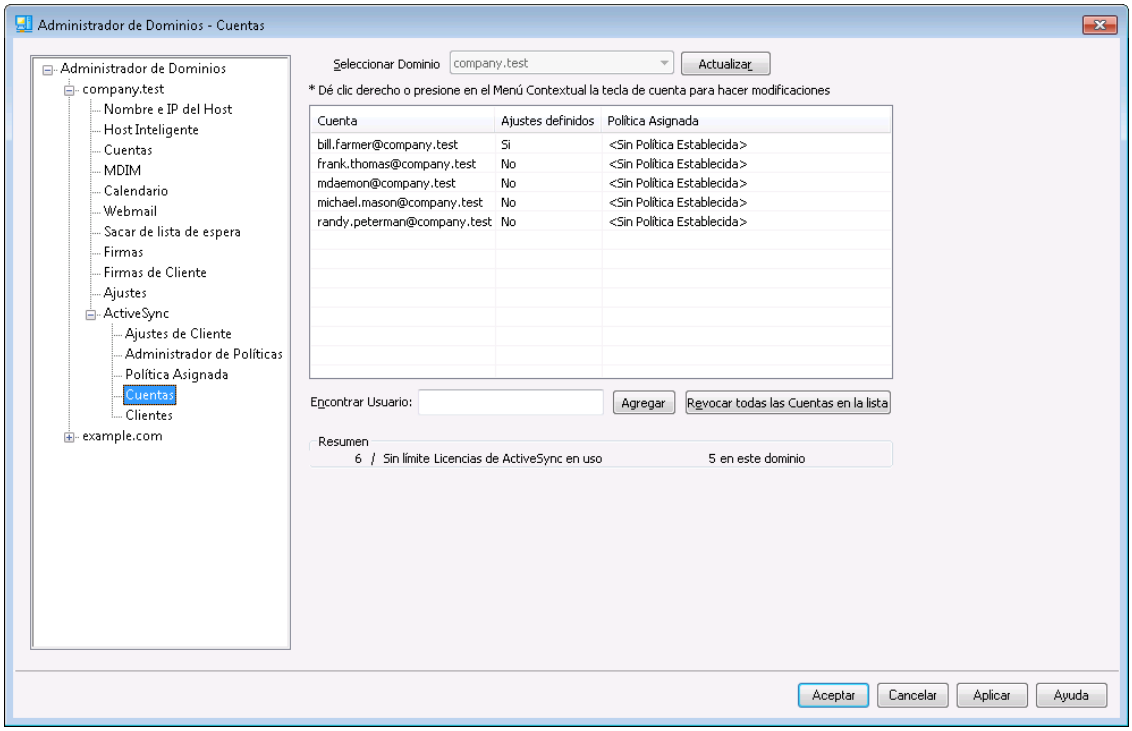
Asignando una Política ActiveSync por omisión

Para asignar una política ActiveSync por omisión para el dominio, dé clic en **Política a Asignar** en el menú desplegable, seleccione la política deseada y dé clic en **OK**.

Ver:

[Administrador de Dominios » Administrador de Políticas](#) 229
[ActiveSync » Cuentas](#) 451
[ActiveSync » Clientes](#) 460

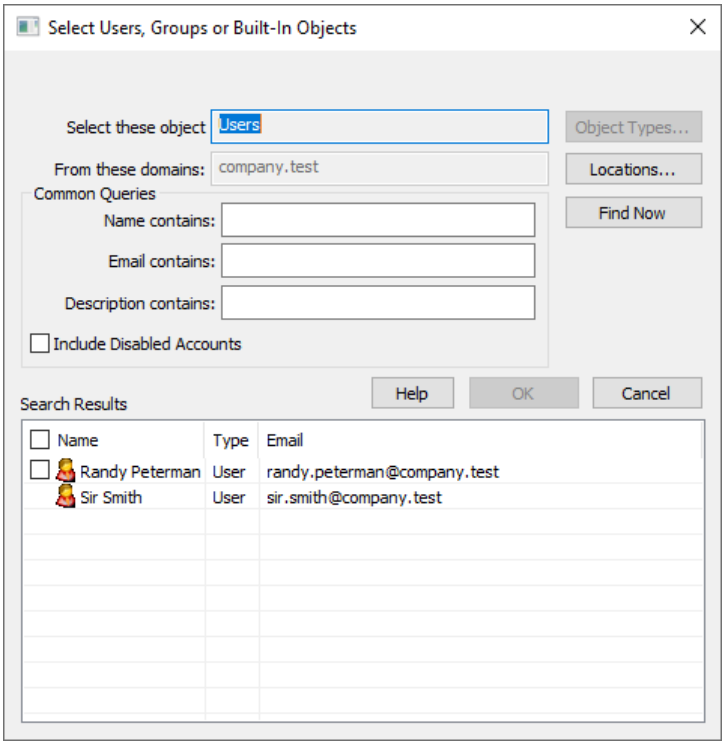
3.2.11.4 Cuentas



Utilice esta pantalla para definir las cuentas del dominio autorizadas para usar ActiveSync, también puede editar los ajustes de cliente de cada una de las cuentas autorizadas y asignar su política ActiveSync.

Autorizar Cuentas

Dé clic en **Agregar** para autorizar manualmente una o más de las cuentas del dominio para utilizar ActiveSync. Esto abre el diálogo Seleccionar Usuarios para encontrar y elegir las cuentas.



Consultas Comunes
Utilice las opciones en esta sección para reducir su búsqueda especificando todo o parte del nombre del usuario, dirección de correo o los contenidos de la Descripción[715] de la cuenta. Deje estos campos en blanco si desea que los resultados de la búsqueda contengan a todos los usuarios que coincidan con las ubicaciones especificadas arriba.

Incluir Cuentas Deshabilitadas

Marque esta caja si desea incluir en su búsqueda las cuentas deshabilitadas[715].

Encontrar Ahora
Luego de que ha definido todos sus criterios de búsqueda, dé clic en **Encontrar Ahora** para ejecutar la consulta.

Resultados de la Búsqueda
Luego de ejecutar la búsqueda, seleccione los usuarios deseados en Resultados de la Búsqueda y dé clic en **OK** para agregarlos a la lista de cuentas autorizadas.

Revocar Cuentas

Para revocar la autorización de una cuenta a utilizar ActiveSync, selecciónela en la lista y dé clic en **Revocar la Cuenta Seleccionada**. Si desea revocar todas las cuentas, dé clic en el botón **Revocar Todas las Cuentas**.

> Si tiene habilitada la opción para *Autorizar todas las cuentas cuando acceden por primera vez el protocolo Active Sync*[451], el revocar el acceso de una cuenta la eliminará de la lista,

> pero la siguiente vez que un dispositivo se conecte con esa cuenta, será autorizado de nuevo..

Asignar una Política ActiveSync

Para asignar una Política 442 a la cuenta:

1. Seleccione una cuenta en la lista.
2. Dé clic en **Asignar Política**. Esto abre el diálogo Aplicar Política.
3. Dé clic en la lista desplegable **Política a Asignar** y seleccione la política deseada.
4. Dé clic en **OK**.

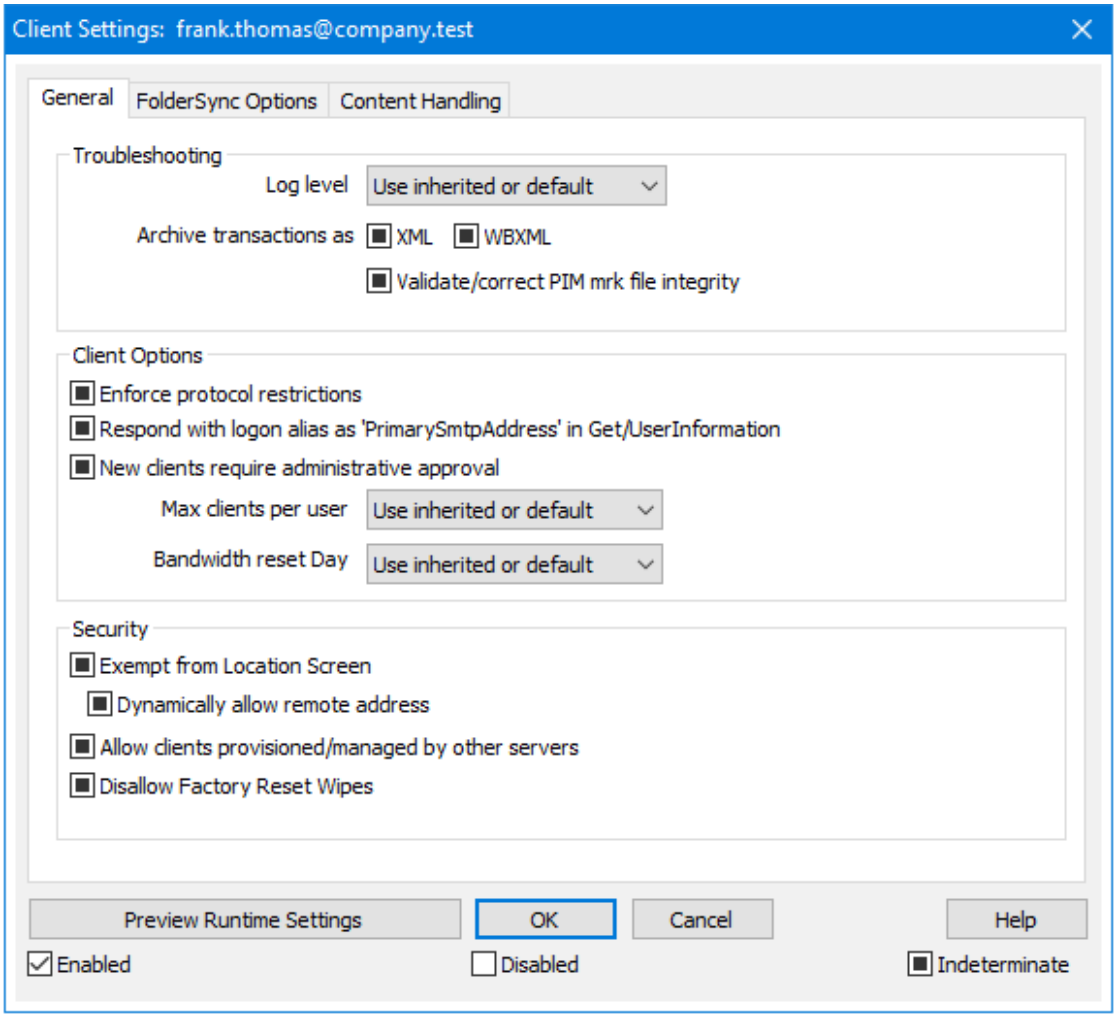
Esta política se asignará a cualquier dispositivo nuevo que se conecte desde esa cuenta.

Consultar la Lista de Cuentas Autorizadas

Si cuenta con un gran número de cuentas autorizadas para utilizar ActiveSync, puede utilizar la casilla **Encontrar Usuario** para buscar en la lista una cuenta en específico. Simplemente teclee las primeras letras de la dirección de correo de la cuenta para seleccionar al usuario.

Ajustes

Seleccione una cuenta y dé clic en **Ajustes** para administrar los Ajustes de Cliente de la cuenta. Estos ajustes se aplicarán a todos los clientes ActiveSync que se conecten con esa cuenta.



Por omisión todas las opciones en esta pantalla están configuradas para "Utilizar el heredado o el de omisión" lo que significa que cada opción tomará su valor de la opción correspondiente en la pantalla Ajustes de Cliente del Dominio 223. Cualquier cambio hecho a los ajustes en aquella pantalla se reflejará en esta. Inversamente, cualquier modificación que realice en esta pantalla omitirá el ajuste definido a nivel Dominio, para esta cuenta.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados

por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar

esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por

omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una

dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido[834] para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

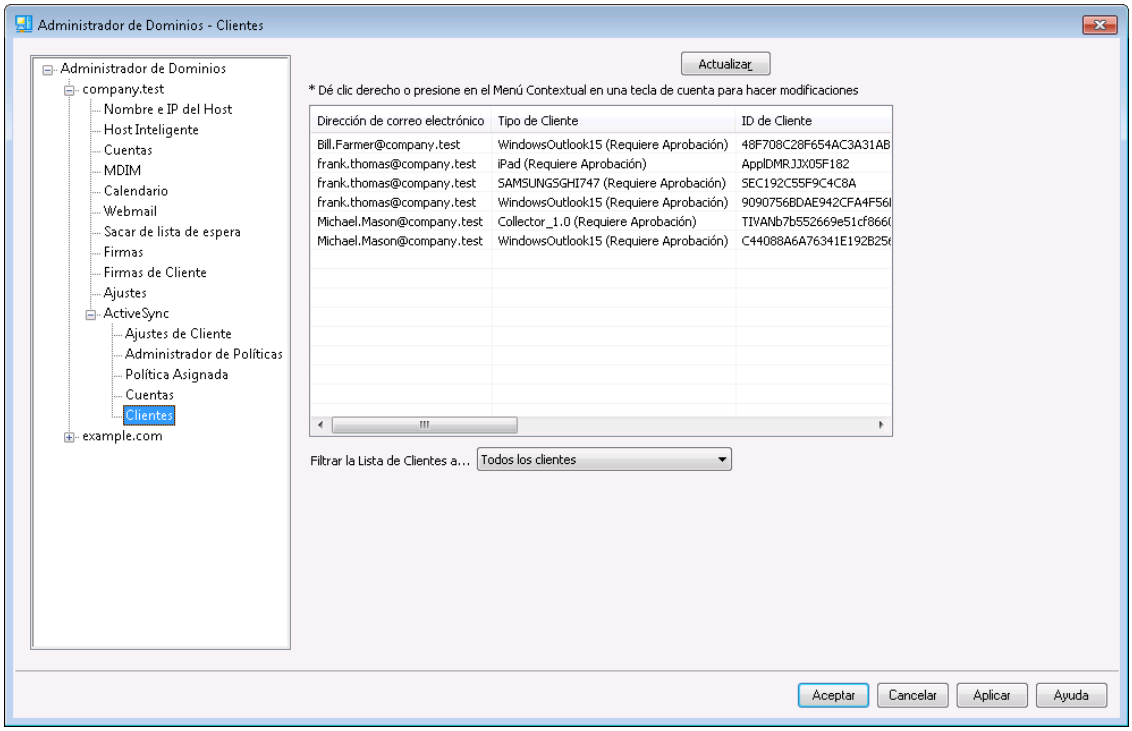
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios[434], cuentas[451] y clientes[460]). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

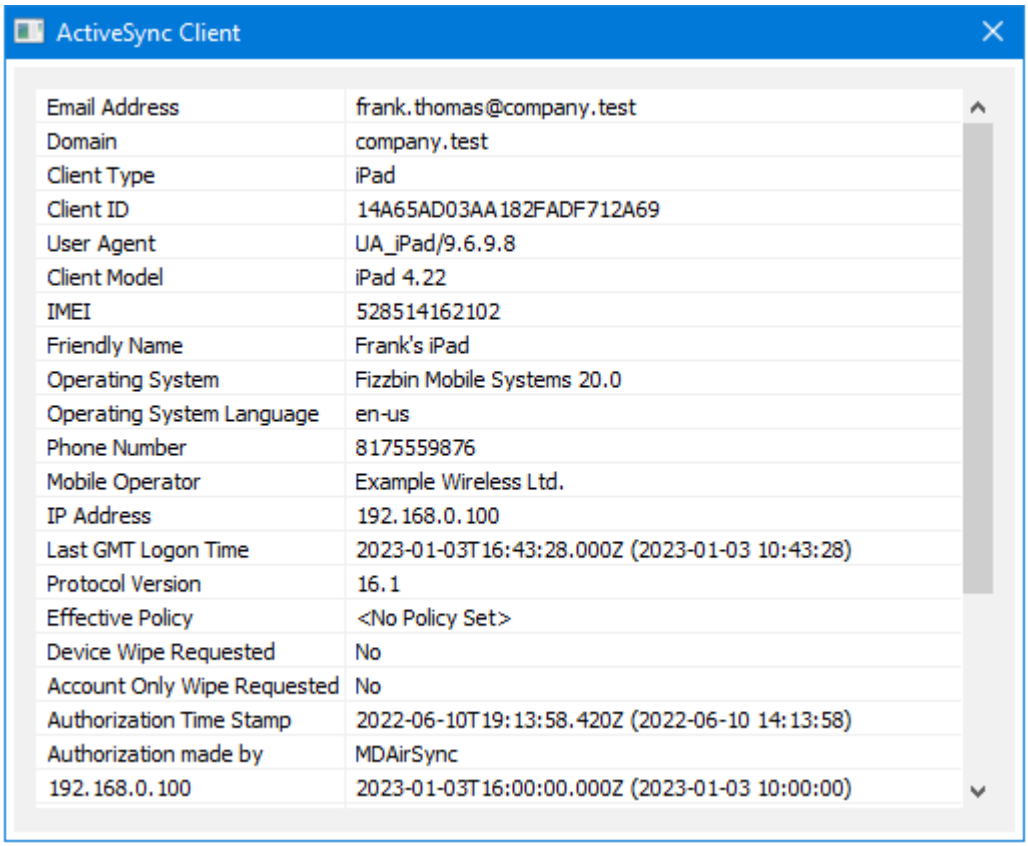
ActiveSync » Ajustes de Cliente[421]
ActiveSync » Dominios[434]
ActiveSync » Clientes[460]

3.2.11.5 Clientes



Esta pantalla contiene un registro por cada dispositivo ActiveSync asociado con el dominio.

Detalles del Cliente ActiveSync



Seleccione una entrada y dé clic en **Ver Detalles del Cliente** para abrir el diálogo de Detalles del Cliente. Esta pantalla contiene información sobre el cliente, tal como su Tipo de Cliente, ID de Cliente, último inicio de sesión y más.

Ajustes de Cliente

dé clic derecho en un cliente y clic en **Personalizar Ajustes de Cliente** para administrar sus Ajustes de Cliente. Por omisión estos ajustes se heredan de la pantalla de Ajustes de Tipo de Cliente, pero se pueden ajustar si lo desea . Vea Administrar Ajustes del Cliente del Dispositivo abajo.

Asignar una Política ActiveSync

Para asignar una Política 442 al dispositivo:

1. Dé clic derecho en un dispositivo en la lista.
2. Dé clic en **Aplicar Política**. Esto abre el diálogo Aplicar Política.
3. Dé clic en **Política a Asignar** en la lista desplegable y seleccione la política deseada.
4. Dé clic en **OK**.

Estadísticas

Dé clic derecho en una entrada y luego clic en **Ver Estadísticas** para abrir el diálogo Estadísticas del Cliente, que contiene varias estadísticas de uso para el cliente.

Restablecer Estadísticas

Si desea restablecer las estadísticas del cliente, dé clic derecho en el cliente, luego clic en **Restablecer Estadísticas** y **OK** para confirmar la acción.

Remover un Cliente ActiveSync

Para remover un cliente ActiveSync, dé clic derecho en el cliente y clic en **Eliminar**, y luego en **Si**. Esto eliminará el cliente de la lista así como toda la información de sincronización relativa al cliente, en MDaemon. Por esto, si en el futuro la cuenta utiliza ActiveSync para sincronizar el mismo cliente, MDaemon lo tratará como si nunca antes hubiera sido utilizado en el servidor: todos los datos del cliente tendrán que resincronizarse con MDaemon.

Borrar por completo un Cliente ActiveSync

Cuando se ha aplicado una política 442 a un cliente ActiveSync seleccionado y el cliente la ha aplicado y respondido, entonces se dispondrá con una opción de Borrado Completo para ese cliente. Para hacer un Borrado completo, dé clic derecho en el cliente (o selecciónelo si está utilizado MDRA) y dé clic en **Borrado Completo**. La próxima vez que se conecte ese cliente, MDaemon le dirá que borre todos los datos o se restaure a sí mismo a sus valores de fábrica. Dependiendo del cliente, esto puede eliminar todo en el dispositivo incluyendo apps descargadas. Más aún, en tanto exista el registro en ActiveSync de ese cliente, MDaemon continuará enviando peticiones de borrado siempre que el dispositivo se conecte en el futuro. Si en algún momento desea eliminar el cliente, asegúrese de agregarlo primero a la Lista de Bloqueados 428, de manera que no se pueda conectar en el futuro. Finalmente, si un dispositivo borrado es recuperado y desea permitirle que se conecte de nuevo, deberá seleccionar el dispositivo y dar clic en **Cancelar Acciones de Borrado**. También deberá eliminarlo de la Lista de Bloqueados.

Borrado de Cuenta de un Cliente ActiveSync

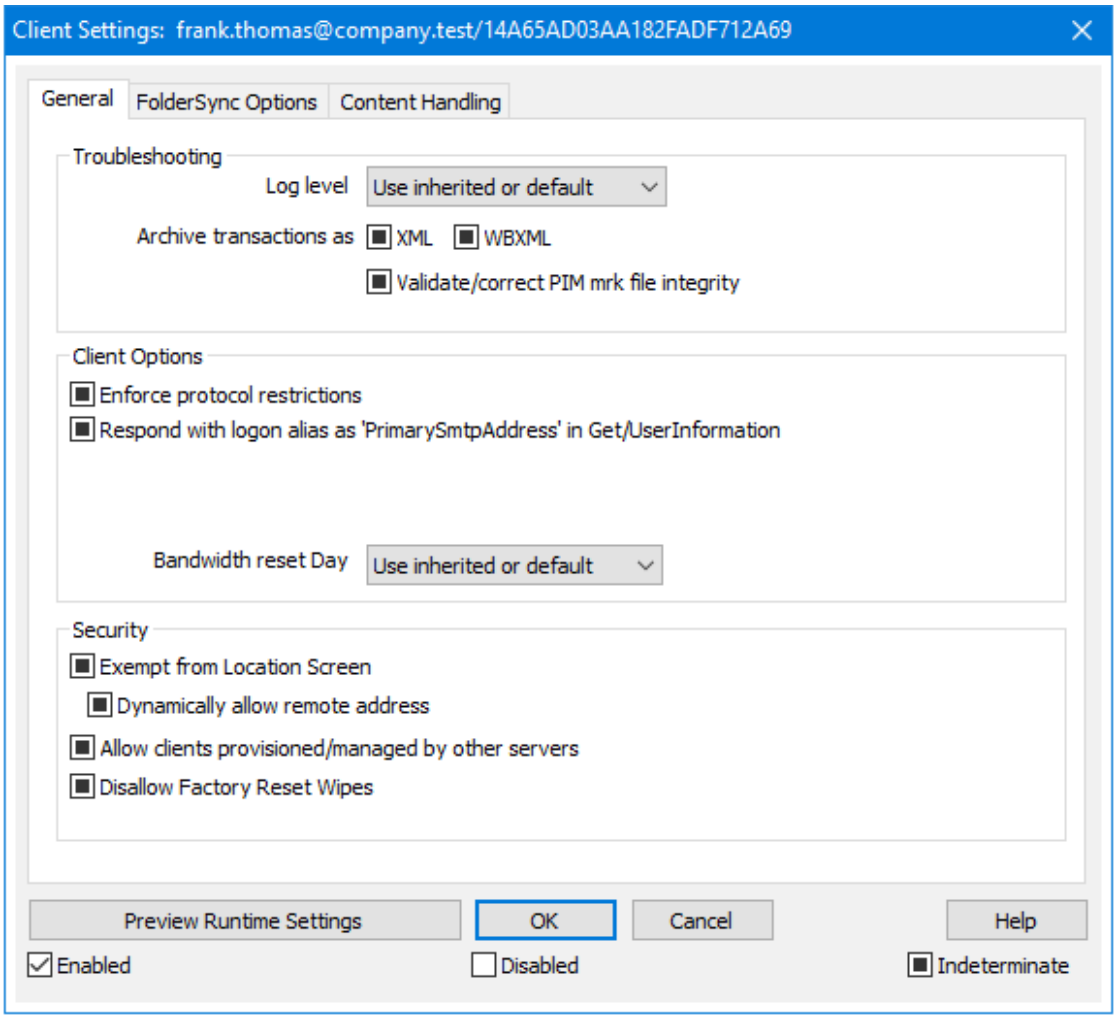
Para borrar la cuenta de correo y datos PIM de un cliente o dispositivo, dé clic derecho y clic en **Borrar Cuenta de Correo y datos PIM del Cliente.** La opción *Borrar Cuenta* es similar a la opción **Borrado Completo** explicada arriba, pero en lugar de borrar todos los datos, solo borrará los datos de la cuenta tales como correos, registros del calendario, contactos y demás. El resto, como son las apps, fotos o música quedarán intactos.

Autorizar un Cliente

Si está habilitada la opción "*Clientes nuevos requiere aprobación administrativa*" en la pantalla Ajustes de Cliente ActiveSync 421, seleccione un cliente y de clic en Aprobar cliente para sync, en este botón para autorizar su sincronización con el servidor.

Administrar los Ajustes del Cliente de un Dispositivo

La pantalla de Ajustes de Cliente a nivel dispositivo le permite administrar los ajustes para un dispositivo en particular.



Por omisión todas las opciones en esta pantalla se establecen como "Usar heredado o el de omisión", lo que significa que cada opción tomará sus ajustes de la opción correspondiente en la pantalla Ajustes de Cliente de la cuenta 451. Cualquier cambio

hecho a los ajustes en esa pantalla se verá reflejado en esta pantalla. En correspondencia, cualquier cambio que realice en esta pantalla omitirá el ajuste a nivel de cuenta para este dispositivo.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de

días[418] localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync**[460] en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas[314] a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas[314] a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta[316] para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas[314] padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas[128] a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas[743] a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la

reunión. Esto solo se deberá configurar en clientes[460] y tipos de clientes[475] que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS)[432] 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido[834] para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios[434], cuentas[451] y clientes[460]). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Cuentas 451
ActiveSync » Seguridad 428

3.3 Administrador de Puertas de Enlace

El Administrador de Puertas de Enlace se encuentra en el menú `Configurar » Administrador de Puertas de Enlace...` . Esta funcionalidad proporciona un nivel secundario limitado pero muy útil para hospedar múltiples dominios o funcionar como servidor de respaldo.

Por ejemplo:

Supongamos que desea actuar como servidor de respaldo o de recepción para un tercero, recibiendo correo entrante y almacenándolo en una carpeta en su servidor, pero no desea hospedar el dominio por completo, manteniendo sus cuentas de usuario individuales. Tomemos como ejemplo el nombre "example.com".

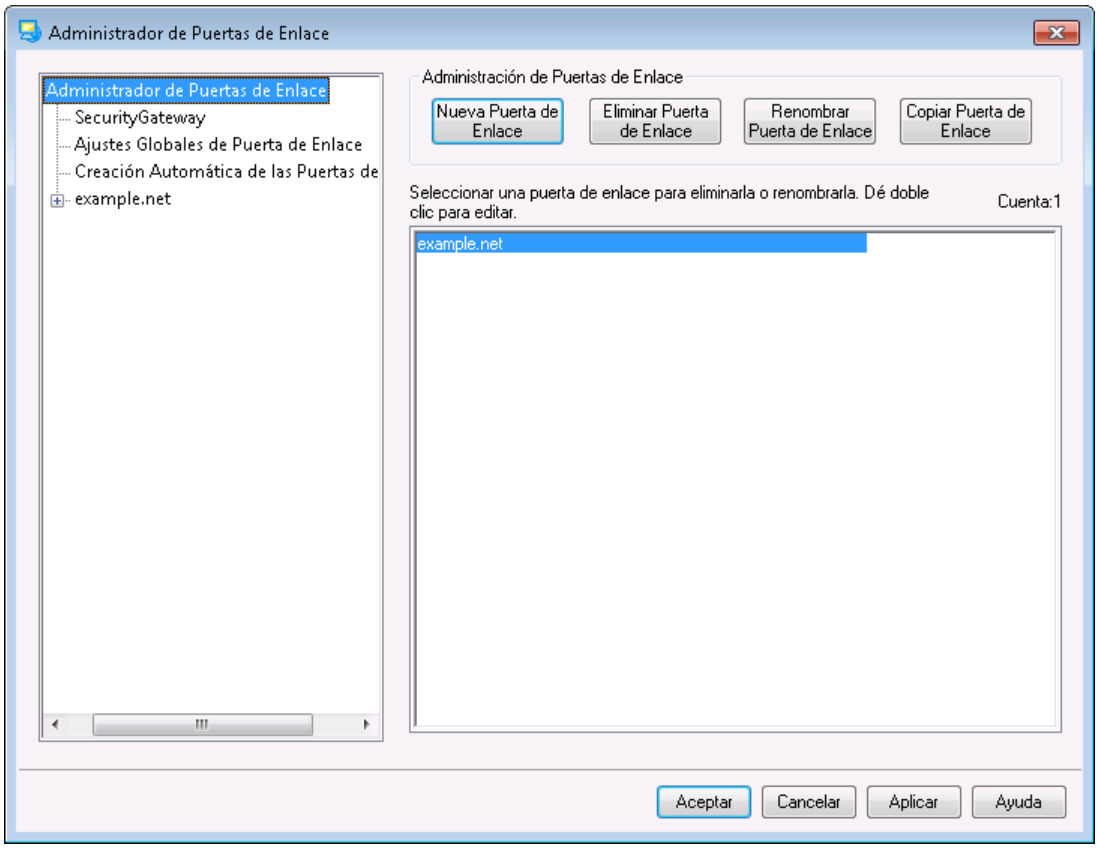
Lo primero que debe hacer es crear la puerta de enlace dando clic en **Nueva Puerta de Enlace** en el Administrador y luego registrar "example.com" como su nombre. Ahora todo el correo que reciba MDaemon para ese dominio será separado del flujo principal de correo y colocado en la carpeta designada en la pantalla Dominio 262, sin importar los individuos específicos a los que va dirigido cada mensaje.

Luego, designará los métodos de recolección o entrega que desea permitir o utilizar para entregar el correo del dominio a su servidor verdadero, donde están hospedadas las cuentas de usuario. Hay dos maneras de hacer esto: utilizar la opción *Entregar mensajes almacenados cada vez que MDaemon procese correo remoto* ubicada en la Pantalla Dominio 262, o utilizar las opciones de Desencolamiento 269. Opcionalmente, también puede crear una cuenta de MDaemon y modificar su Carpeta de Correo 718 para que sea la misma carpeta de almacenamiento 262 que utiliza la puerta de enlace. Esto permite que un cliente de correo se conecte con MDaemon para recolectar el correo de example.com

Finalmente, lo más probable es que tenga que editar los ajustes de DNS para example.com de manera que si servidor MDaemon sea designado como servidor MX para ese dominio.

Existen muchas otras funcionalidades y opciones disponibles, pero el ejemplo de arriba es la forma básica que tomará típicamente una puerta de enlace. Sin embargo, si requiere una configuración atípica es posible que deba hacer las cosas de manera diferente, tal como cuando desea utilizar un nombre de dominio que no existe en realidad en Internet, como "company.mail." Es posible recibir mensajes

para un dominio que de otra manera sería inválido, pero el nombre de dominio debe estar "oculto" dentro de la dirección del dominio por omisión[190]. Al utilizar este método, las direcciones se pueden construir y pasarán a través del dominio por omisión y de ahí a la puerta de enlace. Por ejemplo, si su dominio por omisión es `example.com` y usted tiene una puerta de enlace para `company.mail`, entonces alguien podría enviar un mensaje a "`bob@company.mail`" utilizando la dirección "`bob{company.mail}@example.com`." Dado que "`example.com`" es un dominio registrado hospedado por MDaemon, este mensaje será entregado correctamente, cuando MDaemon reciba el mensaje en ese formato convertirá la dirección a "`bob@company.mail`" y entregará el mensaje a la carpeta especificada para esa puerta de enlace. Por supuesto el método más simple es registrar un nombre de dominio válido para la puerta de enlace y apuntar su DNS o registro MX a `example.com`.



Lista de Puertas de Enlace

El panel de navegación a la izquierda de este diálogo contiene la lista de sus Puertas de Enlace, con ligas a cada pantalla utilizada para configurar los diversos ajustes específicos para cada una de ellas. También da acceso a las pantallas Ajustes Globales de Puertas de Enlace[259] y Creación Automática de Puertas de Enlace[260]. La lista a la derecha se utiliza para eliminar y renombrar dominios. Puede dar doble clic en una puerta de enlace en esta lista para ingresar al editor de puertas de enlace y configurar sus ajustes.

Administración de Puertas de enlace de Dominio

Nueva puerta de enlace
Para crear una nueva puerta de enlace: dé clic en **Nueva puerta de enlace**, ingrese el nombre de esta (ej. example.mail) en el diálogo Crear/Renombrar Puerta de Enlace de Dominio y dé clic en **OK**.

Típicamente el valor ingresado aquí será un nombre de dominio registrado en Internet cuyo servidor DNS resuelve a la dirección IP de la máquina local donde está corriendo el servidor, o un alias calificado de ese nombre. Alternativamente, puede decidir utilizar un nombre de dominio interno, no público y no válido (tal como "company.mail") para el nombre de su puerta de enlace. Esto, sin embargo, requiere que usted utilice el método de nombres de dominio anidados descritos en el ejemplo anterior o deberá utilizar algún otro esquema de filtrado de contenido para que los mensajes lleguen donde pertenecen.

Eliminar puerta de enlace
Para eliminar una puerta de enlace: selecciónela de la lista y dé clic en **Eliminar puerta de enlace** y luego dé clic en **Si** para confirmar su decisión.

Renombrar puerta de enlace
Para modificar el nombre de una puerta de enlace: Selecciónela de la lista, dé clic en **Renombrar Puerta de Enlace**, teclee el nombre nuevo en el diálogo Crear/Renombrar Dominio de la Puerta de Enlace y dé clic en **OK**..

Copiar puerta de enlace
Si desea crear una nueva puerta de enlace con ajustes que coincidan con otra puerta existente, seleccione esta de la lista, dé clic en este botón y especifique el nombre de su nueva puerta de enlace.

Editor de Puertas de Enlace

El Editor de Puertas de Enlace se utiliza para editar los ajustes de cada una de las Puertas. Incluye las pantallas siguientes:

Dominio 262
Utilice esta pantalla para habilitar/deshabilitar la puerta de enlace, definir la carpeta utilizada para almacenar los mensajes del dominio y configurar otras opciones de entrega y manejo de adjuntos.

Verificación 264
Si el servidor del dominio remoto está configurado para mantener un servidor LDAP o Active Directory actualizado con todos sus buzones, alias y listas de distribución o si está ejecutando un servidor Minger para proporcionar verificación remota de direcciones, puede utilizar este diálogo para especificar ese servidor y así verificar la validez de las direcciones de los destinatarios de los mensajes entrantes. Cuando se encuentra que la dirección de un destinatario es inválida el mensaje será rechazado. Con este método puede evitar tener que asumir que todos los destinatarios de los mensajes hacia un dominio son válidos.

Reenvío 268
Con este diálogo puede declarar un host o una dirección a la que será reenviado el correo del dominio tan pronto como llegue. Existen también opciones para establecer si se debe mantener una copia local de esos mensajes y para definir el puerto sobre el que se deberán reenviar esos mensajes.

Desencolar 269
Al utilizar las opciones en este diálogo, puede configurar MDaemon para responder a las peticiones ETRN y ATRN hechas por parte del dominio a fin de desencolar sus mensajes. También puede configurar otras varias opciones relacionadas.

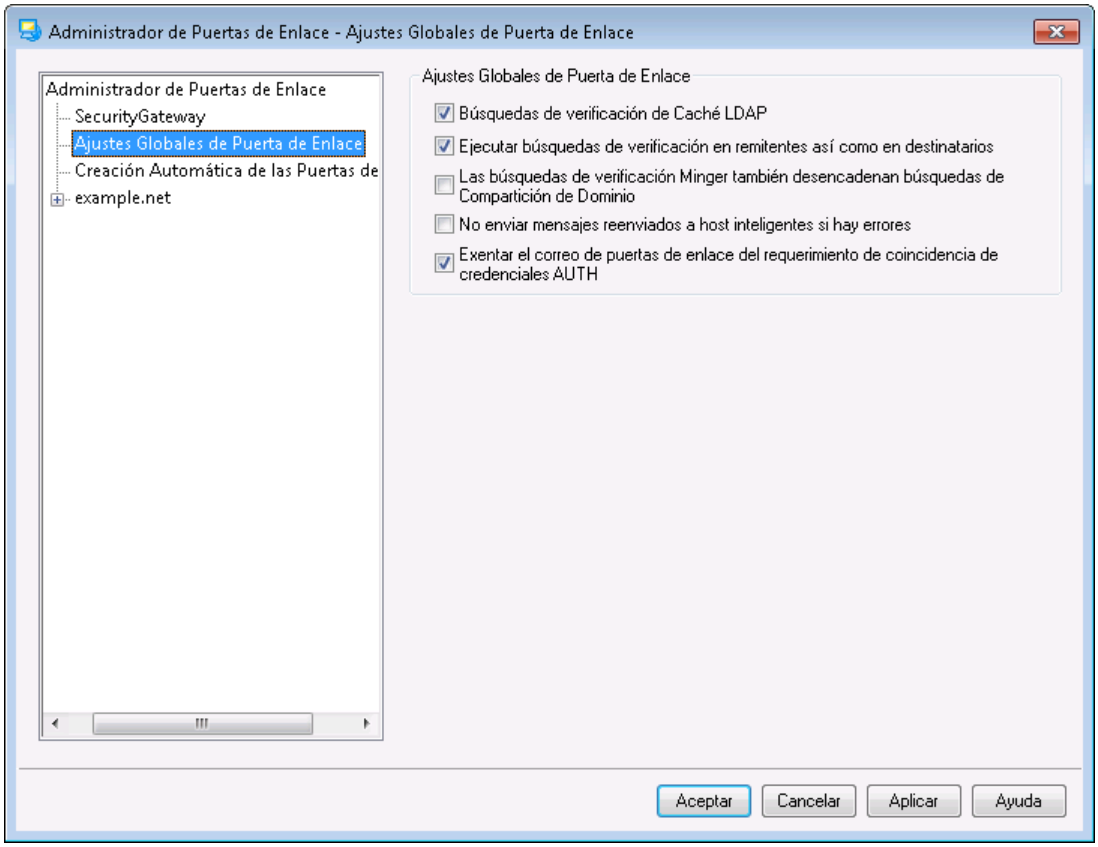
Cuotas 272
Este diálogo se utiliza para asignar un límite a la cantidad de espacio en disco que puede utilizar el dominio y el número máximo de mensajes que puede almacenar.

Ajustes 273
Esta pantalla contiene otras opciones que aplicarán a la puerta de enlace del dominio seleccionado. Por ejemplo, puede habilitar/deshabilitar el escaneo Antivirus y AntiSpam en la puerta de enlace, definir si se requiere o no autentificación para desencolar correo, definir la contraseña de autentificación, definir restricciones de conexión de direcciones IP y varias otras opciones.

Ver:

Ajustes Globales de Puerta de Enlace 259
Creación Automática de Puertas de Enlace 260
Administrador de Dominios 190

3.3.1 Ajustes Globales de Puertas de Enlace



Ajustes Globales de Puertas de Enlace

Las siguientes opciones son globales. No se limitan a cualquier puerta de enlace particular.

Cache de búsquedas de verificación LDAP
Dé clic en esta casilla si desea generar un caché de los resultados de las consultas de verificación[264] LDAP para las puertas de enlace de su dominio.

Realizar búsquedas de verificación en remitentes, así como en destinatarios
Por omisión, cuando están habilitadas las opciones de verificación de dirección[264] para una puerta de enlace, MDaemon intentará verificar a los remitentes y los destinatarios en los mensajes de la puerta de enlace. Deshabilitar esta opción si desea verificar solo a los destinatarios.

Las búsquedas de verificación Minger también detonan búsquedas de Dominios Compartidos
Cuando se habilita esta opción y cualquiera de sus puertas de enlace utiliza Minger[863] para verificación de direcciones, en adición a consultar el host Minger definido en la Pantalla de Verificación[264], MDaemon también consultará los hosts en Dominios Compartidos[123]. Esta opción aplica a todas las puertas de enlace definidas para utilizar Minger para verificación de direcciones.

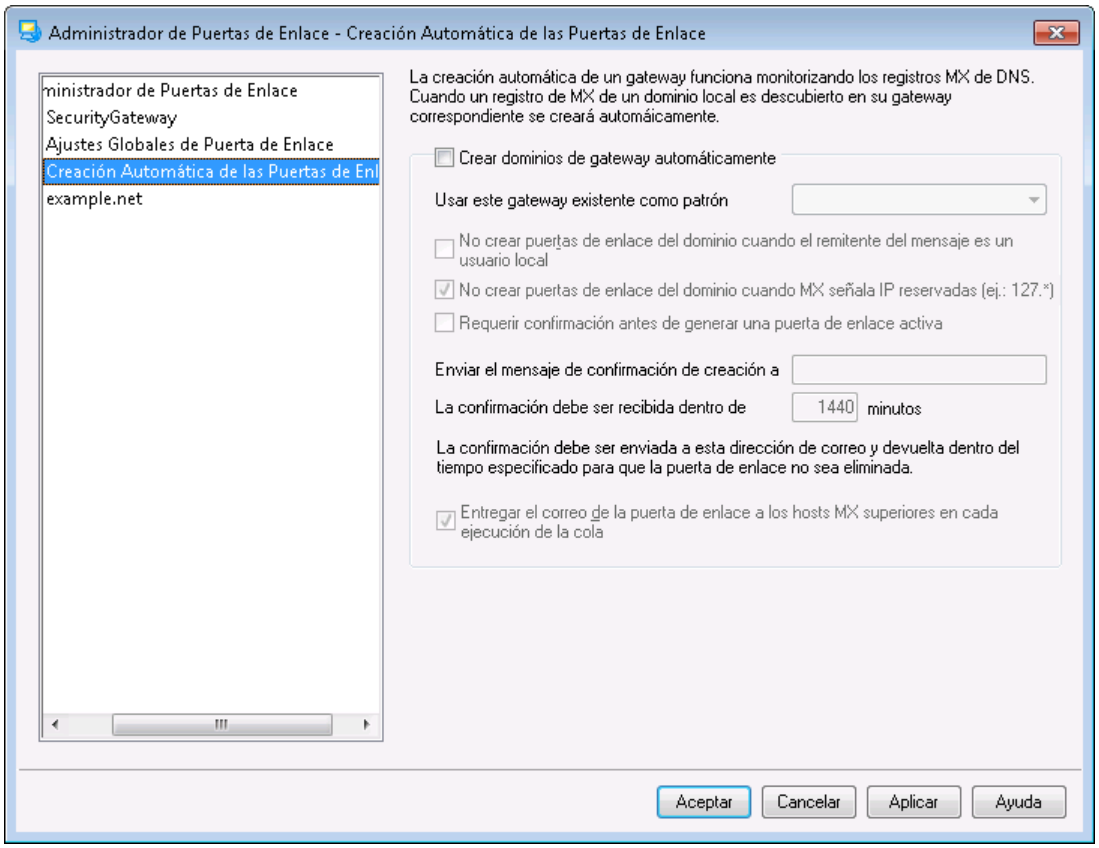
No enviar mensajes reenviados a hosts inteligentes si ocurren errores
Dé clic en esta opción para impedir que el envío de mensajes reenviados al host especificado arriba cuando ocurran errores de entrega. Esta opción se encuentra deshabilitada por omisión.

Exentar el correo de la puerta de enlace de los requerimientos de coincidencia de credenciales AUTH
Por omisión el correo de la puerta de enlace está exento de cumplir con las dos opciones localizadas en la pantalla Autentificación SMTP 523: "*Las Credenciales utilizadas deben coincidir con aquellas en la dirección return-path*" y "*Las credenciales utilizadas deben coincidir con aquellas en el campo 'From:' header address*". Deshabilite esta opción si no desea exentar al correo de la puerta de enlace de estos requerimientos, pero deshabilitarla puede generar algunos problemas para el almacenamiento y reenvío del correo de la puerta de enlace.

Ver:

Administrador de Puertas de Enlace 255
Editor de Puertas de Enlace » Verificación 264
Minger 863
Dominios Compartidos 123

3.3.2 Creación Automática de Puertas de Enlace



Creación Automática de Puertas de Enlace

Esta funcionalidad se usa para crear automáticamente un Dominio de Puerta de enlace para un dominio previamente desconocido cuando otra fuente intenta enviar el mensaje de dicho dominio a MDaemon, y una consulta DNS lista la ubicación de MDaemon como un registro MX válido.

Por ejemplo:

Con la creación automática de puerta de enlace habilitada, si la dirección del Dominio por Defecto de MDaemon es `192.0.2.0` y se envía un mensaje vía SMTP para un dominio `ejemplo.com` desconocido, MDaemon realizará una búsqueda MX y A para `ejemplo.com` para ver si `192.0.2.0` es un host de retransmisión de correo conocido para éste. Si el resultado de las consultas DNS indica que la dirección IP de MDaemon es un host MX válido para `ejemplo.com` entonces MDaemon creará automáticamente un nuevo Dominio de Puerta de Enlace para éste y aceptará su correo. Los mensajes para `ejemplo.com` se almacenarán entonces en una carpeta especial y, si así lo decide, se mandarán al host MX superior a cada intervalo de procesamiento de correo remoto. Esta funcionalidad le permite efectivamente convertirse en servidor de respaldo de otro dominio simplemente configurando el sistema DNS para usar su IP como host MX alternativo.

Para ayudar a proteger esta funcionalidad, MDaemon puede configurarse para enviar una solicitud de confirmación a una dirección de correo de su elección. Mientras MDaemon espera a la respuesta de confirmación, los mensajes para el dominio se aceptarán y almacenarán, pero no se enviarán. Las solicitudes de confirmación deben contestarse dentro de una cantidad de tiempo que se designe o la puerta de enlace creada automáticamente será eliminada y todos los mensajes almacenados borrados. Si la confirmación se recibe antes de que el tiempo haya expirado entonces los mensajes almacenados se enviarán normalmente.

Es posible que las personas malintencionadas o "spammers" intenten explotar esta funcionalidad configurando sus servidores DNS para que listen la dirección IP de MDaemon como uno de sus hosts MX. La creación Automática de Puertas de Enlace debe, por lo tanto, ser usada con precaución. Para ayudar a prevenir la posible explotación recomendamos utilizar la función *Enviar el mensaje de confirmación de creación a...* siempre que sea posible.

Crear dominios de puerta de enlace automáticamente
Haga clic en esta casilla si quiere que MDaemon cree automáticamente Puertas de Enlace de Dominio basándose en los resultados de búsquedas DNS.

Usar esta puerta de enlace existente como patrón
Escoja una puerta de enlace de dominio de esta lista desplegable y MDaemon usará sus configuraciones como una plantilla para todas las automáticamente creadas futuras puertas de enlace.

No crear puertas de enlace del dominio cuando el remitente del mensaje es un usuario local.
Habilite este control si no quiere que los mensajes que se originen de usuarios locales desencadenen la creación automática de puertas de enlace.

No crear puertas de enlace del dominio cuando MX señala IPs reservadas
Haga clic en esta casilla si quiere prevenir la creación automática de puertas de enlace cuando el registro MX apunte a una dirección IP reservada tal como 127.*, 192.*, o similares.

Requerir confirmación antes de generar una puerta de enlace activa
Cuando este control está habilitado, MDaemon enviará un mensaje de confirmación a la dirección de correo que escoja para poder determinar si la puerta creada automáticamente es o no válida. MDaemon continuará

aceptando mensajes para el dominio en cuestión, pero no los enviará hasta que se reciba confirmación.

Enviar el mensaje de confirmación de creación a
Use este cuadro de texto para designar la dirección de correo a la cual los mensajes de confirmación serán enviados.

La confirmación debe ser recibida dentro de XX minutos
Este control es para designar el número de minutos que MDaemon esperará una respuesta para un mensaje de confirmación dado. Si el límite de tiempo expira entonces la Puerta de Enlace en cuestión será borrada.

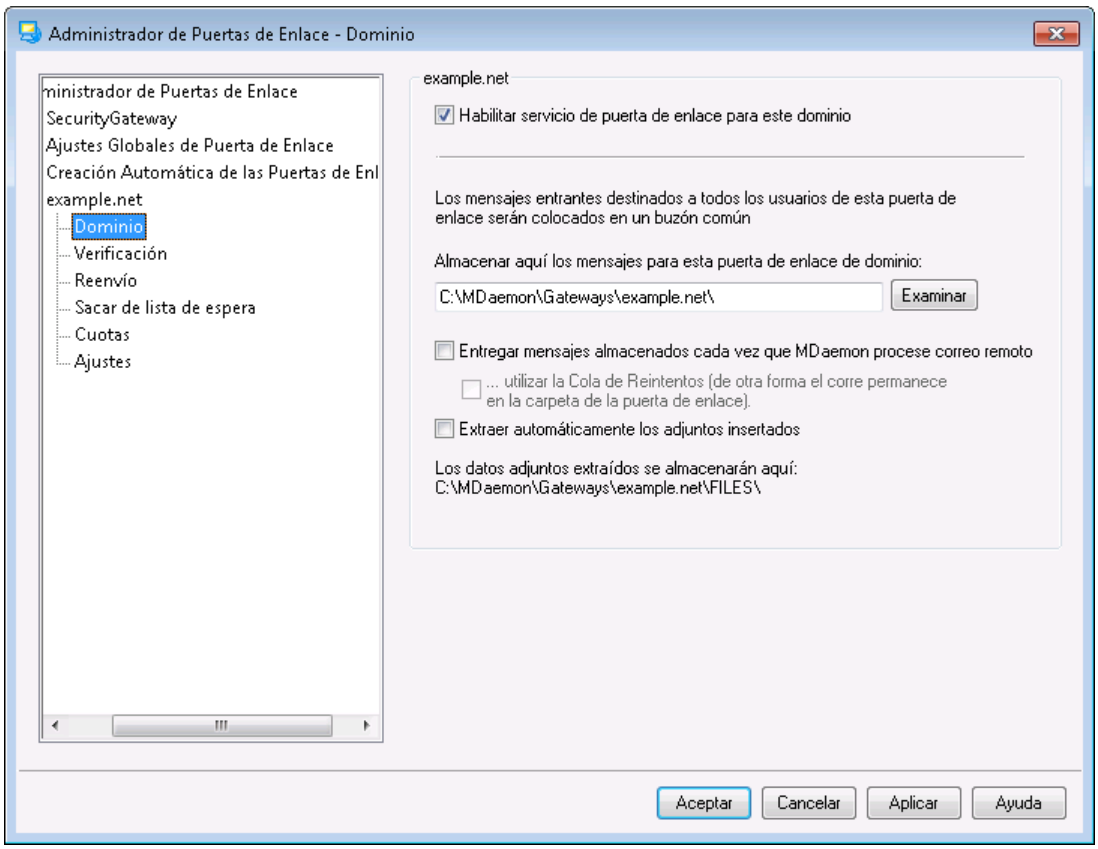
Entregar el correo de la puerta de enlace a los hosts MX superiores en cada ejecución de la cola
Si quiere que MDaemon intente enviar los mensajes de esta puerta de enlace a un host MX de nivel superior cada vez que el correo remoto sea procesado entonces habilite este control.

Ver:

Administrador de Puertas de Enlace 255

3.3.3 Administrador de Puertas de Enlace

3.3.3.1 Dominio



Puerta de Enlace de Dominio

Habilitar el servicio de puerta de enlace para este dominio
Marque esta caja para habilitar la puerta de enlace del dominio.

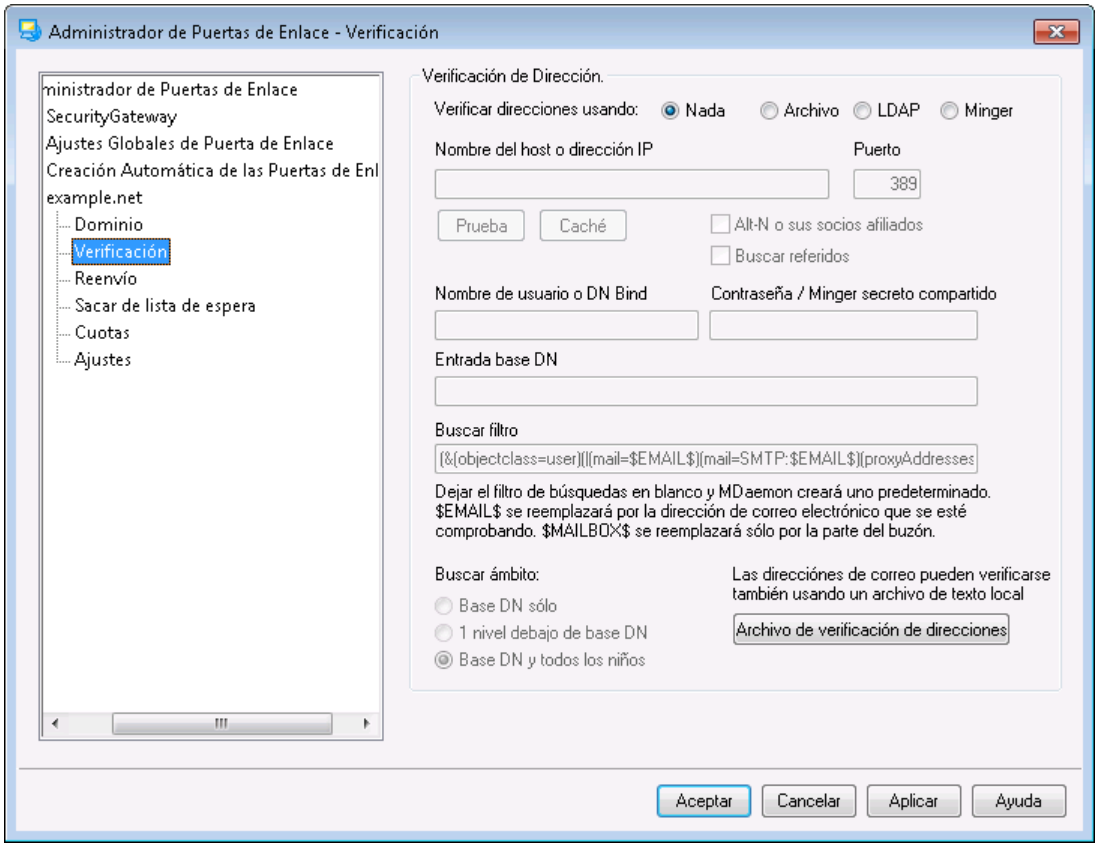
Almacenar los mensajes para esta puerta de enlace de dominio aquí:
Introduzca el directorio donde desea almacenar el correo entrante para el dominio. Todos sus mensajes se almacenarán en la misma carpeta independientemente de los destinatarios individuales a los que cada mensaje esté destinado.

Entregar mensajes almacenados cada vez que MDaemon procese correo remoto
Normalmente, cuando MDaemon recibe el correo que es para una de sus puertas de enlace, almacenará el correo hasta que dicho dominio conecte a MDaemon para recolectarlo. En algunas situaciones puede querer que MDaemon intente enviar el correo directamente vía SMTP en lugar de esperar a que el dominio lo recolecte. Cuando se habilita esta opción, MDaemon intentará enviar los mensajes del dominio cada vez que se procese el correo remoto. El buzón de la puerta de enlace actuará temporalmente como cola remota y se intentará el envío. Cualquier mensaje que no pueda enviarse simplemente se quedará en el buzón de la puerta de enlace hasta que sea recolectado por el dominio o se consiga enviar posteriormente; no se moverán a la cola remota o al sistema de reintentos. Sin embargo, si no tiene los DNS de dominio correctamente configurados, o si tiene su MDaemon configurado para pasar todos los mensajes salientes a algún otro host para entrega, podría causar que todos los mensajes queden atrapados en un bucle de correo y que se traten eventualmente como no entregables.

Utilizar la Cola de Reintentos (o el correo permanecerá en la carpeta de la puerta de enlace)
Habilite esta opción si desea utilizar el mecanismo de la Cola de Reintentos 872 para entregar correo. Esta opción se encuentra deshabilitada por omisión, lo que significa que el correo de la puerta de enlace permanecerá para siempre en la carpeta de la puerta de enlace, aun cuando no pueda ser entregado.

Extraer automáticamente los adjuntos insertados
Algunos sistemas de correo requieren que los archivos adjuntos sean extraídos antes del envío de mensajes de correo al flujo de correo. Para facilitar eso, MDaemon puede autoextraer los adjuntos MIME y colocarlos en la subcarpeta `\Files\` bajo la carpeta de mensajes del dominio. Haga clic en esta casilla si desea extraer automáticamente los adjuntos.

3.3.3.2 Verificación



Un problema común con las puertas de enlace de dominio y los recolectores de correo es que normalmente no tienen un método para determinar si el destinatario de un mensaje entrante es válido. Por ejemplo, si está actuando como puerta de enlace para `ejemplo.com` y viene un mensaje para `user01@ejemplo.com` entonces no tiene manera de saber si existe o no un buzón, alias, o lista de correo que corresponda a dicha dirección en el servidor de correo ejemplo.com. Así pues, no tiene otra opción más que asumir que la dirección es válida y aceptar el mensaje. Además, puesto que los spammers normalmente envían mensajes a muchas direcciones inválidas, este problema puede resultar en una enorme cantidad de correo basura aceptado por la puerta de enlace.

MDaemon contiene un método de prevenir esto verificando la dirección del destinatario. Si el servidor remoto del dominio está configurado para mantener actualizado un servidor LDAP o Active Directory con todos sus buzones, alias, y listas de distribución, o si ejecuta un servidor Minger para proveer de verificación remota de direcciones, entonces puede usar las opciones en esta pantalla para especificar el servidor LDAP, Active Directory, o Minger donde se almacena dicha información. Entonces, cuando un mensaje llega para `ejemplo.com`, puede buscar la dirección del destinatario en el otro servidor y descubrir si es o no válida.

Verificación de Dirección

Verificar direcciones usando:

Nada
Escoja esta opción si no desea usar verificación de correo electrónico para esta puerta de enlace. MDaemon tratará a todos los correos entrantes del dominio como si el destinatario fuera una dirección válida, puesto que no

tiene manera de identificar qué direcciones existen realmente para dicho dominio.

Archivo
Escoja esta opción si desea usar el archivo `GatewayUsers.dat` como la lista de direcciones definitivas que se usarán para verificar si el destinatario de un mensaje entrante es o no válido para este dominio. Esto es una lista global de direcciones, aplicable a todos sus dominios de puerta de enlace, e incluso si ha escogido usar otros métodos de verificación, esta lista se seguirá usando como fuente adicional de direcciones válidas. Cuando utilice la opción *Archivo*, sin embargo, será el único método de verificación usado. Puede abrir y editar la lista de direcciones válidas haciendo clic en el botón *Archivo de verificación de direcciones* abajo.

LDAP
Escoja esta opción para activar la verificación remota de direcciones a través de LDAP o Active Directory. Siempre que un mensaje llega para el dominio remoto su servidor LDAP o Active Directory será consultado para determinar si el recipiente es o no válido. Si no es válido el mensaje será rechazado. Si MDaemon no puede conectar al servidor LDAP/AD entonces asumirá que la dirección es válida.

Minger
Escoja esta opción si desea consultar el servidor de dominio Minger para verificar las direcciones de destinatario para este dominio. Si MDaemon es incapaz de conectar al servidor, asumirá que la dirección es válida. También existe una opción global ubicada en Ajustes Globales de Puertas de Enlace 259 que puede usar para hacer que MDaemon consulte también a sus hosts de Dominios Compartidos 123.

Nombre del host o dirección IP
Introduzca el nombre de host o dirección IP del dominio del servidor LDAP/Active Directory o Minger. Este es el servidor LDAP/AD al que MDaemon conectará para verificar que el destinatario de un mensaje entrante es una dirección válida en el dominio en el que MDaemon actúa como puerta de enlace o servidor de respaldo.

Puerto
Especifique el puerto en que el servidor de Minger o LDAP/AD está utilizando. MDaemon utilizará este puerto cuando verifique información de direcciones vía LDAP, Active Directory, o Minger.

Prueba
Haga clic en este botón para probar si la verificación remota de direcciones está configurada correctamente. MDaemon simplemente intentará conectarse al servidor LDAP/AD designado y verificar que responde a la información especificada.

Caché
Haga clic en este botón para abrir la caché de LDAP/ Minger. Puede habilitar/deshabilitar la caché en Ajustes Globales de Puertas de Enlace 259.

El protocolo del servidor es versión 3
Dé clic en esta casilla si desea que la verificación de la puerta de enlace utilice en su servidor la versión 3 del protocolo LDAP.

Buscar referencias
En ocasiones los servidores LDAP no tienen un objeto solicitado, pero pueden tener una referencia cruzada de su localización, a la que pueden referir un cliente. Si desea que la verificación de puerta de enlace busque (es decir, siga) estas referencias, habilite esta opción. Se encuentra deshabilitada por omisión.

Nombre de usuario o DN Bind
Introduzca el nombre de usuario o DN de la cuenta que tiene acceso administrativo al servidor LDAP/AD del dominio para que MDaemon pueda verificar los destinatarios de los mensajes entrantes dirigidos al dominio para el que se está actuando de puerta de enlace o servidor de respaldo. Este es el DN usado para la autenticación en el proceso de enlace(bind).

Contraseña / Minger secreto compartido
Esta contraseña será pasada al servidor LDAP/AD del dominio juntamente con el valor *DN Bind* para autenticación. Si usa un servidor Minger este será el secreto compartido o contraseña.

Entrada base DN
Este es el Distinguished Name (DN) o punto de inicio en el Árbol de Información de directorio (DIT) al que MDaemon consultará su servidor LDAP/AD para verificación de direcciones.

Buscar filtro
Este es el filtro de búsqueda LDAP/AD que se usará cuando se consulte a su servidor para verificación de direcciones. MDaemon establecerá un filtro de búsqueda por defecto que debería funcionar en la mayoría de los casos.

Buscar ámbito:

Este es el ámbito o extensión de sus búsquedas LDAP/AD.

Base DN sólo
Escoja esta opción si desea limitar su búsqueda a sólo la base DN especificada aquí. La búsqueda no procederá por debajo de dicho punto en su árbol (DIT).

1 nivel debajo de base DN
Use esta opción si desea extender su búsqueda LDAP/AD un nivel por debajo del DN indicado en su DIT.

Base DN y todos los niños
Esta opción extenderá el ámbito de su búsqueda desde el DN indicado a todos sus niveles inferiores, hasta el menor en su DIT.

Archivo de verificación de direcciones
Haga clic en este botón para abrir la Lista de Direcciones Válidas de Puerta de Enlace (el archivo `GatewayUsers.dat`). Este contiene una lista de direcciones que MDaemon considerará como destinatarios válidos para mensajes entrantes dirigidos a sus puertas de enlace de dominio. Independientemente de la opción de verificación seleccionada anteriormente, MDaemon usará esta lista como una fuente extra de datos de direcciones válidas. Cuando use la opción anterior de *Archivo*, sin embargo, será el único y definitivo método de verificación usado.

Usar múltiples configuraciones para sus consultas de verificación LDAP

Puede especificar múltiples configuraciones LDAP para sus dominios de Puerta de Enlace. Para especificar conjuntos extra de parámetros LDAP, establezca su primer conjunto en primer lugar, y luego manualmente edite el archivo `GATEWAYS.DAT` utilizando el Bloc de Notas.

Su nuevo conjunto de parámetros debe crearse usando el siguiente formato:

```
LDAPHost1=<nombre de host>
LDAPPort1=<puerto>
LDAPBaseEntry1=<entrada de base DN>
LDAPRootDN1=<raíz DN>
LDAPObjectClass1=USER
LDAPRootPass1=<contraseña>
LDAPMailAttribute1=mail
```

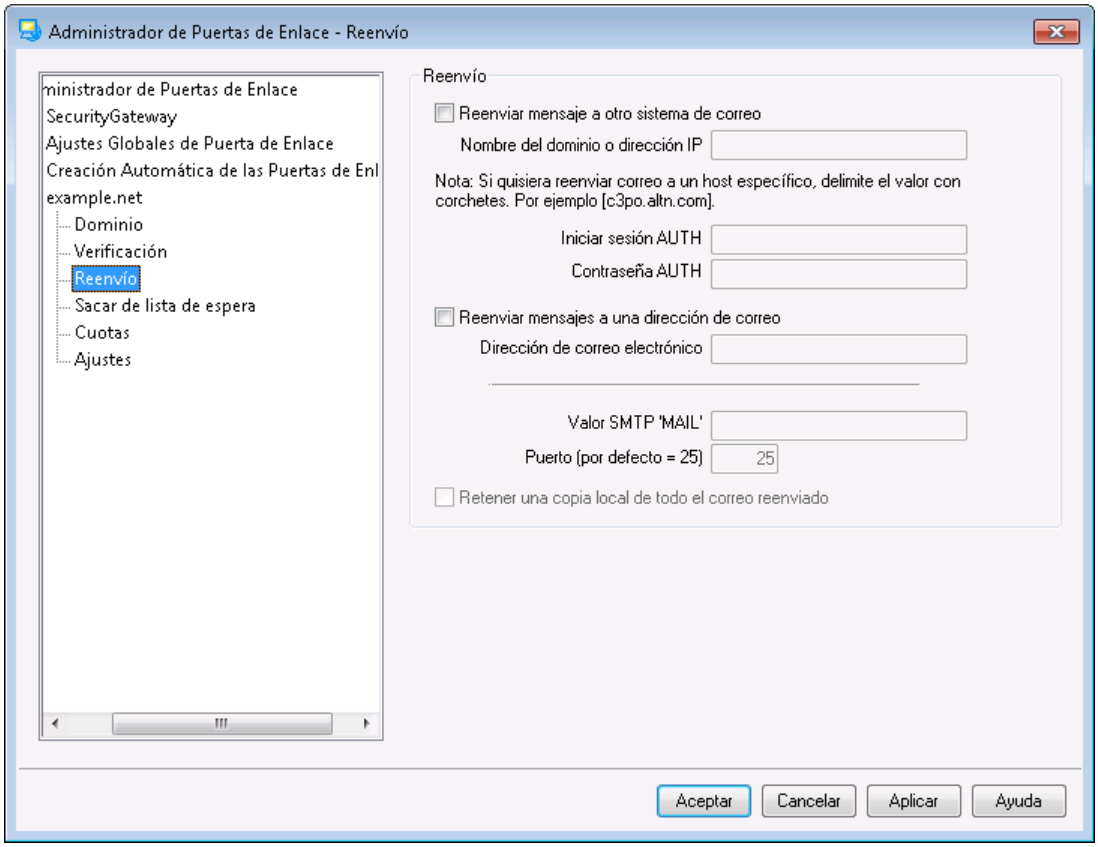
Para cada nuevo conjunto de parámetros, incremente el numeral en cada nombre de parámetro en 1. Por ejemplo, en el conjunto de ejemplo anterior, cada nombre de parámetro acaba en "1". Para crear un conjunto adicional cada nombre deberá acabar en "2". En otro conjunto, cada uno deberá acabar en "3", y así sucesivamente.

Cuando se ejecutan las consultas LDAP, MDaemon ejecutará consultas LDAP múltiples en orden para encontrar una coincidencia. Si se encuentra un error o una coincidencia no se realizarán posteriores comprobaciones.

Ver:

Opciones LDAP/Libreta de Direcciones 831
Minger 863

3.3.3.3 Reenvío



Reenvío

Reenviar correo a otro sistema de correo
Algunas veces es una ventaja simplemente reenviar una copia de todos los mensajes para un dominio tal cual llegan. Si desea configurar MDaemon para hacer esto, introduzca el nombre o la dirección IP para el dominio para el cual las copias del correo entrante de este dominio deberán ser enviadas. Si desea reenviar los mensajes a un host específico entonces coloque el valor entre corchetes (por ejemplo, `[host1.ejemplo.net]`). Utilice la opción AUTH Logon/Contraseña para incluir las credenciales de inicio de sesión para el servidor al que le está reenviando los mensajes.

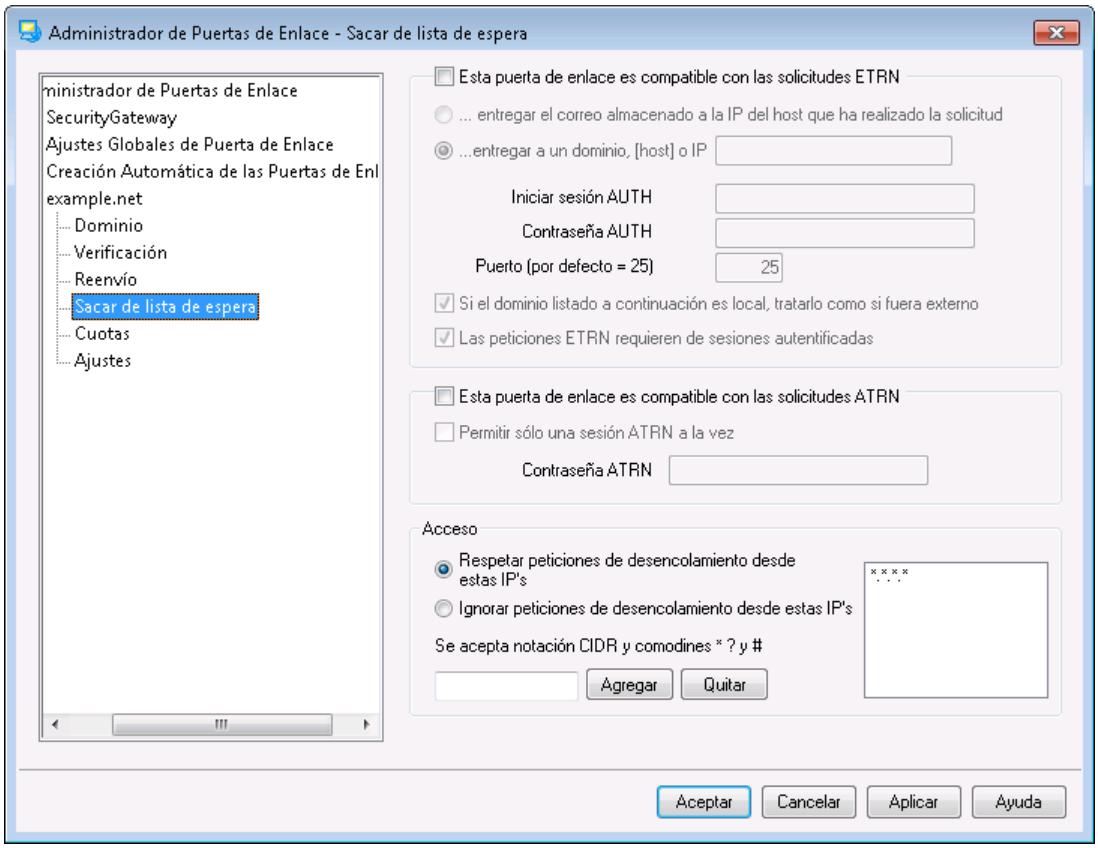
Reenviar correo a una dirección de correo electrónico
Use esta funcionalidad si desea reenviar a una dirección de correo específico todos los mensajes de correo destinados para este dominio cliente.

Valor SMTP 'MAIL'
MDaemon utilizará esta dirección en la transacción SMTP "Mail From" al reenviar los mensajes.

Puerto (por omisión = 25)
MDaemon utilizará este puerto al reenviar los mensajes.

Retener una copia local de todo el correo reenviado
Seleccione esta opción si desea que MDaemon retenga localmente una copia de archivo de cada mensaje una vez que éste haya sido reenviado.

3.3.3.4 Sacar de lista de espera



ETRN

Esta puerta de enlace es compatible con las solicitudes ETRN
Cuando se habilita este control MDaemon responderá a las peticiones ETRN hechas por hosts válidos en nombre del dominio para el que MDaemon está actuando como puerta de enlace de correo. El comando ETRN es una extensión SMTP que manda señales a un servidor que almacena correo para un dominio en concreto indicando que es momento de empezar a procesar el correo. Cuando MDaemon recibe una petición ETRN para un dominio, empezará inmediatamente a procesar el correo almacenado para envío usando transacciones SMTP subsecuentes. Tenga en cuenta que las sesiones de SMTP que emiten las peticiones ETRN no serán las que reciben ningún correo almacenado. MDaemon usará transacciones SMTP subsecuentes e independientes para enviar cualquier correo almacenado para el dominio. Esto preserva el sobre del mensaje y es más seguro. También debe notar que el host al que MDaemon remitirá cualquier correo almacenado puede que no empiece inmediatamente la recepción de dichos mensajes. ETRN sólo garantiza que el correo almacenado se pone en *cola* para envío. El proceso *real* de envío está sujeto a otras restricciones impuestas por el administrador y puede tener que esperar en la cola de salida para el siguiente proceso programado de envío de correo remoto. Debido a dichas limitaciones, recomendamos usar Transmisión bajo Demanda (ODMR) 209 y su comando ATRN

en lugar de ETRN. Este método no está soportado por todos los clientes y servidores, sin embargo, sólo estará disponible para clientes de dominio que use un servidor que lo permita. MDaemon soporta completamente ODMR tanto en el lado del cliente como en el del servidor.

Por defecto MDaemon requiere que el host que se conecta emitiendo una petición ETRN se autentifique primero vía ESMTP AUTH utilizando *la contraseña ATRN* del *Nombre de Dominio* 262 y Puerta de Enlace como credenciales de inicio de sesión. Si no desea requerir autenticación puede deshabilitarlo en Opciones 273 desmarcando la opción el *Desencolamiento ETRN requiere autentificación.*

...entregar el correo almacenado a la IP del host que ha realizado la solicitud
Si selecciona esta opción hará que MDaemon envíe cualquier correo almacenado a la dirección IP de la máquina que ha hecho la petición ETRN. La máquina que ha realizado la petición debe estar ejecutando un servidor SMTP para recibir los mensajes.

...entregar a este dominio, [host] o IP
Este es el nombre de host, nombre de dominio, o dirección IP a la que el correo almacenado se enviará cuando se reciba y procese una petición ETRN. La máquina de destino debe estar ejecutando un servidor SMTP para recibir estos mensajes. Nota: cuando un nombre de dominio se especifica en esta opción, se usarán los registros A y MX, dependiendo de los resultados de DNS durante el envío. Si desea enviar los mensajes a un host particular, coloque el nombre del host entre corchetes (por ejemplo, `[host1.ejemplo.net]`) o especifique una dirección IP en lugar de un nombre de dominio. Registrar las credenciales *AUTH Logon/Password* requeridas para entregar en esa ubicación.

Puerto (omisión = 25)
Use esta casilla para especificar el puerto en el que el dominio de correo será procesado.

Si el dominio listado a continuación es local, tratarlo como si fuera externo
Active este control si el dominio es local, pero quiere que su correo sea tratado como si fuera remoto.

Peticiones ETRN requieren sesiones autentificadas
Al ejecutar peticiones ESMTP ETRN, esta opción se utilizará por omisión para requerir que el host que se conecta primero se autentifique utilizando un comando ESMTP AUTH. Cuando se encuentra habilitada esta opción, debe definir una contraseña de autentificación en la opción "Contraseña ATRN" abajo.

Deshabilite esta casilla si no desea requerir autentificación de hosts que hacen peticiones ETRN.

ATRN

Esta puerta de enlace es compatible con las solicitudes ATRN
Habilite esta opción si quiere que MDaemon responda a los comandos `ATRN` del dominio de la puerta de enlace. `ATRN` es un comando de ESMTP usando en la Transmisión bajo demanda (ODMR) 209, que es actualmente el mejor método de retransmisión disponible para hospedaje de correo. Es superior a ETRN y otros

métodos en el hecho que requiere autenticación antes de que el correo sea quitado de la cola y no requiere una dirección IP estática. Una dirección IP estática no es requerida porque el flujo de datos entre MDaemon y el dominio cliente es inmediatamente revertido y los mensajes se desencolan sin tener que realizar una nueva conexión, a diferencia de `ETRN`, que usa una conexión separada después de que el comando `ETRN` sea enviado. Este dominio cliente con una dirección IP dinámica (no estática) recolecta sus mensajes sin tener que usar POP3 o DomainPOP, puesto que el sobre original de SMTP es preservado.

ATRN requiere una sesión que utilice el comando AUTH. Puede configurar las credenciales de autenticación en la pantalla Ajustes 273.

Permitir sólo una sesión ATRN a la vez
Marque esta casilla si desea restringir ATRN a una sesión a la vez.

Contraseña ATRN
Al utilizar ATRN para desencolar el correo de esta puerta de enlace, o cuando requiere autentificación vía la opción *el desencolamiento ETRN requiere autentificación, e* en la pantalla Ajustes, defina la contraseña ATRN de la puerta de enlace aquí.

Acceso

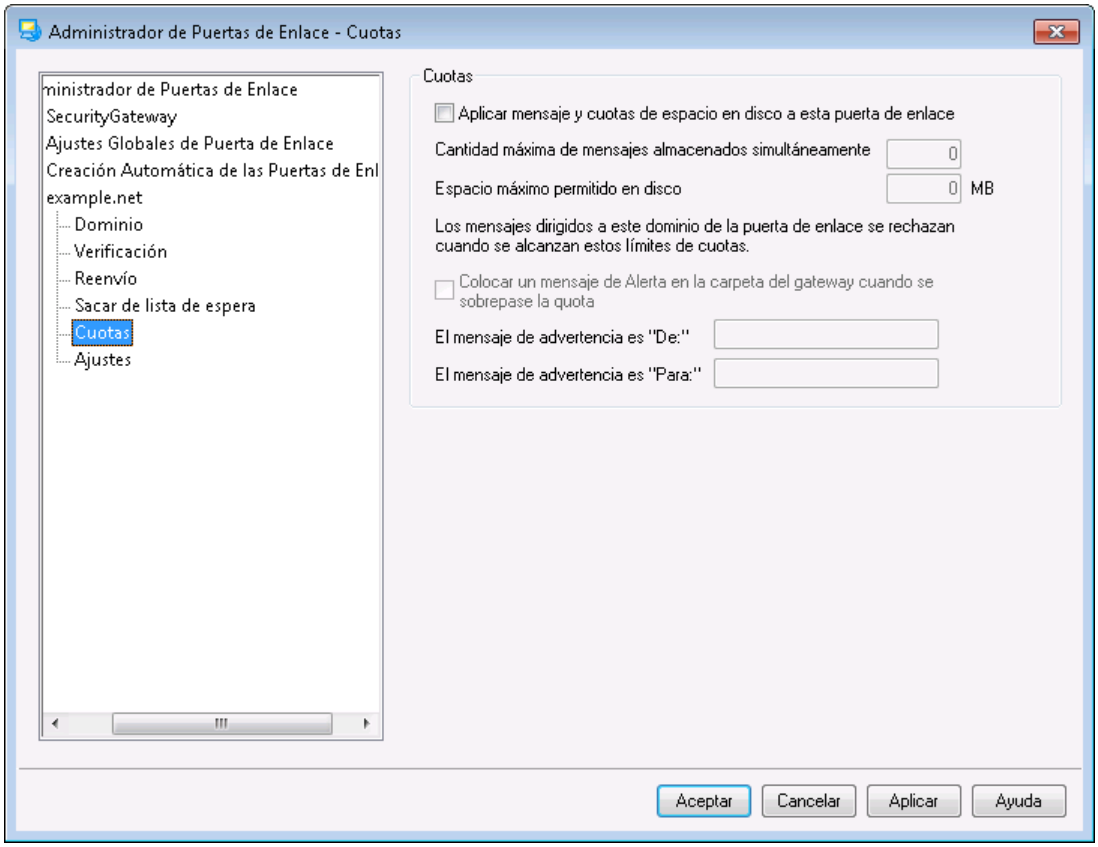
Respetar peticiones de desencolado desde estas IPs
Seleccione esta opción y MDaemon respetará peticiones ETRN/ATRN hechas desde cualquier IP enlistada en la lista de direcciones asociada.

Ignorar peticiones de desencolado desde estas IPs
Seleccione esta opción y MDaemon ignorará peticiones ETRN/ATRN hechas desde cualquier IP enlistada en la lista de direcciones asociada.

Agregar nueva IP
Para agregar una IP nueva a la lista simplemente regístrela en esta caja de texto y dé clic en el botón *Agregar*.

Eliminar
Dé clic en este botón para eliminar el registro seleccionado de la lista de direcciones IP.

3.3.3.5 Cuotas



Cuotas

Aplicar mensaje y cuotas de espacio en disco a esta puerta de enlace
Habilite esta opción si desea designar un número máximo de mensajes permitidos para ser almacenados para el dominio o una cantidad máxima de espacio en disco (en kilobytes) que pueda usar. Esto incluye cualquier archivo adjunto decodificado en su directorio de Archivos. Cuando se alcanza una cuota, cualquier mensaje entrante posterior para el dominio será rechazado.

Cantidad máxima de mensajes almacenados simultáneamente
Use este cuadro para designar el máximo número de mensajes que MDaemon almacenará para este dominio de puerta de enlace. Use "0" en esta opción si no desea limitar el número de mensajes.

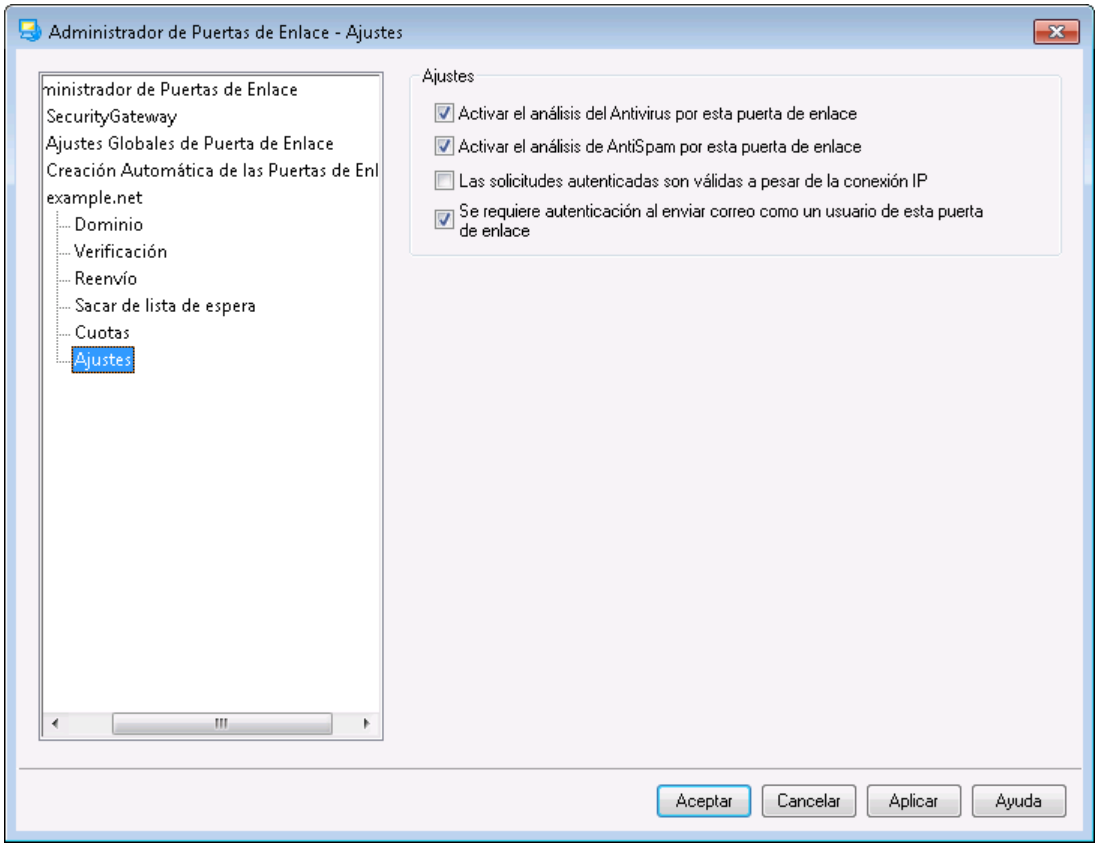
Espacio máximo permitido en disco
Especifique el máximo permitido de espacio en disco aquí. Cuando los mensajes y archivos almacenados para el dominio alcancen este límite, cualquier mensaje entrante posterior será rechazado. Use "0" si no desea establecer un límite de espacio en disco.

Colocar un mensaje de Alerta en la carpeta de la puerta de enlace cuando se sobrepase la cuota
Si esta opción está habilitada y el envío de correo al dominio se intenta cuando excedería las limitaciones de máximo espacio en disco o mensajes, un mensaje de alerta apropiado se colocará en la carpeta de correo de la puerta de enlace. Puede designar las cabeceras "`From:`" y "`To:`" a continuación.

El mensaje de advertencia es "De:"
Use esta opción para especificar la dirección "From:" que se usará en los mensajes de advertencia de sobrecuota.

El mensaje de advertencia es "Para:"
Use esta opción para especificar la dirección "To:" que se usará en los mensajes de advertencia de sobrecuota.

3.3.3.6 Ajustes



Ajustes

Habilitar el análisis del Antivirus para esta puerta de enlace

Haga clic en esta opción si está utilizando las funcionalidades opcionales de MDaemon AntiVirus 645 y quiere que se escaneen los mensajes de esta puerta de enlace de dominio. Si deshabilita esta opción el Antivirus no escaneará los mensajes de esta puerta de enlace.

Activar el análisis de AntiSpam por esta puerta de enlace
Haga clic en esta opción si quiere aplicar las configuraciones del Filtro de Spam a los mensajes de este dominio de puerta de enlace. De otro modo, serán excluidos del escaneo del Filtro de Spam.

Las peticiones autentificadas son válidas sin importar la IP de la que se conectan
Habilite esta casilla si desea aceptar las peticiones autentificadas sin importar la dirección IP de la que provienen. Si no se habilita este control, entonces solo serán aceptadas las peticiones de las direcciones IP especificadas en la sección Acceso serán aceptadas.

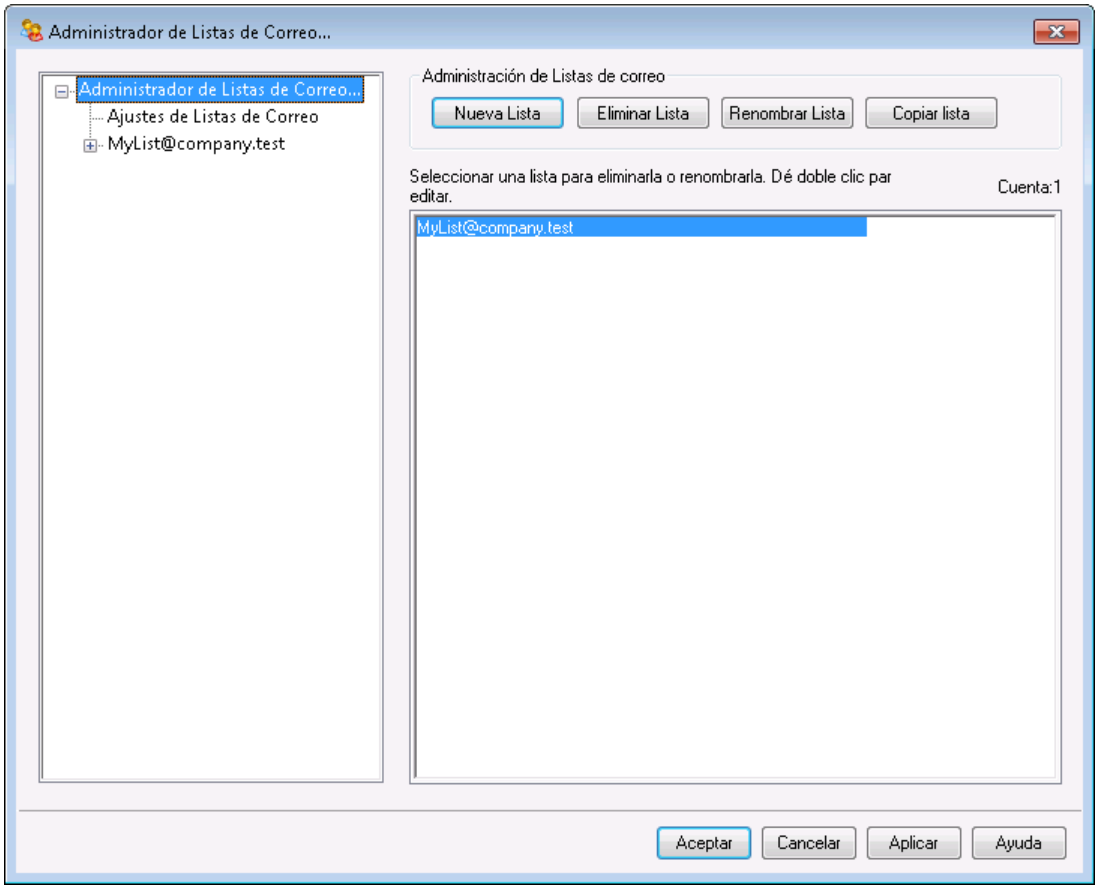
Se requiere autenticación al enviar correo como usuario de esta puerta de enlace
Marque esta casilla si quiere que todos los mensajes que digan ser de este dominio requieran autenticación. Si un mensaje dice ser de este dominio debe usar una conexión autenticada (o conectar desde una dirección IP de Confianza) o será rechazada. Esta opción está habilitada por defecto.

Cuando se crean nuevos dominios de puerta de enlace, esta opción se habilita por defecto. Si desea cambiar la configuración por defecto para que las nuevas puertas de enlace tengan esta opción deshabilitada, entonces edite la siguiente clave en el archivo `MDaemon.ini`:

```
[Special]
GatewaySendersMustAuth=No (por defecto es Yes)
```

3.4 Administrador de Listas de Distribución

Las Listas de Distribución, llamadas a veces Grupos de Correo o Listas de Distribución, permiten a los grupos de usuarios recibir correo como si todos compartieran un buzón común. Copias de los mensajes de correo enviados a la lista se distribuyen a cada uno de los miembros de la lista. Las listas pueden contener miembros locales y/o direcciones de destino remoto, ser públicas o privadas, moderadas o abiertas, ser enviadas en resumen 294 o en formato normal de mensaje y más.



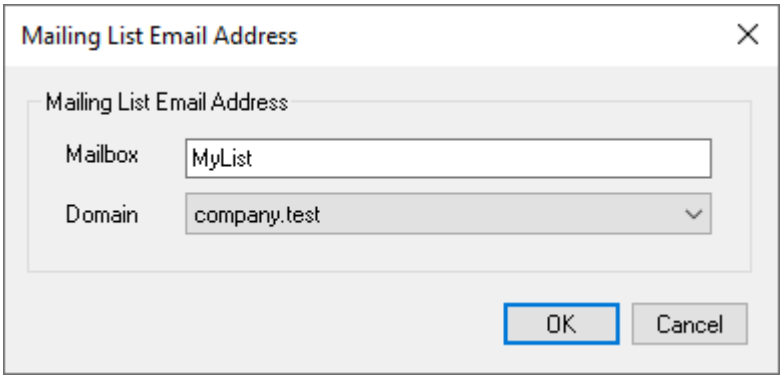
Localizado bajo el menú Ajustes » Administrador de Listas de Distribución..., el Administrador de Listas de Distribución se utiliza para administrar sus listas.

Administración de Listas de Distribución

El panel de navegación al lado izquierdo de este diálogo contiene una entrada por cada una de sus listas de distribución, con ligas a cada pantalla utilizada para configurar varios ajustes específicos para cada lista. También da acceso a la pantalla Ajustes de Listas de Distribución 277, que se utiliza para configurar varias opciones globales relativas a las listas. Las opciones en el lado izquierdo de este diálogo se utilizan para crear, eliminar y renombrar sus listas. Puede dar doble clic en una lista de distribución para pasarse al editor de listas y configurar los ajustes de cada una de ellas.

Nueva lista

Para crear una nueva lista de distribución, dé clic en **Nueva lista** para abrir el diálogo Dirección de Correo de la Lista de Distribución. Cree un nombre de buzón y seleccione un dominio, tal como "MyList" y "example.com" respectivamente. Esta será la dirección de correo de la lista (ej. MyList@example.com). Los mensajes enviados a esta dirección se distribuirán a los miembros de la lista, con base en los ajustes particulares de la misma. Dé clic en **OK** para crear la lista. Luego de esto, puede dar doble clic en su registro para configurar sus ajustes y agregar miembros. **Nota:** Los nombres de lista no pueden contener " ! " o " | "



Eliminar Lista
Para eliminar una lista de distribución: seleccione la lista, dé clic en **Eliminar Lista** y luego clic en **Si** para confirmar su decisión.

Renombrar lista
Para renombrar una lista de distribución, seleccione la lista y dé clic en **Renombrar lista** para abrir el diálogo Dirección de Correo de la Lista de Distribución. Realice los cambios deseados y dé clic en **OK**.

Copiar lista
Si desea crear una lista de distribución con los mismos ajustes y miembros que otra lista existente, seleccione esta, dé clic en este botón y especifique el nombre y dominio para la nueva lista.

Modificar una Lista de Distribución Existente

Para configurar una lista de distribución, dé doble clic en su registro sobre el Administrador de Listas de Distribución. Luego en el panel de navegación de la izquierda dé clic en la pantalla que desea editar:

Miembros 280
Ajustes 283
Encabezado 286
Suscripciones 289
Recordatorios 293
Moderación 298
Resumen 294
Enrutamiento 300
Notificaciones 296
Archivos de Soporte 302
Carpeta Pública 304
Active Directory 305
ODBC 307

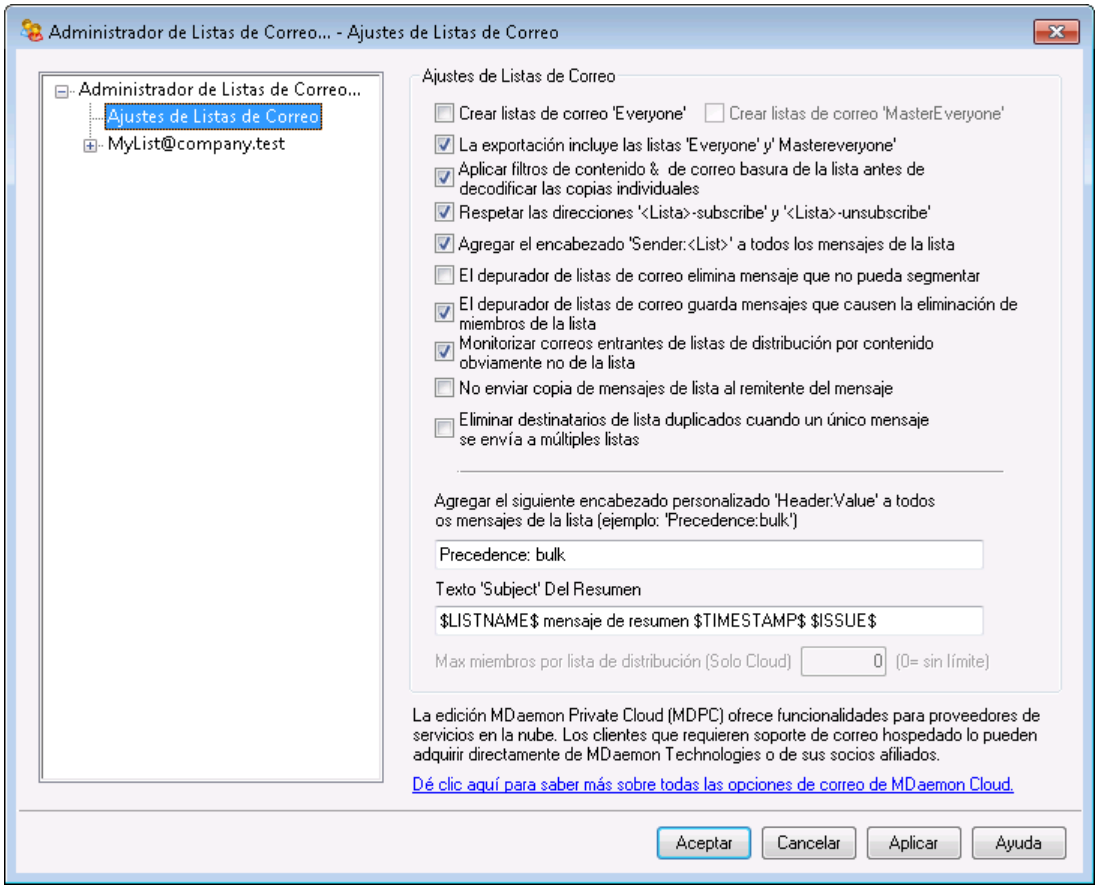
Ajustes de Listas de Distribución

Dé clic en **Ajustes de Listas de Distribución** en el panel izquierdo para abrir la pantalla Ajustes de Listas de Distribución 277, para configurar varios ajustes globales relativos a las listas de distribución.

Ver:

Ajustes de Listas de Distribución 277

3.4.1 Ajustes de Listas de Distribución



Ajustes de Listas de Distribución

Crear lista de distribución "Everyone"
Marque esta casilla si desea crear y mantener listas de distribución "Everyone" para todos sus dominios (ej. "everyone@example.com"). Se creará una lista para cada dominio, lo que le permite enviar mensajes a todos los usuarios de un dominio simplemente dirigiendo los mensajes a "everyone@<domain>". Las Cuentas Privadas 760 están ocultas de las listas de distribución "Everyone". Esta opción está deshabilitada por omisión.

Crear la lista "MasterEveryone"
Habilite esta opción si desea que exista la lista de distribución "MasterEveryone". En ella se incluyen todas las listas "everyone" de todos sus dominios. Esta opción se encuentra deshabilitada por omisión.

La exportación incluye las listas 'Everyone' y 'MasterEveryone'
Por omisión, las listas de distribución 'Everyone' se incluyen cuando utiliza las opciones Cuentas » Exportación..." para exportar listas. Deshabilite esta opción si no desea incluir esas listas en la exportación de listas de distribución.

Aplicar filtro de contenido y de Spam a los correos de la lista antes de generar las copias individuales
Cuando se selecciona la opción *Entregar el correo de la lista a cada miembro individualmente* en la pantalla Enrutamiento 300 del editor de listas de distribución, al habilitar este control se aplicarán las reglas del filtro de contenido y el filtro de Spam a los mensajes de la lista antes de que sean copiados y distribuidos a los miembros de la lista.

Respetar las direcciones '<List>-subscribe' y '<List>-unsubscribe'
Dé clic en esta casilla si desea que MDaemon reconozca como válidas las direcciones de correo de este formato (siempre y cuando la lista exista) a fin de contar con un método sencillo para que los usuarios se unan o salgan de sus listas de distribución. Por ejemplo: suponga que tiene una lista llamada `MyList@example.com`. Los usuarios podrán suscribirse/desuscribirse a la lista enviando un correo a `MyList-Subscribe@example.com` y a `MyList-Unsubscribe@example.com`. El contenido del asunto y el cuerpo del mensaje son irrelevantes. Así mismo, cuando esta funcionalidad está activa, MDaemon insertará el encabezado siguiente en todos los mensajes de la lista:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Algunos clientes de correo pueden reconocer esto y habilitar el botón UNSUBSCRIBE automáticamente.

Puede invalidar esta opción para listas individuales especificando el valor de los encabezados List-Subscribe y List-Unsubscribe en las opciones **URLs de Listas de Distribución** localizada en la pantalla Moderación 298 del editor de Listas de Distribución.

Agregar el encabezado 'Sender: <List>' a todos los mensajes de la lista
Habilite esta opción si desea insertar el encabezado `Sender` en los mensajes de la lista de distribución.

El depurador de Listas de Correo elimina los mensajes que no puede segmentar
Cuando se habilita esta opción, MDaemon eliminará los mensajes de la lista que no contengan direcciones identificables.

El depurador de Listas de Distribución guarda los mensajes que pueden originar la eliminación de miembros de la lista
Cuando MDaemon revisa los mensajes de la lista devueltos, en un intento de eliminar direcciones de miembros que no se pueden contactar, este control hará que se guarden los mensajes que puedan originar la eliminación de un miembro de la lista. Para más información, vea la opción *Eliminar direcciones no entregables...* en la pantalla Ajustes 283.

Monitorizar correo entrante para listas de distribución, buscando contenido obviamente ajeno a la lista
Marque esta casilla si desea que MDaemon rechace mensajes dirigidos a listas de distribución cuando determina que deberían haber sido enviados a la cuenta del sistema. Por ejemplo, un usuario puede suscribirse o desuscribirse de una lista colocando el comando Subscribe o Unsubscribe al inicio de un mensaje de correo, enviándolo a la dirección del sistema (ej. "mdaemon@example.com"). Con frecuencia los usuarios intentan erróneamente enviar esos mensajes a la lista misma. Esta opción impedirá que esos mensajes se entreguen a la lista.

No enviar copias de mensajes de listas al remitente del mensaje
Cuando esta opción se habilita y un miembro de la lista envía un mensaje a la lista, el remitente no recibirá copia del mensaje. Esta opción se encuentra deshabilitada por omisión.

Eliminar destinatarios duplicados cuando un mensaje es enviado a múltiples listas
Cuando se habilita esta opción y un mensaje es dirigido a múltiples listas, MDaemon entregará solo una copia del mensaje a cualquier destinatario que sea miembro 280 de más de una de las listas. Por ejemplo, si `frank@example.net` es miembro de `List-A@example.com` y `List-B@example.com` y un mensaje entrante es dirigido a ambas listas, Frank recibirá solo una copia del mensaje en lugar de dos. Esta opción solo aplica a listas, por lo que en el ejemplo anterior si el mensaje fuera dirigido directamente a Frank más las dos listas, entonces Frank recibiría dos copias del mensaje en lugar de tres. Esta opción se encuentra deshabilitada por omisión.

En general no se recomienda utilizar esta opción. Las listas de distribución se pueden utilizar y organizar de muchas maneras diferentes por los usuarios y no hay manera de saber cuál lista recibirá el mensaje cuando se limitan los duplicados de esta manera. Por esto, el utilizar esta opción generaría dificultades innecesarias para algunos usuarios, debido a preferencias de seguimiento de mensajes, al uso de filtros IMAP 737 para ordenar mensajes hacia carpetas específicos, entre otros.

Agregar el siguiente encabezado personalizado 'Header: value' a todos los mensajes de la lista
Si desea agregar una combinación estática de encabezado/valor (tal como "Precedence: bulk") a todos los mensajes de la lista, especifique aquí ese texto.

Texto del 'Subject:' del Resumen:
Utilice esta opción si desea personalizar el asunto utilizado cuando MDaemon envía mensajes de Resúmenes de listas de distribución 294. El valor por omisión es: "`$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$`." Las macros expanden el nombre de la lista de distribución, la marca de tiempo de la creación del resumen y el número de emisión.

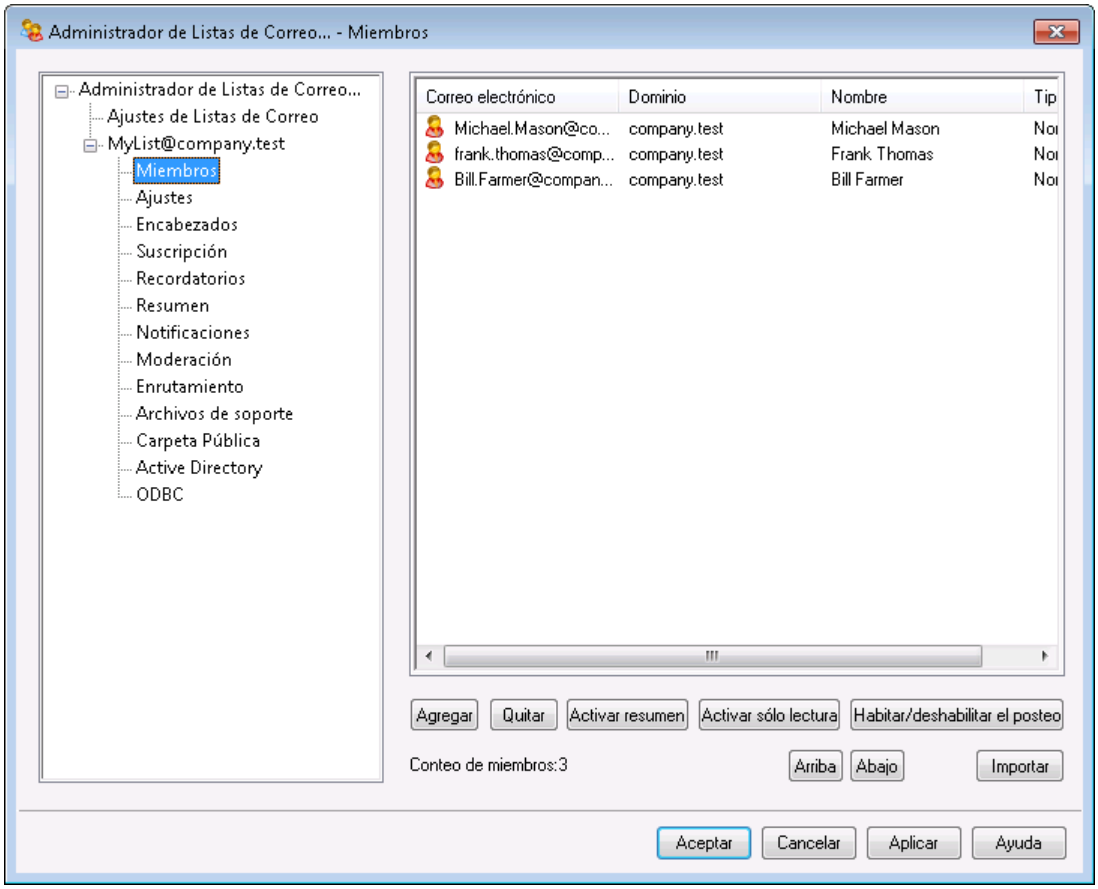
Máximo número de miembros por lista de distribución [xx] (0=sin límite)
Use esta opción si desea establecer un número máximo de miembros permitido por lista de distribución. Puede establecer un máximo por dominio en la pantalla Ajustes 219 del Administrador de Dominios.

Ver:

[Administrador de Listas de Distribución](#) 274

3.4.2 Editor de Listas de Distribución

3.4.2.1 Miembros



Esta pantalla muestra las direcciones de correo y nombres de todos los miembros suscritos actualmente a la lista. Cada registro muestra también el "tipo" de suscripción: normal, resumen, sólo lectura, o sólo publicación. Para editar los ajustes de un miembro, dé doble clic en su registro.

Agregar
Este botón abre la pantalla Nuevo Miembro de la Lista para [agregar nuevos miembros](#) 282.

Eliminar
Para eliminar a un miembro de la lista, seleccione esta entrada y luego haga clic en este botón.

Activar resumen
Seleccione un miembro y dé clic en este botón para que su membresía sea de tipo Resumen[294]. Dé clic en el botón de nuevo para regresar el miembro al modo "normal".

Activar sólo lectura
Seleccione el registro de un miembro y dé clic en este botón para cambiar a modo "Solo Lectura". El miembro seguirá recibiendo mensajes de la lista, pero no se le permitirá enviar a ésta. Dé clic de nuevo en el botón para regresar al miembro al modo "normal".

Activar solo Publicar
Haga clic en este botón después de seleccionar un miembro para configurar su suscripción como "Sólo publicación". Un miembro de Sólo Publicación puede mandar mensajes, pero no puede recibirlos. Dé clic de nuevo en el botón para regresar al miembro al modo "normal".

Arriba/Abajo
Seleccione uno o más miembros y dé clic en estos botones para moverlos hacia arriba o abajo en la lista. También puede ordenar la lista dando clic en el encabezado de cualquier columna. Nota: Si ordena la lista por cualquier encabezado de columna se perderá cualquier ordenamiento manual que haya hecho utilizando los botones Arriba/Abajo.

Importar
Dé clic en este botón para importar miembros de la lista desde un archivo de texto que cuente con encabezados separados por comas (i.e. archivo delimitado por comas). Cada registro debe tener su propia línea y todos los campos se deben separar por comas. Más aun, la primera línea del archivo (base de referencia) debe contener los nombres de los campos y el orden en que aparecen en las líneas siguientes. Uno de los campos se debe llamar "**`Email`**" y contener direcciones de correo. Se tienen dos campos opcionales: "**`FullName`**" y "**`Type`**". `FullName` es para el nombre del miembro de la lista. `Type` puede tener un valor de: "`read only`", "`post only`", "`digest`", o "`normal`". Todos los campos restantes serán ignorados por el importador.

Por ejemplo:

```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St",
"519.555.0100"
```

Los miembros importados no reciben un paquete de bienvenida a la lista (si existe) y el importador no verificará si hay miembros duplicados.

Conteo de Miembros:
El número total de miembros suscritos actualmente a la lista se muestra al final de la pantalla.

Agregar Nuevos Miembros

Nuevo Miembro de la Lista

Correo
Ingrese la dirección de correo que desea agregar a la lista de distribución o dé clic en el ícono cuenta si desea visualizar las cuentas y grupos de MDaemon para agregar una a la lista. Las direcciones de miembros de la lista no pueden contener " ! " o "|".

Si desea agregar todos los usuarios de uno de sus dominios o todos los usuarios de un grupo específico, puede registrar **`ALL_USERS:<domain>`** o **`GROUP:<group-name>`** respectivamente, en lugar de ingresar las direcciones de correo específicas. Por ejemplo, agregar `ALL_USERS:example.com` como miembro de una lista tiene el mismo efecto que agregar todos los usuarios de `example.com` por separado.

También puede utilizar **`CONTACTS:<domain>`** para incluir los contactos públicos 128 de un dominio como miembros de la lista. Por ejemplo, `CONTACTS:example.com`.

Nombre Completo
Introduzca el nombre del miembro en este campo. Este nombre aparecerá en el encabezado "To:" de los mensajes de la lista cuando esté seleccionada la opción "*Reemplazar el encabezado 'TO:' con el Nombre del Miembro de la Lista*" en la pantalla Encabezados 286.

Tipo
Utilice la caja de la lista desplegable para seleccionar un tipo de membresía para el usuario:

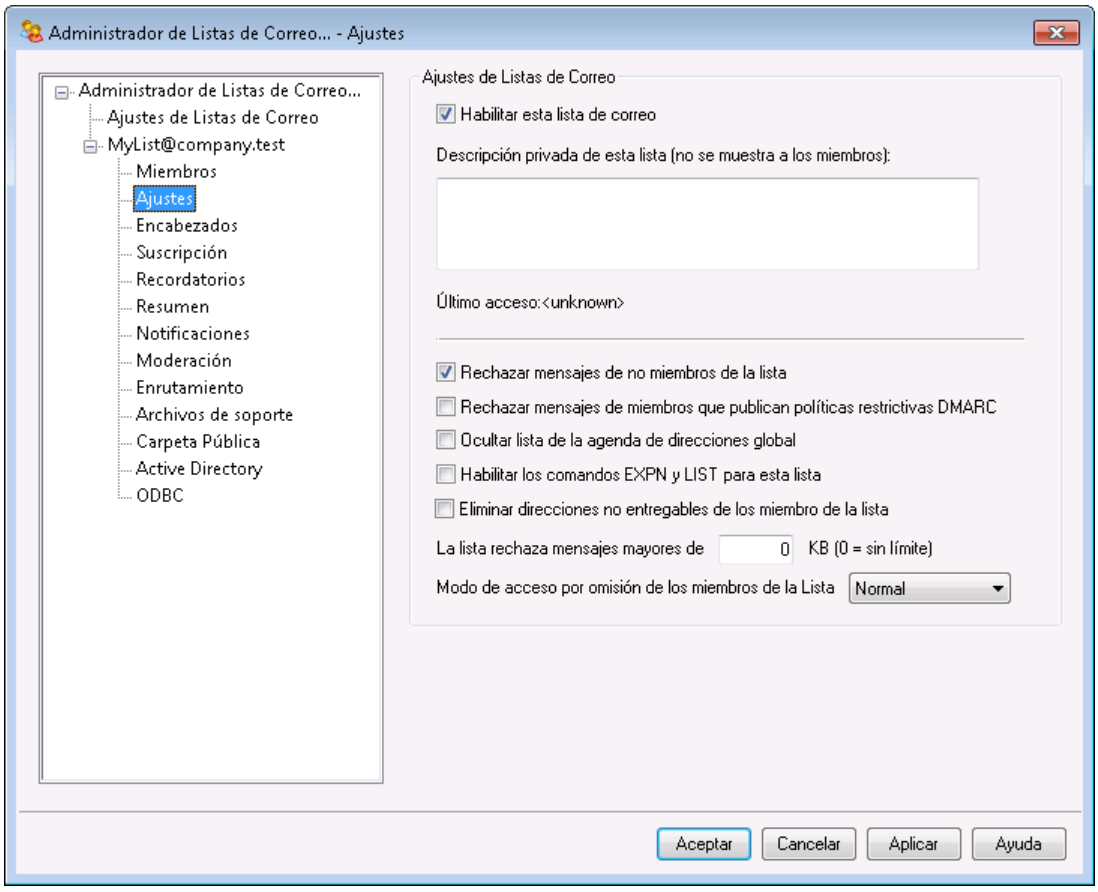
Normal—El miembro puede enviar y recibir mensajes de la lista normalmente.

Resumen—El miembro puede enviar y recibir mensajes de la lista, pero los mensajes recibidos estarán en formato resumen.

Solo Lectura—El miembro recibirá mensajes de la lista, pero no puede enviar mensajes a ella.

Solo publicación—El miembro de la lista puede enviar mensajes, pero no recibirlos.

3.4.2.2 Ajustes



Ajustes de Listas de Distribución

Habilitar esta Lista de Distribución
Deshabilite esta casilla si desea deshabilitar temporalmente la lista de distribución. Mientras la lista esté deshabilitada, cualquier mensaje que se reciba vía SMTP de o para la lista, generará un error temporal 451 y será rechazado.

Descripción Privada de esta lista (No se muestra a los miembros)
Puede registrar aquí una descripción privada de la lista. Esto es para su propia referencia y no se desplegará a ningún miembro o en ningún encabezado.

Último Acceso
Despliega la hora en que alguien accedió por última vez esta lista. Esto puede ayudarle a identificar más fácilmente aquellas listas que no se utilizan o se utilizan raramente.

Rechazar mensajes de no-miembros de la lista
Cuando se habilita este control, la lista se considerará "privada", lo que significa que solo los miembros de la lista pueden enviar mensajes a la misma. Los mensajes provenientes de no-miembros serán rechazados.

Rechazar mensajes de dominios con políticas restrictivas DMARC
Habilite esta opción si desea rechazar cualquier mensaje entrante a la lista que sea enviado por alguien de un dominio que publica políticas restrictivas DMARC 538 (i.e. p=quarantine o p=reject). Generalmente no es necesario habilitar esta opción si está utilizando la opción "*Reemplazar la dirección de correo 'From:' con la dirección de correo de la lista si...*" localizada en la pantalla Encabezados 286.

Si tanto esta como la opción "*Reemplazar la dirección de correo 'From:' con la dirección de correo de la lista si...* 286 " se encuentran deshabilitadas, entonces es probable que algunos mensajes de la lista sean rechazados por algunos servidores destino y en algunos casos podría originar que el destinatario sea eliminado automáticamente de la lista 285. Por lo tanto, deberá tener cuidado en asegurarse de que al menos una de estas dos opciones está habilitada.

Ocultar esta lista de la libreta global de direcciones
Dé clic en esta opción para ocular la lista de distribución de las libretas públicas de direcciones de Webmail y LDAP.

Habilitar los comandos EXPN y LIST para esta lista Por omisión MDaemon no respetará los comandos EXPN y LIST para las listas, a fin de mantener la membresía privada. Si habilita esta opción, la membresía de la lista será reportada en respuesta a los comandos EXPN o LISTS durante una sesión de correo.

Eliminar automáticamente direcciones no entregables de la membresía de la lista
Cuando se habilita esta funcionalidad, MDaemon eliminará automáticamente de la lista aquellas direcciones con las que encuentre un error fatal permanente al intentar hacer la entrega. La dirección también se elimina cuando el mensaje pasa al sistema de Reintentos 872 y subsecuentemente expira en ese sistema.

La opción *Eliminar automáticamente direcciones muertas...* solo está diseñada para ayudar en situaciones donde un servidor de correo remoto rechaza la aceptación de mensajes. Solo funcionará cuando se ha seleccionado la opción "*Entregar correo de la lista a cada miembro individualmente*" en la Pantalla de Enrutamiento 300. Si está enrutando mensajes a un host inteligente, verifique la opción siguiente Depuración Mejorada de Listas 285 abajo para más información.

La lista rechaza mensajes mayores de [xx] KB
Este control define un límite superior al tamaño de los mensajes aceptados para esta lista de distribución. Los mensajes mayores de este límite son rechazados.

Modo de acceso por omisión para miembros de la lista
Utilice el menú desplegable para configurar el modo de acceso por omisión que utilizarán los miembros nuevos. Puede modificar el ajuste del modo de acceso de cualquier miembro existente en la pantalla Miembros 280. Existen cuatro modalidades de membresía:

Normal—El miembro puede enviar y recibir mensajes normalmente.

Digest—El miembro puede enviar y recibir mensajes de la lista, pero los mensajes recibidos llegarán en formato resumen.

Solo lectura—El miembro recibirá mensajes de la lista, pero no puede enviar mensajes a ella.

Solo Posteo—El miembro de la lista puede enviar mensajes a la lista, pero no recibirá.

Depuración Mejorada de Listas

Cuando está habilitada la opción *Automáticamente eliminar direcciones no entregables de la membresía de la lista* y usted ha especificado un buzón local como ruta de devolución para los mensajes de la lista (ver la opción *Dirección 'Bounce' SMTP* en Notificaciones 296), todos los días a medianoche MDaemon intentará segmentar direcciones problema en el correo devuelto y eliminará aquellos miembros que no pudieron ser encontrados. Esto ayudará a depurar más eficientemente las direcciones incorrectas de las listas de distribución, especialmente cuando se están enrutando mensajes de la lista a un host inteligente en lugar de entregarlos directamente.

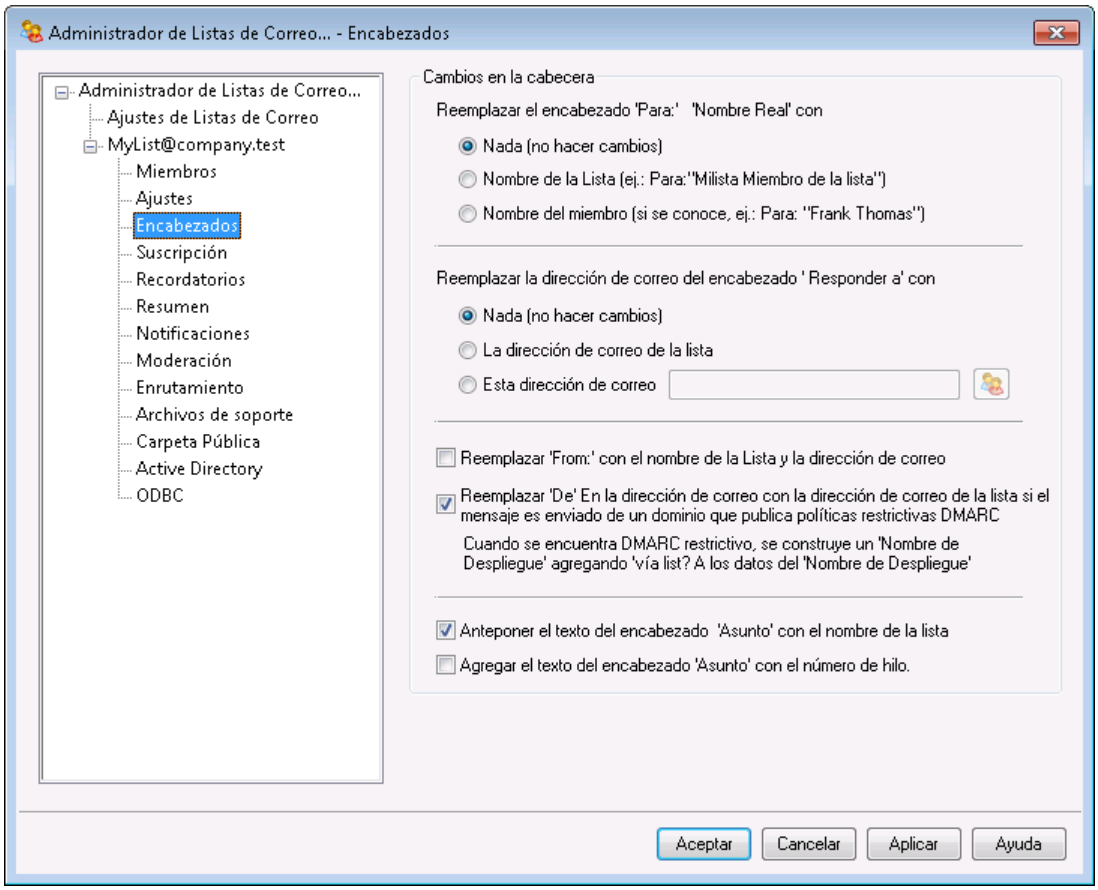
En Ajustes de Listas de Distribución 277 existen dos opciones relacionadas con esta funcionalidad. La opción *El depurador de Listas de Distribución elimina mensajes que no puede segmentar* hará que se eliminen los mensajes devueltos que no contienen direcciones identificables y la opción *El depurador de listas guarda los mensajes que pueden originar una eliminación de miembros* hará que se guarden los mensajes que pudieran ocasionar la eliminación de un miembro de las listas.

Configurar la opción *Dirección 'Bounce' SMTP de la lista* 296 a una dirección de correo local puede hacer que el correo de los usuarios sea eliminado como resultado de los ajustes del

depurador de listas definidos en Ajustes de Listas de Distribución 277.

Cuando la entrega a una dirección origina un error 5xx, la dirección se agregará al archivo `BadAddress.txt localizado` en la carpeta de registros. Esto le puede ayudar, por ejemplo, a identificar direcciones erróneas en sus listas de correo más rápidamente en lugar de buscar en los registros de SMTP saliente. Este archivo se elimina automáticamente a media noche cada noche para impedir que crezca demasiado.

3.4.2.3 Encabezados



Cambios a Encabezados

Reemplazar el encabezado 'TO:' 'Nombre de Despliegue' con
Utilice esta opción para definir el texto a desplegar en la porción de nombre del encabezado TO: siempre que MDaemon reciba un mensaje dirigido a la lista.

Nada (no hacer cambios) - Cuando se selecciona esta opción, MDaemon no hará cambios. El nombre de despliegue y la dirección contenida en el encabezado TO: aparecerán exactamente como las registró el remitente del mensaje.

Nombre de la Lista - Esta opción reemplaza el nombre desplegado con el nombre de la lista más "List Member". Por ejemplo, para una lista de correo llamada "My-Family" la porción del nombre de despliegue en el encabezado To: dirá: "My-Family List Member".

Nombre del Miembro (si se conoce) - Cuando se selecciona esta opción, el encabezado TO: contendrá el nombre (si está disponible) y la dirección del miembro de la lista a quién va dirigido el mensaje.

La opción *Nombre del Miembro* solo se puede seleccionar cuando se ha seleccionado la opción "*Entregar a cada miembro individualmente*" en la Pantalla de Enrutamiento 300. Cuando se selecciona "*Entregar correo de la lista utilizando comandos individuales RCPT para cada miembro*", MDaemon por omisión utilizará la opción *Nombre de la Lista*.

Reemplazar la dirección de correo en el encabezado 'Reply-To:' con
Esta opción es para definir la dirección de correo que aparecerá en el encabezado Reply-To en cada mensaje de la lista.

Nada (no hacer cambios)
Seleccione esta opción si desea dejar sin modificar el encabezado Reply-To de lo que tenga en el mensaje original que será distribuido a la lista. Esta es en general la opción que deberá seleccionar cuando quiera que las respuestas se dirijan a quién sea que haya enviado el mensaje a la lista, en lugar de enviarse a todos los miembros de la lista.

Dirección de correo de la Lista
Seleccione esta opción si desea que las respuestas se dirijan a la lista en lugar de a una persona o dirección específicas. Esta es la opción que debe seleccionar si desea utilizar la lista como herramienta de un grupo de discusión, donde las respuestas se envían a todos los miembros.

Esta dirección de correo
Si existe una dirección específica de correo a la que desea que se envíen las réplicas, tecléela aquí o dé clic en el ícono Cuenta si desea buscar la cuenta específica de MDaemon que va a utilizar. Puede utilizar esta opción, por ejemplo, para algo como un boletín de correo con una dirección de contacto específica para las respuestas.

Reemplazar la dirección de correo 'From:' con la dirección de la lista de correo si el mensaje se envía desde un dominio que publica políticas DMARC restrictivas
Por omisión, cuando un mensaje entrante a la lista se envía de un usuario en un dominio que publica políticas DMARC[538] restrictivas (i.e. p=quarantine o p=reject), MDaemon reemplazará la dirección de correo del usuario en el campo From: con la dirección de la lista, antes de enviar el mensaje a la lista. Esto es necesario para prevenir que el mensaje de la lista sea rechazado por los servidores que respetan las políticas restrictivas DMARC. Además de cambiar la dirección de correo del encabezado From:, el nombre desplegado se modificará también para agregar "vía List Name" para mostrar que es un mensaje enviado por esa lista de correo por parte de la persona nombrada. Más aun, siempre que el encabezado From: sea modificado por esta funcionalidad, el encabezado From: original será movido al encabezado Reply-To: pero solo si el mensaje no cuenta con encabezado Reply-To: para empezar y la lista no está configurada para desplegar un encabezado Reply-To personalizado.

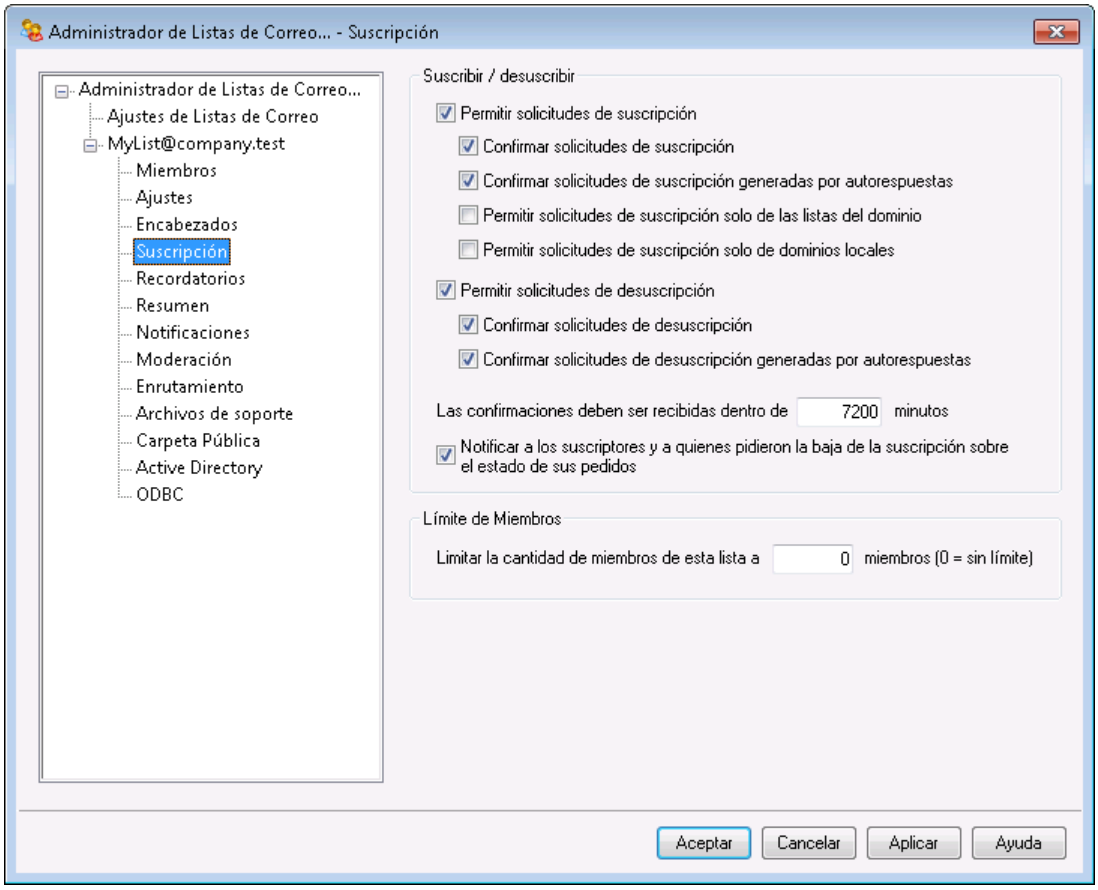
Esta acción solo se ejecutará cuando esté habilitada la opción Verificación DMARC[545] y se haya realizado la verificación del mensaje entrante.

No deshabilite esta opción a menos que entienda verdaderamente las ramificaciones de hacerlo y esté seguro de que necesita deshabilitarla. Al hacerlo podría ocurrir que algunos mensajes de la lista sean rechazados por algunos servidores destino y en algunos casos podría originar que el destinatario sea automáticamente eliminado de la membresía de la lista[285]. Alternativamente, puede habilitar la opción *Rechazar mensajes de dominios con políticas restrictivas*[283], lo que hace que los mensajes entrantes para la lista sean rechazados cuando provengan de un dominio con una política DMARC restrictiva.

Anteponer al texto del encabezado 'Subject:' el nombre de la lista
Este parámetro hace que MDaemon coloque el nombre de la lista entre paréntesis cuadrados (v.g. [ListName]) y lo agregue al inicio de `Subject:` en todos los mensajes enviados a la lista. Esta opción se encuentra habilitada por omisión.

Anteponer al texto del encabezado 'Subject:' el número de hilo
Esta opción le permite activar si se deben desplegar los números de hilo en el `Subject:` para los mensajes de la lista. Se agrega el número al final de la línea del asunto entre corchetes y se utiliza como un pseudo número de hilo. Al ordenar su Bandeja de Entrada por asunto, se alineará el correo de la lista en orden cronológico. Esta opción se encuentra deshabilitada por omisión.

3.4.2.4 Suscripción



Suscribir / Desuscribir

Permitir solicitudes de suscripción
Esta opción controla si la lista permite o no solicitudes de suscripción, bien a través de correos especialmente formateados o bien a través de autorespuestas. Para más información, vea Suscribirse a Listas de Distribución 291.

Confirmar solicitudes de suscripción
Cuando se marca esta casilla, MDaemon intentará confirmar las solicitudes de suscripción generando un código único y luego enviándolo en un mensaje a la dirección solicitando el ingreso a la lista. Si la persona contesta a dicho mensaje de confirmación, MDaemon añadirá automáticamente al miembro a la lista. Los mensajes de confirmación son sensibles al tiempo, lo que significa que el usuario debe contestar al mensaje dentro del número de minutos designado más abajo. **Nota:** Los contenidos del mensaje de confirmación se encuentran en el archivo `SubConf.dat`, localizado en la carpeta "`MDaemon\app\`".

Confirmar solicitudes de suscripción generadas por autorespuestas
Cuando esta casilla está marcada, MDaemon intentará confirmar las solicitudes de suscripción que se generan automáticamente a través de la opción Autorespuesta 726, "*Agregar remitente a esta lista de correo*." Al igual que en la opción anterior, MDaemon generará un código único y lo enviará en un mensaje a la dirección que espera ser añadida a la lista. Si la persona contesta a dicho mensaje de confirmación, MDaemon añadirá automáticamente el miembro a la lista. Estos mensajes de confirmación

también son sensibles al tiempo y deben por lo tanto se les debe responder dentro del número de minutos designados abajo.

Permitir peticiones de suscripción solo del dominio de la lista
Seleccione esta opción si desea permitir peticiones de suscripción solo de usuarios que pertenecen al dominio de la lista. Por ejemplo, solo se permitirá a los usuarios "@example.com" suscribirse a la lista "MyList@example.com".

Permitir peticiones de suscripción solo de dominios locales
Seleccione esta opción si desea permitir peticiones de suscripción solo de usuarios que pertenecen a alguno de los dominios locales del servidor MDaemon.

Desuscribir

Permitir solicitudes de desuscripción
Esta opción controla si la lista permitirá o no solicitudes de desuscripción, bien a través de mensajes especialmente formateados o a través de autorespuestas. Para más información, vea: Suscribirse a Listas de Distribución 291.

Confirmar solicitudes de desuscripción
Cuando se selecciona esta opción, MDaemon intentará confirmar las solicitudes de quitar a un miembro de la lista, generando un código único y enviándolo en un mensaje a la dirección que solicita la desuscripción de la lista. Si la persona contesta al mensaje de confirmación, MDaemon quitará automáticamente al miembro de la lista. Los mensajes de confirmación son sensibles al tiempo, lo que significa que el usuario debe contestar al mensaje dentro del número de minutos abajo designados. **Nota:** Los contenidos del mensaje de confirmación se encuentran en el archivo `UnSubConf.dat`, localizado en la carpeta "`MDaemon\app\`".

Confirmar solicitudes de desuscripción generadas por autorespuestas
Cuando se marca esta opción, MDaemon intentará confirmar las solicitudes de desuscripción que se generan automáticamente a través de la opción de Autorespuesta 726, "*Quitar el remitente de esta lista*." Al igual que con la opción anterior de *Confirmar solicitudes de desuscripción*, MDaemon generará un código único y luego lo mandará en un mensaje a la dirección esperando a ser quitada de la lista. Si la persona luego contesta a dicho mensaje de confirmación, MDaemon quitará automáticamente al miembro. Estos mensajes de confirmación también son sensibles al tiempo y deben por lo tanto ser contestados dentro del número de minutos abajo designados.

Las confirmaciones deben ser recibidas dentro de [XX] minutos
Este es el número de minutos que el destinatario de un mensaje de confirmación de suscripción o desuscripción tiene antes de que el mensaje expire. Si se excede este límite d tiempo antes de que MDaemon reciba una contestación al mensaje, la dirección no se añadirá o quitará de la lista. La dirección necesitará entonces volver a enviar solicitud para entrar o dejar la lista. La configuración por defecto de esta opción es 7200 minutos (5 días).

Este es un valor global—se aplica a todas sus listas de distribución en lugar de solamente a la lista específica que esté editando.

Notificar a los suscriptores y a quienes pidieron la baja de la suscripción sobre el estado de sus pedidos
Cuando se habilita esta casilla, MDaemon enviará un mensaje de notificación de completado al usuario que haya sido suscrito/desuscrito a la Lista de Correo.

Límite de Miembros

Limitar la cantidad de miembros de esta lista a [xx] miembros (0=sin límite)
Con esta funcionalidad puede establecer un límite superior en el número de gente a la que se le permite suscribirse a la Lista de Correo. Introduzca un cero en este campo si no desea limitar las suscripciones de lista.

Este límite sólo aplica a direcciones suscritas a través de métodos de correo descritos en *Suscribirse a Listas de Distribución* 291. Este límite no aplica a las suscripciones entradas manualmente en la pantalla Miembros 280, ni a las solicitudes de suscripción enviadas cuando se incluye una Contraseña de Lista 298.

Ver:

Suscribirse a Listas de Distribución 291
Autorespuestas 726

3.4.2.4.1 Suscribirse a Listas de Distribución

Suscribirse/Desuscribirse vía Comandos de Correo

Para suscribirse o desuscribirse de una lista de correo, mande un mensaje de correo a `MDaemon` (o cualquiera de sus alias) en el dominio que tenga la lista de correo, e introduzca el comando `Subscribe` o `Unsubscribe` en la primera línea del cuerpo del mensaje. Por ejemplo, existe una lista de correo llamada `MD-Support` que está ubicada en `mdaemon.com`. Puede suscribirse a la lista escribiendo un mensaje para "`mdaemon@mdaemon.com`" y colocando el valor: `SUBSCRIBE MD-Support@mdaemon.com` como la primera línea del cuerpo del mensaje. El asunto del mensaje es irrelevante y se puede dejar en blanco.

Para detalles completos de cómo crear éste y otros mensajes de control, vea: Control Remoto del Servidor vía Correo 896.

Ocasionalmente, los usuarios intentarán suscribirse/desuscribirse de las listas enviando un correo con comandos a la lista en sí misma en lugar de a la cuenta de sistema de MDaemon. Esto resulta en que el comando es enviado a la lista en lugar de que el usuario sea suscrito o desuscrito. Para ayudar a prevenir que este tipo de

> mensajes sean enviados a la lista, existe una opción ubicada en Configurar » Preferencias » Sistema 494, llamada "*Monitorizar correos entrantes de listas de distribución por contenido obviamente no de la lista*." Esta opción está habilitada por defecto.

Suscribirse/Desuscribirse vía Direcciones de Correo

La opción, "*Respetar las direcciones '<Lista>-subscribe' y '<Lista>-unsubscribe*", ubicada en Ajustes » Administrador de Listas de Distribución » Ajustes de Listas de Distribución 277, permite que los usuarios se unan o abandonen listas de distribución enviando mensajes a una dirección de correo especial en lugar de requerir que usen los comandos de correo descritos en la opción anterior de *Suscribirse/Desuscribirse vía Comandos de Correo*. Para usar este método para acceder o abandonar una lista, un usuario sólo tiene que mandar un mensaje a la dirección de la lista, pero con "`-subscribe`" o "`-unsubscribe`" añadido a la porción de buzón de la dirección. Por ejemplo, si el nombre de la lista es, "`lista-de-fran@ejemplo.com`," entonces un usuario podría suscribirse a la lista enviando un mensaje a "`lista-de-fran-subscribe@ejemplo.com`." Para desuscribirse de la lista, el mensaje se enviaría a "`lista-de-fran-unsubscribe@ejemplo.com`." En ambos casos el contenido del asunto y del cuerpo del mensaje es irrelevante. Además, cuando esta funcionalidad está activa MDaemon insertará la siguiente cabecera en todos los mensajes de lista:

```
List-Unsubscribe: <mailto:<Lista>-Unsubscribe@ejemplo.com>
```

Algunos clientes pueden detectar esto y mostrar un botón UNSUBSCRIBE disponible automáticamente para los usuarios.

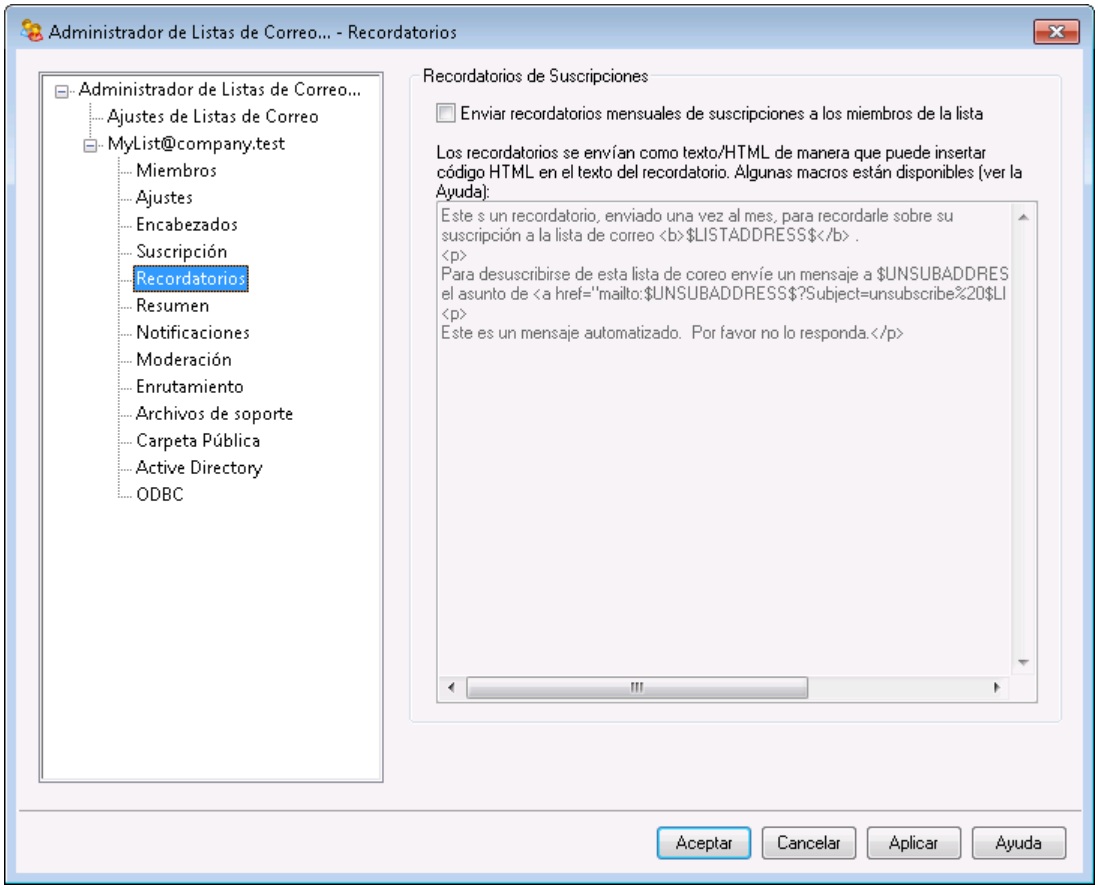
Suscribirse/Desuscribirse vía Autorespuestas

También puede utilizar las Autorespuestas 726 para añadir o quitar automáticamente miembros a la lista. Para hacer esto puede crear una o más cuentas de MDaemon cuyo único propósito sería quitar o poner automáticamente direcciones que envíen a dichas cuentas, a través de las autorespuestas configuradas en cada cuenta. Por ejemplo, si tuviera una lista de correo llamada "`lista-de-fran@ejemplo.com`," podría crear una cuenta de MDaemon con la dirección "`acceder-lista-de-fran@ejemplo.com`." Puede configurar una autorespuesta para que dicha cuenta añada a "`lista-de-fran@ejemplo.com`" cualquier dirección que envíe mensajes a ella. Luego, para unirse a dicha lista, todo lo que alguien tendría que hacer es mandar un correo a "`acceder-lista-de-fran@ejemplo.com`". Esta es una solución sencilla para los usuarios puesto que no requiere que recuerden ningún comando especial de correo requerido por el método *Suscribirse/Desuscribirse vía Comandos de Correo* descrito anteriormente.

Ver:

Suscripción 289
Control Remoto del Servidor vía Correo 896
Autorespuesta 726
Preferencias » Sistema 494
Preferencias » Varios 503

3.4.2.5 Recordatorios



Recordatorios de Suscripción

Enviar recordatorios mensuales de suscripción a todos los miembros de la lista
Habilite esta opción si desea enviar los contenidos de la caja de texto proporcionada como mensaje recordatorio de su suscripción, a cada miembro de la lista el primer día de cada mes. El mensaje recordatorio se envía como texto/HTML de manera que puede utilizar código HTML en el texto del recordatorio que seleccione. Las siguientes macros están disponibles para ser utilizadas en el mensaje recordatorio:

$LISTADDRESS$ - se expande a la dirección de la lista de correo (v.g. MyList@example.com)

$LISTNAME$ - se expande al segmento local de la dirección de correo de la lista (v.g. MyList).

$UNSUBADDRESS$ - se expande a la lista de desuscripción (la dirección de sistema de MDaemon, v.g. mdaemon@example.com)

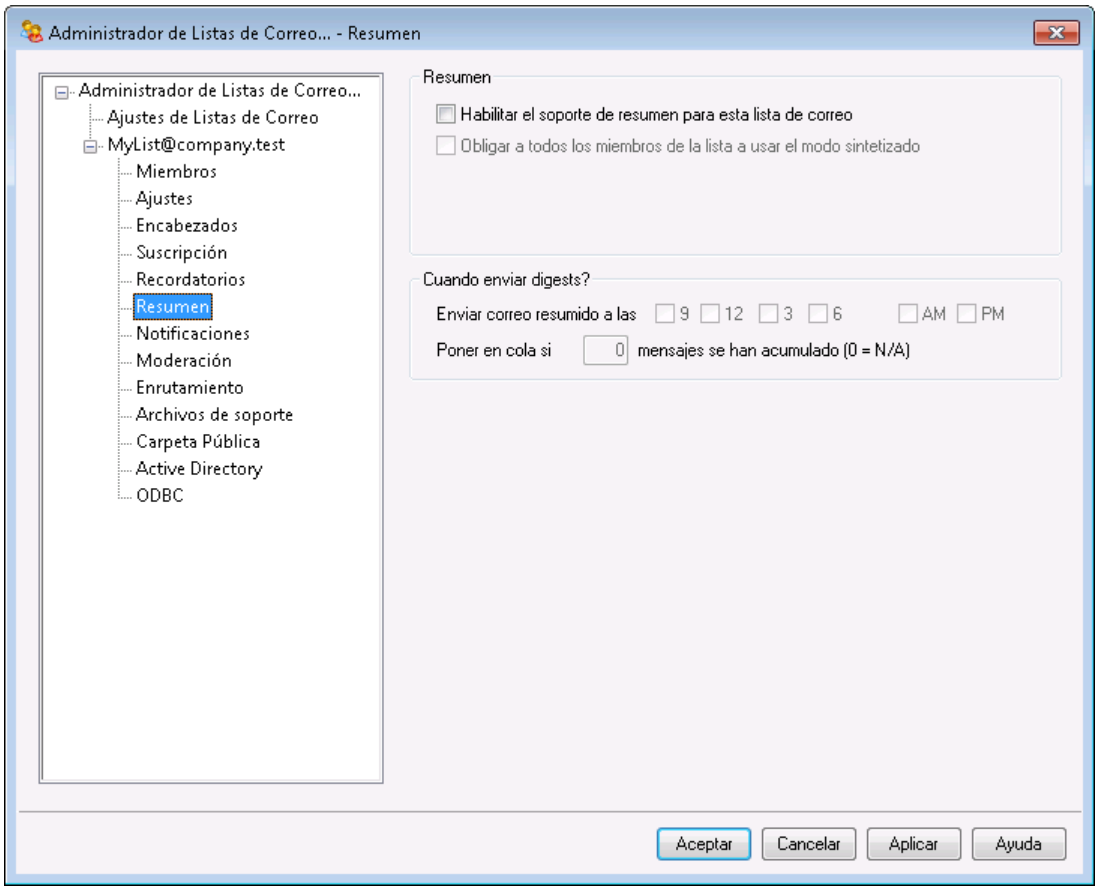
$MEMBERADDRESS$ - se expande a la dirección de correo del miembro de la lista que recibe el recordatorio (v.g. frank.thomas@example.com)

Si desea enviar recordatorios en días distintos del mes, lo puede hacer configurando la llave siguiente en el archivo MDaemon.ini:

```
[Special]
ListReminderDay=X
```

Donde "X" es un número de 1 a 28, representando el día del mes en que desea que se envíen los recordatorios.

3.4.2.6 Resúmenes



Resúmenes

Habilitar el soporte de Resúmenes para esta lista de correo
Haga clic en esta casilla si desea permitir el soporte a resumen para esta lista de correo. Cuando el soporte de resumen está habilitado, una copia de cada mensaje enviado a la lista se archivará para que a los miembros que tengan el

tipo de suscripción 280 establecido en *Resumen* se les envíen periódicamente bloques de dichos mensajes archivados en un formato compacto e indexado en lugar de recibirlos de uno en uno.

Obligar a todos los miembros de la lista a usar el modo sintetizado
Por defecto, los miembros de la lista pueden controlar si desean recibir el tráfico de lista en formato normal o resumen. Marque esta casilla si desea forzar a todos los miembros a usar el modo resumen, independientemente del modo que hayan escogido para ellos mismos.

¿Cuándo enviar Resúmenes?

Las opciones siguientes determinen con qué frecuencia y bajo qué circunstancias Resúmenes que se enviarán a los miembros de lista que estén configurados para recibir el correo en formato resumen. Todas las opciones operan independientemente para cada usuario, lo que significa que todos o cualquiera de ellos pueden hacer que se envíe un resumen.

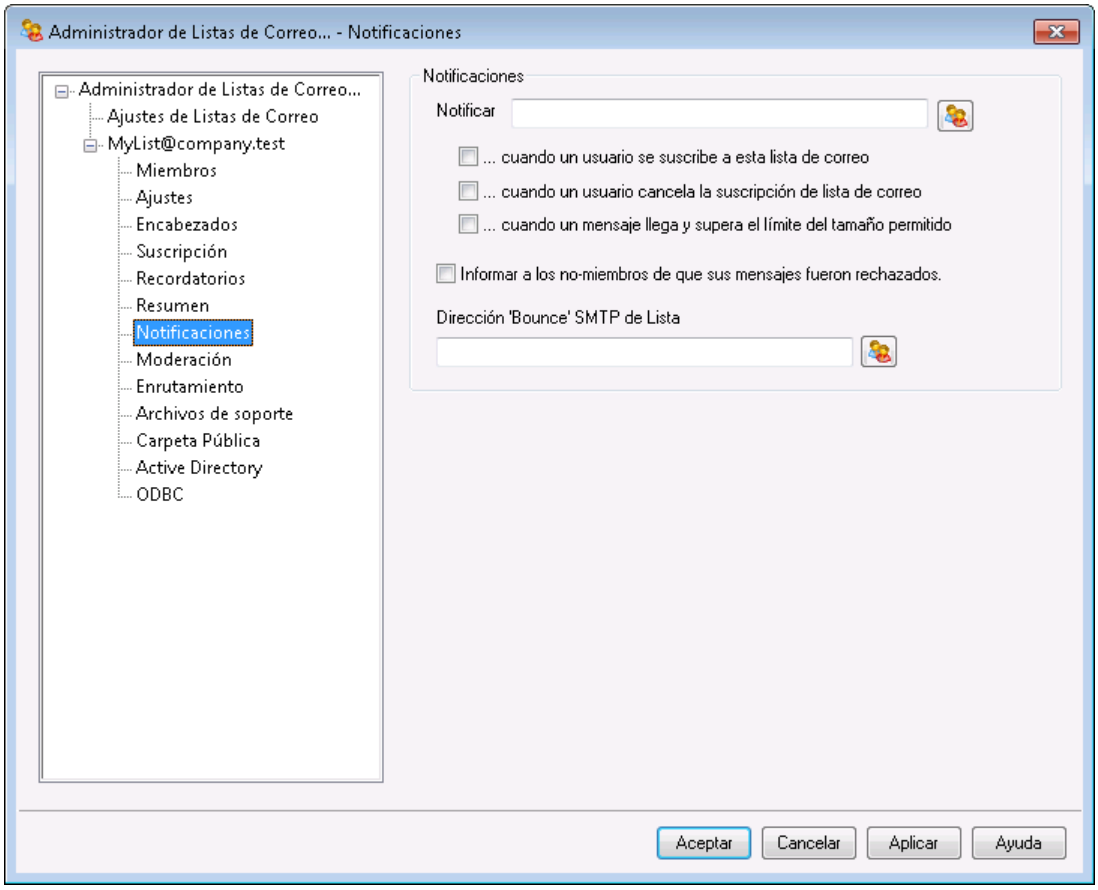
Enviar correo resumido a las 9, 12, 3, 6 AM y/o PM
Use esta opción para programar con qué frecuencia los Resúmenes de la lista se enviarán. Si marca todas las casillas en esta opción los Resúmenes se enviarán cada tres horas, además de poder ser desencadenados por las opciones a continuación.

Poner en cola si [xx] mensajes se han acumulado (0 = n/a)
Si desea enviar Resúmenes automáticamente siempre que un número de mensajes determinado se haya acumulado, especifique aquí dicho número. Use "0" si no desea usar esta opción. "0" es la opción por defecto.

Ver:

Miembros 280
Control Remoto del Servidor vía Comandos de Correo 896

3.4.2.7 Notificaciones



Notificaciones

Notificar
Use esta opción para listar una dirección que será notificada cuando el evento seleccionado se produzca.

...cuando un usuario se suscribe a esta lista de correo
Marque esta casilla si desea enviar una nota a la dirección designada cada vez que alguien suscribe a la lista de correo.

...cuando un usuario cancela la suscripción de lista de correo
Marque esta casilla si desea enviar una nota a la dirección designada cada vez que alguien se desuscribe de la lista de correo.

...cuando un mensaje llega y supera el límite del tamaño permitido
Marque esta casilla si desea enviar una nota a la dirección designada cada vez que alguien envía un mensaje a la lista de correo que es más grande que el límite *La lista rechaza mensajes más grandes que [xx] KB* designado en Configuraciones 283.

Informar a los no-miembros de que sus mensajes fueron rechazados
Cuando esta opción está habilitada y los no-miembros de una lista privada envían correo a la lista, MDaemon les informará que la lista es privada. También se les proporcionará instrucciones de cómo suscribirse a la lista. Las listas se designan

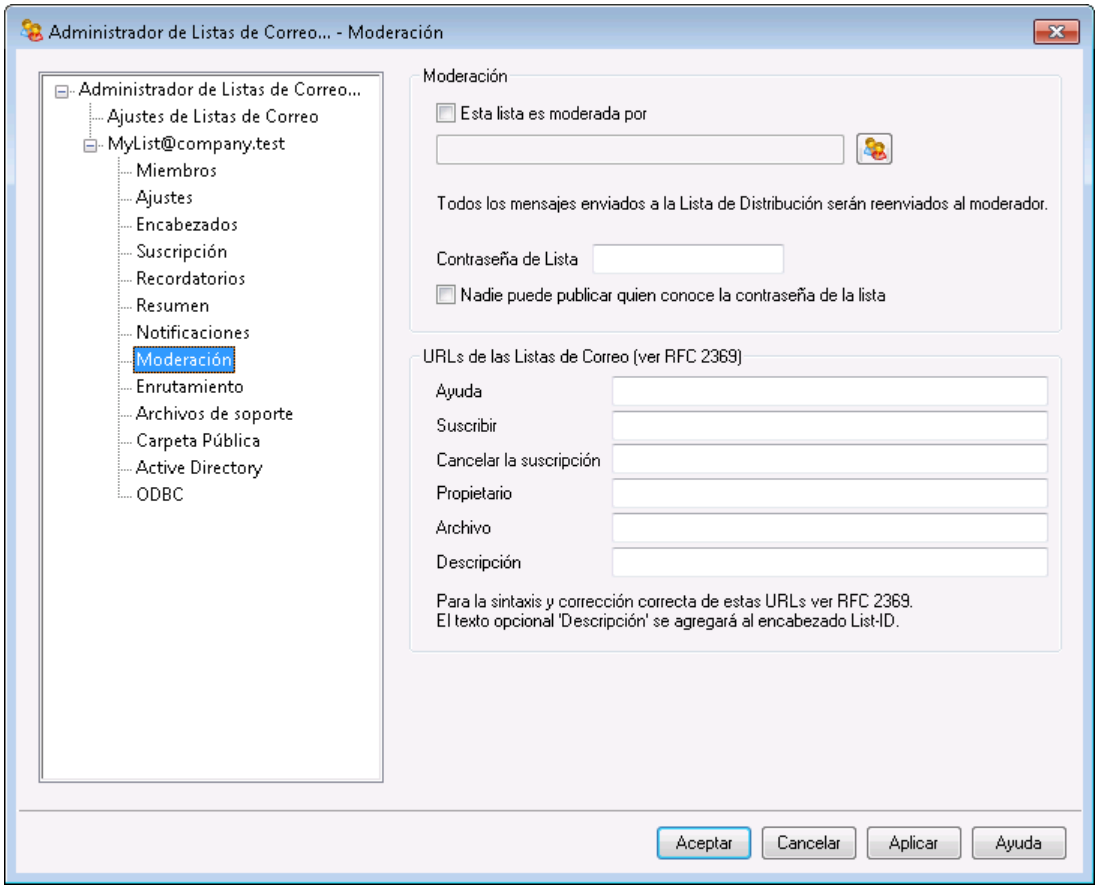
como privadas usando la opción *Sólo los miembros pueden enviar en esta lista* ubicada en Configuraciones 283.

Correo Devuelto

Dirección 'Bounce' SMTP de Lista
Use esta opción para especificar la dirección que debería recibir cualquier correo "devuelto" o notificación de estatus de envío generados por tráfico de la lista. Cualquier mensaje dado a una lista de correo con 100 destinatarios podría tener, por ejemplo, diez direcciones no alcanzables debido a cambios de dirección, servidores caídos, o similar. El sistema SMTP generará y devolverá al remitente del mensaje un mensaje de notificación de dichas condiciones. Usando esta opción puede designar la dirección que deberá recibir estos mensajes de sus listas de distribución. También puede escoger que nadie las reciba, en cual caso MDaemon colocará el correo de la lista en el envío de correo de tal manera que no sea posible devolver el correo. Esta dirección NO puede ser la dirección de la lista de correo.

Si se configura una cuenta de usuario local como Dirección de rechazo SMTP de la lista puede hacer que el buzón del usuario sea eliminado como resultado de la configuración de depuración de la lista, que se define en Ajustes de Listas de Distribución 277. Tenga cuidado antes de configurar esta opción para utilizar una cuenta de correo local. Para más información vea Depuración avanzada de listas 285.

3.4.2.8 Moderación



Moderación

Esta lista es moderada por
Marque esta casilla y especifique una cuenta si desea que la lista sea moderada por un usuario designado. Las listas moderadas reenvían todos los mensajes al moderador. Solo el moderador puede enviar o reenviar mensajes a la lista.

Contraseña de la Lista
Si desea asignar una contraseña a esta lista, regístrela aquí. Las contraseñas de lista se pueden utilizar con la opción *Cualquiera que sepa la contraseña de la lista puede publicar* e ignorar la opción *Límite de Membresía* localizada en la pantalla Suscripción 289. También da acceso a un número de funcionalidades descritas en la sección *Control Remoto del Servidor vía Correo* 896.

Cualquiera que sepa la contraseña de la lista puede publicar
Si se asigna una contraseña a la lista y se habilita esta opción, cualquiera que incluya la contraseña de la lista al inicio del asunto de un mensaje puede publicar en la lista, aun si la lista está siendo moderada pero el remitente no es el moderador.

URLs de Listas de Distribución (ver RFC 2369)

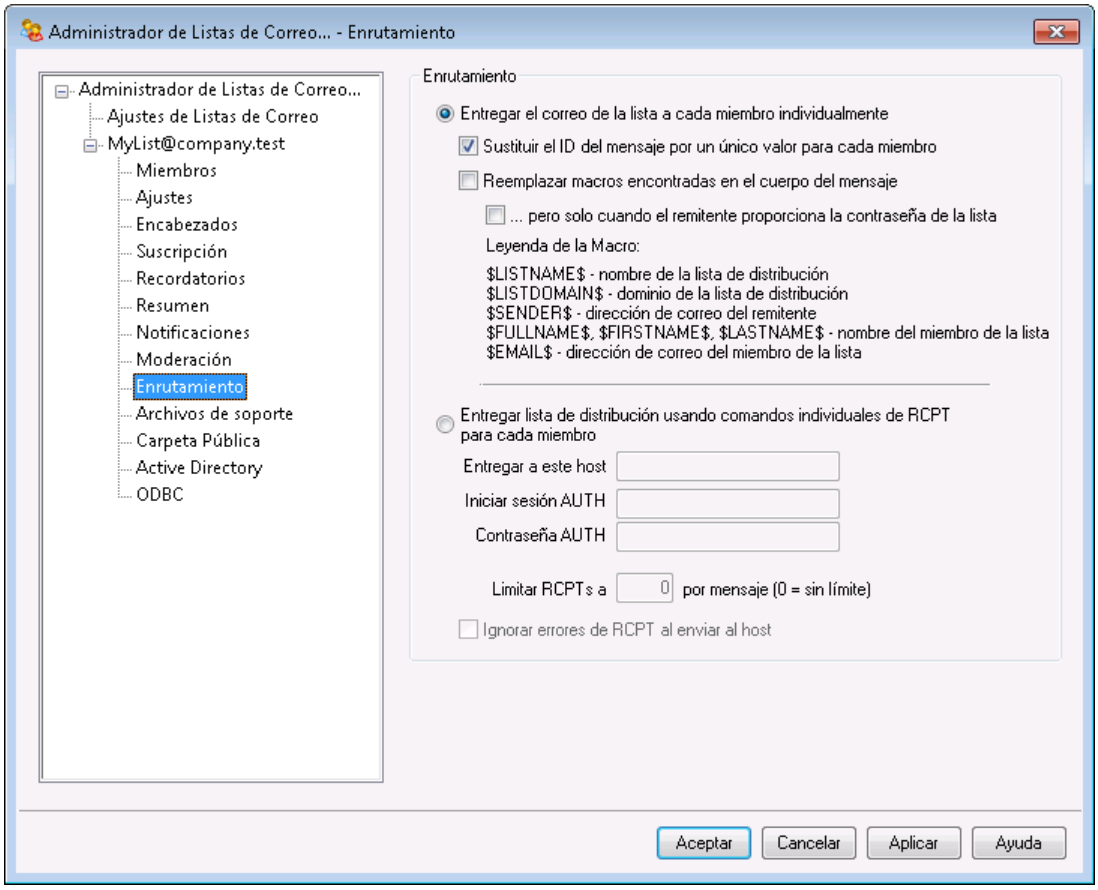
MDaemon puede agregar a los mensajes de las listas cualquiera de entre seis campos de encabezados descritos en la RFC 2369: *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. Los seis encabezados son: **List-Help**, **List-Subscribe**, **List-**

Unsubscribe, **List-Post**, **List-Owner**, y **List-Archive**. Si desea utilizar cualquiera de estos encabezados en los mensajes de la lista, registre el valor deseado en cualquiera de los campos siguientes. Los valores del encabezado deben estar formateados de acuerdo con la especificación RFC 2369 (por ejemplo, `<mailto:list@example.com?subject=help>`). Vea el documento señalado para obtener ejemplos de cada encabezado. MDaemon no modifica estos datos, por lo que si vienen formados incorrectamente no se lograrán resultados.

Descripción (utilizada en List-ID: header)
Registre aquí una descripción corta de su lisa de distribución si desea agregarla al encabezado `List-ID:` incluido en los mensajes que se envíen a la lista. La descripción y el identificador de la lista se incluirán en el encabezado (ej. `List-ID: "Lista de distribución personal de Frank" <MyList.example.com>`) Nótese que el identificador de la lista es la dirección de la lista sustituyendo "." con "@" a fin de cumplir con la Especificación de List-ID. Si deja la opción *Descripción* en blanco el encabezado List-ID contendrá solo el identificador de la lista (ej. `List-ID: <MyList.example.com>`). Si un mensaje entrante dirigido a la lista cuenta con un encabezado List-ID preexistente, MDaemon reemplazará el encabezado anterior con el encabezado correcto para la lista.

Los encabezados List-Subscribe y List-Unsubscribe se incluyen por omisión en todos los mensajes de las listas de distribución cuando se habilita la opción "*Respetar las direcciones '<List>-subscribe' y '<List>-unsubscribe'* " en la pantalla Preferencias » Misceláneos. Si desea omitir esta opción para esta lista, utilizando valores de encabezado distintos a los que agrega esa opción automáticamente, ingrese los valores deseados aquí. Si esa opción se encuentra deshabilitada entonces no se agregarán encabezados List-Subscribe y List-Unsubscribe a los mensajes de la lista a menos que se especifique un valor para ellos aquí.

3.4.2.9 Enrutamiento



Enrutamiento

Entregar el correo de la lista a cada miembro individualmente
Si se selecciona, cuando los mensajes se reciben para distribución a la lista, una copia separada de cada mensaje será creada y entregada para cada miembro de la lista. Esto resultará en numerosos mensajes individuales siendo creados, lo cual podría afectar al funcionamiento del servidor, dependiendo del tamaño de la lista y la carga en el servidor.

Sustituir el campo Message-ID por un único valor para cada miembro
Cuando MDaemon está configurado para generar una copia separada de cada mensaje para cada miembro, haga clic en esta casilla si desea que cada copia de dichos mensajes tenga un único Message-ID. Esta opción se encuentra deshabilitada por omisión y no se recomienda a menos que lo requieran circunstancias especiales.

Sustituir macros encontradas en el cuerpo del mensaje
Habilite esta opción si desea permitir el uso de macros especiales en los mensajes de las listas de distribución. Cuando se encuentra una macro, MDaemon la sustituirá con el valor correspondiente que representa la macro, para cada mensaje por separado, antes de enviarlo a cada miembro de la lista.

...pero solo cuando el remitente proporciona la contraseña de la lista
Al permitir macros en el cuerpo del mensaje, dé clic en esta opción si desear requerir la contraseña de la lista[298] a fin de que alguien utilice

macros en sus mensajes. Cuando está deshabilitada esta opción, cualquiera que puede enviar un mensaje a la lista, podrá utilizar macros.

Macros:

$LISTNAME$	El nombre de la lista, o la porción del "buzón" de la dirección de la lista (ej. "MyList2 de MyList@example.com).
$LISTDOMAIN$	El dominio de la lista (ej. "example.com" de MyList@example.com).
$SENDER$	Dirección de correo del remitente del mensaje.
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	Nombre completo, Nombre o Apellido del miembro de la lista, respectivamente (si están disponibles).
$EMAIL$	Dirección de correo del miembro de la lista.

Entregar lista de distribución usando comandos individuales de RCPT para cada miembro
Si se selecciona, MDaemon enrutará una única copia de cada mensaje de lista al host inteligente especificado, en lugar de enviar mensajes individuales a cada miembro. Este método emplee múltiples comandos `RCPT To` durante la sesión SMTP con el host especificado.

Entregar a este host
Designe el host inteligente al que desea entregar todos los mensajes de lista para envío, usando comandos RCPT To para cada miembro.

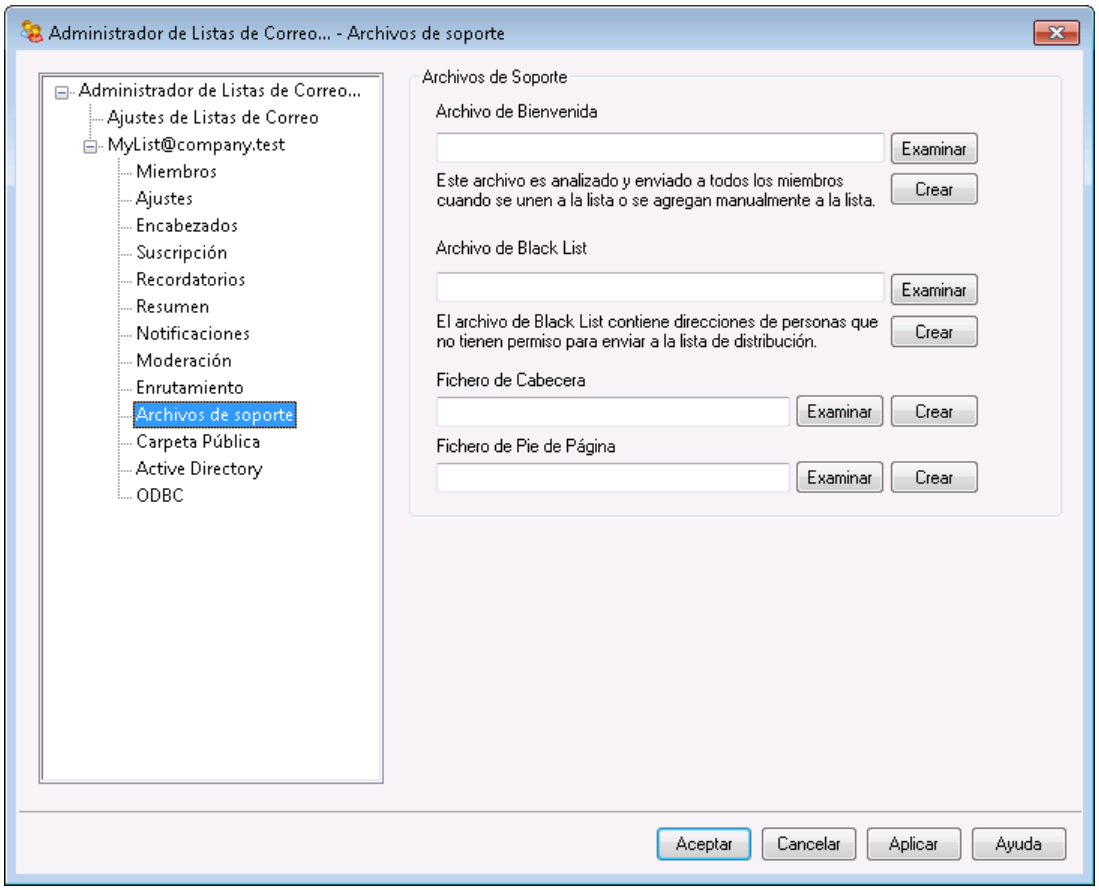
Inicio de sesión/Contraseña AUTH
Credenciales de inicio de sesión requeridas por el host.

Limitar RCPTs a [xx] por mensaje (0=sin límite)
Algunos hosts limitan el número de apariciones de `RCPT To` que aceptarán cuando intente enviar una sola copia de mensaje a través de ellos. Si especifica el límite en este control, entonces MDaemon trabajará alrededor de ello creando copias adicionales del mensaje y dividiendo la lista en grupos más pequeños. Luego remitirá el mensaje a dichos grupos evitando por lo tanto la necesidad de exceder la limitación. Esto es similar al a opción anterior de *Entregar el correo de la lista a cada miembro individualmente,* pero genera menos copias, enviando cada copia a grupos de direcciones en lugar de generar una copia separada para cada miembro.

Ignorar errores de RCPT al enviar al host
Algunos hosts inteligentes rechazarán poner en cola o procesar correo para ciertos dominios, el enrutado de listas podría causar numerosos problemas. Un

código de error devuelto del host inteligente como resultado de este rechazo podría normalmente hacer que MDaemon aborte el intento de entrega. Marque esta opción si quiere que MDaemon ignore los códigos de error devueltos del host inteligente durante el envío de correo de lista enrutado, permitiendo pues a los miembros que sean aceptados tener una oportunidad de recibir el mensaje.

3.4.2.10 Archivos de soporte



Archivos de Soporte

Archivo de Bienvenida
Si se especifican, los archivos aquí listados serán procesados y tendrán su contenido enviado a todos los nuevos miembros justo después de suscribirse. Puede usar las siguientes macros en un nuevo archivo de bienvenida:

`$PRIMARYDOMAIN$`	Esta macro expande el nombre del Dominio por Defecto de MDaemon, que se designa en el Administrador de Dominios 190.

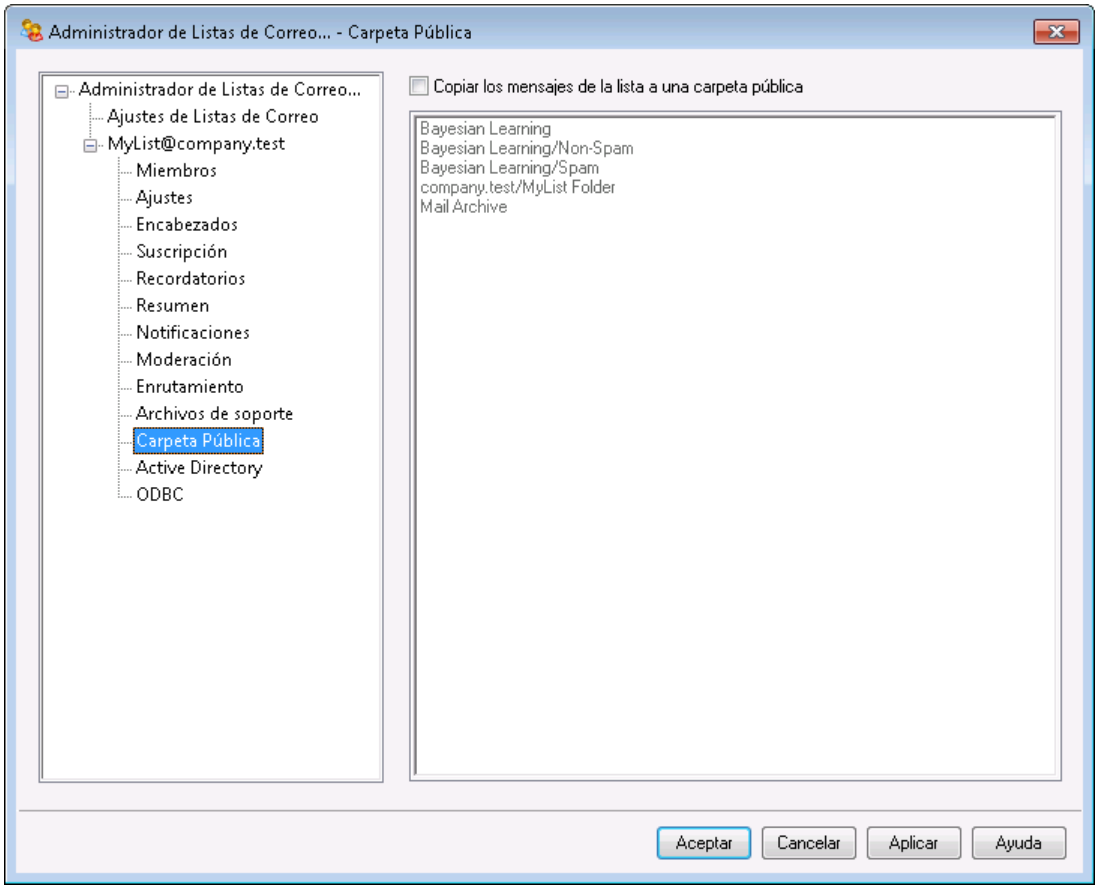
`$PRIMARYIP$`	Esta macro devolverá la dirección IPv4 asociada con el Dominio por Omisión 190 de MDaemon.
`$PRIMARYIP6$`	Esta macro devolverá la dirección IPv6 asociada con el Dominio por Omisión 190 de MDaemon.
`$DOMAINIP$`	Esta macro devolverá la dirección IPv4 asociada con el dominio.
`$DOMAINIP6$`	Esta macro devolverá la dirección IPv6 asociada con el dominio.
`$MACHINENAME$`	Esta macro devolverá el contenido de la opción FQDN definida en la pantalla Dominio.
`$LISTEMAIL$`	Muestra la dirección de correo de la lista. Ejemplo: `MiLista@ejemplo.com`
`$LISTNAME$`	Muestra el nombre de la lista de correo. Ejemplo: `MiLista`
`$LISTDOMAIN$`	Esta macro devuelve el dominio de la lista de correo. Ejemplo: `ejemplo.com`
`%SETSUBJECT%`	Use esta macro para designar un asunto alternativo para el Mensaje de bienvenida. El texto de asunto designado puede incluir otras macros de lista tal como `$LISTEMAIL$`. Ejemplo: `%SetSubject%=Bienvenido a la lista $LISTNAME$.`

Archivo de Lista de Bloqueados
Si se especifica, el archivo aquí listado será usado para suprimir mensajes enviados de usuarios especificados.

Archivo de Cabecera/Pie de página
Los contenidos de los archivos aquí especificados se usarán como los archivos de cabecera y/o pie de los mensajes de lista.

Crear
Para crear un nuevo archivo, haga clic en el botón *Crear* que corresponde al archivo que desea crear, especifique un nombre, y luego haga clic en *Abrir*. Esto abrirá el nuevo archivo creado en Bloc de Notas para su edición.

3.4.2.11 Carpeta Pública

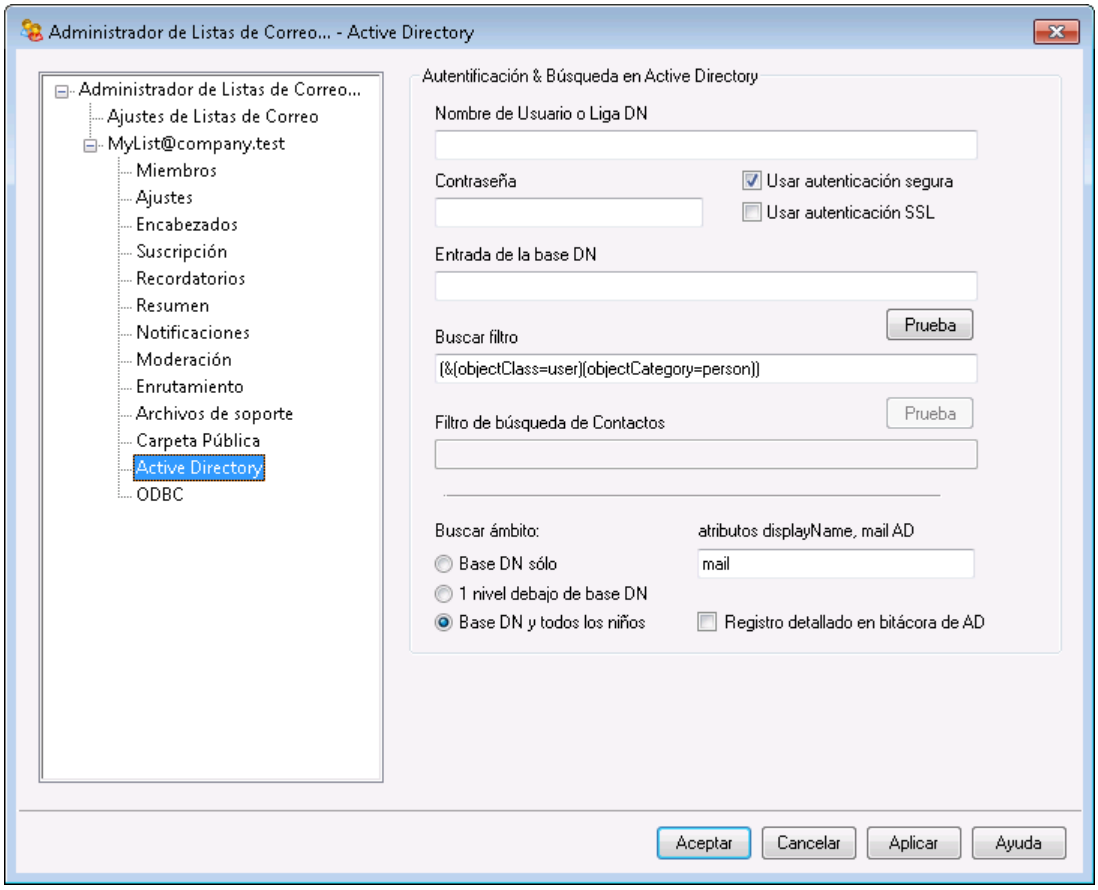


MDaemon soporta el uso de Carpetas Públicas IMAP con las listas de distribución. A diferencia de las carpetas personales IMAP, que son típicamente sólo accesibles por un sólo usuario, las Carpetas Públicas son carpetas extra que están disponibles a múltiples usuarios IMAP. Las opciones en esta pantalla se usan para hacer que todos los mensajes destinados a la Lista de Correo sean automáticamente copiados a una de sus carpetas públicas.

Copiar los mensajes de la lista a una carpeta pública
Habilite este control si desea que estos mensajes de la lista sean copiados a una de sus Carpetas Públicas además de ser enviados a la lista.

Seleccionar una carpeta pública
Haga clic en la Carpeta Pública con la que desea asociar los mensajes de la lista.

3.4.2.12 Active Directory



Utilice las opciones en esta pantalla si desea obtener de Active Directory las direcciones de correo de algunos de los miembros de la lista.

Autentificación & Búsqueda con Active Directory

Nombre de usuario o Enlace DN
Este es el inicio de sesión de Windows o DN que MDaemon utilizará para conectarse a Active Directory utilizando LDAP. El Active Directory permite el uso de una cuenta de Windows o UPN para hacer la conexión.

Si se utiliza un DN en esta opción en lugar de una cuenta de Windows, debe deshabilitar/dejar en blanco la opción siguiente "*Utilizar autentificación segura*".

Contraseña
Esta es la contraseña que corresponde al DN o a la cuenta de Windows utilizada en la opción *Enlazar DN* definida arriba.

Usar autentificación segura
De clic en esta casilla si desea utilizar autentificación segura al ejecutar sus consultas al Active Directory. No puede utilizar esta opción cuando está utilizando un DN en lugar de una cuenta de Windows en la opción *Enlazar DN* definida arriba.

Utilizar autentificación SSL
Dé clic en esta casilla si desea utilizar autentificación SSL al ejecutar búsquedas en el Active Directory.

Para usar esta opción se requiere un servidor SSL e infraestructura en su red de Windows y Active Directory. Contacte a su departamento de Sistemas si no está seguro de que su red está configurada de esta forma e investigue si puede habilitar esta opción.

Atributo Dirección de Correo
Debe utilizar este campo para especificar el atributo que contendrá las direcciones de correo utilizadas por la lista. Por ejemplo, si utiliza "`Mail`" en este campo, entonces cada cuenta del Active Directory que desee sea tratada como miembro de la lista deberá contar con el atributo "`Mail`" y ese atributo debe contener una dirección de correo electrónico.

Búsqueda en Active Directory

Registro DN Base
Especifique el Nombre Distinguido (Distinguished Name - DN) o punto de entrada en el Árbol del Directorio de Información (Directory Information Tree - DIT) en el que MDaemon realizará de las direcciones de correo en Active Directory. Puede utilizar "`LDAP://rootDSE`" en esta opción para empezar la búsqueda en Root DSE, que es el registro más alto en la jerarquía de Active Directory. Al definir un punto de inicio más preciso y cercano a la ubicación de sus cuentas de usuario o grupo deseado de direcciones en su árbol particular de Active Directory, puede reducir la cantidad de tiempo requerida para ejecutar las búsquedas en el DIT. Deje este campo en blanco si no desea extraer ningunas direcciones para la lista, de Active Directory.

Filtro de Búsqueda
Este es el filtro de búsqueda LDAP que será utilizado al realizar búsquedas en Active Directory. Utilice este filtro para habilitar MDaemon para localizar más precisamente las cuentas de usuario deseadas o las direcciones que desea considerar como miembros de la lista.

Prueba
Utilice este botón para probar los ajustes de su filtro de búsqueda.

Atributos AD displayName y mail
Debe utilizar este campo para especificar el atributo que contendrá las direcciones de correo utilizadas por la lista. Por ejemplo, si utiliza "`Mail`" en este campo, entonces cada cuenta de Active Directory que desea sea tratada como miembro de la lista, debe tener un atributo "`Mail`" y ese atributo debe contener una dirección de correo. Adicionalmente puede registrar un atributo de Active Directory para el campo nombre completo de los miembros de la lista antes del atributo dirección de correo, separados por una coma. Por ejemplo, puede registrar: "`displayName, mail`" en lugar de solo "`mail`" en esta opción. El primero es el atributo donde reside el nombre completo en Active Directory y el segundo es el atributo que contiene la cuenta de correo.

Ámbito de búsqueda:

Este es el alcance o extensión de sus búsquedas en Active Directory.

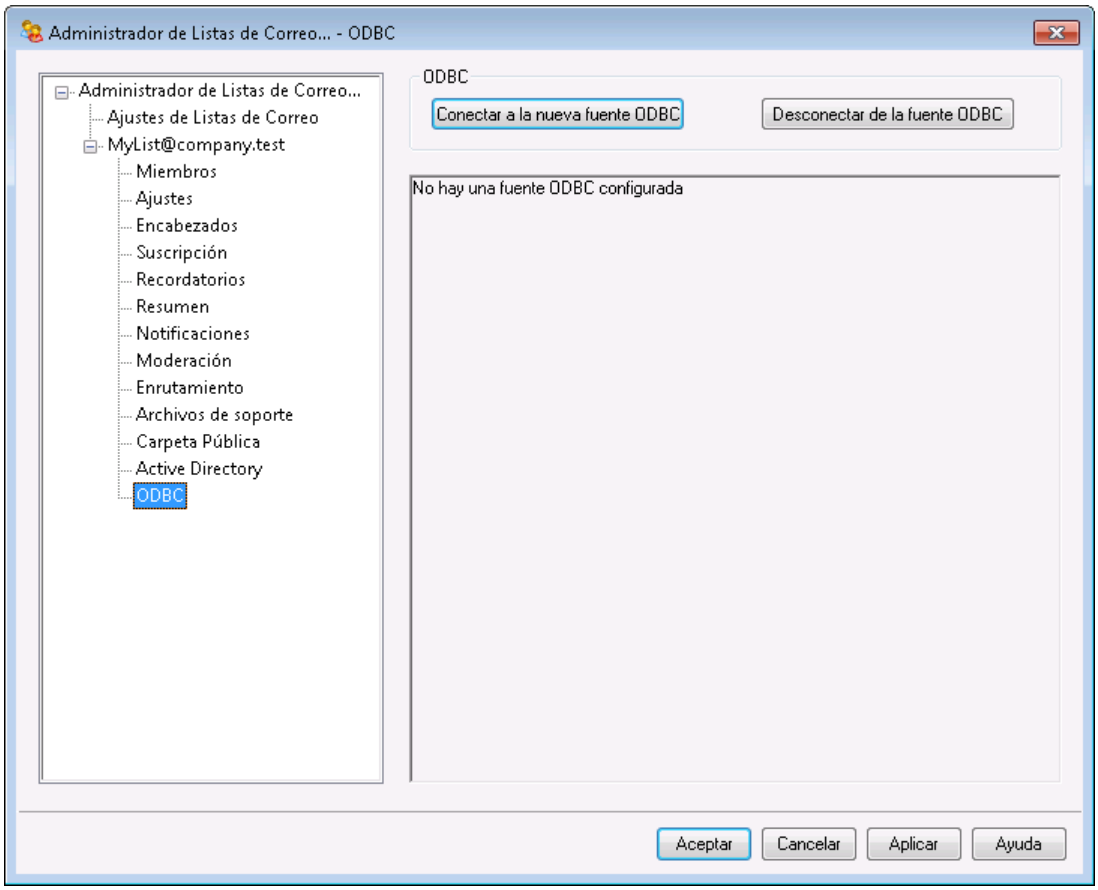
Solo Base DN
Seleccione esta opción si desea limitar su búsqueda solo al DN base especificado arriba. La búsqueda no procederá bajo ese punto en su árbol (DIT).

1 nivel abajo del DN base
Utilice esta opción si desea ampliar su búsqueda en Active Directory un nivel abajo del DN definido en su DIT.

Base DN y todos los hijos
Esta opción extenderá el ámbito de su búsqueda del DN definido a todos sus hijos, hasta el último nivel hijo en su DIT.

Registro detallado en el Log de AD
Por omisión MDaemon utilizará el registro detallado para Active Directory. Deshabilite esta casilla si desea utilizar un registro menos extenso.

3.4.2.13 ODBC



Usando esta funcionalidad puede mantener la lista de miembros en una base de datos ODBC. La pantalla ODBC del editor de Lista de Correo se usa para seleccionar la fuente de datos, tabla, y la asignación de campos para que MDaemon los enlace a la lista. Cuando llegan menajes a la lista uno o más consultas SQL se ejecutarán

automáticamente y la dirección de correo resultante será tratada como parte de los miembros de la lista.

Puede añadir, quitar, y modificar miembros de su lista en la base de datos usando una aplicación compatible con pase de datos ODBC.

ODBC

Esta sección muestra las propiedades ODBC concurrentes que haya establecido para la lista de correo. Muestra las asignaciones de los campos de la base de datos y las consultas SQL que haya configurado para designar el estatus de cada uno de los miembros (Normal, Sólo Publicación, Sólo Lectura, y/o modo Resumen).

Conectar a la nueva fuente ODBC
Haga clic en este botón para abrir el Asistente de Selector ODBC para escoger la fuente de datos de sistema que desea usar para la lista de correo.

Desconectar de la fuente ODBC
Haga clic en este botón para desconectar de la lista de la fuente de datos ODBC listada en el espacio anterior.

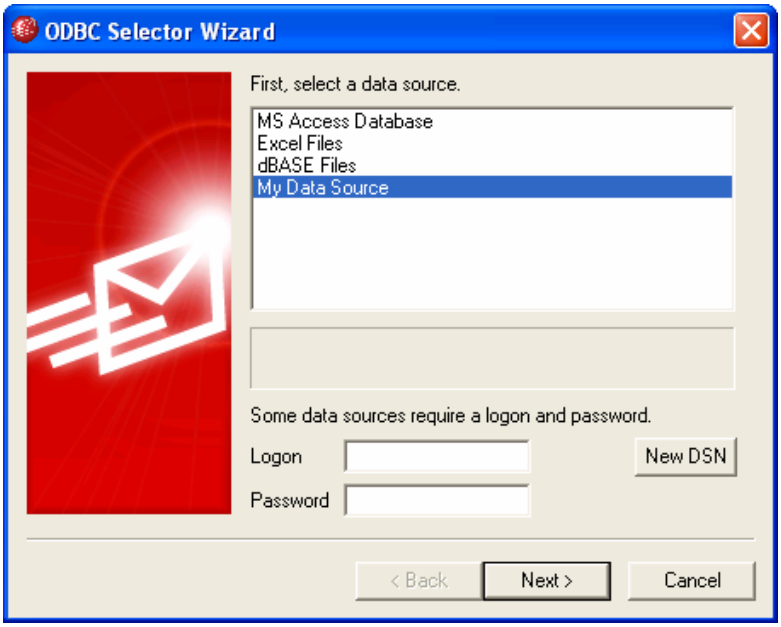
Ver:

Configurar una Fuente de Datos de Sistema ODBC para una Lista de Correo 308
Crear una nueva Fuente de Datos de Sistema 311

3.4.2.13.1 Configurar una Fuente de Datos de Sistema ODBC para una Lista de Correo

Para usar una base de datos accesible ODBC con una lista de correo:

1. En la Pantalla ODBC 307 del Editor de Listas de Distribución, haga clic en **Conectar a la nueva fuente ODBC** para abrir el Asistente de Selector ODBC.

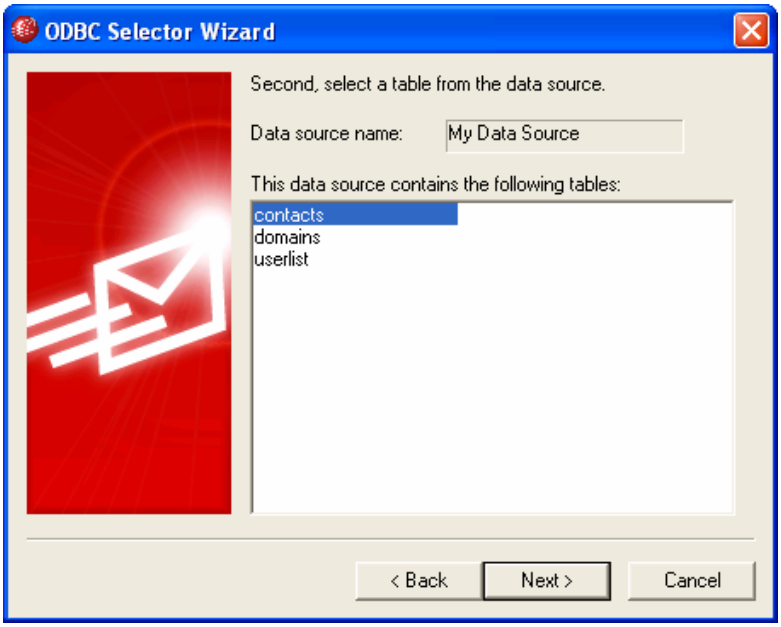


2. Seleccione la **fuente de datos** que desea usar para la lista. Si no existe una fuente de datos compatible listada, haga clic en **Nuevo DSN** y luego siga las instrucciones listadas bajo, **Crear una nueva fuente de datos ODBC** 311.

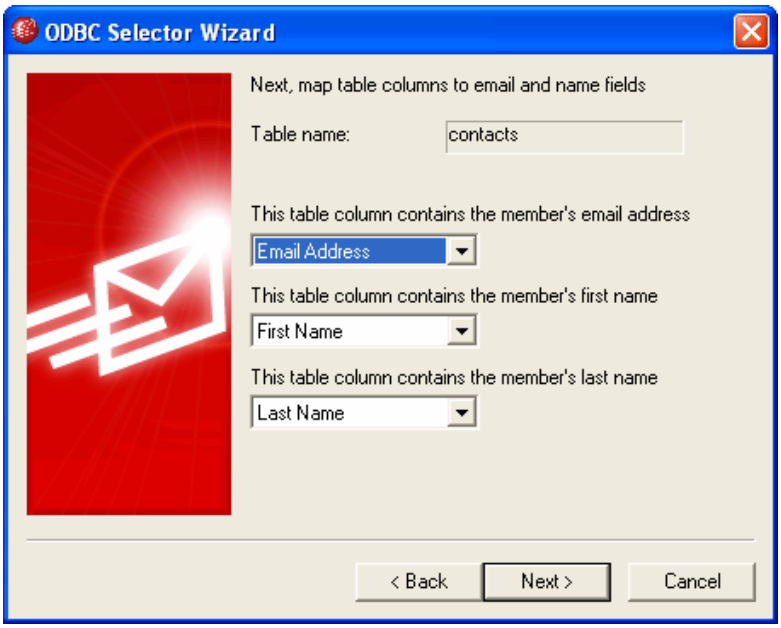
3. Si se requiere, introduzca **Registrarse** y **Contraseña**.

4. Haga clic en **Siguiente**.

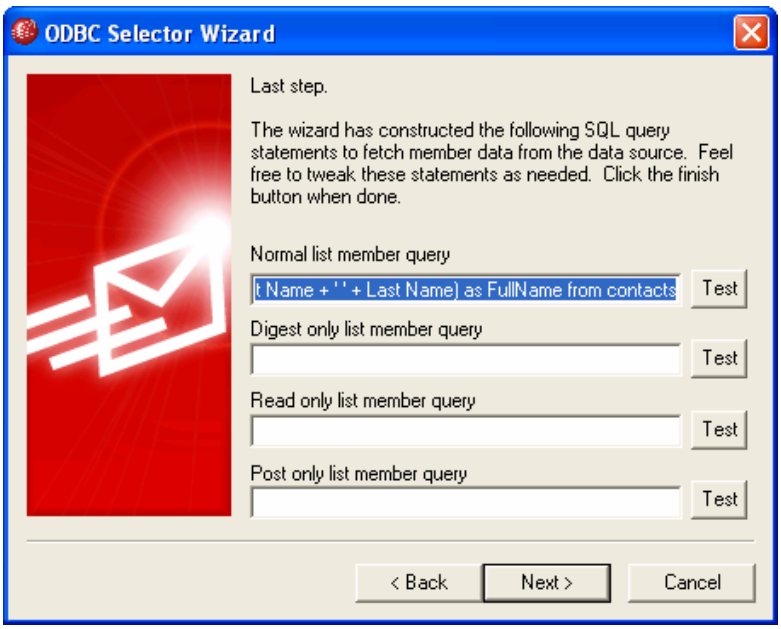
5. La fuente de datos debe contener al menos una tabla con campos para las direcciones de correo y los nombres. Si la fuente de datos contiene una o más de una de tablas compatibles, escoja la tabla deseada y haga clic en **Siguiente**. Si no, haga clic en **Cancelar** para salir del Asistente de Selector de ODBC y use su aplicación de base de datos para añadir una tabla a la base de datos relevante antes de continuar.



6. Use los cuadros de lista para designar los campos de la tabla que se corresponden a **dirección de correo**, **nombre**, y **apellido**. Haga clic en **Siguiente**.



7. El selector de ODBC construirá una sentencia de consulta SQL basada en las selecciones del **Paso 6**. MDaemon lo usará para recopilar los datos de los miembros de la lista de la base de datos. Puede editar esta sentencia según lo desee, e incluir otras sentencias de consulta en los controles restantes para hacer que los miembros reciban los mensajes en modo Resumen, y para designar miembros como Sólo Lectura o Sólo Publicación. Un botón de **Prueba** se ofrece al lado de cada control para que pueda probar las sentencias de consulta para asegurarse que puede recopilar los datos correctos. Cuando haya finalizado de configurar sus sentencias de consulta, haga clic en **Siguiente**.



8. Haga clic en **Finalizar.**

Ver:

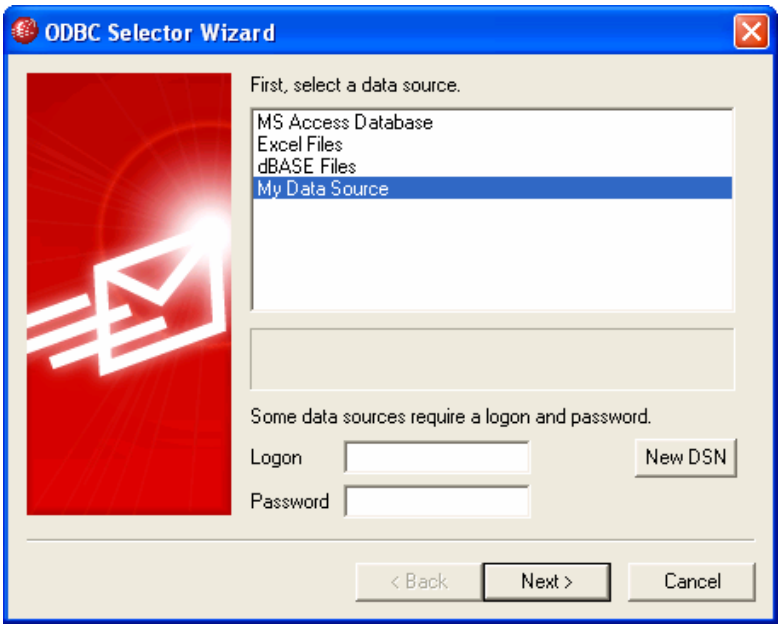
[Editor de Lista de Correo » ODBC 307]
[Crear una Nueva Fuente de Datos ODBC 311]

3.4.2.13.2 Crear una nueva Fuente de Datos de Sistema

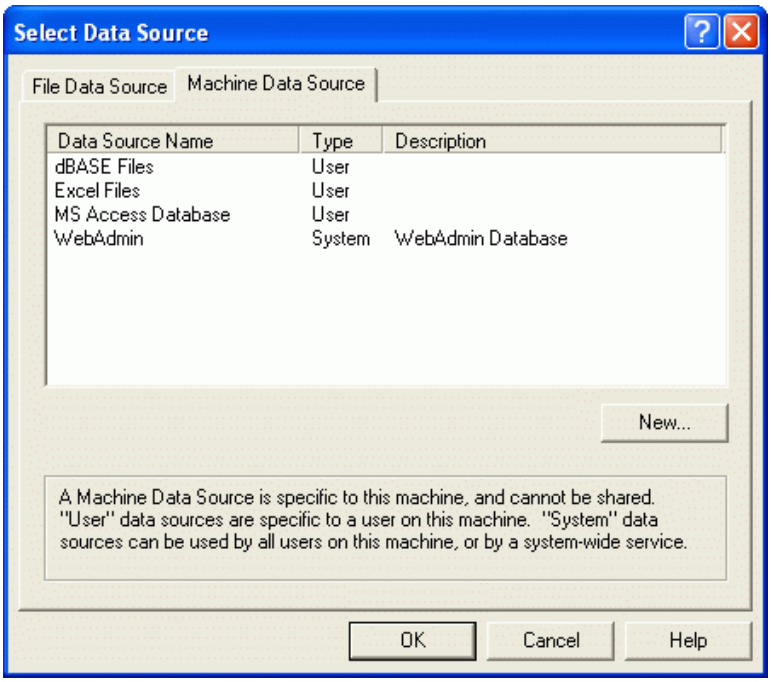
Para crear una nueva fuente de datos ODBC para usar con una lista de correo:

1. En la Pantalla ODBC 307 del Editor de Lista de Correo, haga clic en **Conectar a nueva fuente ODBC** para abrir el Asistente de Selector ODBC.

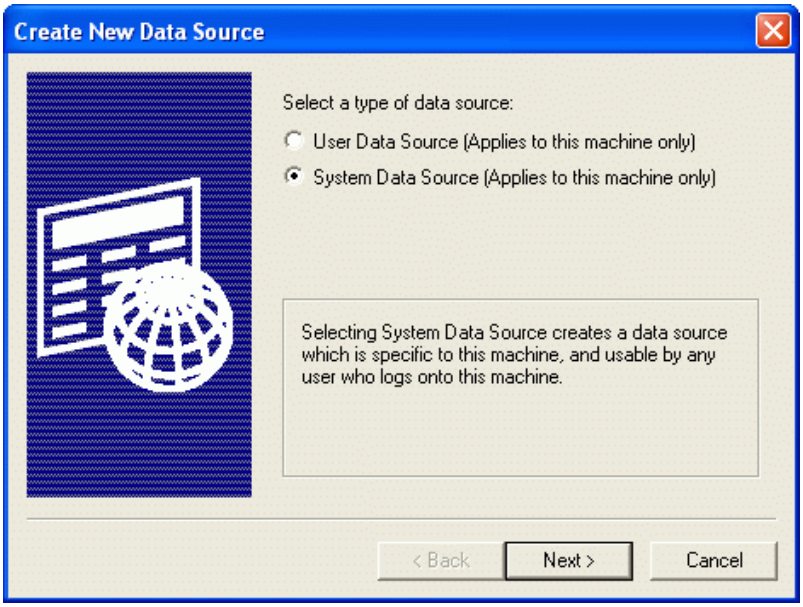
2. Haga clic en **Nuevo DSN** para abrir el diálogo de Seleccionar Fuente de Datos.



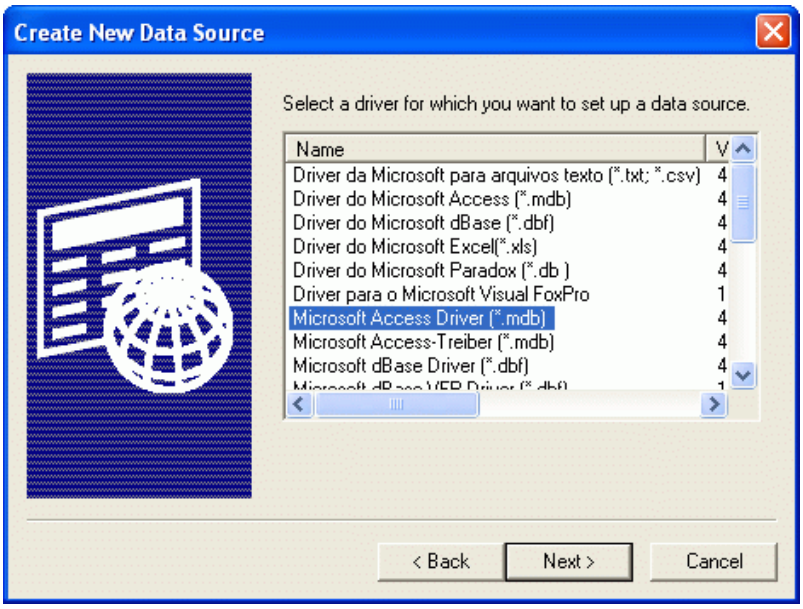
3. Cambie a la pestaña **Fuente de Datos de Máquina**, y haga clic en **Nuevo...** para abrir el diálogo de Crear Nueva Fuente de Datos.



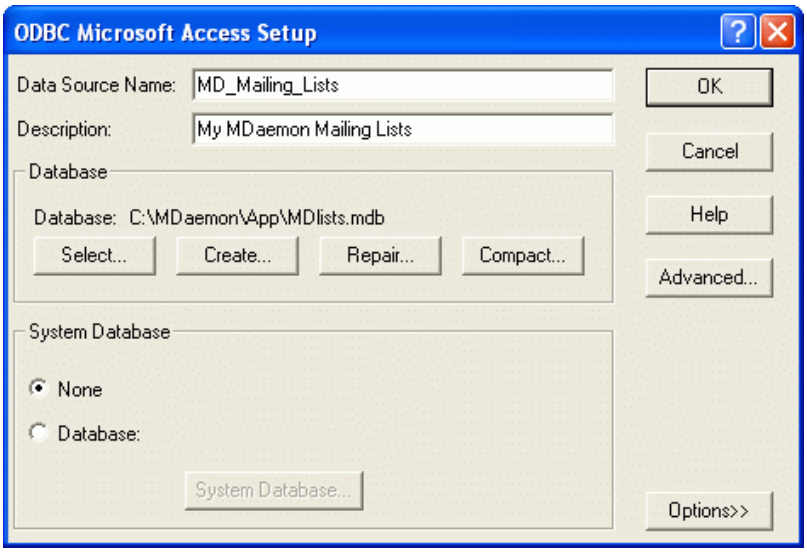
4. Seleccione **Fuente de Datos de Sistema**, y luego haga clic en **Siguiente**.



5. Seleccione el **driver de base de datos** para el que desea configurar la fuente de datos y luego haga clic en **Siguiente**.



6. Haga clic en **Finalizar** para mostrar el diálogo de configuración específico de driver. La apariencia de este diálogo estará basada en el driver seleccionado (diálogo Microsoft Access Setup mostrado abajo).



7. Designe un **Nombre de Fuente de Datos** para su nueva fuente de datos y provea cualquier otra información requerida por el diálogo específico del driver (tal como crear o especificar una base de datos, escoger un directorio o servidor, y demás).

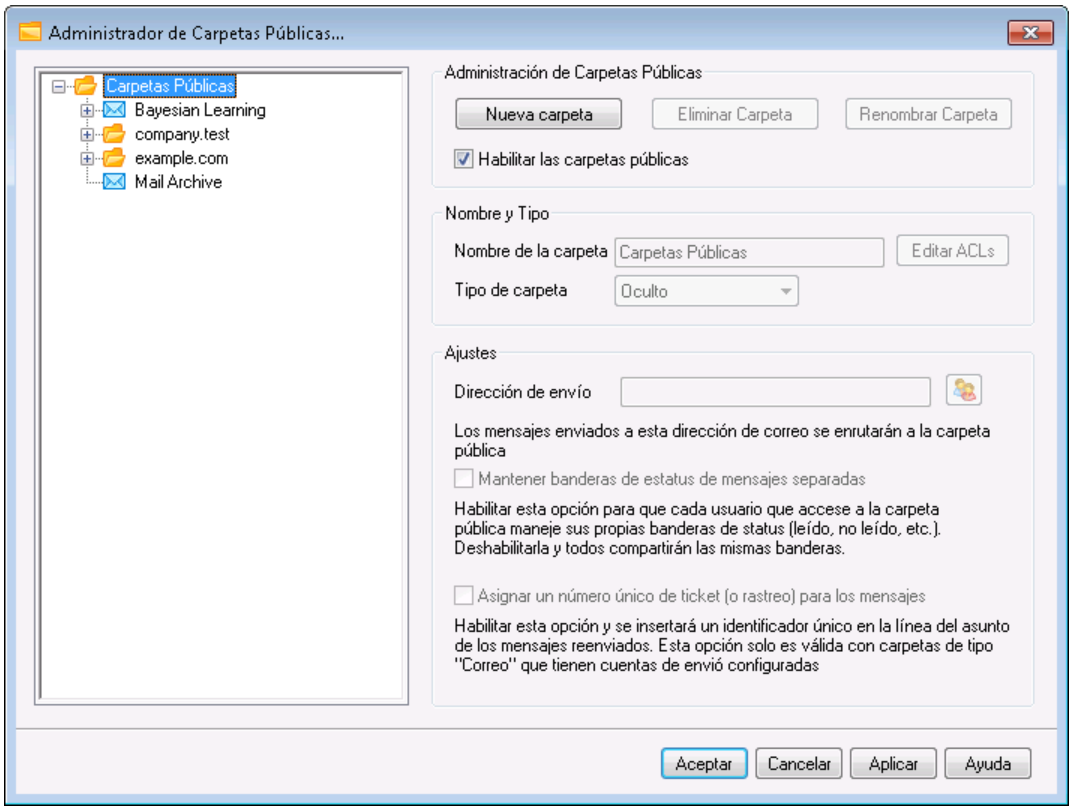
8. Haga clic en **Aceptar** para cerrar el diálogo específico del driver.

9. Haga clic en **Aceptar** para cerrar el diálogo de Seleccionar Fuente de Datos.

Ver:

[ODBC - Listas de Distribución](#) 307
[Configurar un Sistema de Fuente de Datos ODBC para Lista de Correo](#) 308

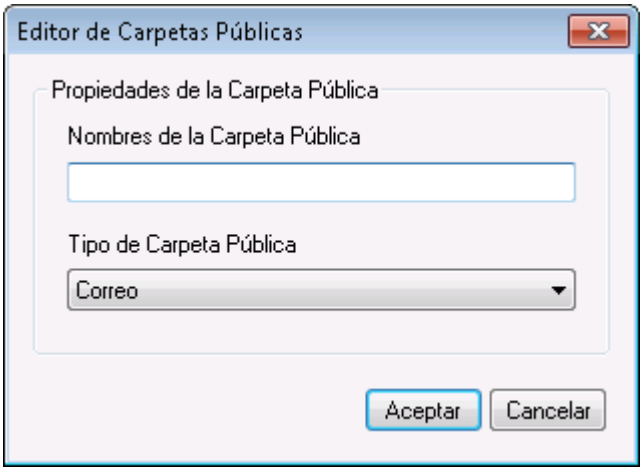
3.5 Administrador de Carpetas Públicas



Utilice esta pantalla para administrar sus carpetas públicas 125. Para ingresar a la Administración de Carpetas Públicas dé clic en "Configuración » Administrador de Carpetas Públicas...".

Administración de Carpetas Públicas

Carpeta Nueva
Para crear una carpeta pública nueva, seleccione en la lista la carpeta que la contendrá y dé clic en *Carpeta Nueva*. Registre el nombre de la carpeta nueva, seleccione el tipo de carpeta y dé clic en *OK*.



Eliminar carpeta
Para eliminar de la lista una carpeta pública, seleccione la carpeta deseada y dé clic en el botón *Eliminar carpeta*.

Renombrar carpeta
Para renombrar una carpeta pública, selecciónela y dé clic en *Renombrar carpeta*. Teclee un nombre nuevo y dé clic en *OK*.

Habilitar Carpetas Públicas
Dé clic en esta casilla si desea permitir a los usuarios tener acceso a las carpetas públicas. Qué usuarios tendrán acceso y el de acceso a las carpetas se controla seleccionando cada carpeta y dando clic en el botón *Editar ACLs*.

Nombre y Tipo

Nombre de Carpeta
Esta caja despliega el nombre de la carpeta que ha seleccionado en la lista. Las opciones siguientes en esta pantalla se aplican a la carpeta seleccionada.

Tipo de Carpeta
Utilice la lista desplegable para definir el tipo de carpeta: Correo, Contactos, Calendario, etc.

Editar ACLs
Seleccione una carpeta y luego dé clic en este botón para abrir el diálogo de la Lista de Control de Acceso 316 para esa carpeta. Utilice la Lista de Control de Acceso para designar los usuarios o grupos que podrán tener acceso a la carpeta y los permisos para cada usuario o grupo.

Ajustes

Dirección de Envío
Registre una dirección de correo local o elija una cuenta específica de MDaemon para asociarla con la carpeta compartida, de manera que los mensajes destinados a esa *Dirección de Envío* sean enrutados automáticamente a la carpeta compartida. Sin embargo, solo los usuarios a los que se les ha otorgado permisos de "publicar" en la carpeta podrán enviar a esa dirección.

Mantener banderas de estatus separadas por mensaje
Dé clic en esta caja si desea que las banderas de los mensajes en la carpeta (leído, no leído, reenviado y demás) se definan por usuario en lugar de globalmente. Cada usuario verá el estatus de los mensajes en la carpeta compartida desplegados de acuerdo con su interacción personal con ellos. El usuario que no haya leído un mensaje lo verá marcado como "no leído" mientras que el usuario que lo haya leído verá el estatus de 'leído'. Si esta opción se deshabilita, entonces todos los usuarios verán el mismo estatus. Así, una ver que cualquier usuario haya leído un mensaje, todos los usuarios lo verán marcado como 'leído'.

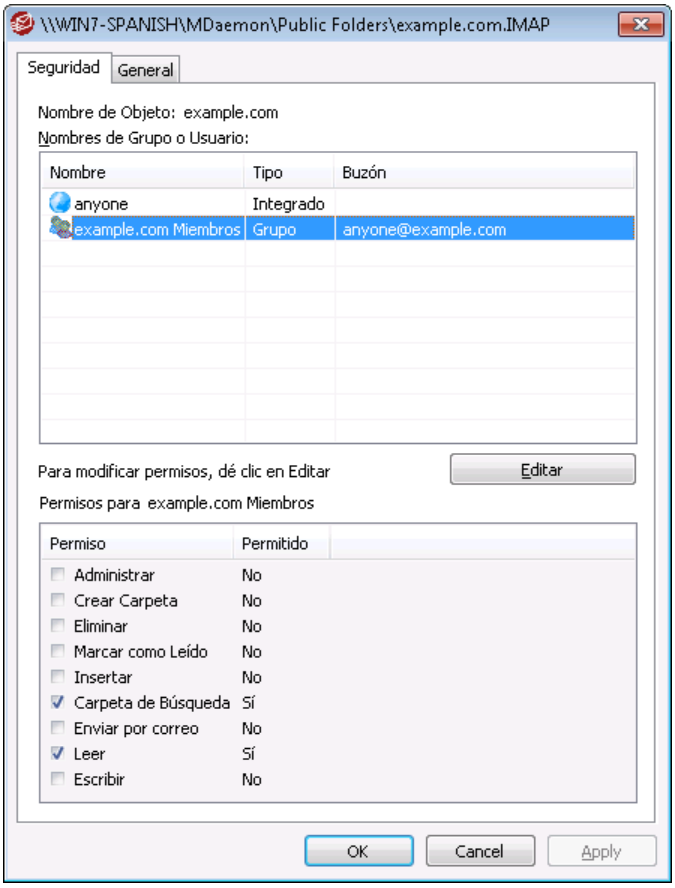
Asignar un número único de ticket (o rastreo) a los mensajes
Utilice esta opción si desea configurar la carpeta pública como carpeta pública de tickets de mensajes. MDaemon agregará el *Nombre de la carpeta* y un identificador único al asunto de los mensajes enviados a la *Dirección de envío* de la carpeta pública. A cualquier mensaje saliente que tenga el asunto con este formateo especial, se le cambiará la dirección 'De' a la Dirección de envío de la carpeta pública y se colocará una copia del mensaje saliente en una subcarpeta pública llamada "Respondido a". Adicionalmente, cualquier mensaje entrante que tenga el asunto formateado de esta manera se redirigirá automáticamente a la carpeta pública, sin importar la dirección de la que provenga el mensaje.

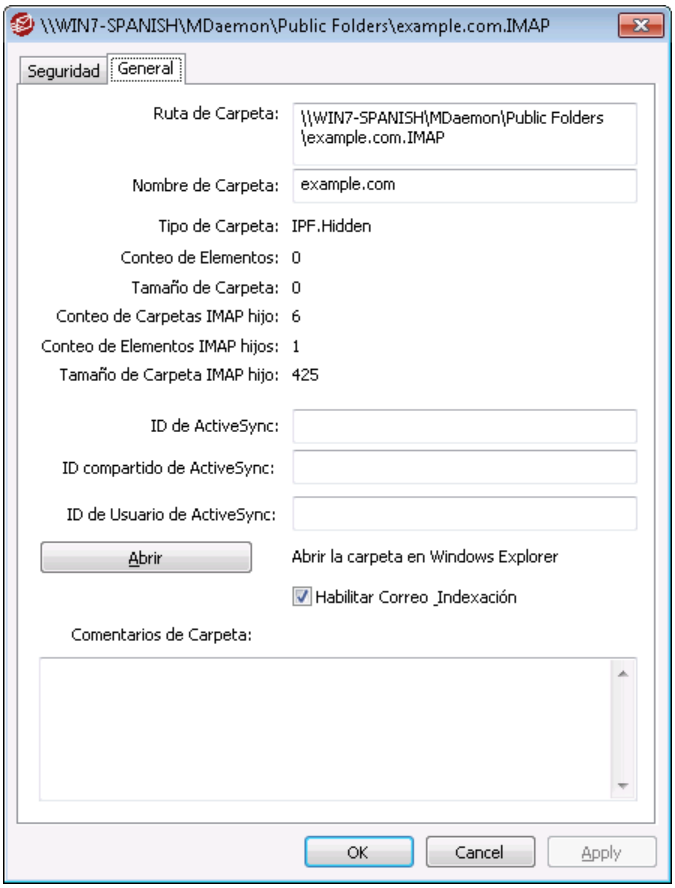
Ver:

Lista de Control de Acceso 316
Descripción de Carpetas Públicas 125
Carpetas Públicas y Compartidas 128
Editor de Cuentas » Carpetas Compartidas 743
Listas de Distribución » Carpetas Públicas 304

3.5.1 Lista de Control de Acceso

La Lista de Control de Acceso (Access Control List - ACL) se utiliza para asignar permisos de acceso a usuarios o grupos para sus carpetas públicas y compartidas 125. Se ingresa a través del botón *Editar ACLs* en el Administrador de Carpetas Públicas 314 o con el botón *Editar lista de control de acceso* en la pantalla Carpetas Compartidas 743 del Editor de Cuentas.





Seguridad

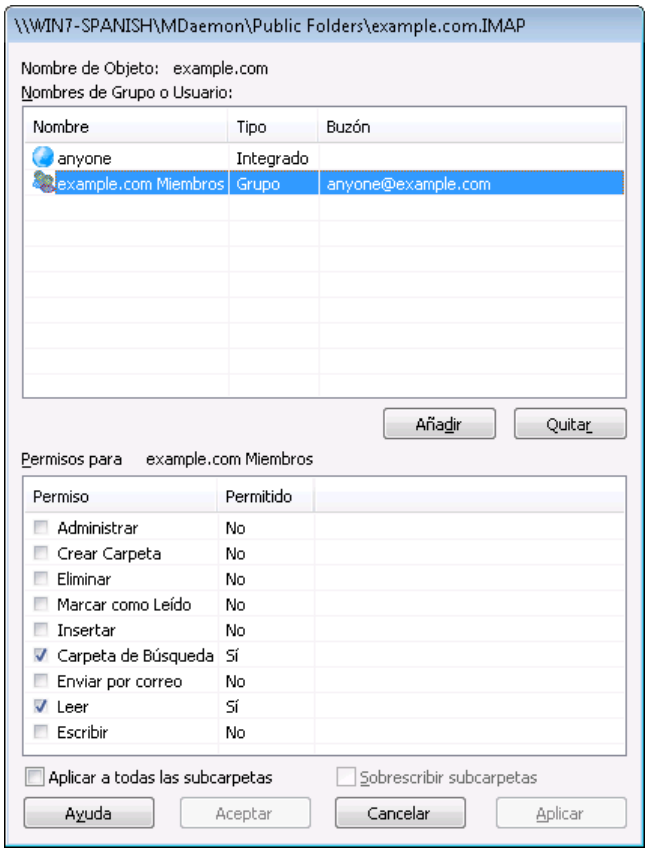
Esta pestaña despliega la lista de grupos o usuarios asociados con la carpeta y los permisos de acceso específicos otorgados a cada uno. Seleccione un grupo o usuario en la lista para desplegar sus permisos 319 y revisarlos en la ventana de Permisos abajo. Para editar los permisos, dé clic en **Editar** 318.

General

Esta pestaña despliega las propiedades de la carpeta, tales como su ruta, nombre, tipo, tamaño y demás.

Editor de ACLs

De clic en **Editar** en la pestaña Seguridad de los ACLs para abrir el Editor de ACLs para modificar los permisos de acceso.



Nombre del Objeto
Este es el nombre del objeto o carpeta al que se aplicará los permisos ACL.

Grupo o nombres de usuarios
Estos son los grupos o usuarios para los que se pueden haber otorgado algún nivel de permisos de acceso. Seleccione un grupo o usuario para desplegar sus permisos en la ventaja abajo *Permisos para <grupo o usuario>*. Marque la casilla siguiente para seleccionar cualquier permiso de acceso que desee otorgar al grupo o usuario.

Agregar
Par otorgar permisos de acceso a un grupo o usuario que no aparezca en la lista arriba, dé clic en **Agregar**[320].

Remover
Para remover un grupo o usuario, seleccione su entrada en la lista arriba y dé clic en **Remover**.

Permisos para <grupo o usuario>
Marque la casilla siguiente para cualquier permiso de acceso que desee otorgar al grupo o usuario seleccionado arriba.

Puede otorgar los siguientes permisos de control de acceso:

Administrar – el usuario puede administrar los ACL para esta carpeta.

Crear – el usuario puede crear subcarpetas dentro de esta carpeta.

Eliminar – el usuario puede eliminar elementos de esta carpeta.

Marcar Leído – el usuario puede modificar el estatus leído/no leído de los mensajes en esta carpeta.

Insertar – el usuario puede agregar y copiar elementos a esta carpeta.

Carpeta de Búsqueda – el usuario puede ver esta carpeta en su lista personal de carpetas IMAP.

Postear – el usuario puede enviar correo directamente a esta carpeta (si la carpeta lo permite).

Leer – el usuario puede abrir esta carpeta y visualizar sus contenidos.

Escribir – el usuario puede modificar las banderas de los mensajes en esta carpeta.

Aplicar a todas las carpetas hijo
Marque esta casilla si desea aplicar los permisos de control de acceso de esta carpeta a cualquier subcarpeta que contenga. Agregará los permisos de usuario y de grupo a las carpetas hijo, reemplazando donde exista conflicto. Sin embargo, no eliminará los permisos de cualquier otro usuario o grupo que en ese momento tenga acceso a esas carpetas.

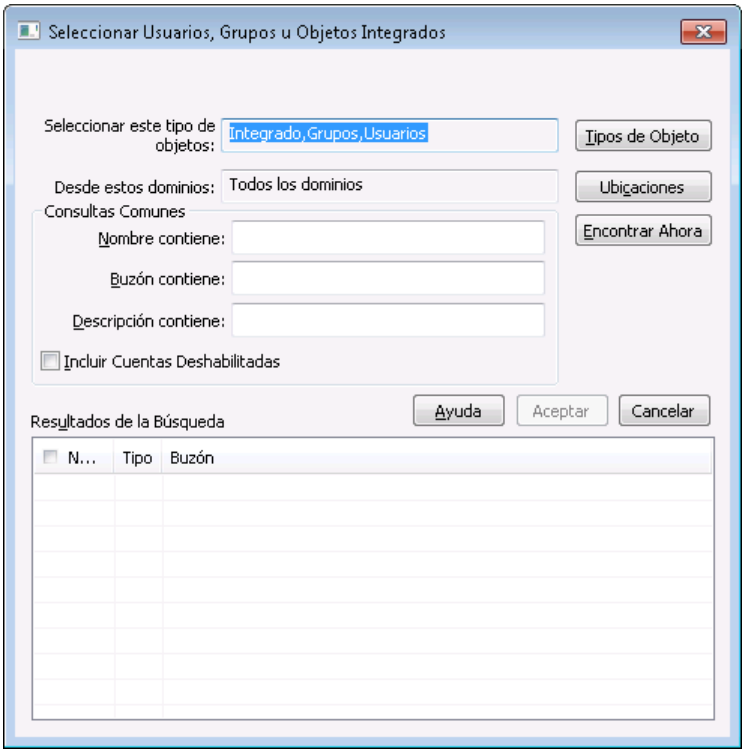
Ejemplo,

La carpeta padre otorga ciertos permisos a `Usuario_A` y `Usuario_B`. La carpeta hijo otorga permisos a `Usuario_B` y `Usuario_C`. Esta opción agregará los permisos de `Usuario_A` a la carpeta hijo, reemplazará los permisos en la carpeta hijo del `Usuario B` con los de la carpeta padre y no hará nada con los permisos del `Usuario C`. Por consiguiente, la carpeta hijo tendrá entonces permisos para `Usuario A`, `Usuario_B` y `Usuario C`.

Sobrescribir carpetas hijo
Marque esta casilla si desea reemplazar todos los permisos de acceso de las carpetas hijo con los permisos actuales de la carpeta padre. Los permisos de las carpetas hijo serán entonces idénticos a los de la carpeta padre.

Agregar un Grupo o Usuario

Dé clic en **Agregar** en el Editor ACL si desea agregar otro grupo o usuario a la Lista de Control de Acceso. Esto abre la pantalla Agregar Grupo o Usuario que puede utilizar para buscarlos y agregarlos.



Seleccionar esos tipos de objeto
Dé clic en **Tipos de Objeto...** para seleccionar los tipos de objeto que desea buscar para los grupos o usuarios que desea agregar. Puede seleccionar: Predeterminados, Grupos y Usuarios.

De estas ubicaciones
Dé clic en **Ubicaciones...** para seleccionar los dominios en los que desea buscar. Puede seleccionar todos sus dominios de MDaemon o algún dominio en específico.

Consultas Comunes
Utilice las opciones en esta sección para reducir su búsqueda especificando toda o una parte del nombre de usuario, dirección de correo o los contenidos de la Descripción 715 de la cuenta. Deje estos campos en blanco si desea que los resultados de la búsqueda contengan todo grupo y usuario que coincida con los Tipos de Objeto y Ubicaciones especificados arriba.

Incluir Cuentas Deshabilitadas
Marque esta casilla si desea incluir cuentas deshabilitadas 715 en su búsqueda.

Encontrar Ahora
Luego de que haya especificado todos los criterios de búsqueda, dé clic en **Encontrar Ahora** para ejecutar la consulta.

Resultados de la Consulta
Luego de ejecutar la búsqueda, seleccione cualquiera de los grupos o usuarios deseados en los Resultados de la Consulta y dé clic en **OK** para agregarlos al ACL.

Los Permisos de Acceso se controlan a través del soporte de MDaemon para Listas de Control de Acceso (Access Control Lists - ACL). ACL es una extensión de Internet Message Access Protocol (IMAP4), que le permite crear una lista de acceso para cada una de sus carpetas IMAP de mensajes, otorgando permisos de acceso por carpeta a otros usuarios que también tengan cuentas en su servidor de correo. Si su cliente de correo no soporta ACL aún puede establecer los permisos vía los controles de este diálogo.

ACL se discute completamente en la RFC 2086, que se puede encontrar en: http://www.rfc-editor.org/rfc/rfc2086.txt.

Ver:

Administrador de Carpetas Públicas 314
Descripción General de Carpetas Públicas 125
Carpetas Públicas & Compartidas 128
Editor de Cuentas » Carpetas Compartidas 743
Listas de Distribución » Carpetas Públicas 304

3.6 Web & Servicios IM

3.6.1 Webmail

3.6.1.1 Descripción General

MDaemon Webmail es una solución de correo basada en web que se incluye en MDaemon y que está diseñada para ofrecer funcionalidades de cliente de correo utilizando su navegador web favorito. Webmail se equipara fácilmente con clientes de correo tradicionales proporcionando la ventaja adicional de permitir a los usuarios acceder al correo desde cualquier sitio en cualquier momento, mientras tengan una conexión a Internet o a la red. Además, dado que todas sus carpetas de correo, contactos, calendarios y demás residen en el servidor en lugar de en sus ordenadores, tienen acceso a todo igual que si estuvieran en su lugar de trabajo.

MDaemon Webmail provee muchos beneficios a los administradores de correo electrónico. Puesto que Webmail no depende de la estación de trabajo, se puede configurar todo desde el servidor, a diferencia de muchas aplicaciones cliente. También puede personalizar las imágenes y las páginas HTML que se usan en Webmail para adaptarse a sus necesidades corporativas, o las necesidades del cliente. Además, puede darles a los usuarios la posibilidad de mantener sus propias

configuraciones de cuenta, ahorrándole tiempo — puede dar tanto o tan poco control a sus usuarios como desee.

Finalmente, además de la facilidad de tener un cliente basado en web, existen muchas funciones adicionales que beneficiarán a sus usuarios, tales como: funcionalidades de correo extensivas, interfaz de cliente disponible en casi 30 idiomas, libretas de direcciones personales y globales, carpetas y filtros de correo fácilmente administrables, enviar/recibir archivos adjuntos, múltiples "temas" visuales para la interfaz, temas para los dispositivos móviles, funciones de calendario, funciones de grupo, mensajería instantánea integrada y mucho más.

Calendario & Sistema de Programación

MDaemon viene equipado con un sistema completo de colaboración. Desde Webmail puede crear de manera sencilla citas, programar reuniones y trabajar con libretas de direcciones. Las citas recurrentes tienen pleno soporte y tienen muchos campos disponibles para describirlas. A través de Webmail, sus usuarios pueden acceder a estas carpetas personales y controlar qué otros usuarios tienen acceso a ellas. Todos los temas de Webmail (especialmente LookOut) tienen plantillas que muestran los contactos, calendario, notas y tareas de una manera lógica y atractiva.

Puesto que el sistema de Calendario está integrado con MDaemon, existe además el beneficio añadido de las notificaciones de correo de las citas, ya sea programadas por usted o por un tercero. Siempre que alguien que no sea usted programe una cita para usted, recibirá un mensaje de correo resumiendo dicha cita. Cada asistente designado a una cita recibirá un mensaje de correo detallando la fecha, hora, localización y asunto de la cita, y una lista de todos los asistentes. Además, cualquier asistente que tenga entradas de calendario en conflicto con el período de tiempo de la cita, recibirá una notificación indicándole el conflicto con su calendario. La persona que haya programado la reunión recibirá un mensaje resumen listando todos los detalles de la reunión y los asistentes invitados que tienen o no tienen conflictos de calendario.

El Sistema de Calendario también está equipado con soporte para Internet Calendar (iCal) utilizado por Microsoft Outlook y otros programas de correo electrónico. El Sistema de Calendario puede detectar y procesar información iCalendar enviada por sus usuarios y actualizar sus calendarios en concordancia. Cuando un usuario abre un adjunto iCalendar desde dentro de Webmail la información contenida en los adjuntos se reflejará en los calendarios de usuario de Webmail. Además, cuando los usuarios creen nuevas reuniones o citas pueden listar una o más direcciones de correo que deseen que se les envíe un correo iCalendar. Esta funcionalidad puede establecerse por los usuarios de manera individual en sus opciones de Webmail.

MDaemon Mensajería Instantánea

MDaemon Mensajería Instantánea (MDIM) es el cliente y applet del sistema de mensajería instantánea segura de MDaemon, que provee acceso rápido a las funcionalidades de correo de Webmail. MDIM puede ser descargado e instalado localmente por cada usuario de Webmail. Se preconfigura para cada usuario específico al momento de descargarse, por lo que se limita la necesidad de configurarlo manualmente.

MDIM se ejecuta en segundo plano y verifica si su cuenta ha recibido correo nuevo consultando el servidor de Webmail directamente. Esto elimina la necesidad de abrir un navegador o de mantener uno abierto para comprobar su correo — MDIM comprueba el correo y le notifica con un sonido o por alerta visual cuando llega nuevo correo. MDIM también muestra una lista de sus carpetas de correo y del

número y tipo de mensajes que cada una contiene (nuevo, no leído, y leído). Además, puede ser utilizado para lanzar su navegador y moverse inmediatamente a una carpeta de correo específica.

MDIM también está equipado con un cliente de mensajería instantánea. Puede ver su lista de "contactos" de MDIM y cada uno de sus estatus (en línea, lejos, fuera de línea), empezar una conversación con alguno o con un grupo de ellos, establecer su propio estatus en línea y ver conversaciones pasadas en la carpeta de historial.

Para instrucciones específicas de cómo usar MDIM, consulte la Ayuda en línea.

Sistema de Mensajería Instantánea de MDaemon Mensajería Instantánea

MDIM está equipado con un cliente de mensajería instantánea (IM) que utiliza el servidor XMPP 374 de MDaemon. Al utilizar esta funcionalidad puede agregar otros usuarios que comparten su dominio (y opcionalmente otros dominios hospedados en su servidor MDaemon) con su lista de contactos MDIM y luego comunicarse con ellos instantáneamente. Puede establecer su estatus en línea, visualizar el estatus de sus contactos, utilizar emoticons, definir el color de texto, enviar archivos, configurar sonidos de notificaciones y controlar otras preferencias. También puede iniciar conversaciones grupales involucrando varios contactos al mismo tiempo. Las funcionalidades IM también están disponibles desde un ícono en la bandeja y desde la ventana MDIM.

MDIM de WorldClient también es programable, lo que permite que programas personalizados interactúen con él. Creando archivos de semáforo (`SEM`) en la carpeta \MDaemon\WorldClient\, una aplicación externa puede mandar mensajes instantáneos a los usuarios de MDIM. A continuación, el formato del archivo SEM:

`To: usuario01@ejemplo.com`	Dirección de correo del usuario de MDIM.
`From: usuario02@ejemplo.com`	Dirección de correo del remitente del mensaje instantáneo.
`<blank line>`	
`Texto del mensaje instantáneo.`	Este es el mensaje que se envía como mensaje instantáneo. .

El nombre de archivo `SEM` debe empezar con los caracteres "`IM-`" y llevar a continuación un valor numérico único. Por ejemplo, "`IM-0001.SEM`". Las aplicaciones deben poder crear también el correspondiente archivo llamado "`IM-0001.LCK`" para bloquear el archivo `SEM`. Una vez el archivo `SEM` sea completado, borre el archivo `LCK` y el archivo `SEM` será procesado. MDaemon utiliza este sistema de script para mandar recordatorios de Mensajería Instantánea sobre reuniones y citas próximas.

El sistema de Filtro de Contenido está equipado con una Acción que utiliza este método para enviar mensajes instantáneos. Además, las reglas que utilizan dicha acción pueden utilizar las Macros del Filtro de Contenidos en IM. Por ejemplo, puede crear una regla que envíe un mensaje instantáneo que contenga líneas como éstas:

```
Ha recibido un mensaje de $SENDER$.
Asunto: $SUBJECT$
```

Esta regla sería una manera efectiva de enviar alertas de mensajes nuevos a través de MDIM.

Dado que muchos administradores tienen reservas acerca del uso de sistemas de Mensajería Instantánea en sus empresas, dado la inherente falta de centralización y la poca posibilidad de monitorización del tráfico IM asociado a los clientes tradicionales de IM ampliamente conocidos, hemos diseñado el sistema de mensajería instantánea de MDIM para minimizar dichas deficiencias. En primer lugar, nuestro sistema no es punto a punto — los clientes individuales de MDIM no se conectan directamente uno con otro. Además, dado que cada IM pasa a través del servidor, todos los mensajes son registrados en una ubicación central accesible para el administrador de MDaemon. Así, se puede mantener registro de todas las conversaciones por seguridad de su empresa y de sus empleados o usuarios. La actividad IM es registrada en un archivo llamado `XMPPServer-<date>.log` localizado en el directorio `MDaemon\LOGS\`.

La mensajería instantánea se provee por dominio. Los controles para activar la mensajería instantánea y definir si el tráfico IM debería o no ser registrado se ubican en la pantalla MDIM 332 del diálogo de Webmail (Configuración » Web & Servicios IM» Webmail » MDIM).

Temas de MDaemon Mensajería Instantánea

La interfaz de MDIM es compatible con temas *msstyles*, los cuales se pueden encontrar en Internet. Algunos estilos se incluyen, pero para instalar un nuevo estilo, descargue el archivo `*.msstyles` y colóquelo bajo la carpeta de MDIM `\Styles\` en una subcarpeta con el mismo nombre que el archivo. Por ejemplo, si el archivo se llama `Red.msstyles` entonces la ruta para el archivo sería: "`\.\Styles\Red\Red.msstyles`"

Integración con Dropbox

Se ha agregado una pantalla nueva en Ctrl+W|Webmail|Dropbox. Aquí encontrará controles donde puede ingresar sus valores de Dropbox "app key", "app secret" y su texto de política de privacidad. Todos son requeridos a fin de habilitar el servicio integrado y se obtienen cuando registra su Webmail como "app" de Dropbox visitando el sitio web de Dropbox. Nosotros no podemos hacerlo, pero usted solo requerirá hacerlo en una ocasión. Por favor vea el artículo 1166 en la Base de Conocimientos para obtener instrucciones completas sobre cómo registrar su Webmail como app de Dropbox.

Una vez que se han configurado los valores "app key" y "app secret", Webmail podrá conectar sus cuentas con una cuenta de Dropbox. La primera vez que el usuario ingresa ya sea al tema WorldClient o LookOut, se le presentará con un menú desplegable en la parte superior de la pantalla. El usuario tendrá 3 opciones, visualizar ese menú la siguiente ocasión que ingrese, nunca verlo de nuevo o ir a la nueva vista Opciones | Apps en la Nube. En esta opción, el usuario puede dar clic en el botón Ajustes de Dropbox. Al hacerlo se abrirá una ventana emergente OAuth 2.0. Ahí se detalla hacia donde se está conectando el usuario y que autorizaciones solicita Webmail. También se presenta una liga a la política de privacidad y el botón "Conectarse a Dropbox". Una vez que el usuario da clic en el botón "Conectarse a Dropbox", la página navegará al sitio de Dropbox. Si el usuario no ha abierto sesión, Dropbox le presentará la opción de ingresar sus credenciales o crear una cuenta. Una vez que se ha completado este paso, se presentará al usuario otra página de Dropbox que le pregunta al usuario si desea permitir a Webmail tener acceso total a su cuenta. Al dar clic en "Permitir" la pantalla regresará a Webmail y le dirá al usuario si la autorización fue exitosa o no. Esta autorización es válida por una semana, después de ese tiempo se presentará de nuevo la misma pantalla y se obtendrá otro token de acceso para utilizar en la semana siguiente. Una vez que se

completa la autorización, el usuario contará con un ícono de Dropbox al lado de cada mensaje adjunto. Si da clic en el ícono el adjunto se guardará en la cuenta de Dropbox del usuario en la carpeta /WorldClient_Attachments.

En la vista de redacción en los temas WorldClient y LookOut, los usuarios podrán elegir archivos de sus cuentas de Dropbox dando clic en el ícono de Dropbox en la barra de edición HTML (arriba a la izquierda). Esta funcionalidad no requiere que los usuarios configuren acceso a sus cuentas vía la vista Opciones | Apps en la Nube y OAuth 2.0. Solo requiere los valores "app key" y "app secret".

El soporte a Dropbox se encuentra deshabilitado por omisión, pero se puede habilitar en la pantalla Dropbox 337 en MDaemon. Si desea habilitar o deshabilitar Dropbox dependiendo del usuario, lo puede hacer agregando el parámetro "DropboxAccessEnabled=Yes" en el archivo User.ini.

Utilizando Webmail

Iniciar Webmail

Existen tres maneras de iniciar/detener el servidor Webmail:

1. En el panel Stats en el lado izquierdo de la interface gráfica de MDaemon, dé clic derecho en Webmail y seleccione *Alternar Activo/Inactivo* en el menú.
2. Dé clic en "Archivo » Habilitar Webmail" en la interface principal
3. Dé clic en "Configuración » Web & Servicios IM " en la interface principal y luego dé clic en *Webmail se ejecuta usando el servidor web incorporado* en la pantalla Servidor Web.

Ingresando a Webmail

1. Abra su navegador en `http://example.com:WebmailPuertoNúmero`. Este puerto se define en la pantalla Servidor Web 326 en la sección Webmail. Si configura Webmail para escuchar en el puerto web por omisión (puerto 80) entonces no necesita definir el número de puerto en la URL para ingresar al servicio (v.g. `www.example.com` en lugar de `www.example.com:3000`).
2. Teclee el nombre de usuario y contraseña de su cuenta de MDaemon
3. Dé clic en Aceptar.

Cambiar la configuración de Puerto de Webmail

1. Dé clic en "Configuración » Web & Servicios IM " en la barra de menú.
2. Teclee el número de puerto deseado en el *Ejecutar Webmail utilizando este puerto TCP.*
3. Dé clic en OK.

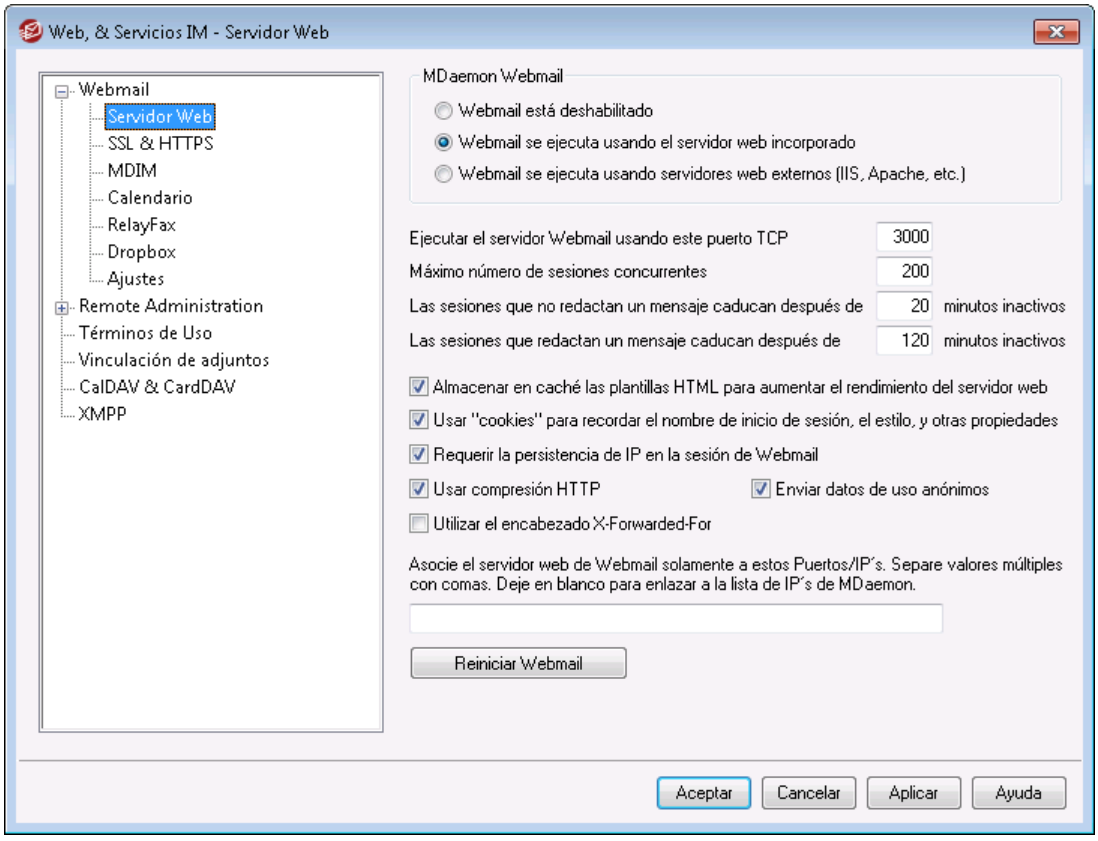
Ayuda para el Cliente

Webmail cuenta con una Ayuda extensa para el cliente, para ayudar a sus usuarios. Vea el sistema de ayuda en línea de Webmail para más información sobre funcionalidades y opciones en el cliente.

Para más opciones de Libreta de Direcciones, ver:

Webmail » MDIM 332
LDAP 831

3.6.1.2 Servidor Web



Esta pantalla contiene diversas configuraciones a nivel global y de servidor que gobiernan la configuración y el comportamiento de Webmail, independientemente de los usuarios o dominios a los que pertenezcan.

MDaemon Webmail

Webmail está deshabilitado
Seleccione esta opción para deshabilitar Webmail. Puede cambiar también entre los estados activo/inactivo de Webmail desde el menú Archivo, o desde la sección Servidores del panel de Estado en la interfaz principal de MDaemon.

Webmail debe estar activo para utilizar la función de Vinculación de Adjuntos 366.

Webmail se ejecuta usando el servidor Web incorporado
Escoja esta opción para ejecutar Webmail utilizando el servidor integrado en MDaemon. Puede cambiar entre los estados activo/inactivo desde el menú Archivo, o desde la sección Servidores del panel de Estado en la interfaz principal de MDaemon.

Webmail se ejecuta usando servidores Web externos (IIS, Apache, etc.)
Escoja esta opción cuando desee ejecutar Webmail bajo Internet Information Server (IIS) u otro servidor Web en lugar del servidor integrado de MDaemon. Esto previene que ciertos elementos de interfaz sean accedidos lo que de otra manera podría provocar conflictos con el servidor alternativo.

Para más información, vea el artículo base de MDaemon Technologies: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS

Ejecutar el servidor Webmail usando este puerto TCP
Este es el puerto en el cual Webmail escuchará para conexión de los navegadores Web de sus usuarios.

Máximo número de sesiones concurrentes
Este es el máximo número de sesiones que se podrán conectar a Webmail a la misma vez.

Las sesiones que no redactan un mensaje caducan después de xx minutos inactivos
Cuando un usuario ha accedido a Webmail, pero no está redactando un mensaje, esta es la cantidad de tiempo que su sesión permanecerá activa antes de que Webmail la cierre.

Las sesiones que redactan un mensaje caducan después de xx minutos inactivos
Este temporizador gobierna cuánto tiempo la sesión del usuario se mantendrá abierta mientras están redactando un mensaje y la sesión permanezca inactiva. Es una buena idea tener este indicador más alto que el de *Sesiones que no redactan mensaje...,* puesto que el tiempo de inactividad es típicamente superior cuando un usuario está redactando un mensaje. Esto se debe a que redactar un mensaje no requiere comunicación con el servidor hasta que el mensaje se envía.

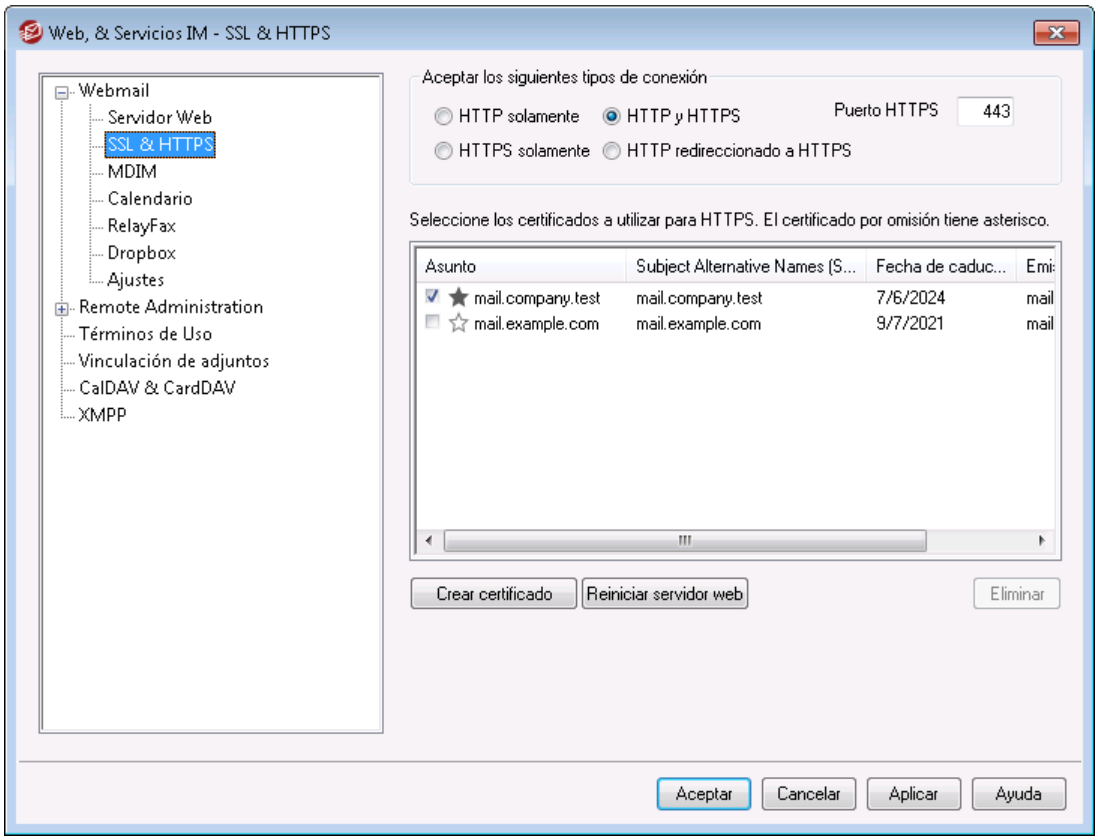
Almacenar en caché las plantillas HTML para incrementar el rendimiento del servidor Web
Hacer clic en esta casilla hará que Webmail almacene las plantillas en memoria caché en lugar de leerlas cada vez que necesiten accederse. Esto puede

aumentar considerablemente el rendimiento del servidor, pero Webmail necesitará ser reiniciado siempre que haga un cambio a uno de los archivos de plantilla.

Usar "cookies" para recordar el nombre de inicio de sesión, el estilo, y otras propiedades
Haga clic en esta opción si desea que Webmail almacene el nombre de cada usuario, tema, y algunas otras propiedades en una cookie de su ordenador loca. Esta función da a los usuarios una experiencia de acceso más "personalizada" pero requiere que tengan soporte para cookies habilitado en sus navegadores.

Requerir persistencia de IP en la sesión de Webmail
Como una medida adicional de seguridad puede hacer clic en esta casilla para provocar que Webmail restrinja la dirección IP de conexión de la sesión de cada usuario cuando éste la inició. Así, nadie puede "robar" la sesión del usuario desde el momento en que se requiera la persistencia IP. Esta configuración es más segura, pero puede causar problemas en usuarios que puedan estar utilizando un servidor proxy o conexión de Internet que asigne dinámicamente y cambie las direcciones IP.

3.6.1.3 SSL & HTTPS



El servidor web integrado de MDaemon soporta el protocolo Secure Sockets Layer (SSL). SSL es el método estándar para asegurar comunicaciones web cliente/servidor. Proporciona autentificación del servidor, encripción de datos y autentificación opcional del cliente para conexiones TCP/IP. Más aun, dado que el soporte de HTTPS (i.e. HTTP sobre SSL) está integrado en la mayoría de los navegadores, al instalar simplemente un certificado digital válido se activará la

conexión del cliente utilizando capacidades SSL.

Las opciones para habilitar y configurar Webmail para utilizar HTTPS se localizan en la pantalla SSL & HTTPS bajo Configuración » Servicios Web & IM » Webmail". Para su conveniencia, sin embargo, estas opciones también se encuentran bajo "Seguridad » Administrador de Seguridad » SSL & TLS » Webmail".

Para más información acerca del protocolo SSL y los Certificados, vea: **SSL y Certificados** 575

Esta pantalla sólo aplica a Webmail cuando se utilice el servidor web integrado. Si configura Webmail para que use algún otro servidor como IIS, estas opciones no se usarán — el soporte SSL/HTTPS tendrá que ser configurado usando las herramientas del otro servidor web.

Aceptar los siguientes tipos de conexiones

Sólo HTTP
Escoja esta opción si no desea permitir ninguna conexión HTTPS a Webmail. Sólo se aceptarán conexiones HTTP.

HTTP y HTTPS
Escoja esta opción si desea activar el soporte SSL dentro de Webmail, pero no desea forzar a los usuarios de Webmail a que utilicen HTTPS. Webmail escuchará conexiones en el puerto HTTPS designado aquí, pero seguirá respondiendo a las conexiones http normales en el puerto TCP de Webmail designado en la pantalla Servidor Web 326 de Webmail.

Sólo HTTPS
Escoja esta opción si desea requerir HTTPS cuando conecte con Webmail. Webmail responderá sólo a conexiones HTTPS cuando se active esta opción — no responderá a solicitudes HTTP.

HTTP es redireccionado a HTTPS
Escoja esta opción si desea redireccionar todas las conexiones HTTP a HTTPS en el puerto HTTPS.

Puerto HTTPS
Utilice este puerto TCP para que Webmail escuche a conexiones SSL. El puerto por defecto para SSL es 443. Si se usa el puerto por defecto, no tendrá que escribir el número de puerto en la URL de WorldClient cuando se conecte vía HTTPS (p. ej. "https://ejemplo.com" es equivalente a "https://ejemplo.com:443").

Esto no es lo mismo que el puerto de Webmail designado en la pantalla Servidor Web 326 de Webmail. Si sigue permitiendo conexiones HTTP a Webmail entonces dichas conexiones deben usar ese otro puerto para conectarse correctamente. Las conexiones HTTPS deberán usar el puerto HTTPS.

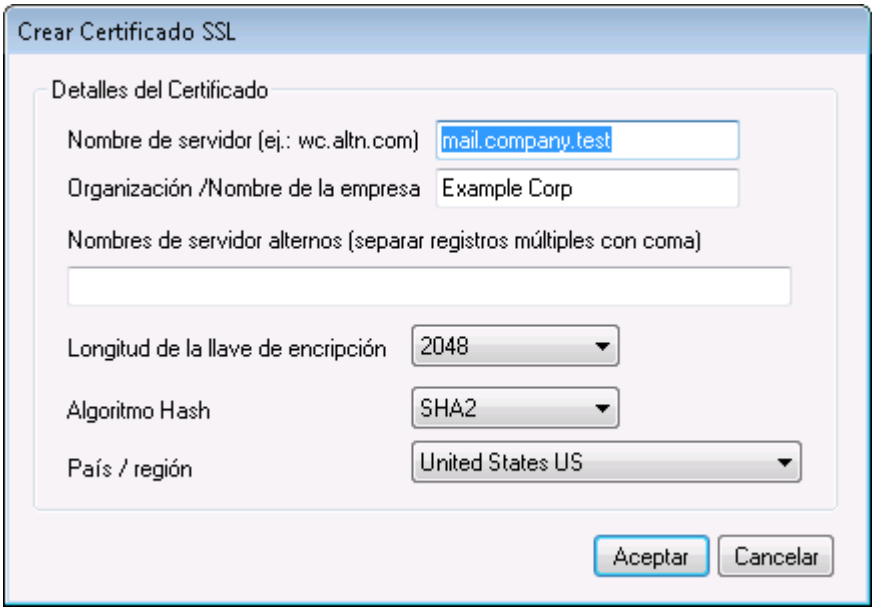
Seleccionar el certificado a utilizar para HTTPS/SSL

Esta caja muestra sus certificados SSL. Marque la caja al lado de cualquier certificado que desee se encuentre activo. Dé clic en la estrella al lado del certificado que desee configurar como el certificado por omisión. MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite utilizar un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará en los certificados activos y elegirá aquel que contenga el nombre de host solicitado en el campo Subject Alternative Names (puede especificar los nombres alternativos al crear el certificado). Si un cliente no solicita un nombre de host o si no se encuentra un certificado coincidente, se utilizará el certificado por omisión. Dé doble clic en cualquier certificado para abrir el diálogo de Certificados de Windows para revisarlo (solo disponible en la interface de escritorio, no en la administración remota vía web).

Eliminar
Seleccione el certificado de la lista y haga clic en este botón para eliminarlo. Un mensaje de confirmación se abrirá y le preguntará si está seguro de que quiere borrar el certificado.

Crear Certificado

Dé clic en este botón para abrir el diálogo Crear Certificado.



Detalles del Certificado

Nombre de Servidor
Al crear un certificado, registre el nombre del servidor al que se conectarán sus usuarios (por ejemplo, "wc.example.com").

Nombre de Organización/empresa
Registre aquí la organización o empresa "propietaria" del certificado

Nombres de servidor alternos (separe múltiples registros con una coma)
Si existen nombres de host alternos a los que se puedan conectar los usuarios y desea que este certificado se aplique también a esos nombres, registre aquí esos nombres de dominio separados por comas. Se permiten comodines, de manera

que "*.example.com" aplica para todos los subdominios de example.com (por ejemplo, "wc.example.com", " mail.example.com", etc.).

MDaemon soporta la extensión del protocolo TLS denominada Server Name Indication (SNI), que permite que se utilice un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará en los certificados activos y seleccionará aquel que contenga el nombre de host solicitado en el campo Subject Alternative Names. Si el cliente no solicita un nombre de host o no se encuentra un certificado coincidente, se utiliza el certificado por omisión.

Longitud de la llave de Encripción
Seleccione la longitud de bit deseada para la llave de encripción de este certificado. Mientras más larga sea la llave más segura será la transferencia de datos. Note, sin embargo, que no todas las aplicaciones soportan longitudes de llave superiores a 512.

País/región
Elija el país o región en que reside su servidor.

Algoritmo Hash
Elija el algoritmo hash que desea utilizar: SHA1 o SHA2. El valor por omisión es SHA2.

Reiniciar servidor web

Dé clic en este botón para reiniciar el servidor web. Este debe reiniciarse ante de que se utilice un nuevo certificado.

Utilizar Let's Encrypt para Administrar su Certificado

Let's Encrypt es una autoridad de Certificación (Certificate Authority - CA) que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los procesos completos de creación, validación, firma y renovación manuales de certificados para sitios web seguros.

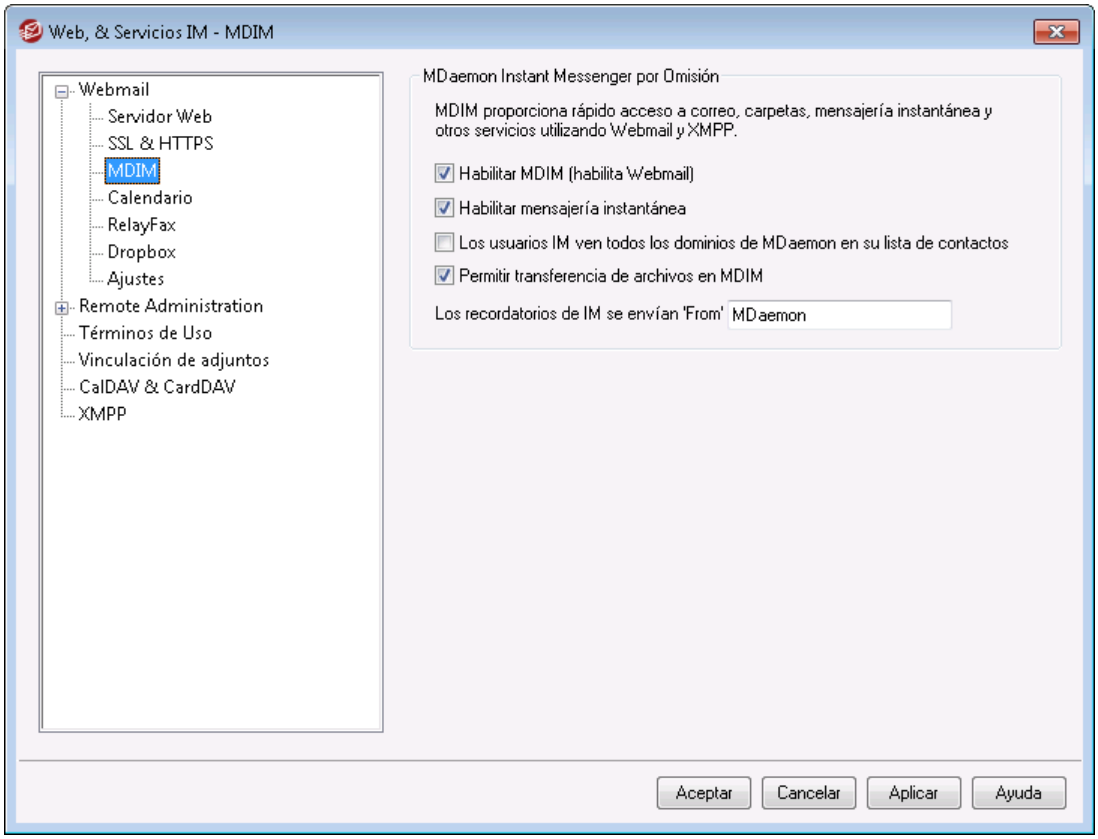
Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se cuenta con la pantalla Let's Encrypt 594 para ayudarle a configurar y ejecutar fácilmente el script de PowerShell incluido en la carpeta "MDaemon\LetsEncrypt". Al ejecutar el script se configurará todo lo necesario para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta HTTP de Webmail para completar la validación http-01. Utiliza el Nombre de host SMTP 192 del dominio por omisión 190 como dominio para el certificado, incluye cualesquiera *Nombres de host Alternos* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para utilizar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "MDaemon\Logs\" , denominado LetsEncrypt.log. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora del inicio de ejecución del script. También, se envían mensajes de notificación de la ocurrencia de errores, si se especifica una *Cuenta de correo de*

Admin para notificaciones. Vea el tema Let's Encrypt 594 para más información.

Ver:

SSL & Certificados 575
Crear y Utilizar Certificados SSL 912

3.6.1.4 MDIM



Esta pantalla controla los parámetros por omisión para dominios nuevos para MDaemon Mensajería Instantánea (MDIM) 322. La configuración se puede modificar para dominios específicos vía la pantalla MDIM 198 del Administrador de Dominios. Los servicios de MDIM se pueden habilitar o deshabilitar para cuentas o grupos específicos vía las pantallas Servicios Web 720 y Propiedades de Grupo 783 respectivamente.

MDaemon Mensajería Instantánea por omisión

Habilitar MDIM (habilita Webmail)
Habilite esta opción si desea hacer que MDaemon Mensajería Instantánea se encuentre disponible por omisión para descarga desde Webmail. Los usuarios pueden descargarlo de la página Opciones » MDaemon Mensajería Instantánea.

El archivo descargable de instalación estará personalizado automáticamente con la información de la cuenta del usuario para facilitar la instalación y configuración. Esta opción también permite a MDIM utilizar las funcionalidades de Mis Carpetas de Correo, permitiendo a los usuarios verificar correo nuevo y abrir Webmail directamente desde el menú de MDIM. MDIM se encuentra habilitado por omisión.

Habilitar Mensajería Instantánea
Por omisión, las cuentas pueden utilizar MDIM y clientes de terceros tipo XMPP 374 para intercambiar mensajes con miembros de su dominio. Deshabilite esta casilla si no desea permitir la mensajería instantánea por omisión.

Los usuarios de IM ven todos los dominios de MDaemon en su lista de contactos
Dé clic en esta opción si desea que sus usuarios, por omisión, pueda agregar usuarios a su lista de contactos, pertenecientes a todos sus dominios de MDaemon. Cuando se deshabilita esta opción, los contactos deben estar en el mismo dominio. Por ejemplo, si su MDaemon está dando servicio de correo a example.com y example.org, al activar esta opción los usuarios podrán agregar a sus contactos de mensajería instantánea, usuarios de ambos dominios. Al deshabilitar la opción, los usuarios de example.com solo podrán agregar contactos de los usuarios de example.com y example.org. solo podrá agregar a los usuarios de example.org. Esta opción se encuentra deshabilitada por omisión. Existe una opción equivalente en el Administrador de Dominios 198 para habilitar o deshabilitar esta funcionalidad para dominios específicos.

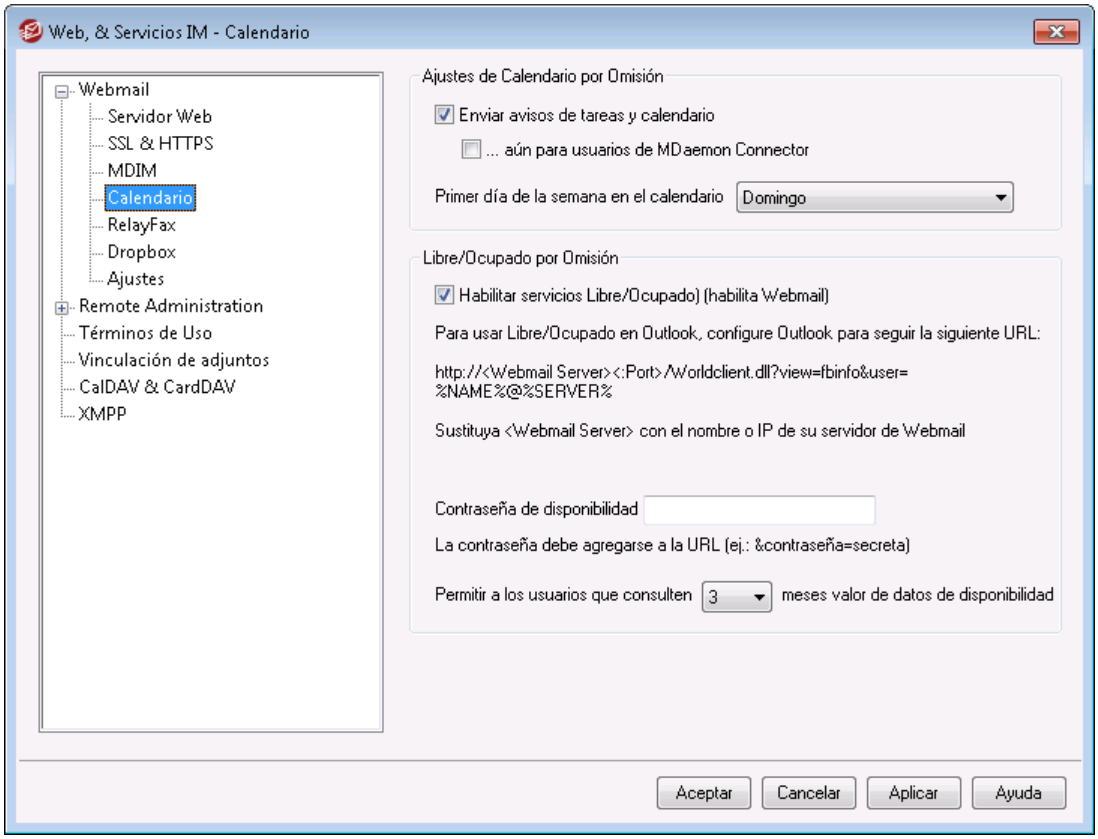
Permitir transferencias de archivos en MDaemon Mensajería Instantánea
Por omisión, los usuarios de MDIM pueden transferir archivos a sus contactos de MDIM. Deshabilite esta opción si no desea permitir que MDIM se utilice para transferir archivos.

Los recordatorios de IM se envían 'From:'
Cuando se programa una Cita en el calendario de Webmail de un usuario, el evento puede configurarse para que envíe un recordatorio al usuario en una fecha/hora específica. Si el sistema IM está activo para el dominio del usuario, el recordatorio será enviado en un mensaje instantáneo si el usuario está utilizando MDIM. Utilice esta caja para especificar el nombre que desea que aparezca en el campo 'De:' del mensaje. Esta es la configuración por omisión para dominios nuevos. La puede modificar para dominios específicos vía la pantalla MDaemon Mensajería Instantánea 198 del Administrador de Dominios.

Ver:

Administrador de Dominios » MDaemon Mensajería Instantánea 198
Editor de Cuentas » Servicios Web 720
Propiedades de Grupo 783

3.6.1.5 Calendario



Esta pantalla controla los ajustes por omisión de las funcionalidades del Calendario de MDaemon. La configuración para dominios específicos se puede controlar desde la pantalla Calendario del Administrador de Dominios.

Ajustes de Calendario por Omisión

Enviar avisos de tareas y calendario
Dé clic en esta casilla si desea permitir que WorldClient envíe los recordatorios de calendario y tareas a sus usuarios mediante correo electrónico y MDaemon Mensajería Instantánea.

...aun para usuarios de MDaemon Connector
Si ha habilitado la opción "*Enviar avisos de tareas y calendario*", dé clic en esta opción si desea también habilitar los recordatorios para los usuarios de MDaemon Connector.

Primer día de la Semana
Elija el día de la lista desplegable. Este aparecerá en los calendarios como el primer día de la semana.

Libre/Ocupado por omisión

MDaemon incluye un servidor Libre/Ocupado, que posibilita al usuario que va a organizar una junta, visualizar la disponibilidad de los posibles invitados al evento. Para accesar a esta funcionalidad, dé clic en Programación desde Webmail al crear una cita nueva. Esto abre una ventana de Programación que contiene la lista de participantes y un calendario codificado en color con una cuadrícula donde se asigna una línea a cada uno de ellos. Esta línea indica por colores, los

horarios en los que el participante puede estar disponible para la sesión. Se tienen colores para Ocupado, Tentativo, Fuera de la Oficina o Sin Información. También se tiene un botón de AutoSeleccionar Siguiente que le permite consultar al servidor cual es el siguiente horario en el que todos los participantes pueden estar disponibles. Cuando haya terminado de crear la junta, enviará una invitación a todos los asistentes, que podrán aceptar o declinar.

El servidor Libre/Ocupado de Webmail es compatible con Microsoft Outlook. Para utilizarlo, configure Outlook para consultar los datos Libre/Ocupado en la URL listada abajo. En Outlook 2002, por ejemplo, las opciones Libre/Ocupado se encuentran bajo "Herramientas » Opciones » Calendario Opciones... » Opciones Libre/Ocupado..."

URL Libre/Ocupado para Outlook:

```
http://<WorldClient><:Port>/Worldclient.dll?view=fbinfo&user=%
NAME%@%SERVER%
```

Reemplace "<WorldClient>" con la dirección IP o el nombre de dominio de su servidor WorldClient y "<:Port>" con el número de puerto (si es que no está utilizando el puerto por omisión). Por ejemplo:

```
http://ejemplo.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@
%SERVER%
```

Para más información sobre cómo utilizar las funcionalidades Libre/Ocupado en Webmail para programar reuniones, vea el sistema de Ayuda en Línea directamente en Webmail.

Habilitar Servicios Libre/Ocupado
Dé clic en esta opción si desea dar acceso a los usuarios a la funcionalidad Libre/Ocupado.

Contraseña Libre/Ocupado
Si desea requerir una contraseña cuando los usuarios intenten acceder a las funcionalidades de Libre/Ocupado vía Outlook, entonces introduzca la contraseña aquí. Esta contraseña debe agregarse a la URL antes listada (en la forma: "&password=Contraseña") cuando los usuarios configuren sus opciones Libre/Ocupado dentro de Outlook. Por ejemplo:

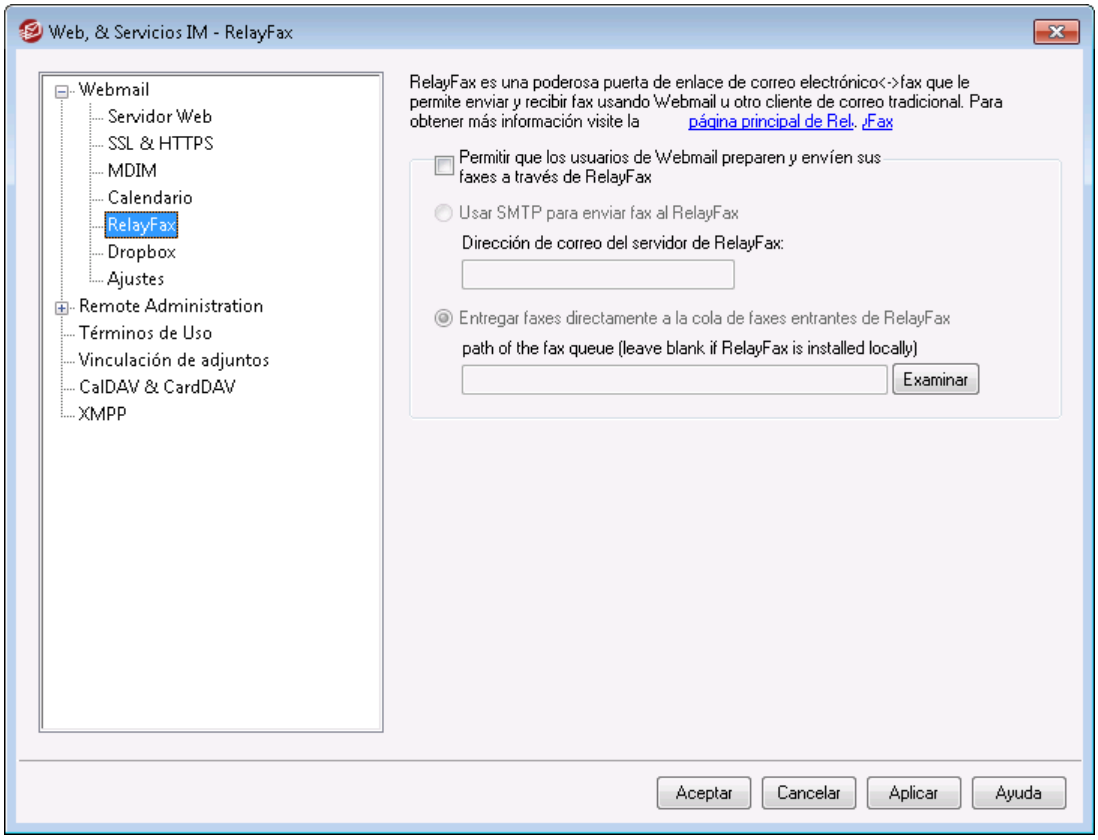
```
http://ejemplo.com:3000/WorldClient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=Contraseña
```

Permitir a los usuarios consultar X meses de disponibilidad Libre/ocupado
Utilice esta opción para definir cuantos meses de información de disponibilidad Libre/Ocupado pueden consultar los usuarios.

Ver:

Administrador de Dominios » Calendario

3.6.1.6 RelayFax



El servidor RelayFax de MDaemon Technologies es una puerta de enlace a correo electrónico que puede ser integrada de manera transparente con Webmail para proveer de sus servicios a sus usuarios. Cuando se habilita su funcionalidad, los usuarios de Webmail tendrán acceso a diversas funcionalidades que les permitirán escribir y enviar faxes a través de las páginas de cliente de Webmail. Para más información, visite la sección RelayFax de www.mdaemon.com.

Opciones de Integración con RelayFax

Permitir a los usuarios de Webmail redactar y enviar faxes a través de RelayFax
Haga clic en esta opción para integrar RelayFax con Webmail. Cuando lo active hará que un control de "Redactar Fax" y otras funciones relacionadas con el fax aparezcan en las páginas de Webmail.

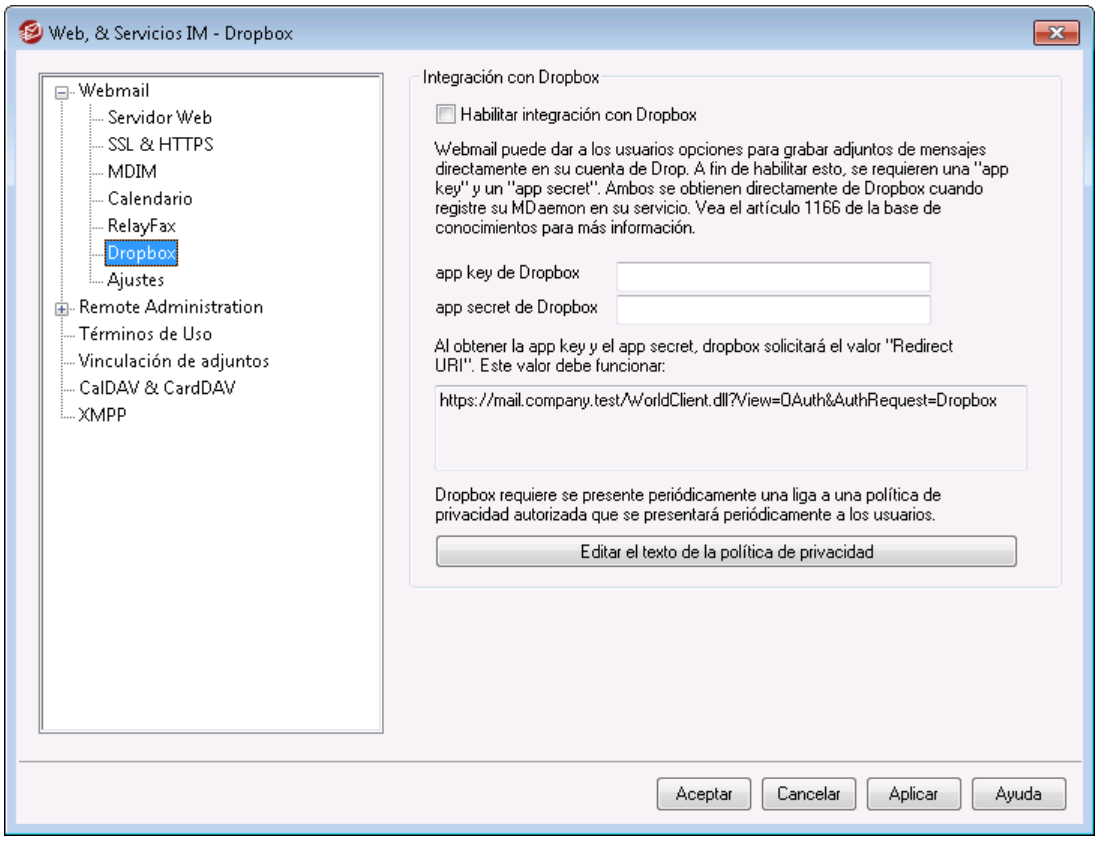
Usar SMTP para enviar fax al RelayFax
RelayFax monitorea un buzón específico para mensajes entrantes que han de enviarse por fax. Haga clic en esta opción y MDaemon utilizará el proceso de envío normal de correo para enviar este mensaje a la dirección del buzón. Esta opción es útil cuando RelayFax monitorea un buzón ubicado en algún lugar distinto de su red local. Si RelayFax reside en su red, puede escoger que MDaemon envíe los mensajes directamente a la cola de mensajes de RelayFax y así pues se salte el proceso de envío de SMTP. Para más información acerca de este método, vea *Entregar fax directamente a la cola de fax entrante de RelayFax* siguiente.

Dirección de correo del servidor de RelayFax
Especifique la dirección de correo a la cual quiere enviar los mensajes destinado para el fax. Este valor debe coincidir con la dirección que haya configurado en RelayFax para monitorear dichos mensajes.

Entregar fax directamente a la cola de fax entrante de RelayFax
Si RelayFax reside en un LAN puede escoger este método en lugar del envío SMTP para distribuir los mensajes de fax. Cuando MDaemon recibe mensajes destinados a RelayFax los colocará directamente en la cola entrante de RelayFax en lugar de enviarlos usando SMTP.

Ruta de la cola de Fax
Si RelayFax reside en la misma máquina en la que MDaemon se está ejecutando, puede dejar esta ruta de archivo vacía. Si no, deberá especificar la ruta de red a la carpeta \app\ de RelayFax.

3.6.1.7 Dropbox



Webmail está equipado con soporte directo para Dropbox, que permite a los usuarios guardar sus archivos adjuntos en sus cuentas Dropbox, así como insertar ligas directas de archivos en Dropbox en sus mensajes salientes. Para proporcionar esta funcionalidad a sus usuarios de Webmail, debe configurar Webmail como app de Dropbox en la Plataforma Dropbox. Este es un proceso simple, que le requiere firmarse a una cuenta Dropbox, crear un nombre único para una app con acceso

total a Dropbox, especificar la URL de redireccionamiento hacia Webmail y modificar un ajuste por omisión. Entonces podrá copiar y pegar las App Key y App Secret de Dropbox desde ahí a la página de opciones de MDaemon. Luego de eso sus usuarios podrán ligar sus cuentas de Dropbox con Webmail la siguiente vez que se inicien sesión en Webmail. para obtener instrucciones paso a paso de como cread su app de Dropbox y ligarla a Webmail, vea: Crear y ligar su App de Dropbox 339 abajo.

Cuando cree si app de Dropbox tendrá inicialmente un estatus de "Desarrollo". Esto permite hasta a 500 usuarios de Webmail ligar sus cuentas de Dropbox con la app. Sin embargo, de acuerdo con Dropbox, "una vez que su app liga 50 usuarios de Dropbox, le quedarán dos semanas para solicitar y recibir la aprobación del estatus de "Producción" antes de que la capacidad de su app para ligar usuarios de Dropbox adicionales se congele, sin importar cuantos usuarios entre 0 y 500 haya ligado su app." Esto significa que hasta que reciba la aprobación de producción, la integración de Dropbox continuará funcionando, pero no podrá habilitar usuarios adicionales para ligar sus cuentas. Obtener la aprobación para producción es un proceso sencillo para asegurar que su app cumple con los lineamientos de Dropbox y los Términos de Servicio. Para más información, vea la sección Aprobación para Producción en la Guía para desarrolladores de la plataforma Dropbox.

Una vez que su app de Webmail es creada y configurada correctamente, cada usuario de Webmail tendrá la opción de conectar su cuenta de Dropbox cuando inicien sesión en Webmail. Se requiere al usuario iniciar sesión en Dropbox y otorgar permisos a la app para tener acceso a la cuenta Dropbox. Entonces el usuario será redirigido de regreso a Webmail utilizando la URL que se pasó a Dropbox durante el proceso de autentificación. Por seguridad, esa URL debe coincidir con una de las URL de redireccionamiento (ver abajo) que especificó en su página de información de la app en Dropbox.com. Finalmente, Webmail y Dropbox intercambiarán un código de acceso y un token de acceso que le permitirá a Webmail conectarse a cuenta de Dropbox del usuario para que pueda guardar sus adjuntos ahí. Los tokens de acceso intercambiados expiran cada 7 días, lo que significa que el usuario periódicamente deberá reautorizar la cuenta para utilizar Dropbox. Los usuarios también pueden desconectar manualmente su cuenta de Dropbox o reautorizarla cuando sea necesario, desde la pantalla de opciones Apps de Nube en Webmail.

Integración con Dropbox

Habilitar integración con Dropbox
Una vea que ha creado su app de Dropbox y la ha ligado a Webmail, dé clic en esta casilla para permitir a sus usuarios de Webmail ligar sus cuentas de Dropbox. Si desea habilitar o deshabilitar Dropbox por usuario, lo puede hacer agregando la variable "`DropboxAccessEnabled=Yes` (o `No`)" en el archivo `User.ini`.

App key y app secret de Dropbox
Los valores App key y App secret se localizan en su página de información de la app en Dropbox.com. Regístrelos aquí para ligar Webmail a su app de Dropbox. MDaemon automáticamente despliega una URL aquí que usted podrá utilizar allá. Sin embargo, puede agregar múltiples URL´s de Redireccionamiento. Por eso puede agregar una URL por cada uno de sus dominios y hasta una para su localhost, que se podría utilizar si el inicio de sesión en Webmail se realiza desde la máquina en que se está ejecutando MDaemon.

Por ejemplo:

```
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 requiere que sus URL de redireccionamiento sean seguras, por esto HTTPS 328 deben estar habilitados para Webmail.

Editar texto de la política de privacidad
Dé clic en este botón para editar el archivo de texto que contiene su política de privacidad de la App de Webmail. Dado que Dropbox requiere que se presente a sus usuarios periódicamente una política de privacidad aprobada, se proporciona una liga a la "Política de Privacidad" con el contenido de este archivo en la página **Conectarse a Dropbox** que se despliega a sus usuarios. Esa liga abre una pequeña ventana que contiene el texto y un botón de Descarga en que los usuarios pueden dar clic para descargar el archivo. Utilice código HTML en el archivo si desea formatear el texto o desea que contenga cualquier otra liga.

Crear y Ligar su App de Dropbox

Instrucciones paso a paso para crear su app de Dropbox y ligarla a Webmail.

1. En su navegador vaya a Plataforma Dropbox
2. Inicie sesión en su cuenta Dropbox
3. Seleccione **Dropbox API**
4. Seleccione **Full Dropbox**
5. Asigne a su app un nombre único
6. Dé clic en **Create App**
7. Dé clic en **Enable additional users** y dé clic en **Okay**
8. Modifique **Allow implicit grant** a **Disallow**
9. Ingrese una o más URL de Redireccionamiento, dando clic en **Add** después de cada una. Debe ser URL´s seguras hacia su Webmail (HTTPS debe estar habilitado en Webmail).

   Por ejemplo:

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
10. Deje su navegador abierto en la página de info de su app y abra la IU de MDaemon.
11. Dé clic en **Configuración**
12. Clic en **Web & Servicios IM**
13. Clic en **Dropbox** bajo **Webmail**
14. Copiar/Pegar la **App key** y **App secret** desde la pantalla **Dropbox** en su navegador, hacia MDaemon.
15. Clic en **Apply**

16. Clic en **OK**

Para instrucciones sobre cómo ligar una cuenta de usuario de Webmail a la cuenta de Dropbox del usuario, vea el sistema de ayuda en línea en Webmail o vea el artículo de la base de conocimientos de MDaemon 1166.

3.6.1.8 Google Drive

Esta página solo está disponible en la interface web MDaemon Administración Remota 354 (MDRA).

Integración con Google Drive

MDaemon Webmail puede ofrecer a los usuarios opciones para grabar los adjuntos de sus mensajes directamente en su cuenta de Google Drive y editar y trabajar los documentos almacenados ahí. A fin de habilitar esto, se requieren una **Llave Api**, un **ID de Cliente** y un **Secreto de Cliente**. Todos se obtienen directamente de Google creando una App utilizando la Consola Google API y registrando MDaemon en ese servicio. Parte de esa app es un componente de autentificación OAuth 2.0, que permite a sus usuarios de Webmail iniciar sesión en Webmail y luego autorizar el acceso a su cuenta de Google Drive desde MDaemon. Una vez autorizada, los usuarios pueden visualizar las carpetas y archivos que tienen en Google Drive. Más aún, pueden subir, descargar, mover, copiar, renombrar y eliminar archivos, así como copiar/mover archivos de y hacia carpetas locales de documentos. Si el usuario desea editar un documento, si da clic en la opción para visualizar el archivo en Google Drive, podrá realizar ediciones de acuerdo con los permisos establecidos en Google Drive. El proceso de configuración de Google Drive es similar a las funcionalidades Integración con Dropbox 337 e Integración MultiPOP OAuth 151.

Habilitar Integración con Google Drive
Dé clic en esta casilla para habilitar la Integración con Google Drive. Ver: **Configurar la Integración con Google Drive Integration** abajo.

Llave API de Google Drive:
Esta es su llave API única que será generada para usted en la consola Google Drive API cuando esté creando su app. Copie y pegue esa llave aquí.

ID de Cliente de Google Drive
Este es el único ID de Cliente asignado a su app de Google Drive cuando la crea en la Consola de Google API. Luego de crear la app, copie el ID de Cliente y péguelo aquí.

Secreto de Cliente de Google Drive
Este es el Secreto de Cliente único asignado a su app de Google Drive cuando la crea en la Consola de Google API. Luego de crear la app, copie este Secreto de Cliente y péguelo aquí.

URI de Redireccionamiento
Debe especificar una o más URIs de Redireccionamiento al crear su app de Google Drive. La URI de Redireccionamiento de muestra se construye a partir de su

Nombre de host SMTP de su Dominio por omisión 190, que debería funcionar para los usuarios de ese dominio al iniciar sesión en Webmail. Deberá agregar URIs de Redireccionamiento adicionales a su app para cualquier dominio de MDaemon adicional que utilicen sus usuarios para iniciar sesión en Webmail. Por ejemplo, "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" debe funcionar para cualquiera de sus usuarios que van a `mail.example.com` cuando inician sesión en Webmail. Ver: **Crear y Vincular su App de Google Drive** abajo para más información.

Editar texto de la política de privacidad
La integración con Google Drive requiere que periódicamente presente una liga a sus usuarios de la política de privacidad aprobada. Dé clic en este botón para editar su política de privacidad.

Crear y Vincular su App de Google Drive

Instrucciones paso a paso para crear su app de Google Drive.

Siga los pasos siguientes para crear una aplicación de Google para permitir a sus usuarios tener acceso a su Google Drive desde Webmail en la página **Documentos**.

1. Inicie sesión en MDaemon Administración Remota 354, vaya a la página Google Drive (localizada bajo Inicio » Ajustes de Webmail) y habilite la opción **Habilitar Integración con Google Drive**.
2. En una pestaña por separado en el navegador, inicie sesión sen su cuenta de Google y vaya a la Consola de API de Google.
3. En la Lista de Proyectos, dé clic en **PROYECTO NUEVO** o si se encuentra en la página Administrar Recursos, dé clic en **(+) CREAR PROYECTO**.
4. Escriba un **Nombre de Proyecto,** como "Google Drive para MDaemon," y luego dé clic en **Editar** si desea editar el ID de Proyecto o déjelo configurado con el valor por omisión. **Nota:** el ID de Proyecto no se puede modificar luego de que el proyecto sea creado.
5. Si cuenta con un Recurso de Organización, selecciónelo en **Localización**. De otra forma déjelo configurado como "Sin organización."
6. Una vez cargada, dé clic en **+ HABILITAR APIs Y SERVICIOS**.
7. En el campo consulta, teclee "Google Drive", seleccione **API de Google Drive** y dé clic en **Habilitar**.
8. En el panel izquierdo, bajo **APIs & Servicios**, dé clic en **Credenciales**.
9. Dé clic en **+ Crear Credenciales** en la parte superior de la página y seleccione **clave de API** en el menú desplegable.
10. Copie su **clave de API** (a un lado hay un ícono para copiar al portapapeles).
11. Regrese a la pestaña de MDaemon en su navegador y pegue la **llave API de Google Drive** en el campo **llave API de Google Drive API Key** en la página Google Drive en MDaemon (o guárdela en otro lado si desea hacerlo más tarde).
12. En el panel izquierdo, bajo **APIs & Servicios,** dé clic en **pantalla de consentimiento OAuth**.

13. Bajo Tipo de Usuario, seleccione **Externos**, y dé clic en **Crear**. **Nota:** si cuenta con un Recurso de Organización, o dependiendo de el Estatus de Publicación de su app, seleccionar Interno puede ser la mejor elección. Vea la nota abajo Estatus de Publicación[343] para más información.
14. Escriba el **Nombre de App** (ej. Google Drive para Webmail), una **Cuenta de correo de soporte** para que contacten los usuarios y una **Cuenta de correo de desarrollador** para que Google lo contacte sobre modificaciones en su proyecto. Esto es todo lo que se requiere en esta página en cuanto a configuración, pero dependiendo de su organización en particular o los requerimientos de verificación, también puede registrar el logo de su empresa y ligas a sus Términos de servicio[365] y Política de Privacidad (ver arriba). Los campos **Dominios Autorizados** se llenarán en automático cuando agregue las *URIs de Redireccionamiento* en un paso posterior. **Nota:** Esta información se utiliza para la pantalla de Consentimiento que se presentará a los usuarios para autorizar que Webmail tenga acceso al Google Drive del usuario.
15. Dé clic en **Grabar y Continuar**.
16. Dé clic en **AGREGAR O QUITAR PERMISOS**, y copie/pegue las URIs siguientes (puede copiar/pegar todas de una vez) en la casilla bajo "Agregar permisos manualmente". Luego de clic en **AGREGAR A LA TABLA.**

```
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. Dé clic en **Actualizar y luego en Guardar y Continuar**.
18. Bajo Usuarios de prueba, dé clic en **AGREGAR USUARIOS** y capture cada cuenta de Google Drive a la que MDaemon estará accediendo a través de esta app y dé clic en **AGREGAR** (ver la nota abajo sobre el Estatus de Publicación[343] de su app).
19. Dé clic en **Guardar y Continuar**.
20. En resumen, dé clic en **VOLVER AL PANEL** en el fondo de la página.
21. Dé clic en **Credenciales** en el panel izquierdo, clic **(+) Crear Credenciales** y seleccione **ID de cliente OAuth**.
22. En el menú desplegable "Tipo de Aplicación" seleccione **aplicación Web** y bajo "URIs de redireccionamiento autorizados" dé clic en **+ AGREGAR URI**. Escriba la URI de redireccionamiento. La URI de redireccionamiento desplegada en la página Google Drive en MDaemon es un ejemplo construido a partir de su Nombre de host SMTP de su Dominio por Omisión[190], que deberá funcionar para los usuarios de ese dominio al iniciar sesión en Webmail. Deberá agregar URIs de Redireccionamiento adicionales a su app para cualquier dominio adicional de MDaemon que utilicen sus usuarios para iniciar sesión en Webmail. Por ejemplo, "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" funcionará para cualquiera de sus usuarios que van a `mail.example.com` cuando inician sesión en Webmail. Si

también tiene un dominio llamado "`mail.company.test`", entonces deberá registrar una URI de Redireccionamiento para ese dominio, ej. "`https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`".

23. Dé clic en **CREAR**.
24. Copie los valores en **Su ID de Cliente** y **Su Secreto de Cliente** en las casillas *ID de Cliente Google Drive* y *Secreto de Cliente Google Drive* en la página Google Drive en MDaemon. También puede ingresar su API Key de Google Drive si no lo hizo previamente.

Estatus de Publicación — Estas instrucciones son para crear una app de Google con el Estatus de Publicación configurado como "**Prueba**". Esto requiere que agregue cada cuenta específica de Google que estará utilizando la app para acceder a su Google Drive y está limitado a 100 usuarios. Más aún, en Webmail cuando se solicita a sus usuarios autorizar MDaemon para acceder a Google, se desplegará un mensaje de advertencia "para confirmar que el usuario tiene acceso a su proyecto deberá considerar los riesgos asociados con otorgar acceso a sus datos desde una app no verificada". También, la autorización expira en siete días, por lo que cada usuario deberá reautorizar el acceso a Google cada semana.

Si desea eliminar estos requerimientos y limitaciones, debe modificar su estatus a "**Producción**" lo que puede requerir o no que modifique su Tipo de Usuario de externo a interno y realizar un proceso de verificación de app o ambas opciones. Para más información sobre verificación de app y estatus de publicación, vea los siguientes artículos de Google: Setting up your OAuth consent screen y OAuth API verification FAQs.

Autorizar Google Drive en Webmail

Una vez que ha creado su app de Google Drive y configurado Google Drive en la página de MDaemon de acuerdo a las instrucciones anteriores, cada usuario que desee tener acceso a su Google Drive en Webmail deberá primero autorizar el acceso. Para hacerlo, cada usuario deberá:

1. Iniciar sesión en Webmail.
2. Dar clic en el **ícono Opciones** en la esquina superior derecha y luego clic en **Apps Cloud**
3. Dar clic en **Configurar Google Drive** (esto abrirá la página **OAuth 2.0)**
4. Dar clic en **Conectar a Google Drive.**Si
5. Si no ha iniciado sesión, Google Drive le pedirá la información de acceso o que seleccione una cuenta.
6. Es posible que se presente un mensaje de advertencia que dice "Google no ha verificado esta app. Se le ha dado acceso a una app que actualmente está siendo probada. Solo deberá continuar si conoce al desarrollador que lo invitó". Dar clic en **Continuar**

7. Seleccione a qué funcionalidades de Google Drive tendrá acceso Webmail y dé clic en **Continuar.**
8. Se desplegará una página final estableciendo que MDaemon ahora está conectado a Google Drive. Se puede cerrar esa ventana.
9. Se podrá tener acceso a Google Drive desde la página **Documentos** en Webmail.

Ver:

MultiPOP OAuth 151
Integración con Dropbox 337

3.6.1.9 Categorías

Las opciones de Categorías se localizan en la interface de MDaemon Administración Remota, en: **Inicio » Ajustes de Webmail » Categorías**.

Webmail soporta categorías para correo electrónico, eventos, notas y tareas en los temas LookOut y WorldClient. Los usuarios pueden agregar la columna Categorías a la lista de mensajes habilitando "**Categorías**" en "**Opciones » Columnas**" en la sección Lista de Mensajes.

Para establecer las categorías para uno o más mensajes en la lista de mensajes, seleccione los mensajes y dé clic-derecho en uno de ellos. Utilice el menú contextual para establecer la categoría. Alternativamente, puede abrir un mensaje y establecer la categoría utilizando la opción en la barra de herramientas.

Categorías

En la página Categorías en la interface de MDaemon Administración Remota, puede establecer las Categorías del Dominio, que son una lista fija de categorías que verán los usuarios en Webmail pero que no pueden editar o eliminar. También puede crear la lista por omisión de Categorías Personales que se desplegará a los usuarios nuevos.

Categorías del Dominio

Las Categorías del Dominio son categorías fijas que no pueden ser reordenadas, editadas o eliminadas por sus usuarios. Cuando está habilitada la opción *Habilitar Categorías del Dominio*, la lista aparecerá en la parte superior de la lista de categorías del usuario en Webmail. Puede reordenar, editar, eliminar o crear nuevas Categorías de Dominio utilizando las opciones proporcionadas.

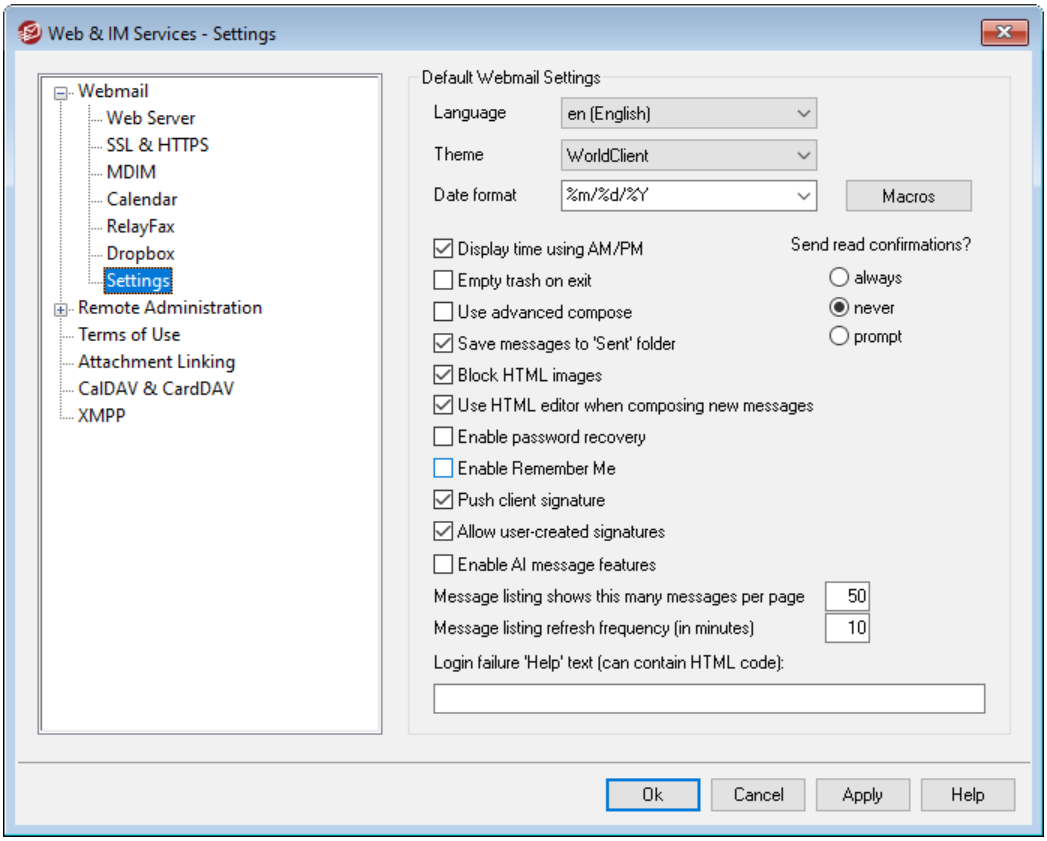
Categorías Personales

Esta es la lista por omisión de categorías que se copiará a las cuentas de los usuarios nuevos de Webmail. Los usuarios tienen control completo sobre la lista de categorías personales. Pueden reordenar, editar o eliminarlas y pueden crear categorías nuevas. Sí, sin embargo, también está utilizando Categorías del Dominio, entonces esas categorías aparecerán al inicio de la lista del usuario y no pueden ser editadas o duplicadas. Cualquier categoría personal con un nombre que coincida con una categoría del dominio, será ocultada. Si no desea permitir categorías

personales, deshabilite la opción **Los Usuarios pueden editar categorías personales**. En ese caso solo se desplegarán las categorías del dominio, Si la opción Categorías del Dominio también se deshabilita entonces no estará disponible la opción de Categorías para los usuarios.

Para obtener información detallada relativa de los archivos de MDaemon en que se administran las categorías y sus traducciones, vea:
`MDaemon\WorldClient\CustomCategories.txt`.

3.6.1.10 Ajustes



Esta pantalla define los ajustes por omisión para la pantalla Ajustes de Webmail del Administrador de Dominios. Cuando un usuario se firma en Webmail, estas opciones determinan cómo funcionan inicialmente varias funciones de Webmail para ese usuario. Muchos de estos ajustes pueden ser personalizados por el usuario vía la página Opciones en Webmail.

Ajustes por Omisión de Webmail

Idioma
Utilice el cuadro de lista desplegable para escoger el idioma por defecto en el cual aparecerá la interfaz de Webmail cuando sus usuarios entren primero al dominio seleccionado. Los usuarios pueden cambiar sus configuraciones

personales de dominio en la página de inicio de Webmail, y a través de una opción en Opciones » Personalizar dentro de Webmail.

Tema
Utilice esta lista desplegable para designar el tema por defecto de Webmail para los usuarios cuando accedan por primera vez. Los usuarios pueden personalizar la configuración de tema desde Opciones » Personalizar dentro de Webmail.

Formato de fecha
Use este cuadro de texto para designar cómo se formatearán las fechas en Webmail. Haga clic en el botón Macros para mostrar una lista de los códigos de macro que se pueden usar en este cuadro de texto. Puede usar los siguientes macros en este control:

%A — Nombre del día de la semana completo

%B — Nombre del mes completo

%d — Día del mes (se muestra como "01-31")

%m — Mes (se muestra como "01-12")

%y — dígitos del año en formato 2 dígitos

%Y — dígitos del año en formato 4 dígitos

Por ejemplo, "`%d/%m/%Y`" puede mostrarse en Webmail como "`25/12/2011`".

Macros
Haga clic en este botón para mostrar una lista de los códigos macro que se pueden usar en el *Formato de Fecha.*

¿Enviar confirmaciones de lectura?
Esta opción administra como responderá Webmail a los mensajes entrantes que contienen una petición de confirmación de lectura.

siempre
Si se selecciona esta opción, MDaemon enviará una notificación al remitente indicando que el mensaje fue leído. El usuario de Webmail que recibió el mensaje no tendrá ninguna indicación de que la petición de lectura fue hecha o que se envió la respuesta.

nunca
Seleccione esta opción si desea que Webmail ignore las peticiones de confirmación de lectura.

preguntar
Seleccione esta opción si desea que se pregunte a los usuarios de Webmail si desean o no enviar la confirmación de lectura cada vez que se abra un mensaje que la solicita.

Mostrar hora usando AM/PM
Haga clic en esta opción si desea que se use un reloj de 12 horas en formato AM/PM dentro de Webmail cuando se muestre la hora. Despeje esta casilla si quiere utilizar un reloj de 24 horas. Los usuarios pueden modificar esta configuración a través de la opción *"Presentar la hora en formato AM/PM"* ubicado en la página Opciones » Calendario dentro de Webmail.

Vaciar basura a la salida
Esta opción provoca que la papelera de los usuarios se vacíe cuando él o ella se desconecten de Webmail. Los usuarios individuales pueden cambiar esta configuración desde la página Opciones » Personalizar dentro de Webmail.

Usar redacción avanzada
Haga clic en esta casilla si desea que los usuarios vean la ventana de Redacción Avanzada en lugar de ver la ventana normal de Redacción por defecto. Los usuarios pueden personalizar esta configuración desde la página Opciones » Redactar dentro de Webmail.

Guardar mensajes en la carpeta 'Enviados'
Dé clic en esta opción si desea que se guarde una copia de cada mensaje enviado en la carpeta Enviados de su buzón. Los usuarios individuales pueden modificar este parámetro desde la página Opciones » Redacción dentro de Webmail.

Bloquear imágenes HTML
Habilite esta opción si desea impedir que se desplieguen automáticamente imágenes remotas al visualizar mensajes de correo con formato HTML, en Webmail. Con el fin de visualizar las imágenes, el usuario deberá dar clic en la barra que aparece arriba del mensaje en la ventana del navegador. Esta es una función para prevenir el Spam, porque muchos mensajes de Spam contienen imágenes con URLs especiales que identifican la dirección de correo del usuario que las visualizó, confirmando al spammer que es una dirección válida. Esta opción está habilitada por omisión.

> **...excepto cuando el encabezado De coincide con un contacto en la lista de Remitentes Permitidos del dominio o del usuario**
> Marque esta casilla si desea permitir que se desplieguen en automático las imágenes en mensajes cuando el encabezado De del mensaje coincide con un contacto que se encuentra en la lista de Remitentes Permitidos del dominio o del usuario. **Nota:** Esta opción solo está disponible en MDRA 354.

Deshabilitar hipervínculos en spam y mensajes que fallan la autenticación DMARC, DNSBL, o SPF
Por omisión, cuando se marca un mensaje como spam o falla la verificación DMARC 545, DNS-BL 701, o SPF 526, los hipervínculos contenidos en el mensaje serán deshabilitados. Deshabilite esta casilla si no desea deshabilitar los hipervínculos en esos mensajes. **Nota:** Esta opción solo está disponible en MDRA 354.

> **...excepto cuando el encabezado De coincide con un contacto en la lista de Remitentes Permitidos del dominio o del usuario**
> Marque esta casilla si desea exentar a los mensajes marcados de que se deshabiliten los hipervínculos cuando el encabezado De del mensaje coincide con un contacto en la lista de Remitentes permitidos del dominio o del usuario. **Nota:** Esta opción solo está disponible en MDRA 354.

Usar editor HTML cuando redacte nuevos mensajes
Haga clic en esta casilla si quiere que los usuarios vean la ventana de redacción HTML por defecto en Webmail. Pueden controlar la configuración por ellos mismos desde Opciones » Redactar dentro de Webmail.

Habilitar recuperación de contraseña
Si se habilita, los usuarios que tienen permisos para editar sus contraseñas[720] podrán registrar una dirección de correo alterna en Webmail, a la que se puede enviar una liga para restablecer su contraseña si la olvidan. Para configurar esta funcionalidad, los usuarios deben registrar tanto su dirección de correo de recuperación como su contraseña actual en la página Opciones » Seguridad de Webmail. Una vez configurada, la liga "olvidó su contraseña" en la página de inicio de sesión de Webmail los llevará a una página para confirmar la dirección de correo para recuperación de su contraseña. Si se registra correctamente, se enviará un mensaje con una liga a una página para modificar la contraseña. Esta funcionalidad está habilitada por omisión.

Puede habilitar o deshabilitar esta opción por usuario agregando la llave siguiente en el archivo `user.ini` del usuario en Webmail (ej. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (o "=No" para deshabilitar la opción
para este usuario)
```

Permitir Recuérdame en la Autentificación de Dos Factores (también aplica a Administración Remota)
Cuando alguien utiliza Autentificación de Dos Factores (2FA) al iniciar sesión en Webmail o Administración Remota, normalmente se tiene la opción Recuérdame disponible para el usuario en la página de autentificación 2FA, lo que impedirá que el servidor requiera 2FA de nuevo de ese usuario durante un número determinado de días (ver la opción *"Habilitar Recuérdame*" abajo). Deshabilite esta casilla si no desea desplegar la opción Recuérdame 2FA, lo que significa que todos los usuarios con 2FA habilitada deberán ingresar su código 2FA cada vez que inicien sesión. Nota: Esta opción solo está disponible en la interface web de MDaemon Remote Administration (MDRA)[354].

Habilitar Recuérdame
Marque esta casilla si desea que se presente la opción *Recuérdame* en la página de inicio de sesión de MDaemon Webmail cuando los usuarios se conecten vía el puerto https[328]. Si los usuarios marcan esta casilla al iniciar sesión, sus credenciales serán recordadas en ese dispositivo. Entonces, cada vez que utilicen el dispositivo para conectarse a Webmail, se abrirá su sesión automáticamente, hasta el momento en que cierren la sesión manualmente o en que expire el token de Recuérdame de su cuenta.

Por omisión, las credenciales de usuario se recuerdan un máximo de 30 días antes que se force al usuario a iniciar sesión de nuevo. Si desea incrementar el tiempo de expiración, lo puede hacer modificando el valor de la opción *Los tokens de Recuérdame expiran luego de estos días* en la interface web de MDaemon Administración Remota (MDRA)[354]. También puede modificarlo editando la llave `RememberUserExpiration=30` en la sección `[Default:Settings]` del archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. El valor de expiración se puede configurar a un máximo de 365 días. **Nota:** La Autentificación de dos Factores[720] (2FA) cuenta con su propia llave de expiración de Recuérdame (`TwoFactorAuthRememberUserExpiration=30`), localizada en la sección `[Default:Settings]` del archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. Por esto, 2FA requerirá de nuevo el inicio de sesión cuando expire el token Recuérdame de 2FA, aun cuando el token regular aun sea válido.

La opción *Recuérdame* se encuentra deshabilitada por omisión y aplica a todos sus dominios. Si desea configurar este ajuste para dominios específicos utilice el ajuste *Recuérdame* localizado en la pantalla de Administrador de Dominios de Webmail 201.

Dado que *Recuérdame* permite a los usuarios tener una sesión persistente en múltiples dispositivos, se deberá sugerir a los usuarios que no utilicen esta funcionalidad en redes públicas. Más aun, si en algún momento sospecha que una cuenta está comprometida, en MDRA se cuenta con un botón para *Restablecer Recuérdame,* que puede utilizar para restablecer los tokens de Recuérdame para todos los usuarios. Esto requerirá que todos los usuarios inicien sesión de nuevo.

Habilitar la Carpeta Documentos
La carpeta Documentos está disponible por omisión para los usuarios de Webmail. Esta opción controla el estado por omisión, por dominio, de la opción del mismo nombre localizada en la página de Administración de Dominios en Webmail 201. Si modifica ese ajuste para un dominio específico se omitirá el ajuste global para ese dominio. **Nota:** Esta opción y la de Hipervínculos de Documentos abajo, solo están disponibles en la interface web MDaemon Administración Remota (MDRA) 354 .

Permitir a los usuarios crear hipervínculos temporales a sus documentos personales
Cuando se habilita esta opción, los usuarios podrán crear hipervínculos a sus documentos personales, que podrán compartir con cualquier persona. Los hipervínculos mayores de 30 días se depuran automáticamente.

Ver Hipervínculos de Documentos
Dé clic en este botón para desplegar la página Hipervínculos de Documentos, que contiene una lista de todos los hipervínculos de documentos activos. Desde esa página puede revocar cualquier hipervínculo que elija. Los hipervínulos mayores de 30 días se revocarán automáticamente.

Entregar firma de cliente
Marque esta casilla si desea entregar la Firma de Cliente por Omisión 147 a los usuarios de Webmail. En Webmail, esto creará una firma llamada "Sistema" bajo las opciones de firma en: **Opciones » Redacción**. Entonces, los usuarios pueden elegir que se inserte esta firma en automático en la vista de redacción al preparar un mensaje nuevo. Si desea personalizar o habilitar/deshabilitar la firma de cliente para dominios específicos, utilice las Firmas de Cliente 215 del Administrador de Dominios y las opciones en Webmail 201.

Permitir firmas creadas por los usuarios
Marque esta casilla si desea permitir a los usuarios crear sus propias firmas personalizadas en Webmail. Entonces, los usuarios pueden elegir qué firma desea insertar en automático en la vista de redacción al redactar mensajes. Cuando no permite las firmas creadas por el usuario, pero la opción ya mencionada *Entregar firma de cliente* se encuentra habilitada, solo la Firma de Cliente 147 (i.e. la firma "Sistema" en Webmail) puede ser insertada en automático. En Webmail, las opciones de firma se encuentran en: **Opciones » Redacción**.

Permitir a los usuarios editar los nombres de despliegue de sus alias
Marque esta casilla si desea permitir a los usuarios editar el nombre de despliegue de cualquier alias asociado con su cuenta. Pueden hacerlo utilizando la opción *Editar Nombre de Despliegue de Alias*, localizada en el tema Pro de Webmail, bajo Ajustes » Redacción. Esta opción está deshabilitada por omisión. **Nota:** Esta opción solo está disponible en la interface web de MDaemon Administración Remota (MDRA) 354.

Habilitar funcionalidades de IA en mensajes
Marque esta casilla si desea habilitar el soporte de MDaemon a Funcionalidades de IA en Mensajes en MDaemon Webmail, para todos sus dominios. Puede ignorar este ajuste para dominios específicos utilizando la opción del mismo nombre ubicada en la pantalla Ajustes de Webmail 201 en el Administrador de Dominios. **Nota:** al habilitar el soporte a las Funcionalidades IA en Mensajes para un dominio no se otorga acceso a todos los usuarios del dominio. Debe activar la opción *Habilitar funcionalidades de IA en mensajes* en la pantalla Servicios Web 720 del editor de cuentas si desea permitirle usarlos. Alternativamente, puede utilizar las funcionalidades de Plantillas de Cuentas 791 y Grupos 781 para asignar usuarios a un grupo que tenga acceso a las funcionalidades de IA en mensajes. Ver: "Funcionalidades de IA en Mensajes en Webmail 352" abajo para obtener información importante y precauciones sobre el uso de estas funcionalidaes.

El listado de mensajes muestra esta cantidad de mensajes por página
Este es el número de mensajes que se enlistarán en cada página del Listado de Mensajes para cada una de sus carpetas de correo. Si una carpeta contiene más de este número de mensajes, entonces se presentarán controles arriba y abajo del listado que le permitirán moverse a las otras páginas. Los usuarios individuales pueden modificar este parámetro en Opciones » Personalizar desde Webmail.

Frecuencia de refresco del listado de mensajes (en minutos)
Esta es la cantidad de minutos que esperará Webmail antes de refrescar automáticamente el Listado de Mensajes. Los usuarios individuales pueden modificar este parámetro desde Opciones » Personalizar desde Webmail.

Texto de 'Ayuda' cuando falla el inicio de sesión (puede contener código HTML)
Puede utilizar esta opción para especificar una oración (ya sea en texto plano o HTML) para desplegar en la página de inicio de sesión de Webmail cuando un usuario tenga problemas para ingresar. El texto se despliega bajo el siguiente texto por omisión: "*Registro incorrecto, por favor intente de nuevo. Si requiere ayuda por favor contacte a su administrador de correo*". Este texto puede utilizarse para dirigir a los usuarios a una página o información de contacto para ayudarles a ingresar a Webmail.

Ajustes de Seguridad (**Nota:** Las opciones en esta sección solo están disponibles en la interface web de MDaemon Administración Remota (MDRA) 354.)

Permitir WebAuthn al inicio de sesión
Marque esta casilla si desea permitir que los usuarios de MDaemon Webmail inicien sesión utilizando la API de Autenticación Web (también conocida como WebAuthn), que les da una experiencia segura de inicio de sesión sin contraseña, permitiéndoles utilizar biométricos, llaves de seguridad USB, Bluetooth y otras opciones para autenticación. WebAuthn está habilitada por omisión.

Solicitar a los usuarios registrar el dispositivo actual al primer inicio de sesión
Marque esta casilla si desea solicitar a los usuarios registrar su dispositivo actual (teléfono, biométricos, etc.) para inicio de sesión sin contraseña cuando inician sesión por primera vez en su cuenta.

Permitir que el inicio de sesión con WebAuthn omita la página de Autenticación de Dos Factores
Dado que WebAuthn ya es una forma de autenticación multi-factor, utilizar otra Autenticación de Dos Factores (2FA) luego de que el usuario ya ha utilizado WebAuthn para iniciar sesión se puede considerar como redundante o excesivo para algunos usuarios o administradores. Por esto, puede marcar esta casilla si desea omitir 2FA cuando alguien utiliza WebAuthn al iniciar sesión. **NOTa:** Sin importar este ajuste, cuando una cuenta está configurada específicamente para *Requerir Autenticación de Dos Factores* 720, esa cuenta no podrá omitir 2FA, aún cuando esté utilizando WebAuthn para iniciar sesión.

Visite: **webauthn.guide**, para más información sobre WebAuthn y como funciona.

Habilitar recuperación de contraseñas
Si se habilita, los usuarios que tengan permiso para editar su contraseña 720 podrán registrar una dirección alterna de correo en Webmail, a la que se enviará una liga para restablecer su contraseña si la olvidan. Para habilitar esta funcionalidad, los usuarios deben registrar la dirección de correo de recuperación de contraseña y su contraseña actual en la página Opciones » Seguridad en Webmail. Una vez establecidas, si el usuario intenta iniciar sesión en Webmail con una contraseña incorrecta, aparecerá una liga con el texto "¿olvidó su contraseña?". Esta liga los llevará a una página que les pide confirmar la dirección de correo de recuperación de contraseña. Si se registra correctamente, se le enviará un mensaje con una liga hacia la página para modificar la contraseña. Esta funcionalidad está deshabilitada por omisión.

Puede habilitar o deshabilitar esta opción por usuario agregando la llave siguiente al archivo `user.ini` del usuario en Webmail (ej. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (o "=No" para deshabilitar la opción
para el usuario)
```

Permitir que los usuarios de Active Directory modifiquen sus contraseñas desde Webmail
Cuando esta casilla se habilita/deshabilita, los usuarios cuyas cuentas están configuradas para utilizar autentificación de Active Directory, pueden utilizar la opción de Webmail "Modificar Contraseña". Cuando esta opción está deshabilitada, solo los usuarios cuyas contraseñas se definan en MDaemon en lugar de Active Directory, podrán modificar su contraseña desde Webmail. El Administrador de Dominios cuenta con una opción con el mismo nombre 201 que se puede utilizar para ignorar este ajuste para dominios específicos.

Permitir a los usuarios visualizar sus contraseñas al teclearlas
Cuando está habilitada esta opción, el campo contraseña en la página de inicio de sesión de Webmail tiene un ícono en el que el usuario puede dar clic para

hacer visible la contraseña tecleada. Deshabilite esta casilla si no desea permitir que la contraseña se vea.

Permitir a los usuarios recibir por correo códigos de verificación de Autenticación de dos factores
Por omisión, se permite a los usuarios registrar una dirección de correo alternativa en Webmail al configurar la Autenticación de Dos Factores, de manera que pueden recibir códigos de verificación vía correo en lugar de tener que utilizar la app Autenticador de Google. Deshabilite esta opción si no desea permitir los códigos de verificación vía correo electrónico. Puede omitir esta opción por separado para cada uno de sus dominios utilizando la opción del mismo nombre en la página Ajustes de Webmail en el Administrador de Dominios.

El código de Autentificación de Dos Factores enviado por correo expira luego de: [xx] minutos
Al recibir los códigos de Autentificación de Dos Factures vía correo, este es el lapso que tendrá el usuario para registrarlo antes de que expire. Por omisión está configurado a **10** minutos.

Permitir WebAuthn para la Autenticación de Dos Factores
Marque esta casilla si desea permitir que los usuarios de MDaemon Webmail utilicen la API de Autenticación Web (también conocida como WebAuthn) para la autenticación de dos factores. WebAuthn permite a los usuarios utilizar datos biométricos, llaves de seguridad USB, Bluetooth y más, para autenticación. WebAuthn está habilitada por omisión para la autenticación de dos factores.

Por seguridad, no puede utilizar el mismo método de autenticación para el inicio de sesión sin contraseña y para la autenticación de dos factores. Por esto, si desea utilizar ambas opciones, deberá elegir un método distinto de autenticación para cada una de ellas.

Visite: **webauthn.guide**, para más información sobre WebAuthn y como funciona.

Permitir Recuérdame en Autentifición de Dos Factores (también aplica para Administración Remota)
Cuando alguien utiliza la Autenticación de Dos Factores (2FA) al iniciar sesión en Webmail o Administración Remota, normalmente existe la opción Recuérdame disponible para el usuario en la página de autentificación 2FA, lo que impedirá al servidor requerir 2FA de nuevo de ese usuario durante un número determinado de días (ver la opción abajo "*Expirar tokens de Recuérdame luego de estos días*"). Deshabilite esta casilla si no desea desplegar la opcíon Recuérdame en 2FA, lo que snigifica que los usuarios con 2FA habilitada deberán ingresar un código 2FA cada vez que inicien sesión.

Funcionalidades IA en Mensajes de Webmail

Al igual que MDaemon 23.5.0, el tema Pro en el cliente Webmail de MDaemon incluye varias funcionalidades de Inteligencia Artificial (IA para ayudar a sus usuarios a administrar su correo e incrementar la productividad. Estas funcionalidades son opcionales y están deshabilitadas por omisión, pero se pueden habilitar para

cualquier usuario.

Con estas funcionalidades, en MDaemon Webmail puede utilizar IA :

- Generar un resumen de los contenidos de un mensaje de correo.
- Sugerir una respuesta al mensaje, de acuerdo a varios lineamientos que le puede indicar a la IA. También puede definir el *Tono* de la respuesta ya sea profesional respetuoso o casual. La *Posición*, o sentido de la respuesta puede definirse como interesado, no interesado, de acuerdo, en desacuerdo o escéptico. La respuesta con *Actitud* podrá definirse como confiado, emocionado, calmado o arrepentido. Por último, puede definir la *Longitud* de la respuesta, que puede ser desde muy breve a detallada.
- Puede ayudar a redactar un nuevo mensaje de correo, con base en algún texto que ya se haya incluido. Al igual que en la opción mencionada *Sugerir Respuesta*, también se puede definir el Tono, Posición, Actitud y Longitud como criterios a utilizar por la IA al redactar el mensaje.

La opción *Habilitar funcionalidades de IA en Mensajes* en la pantalla Ajustes de Webmail 345 controla si está o no habilitado el soporte a las funcionalidades de IA por omision para sus dominios. Existe una opción con el mismo nombre localizada en el diálogo Webmail 201 del Administrador de Dominios, que se puede utilizar para ignorar el ajuste principal para dominios específicos. **Nota:** el habilitar el soporte a Funcionalidades IA en Mensajes no garantiza acceso a ellas para todos los usuarios del dominio. Se deberá activar la opción *Habilitar funcionalidades IA en mensajes* en la pantalla Servicios Web 720 del editor de cuentas para los usuarios a los que desee dar permiso. Alternativamente, puede utilizar las opciones de Plantillas de Cuentas 791 y Grupos 781 para asignar usuarios a un grupo que tenga acceso a funcionalidades IA en mensajes.

Cuando se habilitan en MDaemon las cuentas para utilizar las funcionalidades IA en mensajes se permite a los usuarios enviar y recibir información para y de servicios generativos IA de terceros, específicamente ChatGPT de OpenAI. Los Administradores y usuarios deberán estár conscientes de que esto introduce varios temas de privacidad debido a la habilidad de la funcionalidad de procesar datos personales y generar información potencialmente sensitiva. Para resolver los temas de privacidad, es vital que las organizaciones capaciten a sus empleados para usar IA con responsabilidad. **Nota:** Los datos enviados para/de Open AI no se almacenan en el servidor local o en nuestra red.

Puede encontrar la Política de Uso de MDaemon Technologies en la Página Artifical Intelligence (AI) Information. En esa misma página existe una liga a los Terminos de Uso de OpenAI.

Personalizar Carpetas de Remitentes Permitidos y Bloqueados

Existen varias funcionalidades estándar que se pueden personalizar editando ciertos archivos en la carpeta `MDaemon\WorldClient\`:

Puede ocultar para los usuarios de Webmail, las carpetas de Remitentes Permitidos y Bloqueados por omisión. Para esto, abra el archivo `MDaemon\WorldClient\Domains.ini y bajo [Default:UserDefaults]` modifique el valor de "`HideWhiteListFolder=`" o "`HideBlackListFolder=`" de "`No`" a "`Yes`". Puede ocultar o mostrar estas carpetas para usuarios específicos editando esas mismas llaves en el archivo `User.ini` en la sección `[User]`.

Ver:

Administrador de Dominios » Ajustes de Webmail 201

3.6.1.11 Logo Corporativo

Si desea personalizar las imágenes de Webmail que aparecen en la página de inicio y en la barra lateral de navegación, lo puede hacer desde la página Logo Corporativo en la interface web de la Administración Remota 354 de MDaemon.

Para utilizar sus imágenes personalizadas:

1. Dé clic en **Utilizar imágenes personalizadas** en la sección Personalizar.
2. En la sección Imagen de la Página de inicio de sesión, utilice la opción **Elegir Archivo** o **Navegar** (dependiendo de su navegador) para seleccionar el archivo que desea cargar. Esta sección también enlista el tamaño por omisión de cada imagen.
3. Dé clic en **Cargar Imagen Personalizada**.
4. Repita los pasos 2 y 3 para las Imágenes del fondo de la página de inicio de sesión, la Barra Lateral de Navegación y de la Barra de Navegación Lateral.

Las imágenes cargadas aparecerán en las posiciones correspondientes y serán utilizadas en lugar de las imágenes por omisión de Webmail.

3.6.2 Administración Remota

La interface web MDaemon Administración Remota está diseñada para permitirle administrar MDaemon remotamente utilizando un navegador web. Es una aplicación que corre en el servidor, diseñada para correr en segundo plano en el mismo equipo donde corre MDaemon. Para ingresar a la Administración Remota, abra su navegador en la URL y número de puerto en las que se haya configurado la administración

remota (v.g. `www.example.com:1000`). Luego de proporcionar sus credenciales, tendrá acceso a varios controles y ajustes de MDaemon. El tipo y número de ajustes a los que tendrá acceso dependen del nivel de acceso que le hayan dado. Existen tres niveles de acceso para ingresar a la Administración Remota: Global, de Dominio y de Usuario.

Administradores Globales — Los administradores globales son usuarios que tienen permiso de acceso global activado bajo sus configuraciones de cuenta dentro de MDaemon. Acceso global significa que puede ver y configurar cada opción y control que sea accesible vía MDaemon Administración Remota. Los administradores globales pueden añadir, y borrar usuarios, dominios y listas de distribución. Pueden editar los archivos INI de producto, designar otros usuarios como administradores de Dominio, gestionar contraseñas y muchas otras cosas; tienen completo control administrativo.

Administradores de Dominio — Similar a los Administradores Globales, los Administradores de Dominio tienen completo control sobre los usuarios y ajustes accesibles vía MDaemon Administración Remota. Su control administrativo, sin embargo, se limita al dominio o dominios a los que se les haya dado acceso y los permisos definidos en la pantalla Servicios Web 720. Los Administradores de Dominio y los dominios sobre los que tienen control se designan desde dentro de MDaemon Administración Remota por un Administrador Global, o bien por otro Administrador de Dominio con acceso a esos dominios.

Usuarios — El nivel más bajo posible de acceso a MDaemon Administración Remota es Usuario. Los usuarios de MDaemon pueden acceder a MDaemon Administración Remota y, por ejemplo, ver sus configuraciones individuales de cuenta, así como editar sus entradas de MultiPOP, filtros de correo, autorespuestas y demás. El tipo y número de configuraciones que pueden ser editadas depende de los permisos que se den a cada una de las configuraciones de cuenta.

Todo el que tenga permisos para acceder tanto a Webmail como a MDaemon Administración Remota puede acceder a MDaemon Administración Remota desde Webmail, en lugar de tener que firmarse a cada uno por separado. La Administración Remota se abrirá en una ventana de navegador separada desde Webmail si hace clic en el enlace "Configuración Avanzada" dentro de "Opciones".

Ver:

Administración Remota » Servidor Web 356

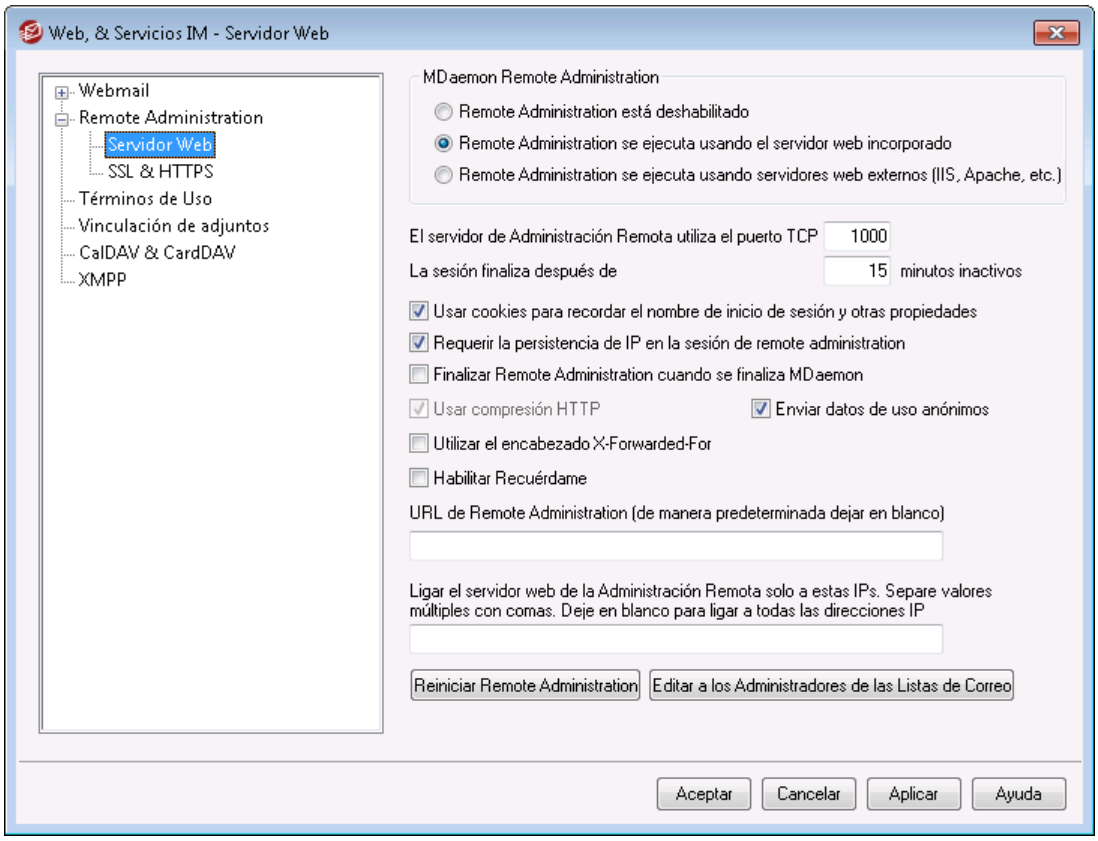
Administración Remota » HTTPS 361

Administrador de Plantillas » Servicios Web 798

Editor de Cuentas » Servicios Web 720

Artículo de la Base de Conocimientos: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS

3.6.2.1 Servidor Web



MDaemon Administración Remota

MDaemon Administración Remota está deshabilitada
Escoja esta opción para deshabilitar MDaemon Administración Remota. También puede cambiar entre activa/inactiva para MDaemon Administración Remota desde el menú Archivo, o desde la sección Servidores de la pantalla de Estatus en la interfaz principal de MDaemon.

MDaemon Administración Remota se ejecuta usando el servidor web incorporado
Escoja esta opción para utilizar el servidor web incorporado. También puede alternar entre los estados activo/inactivo de MDaemon Administración Remota desde el menú Archivo, o desde la sección Servidores de la pantalla de Estatus de la interfaz principal de MDaemon.

MDaemon Administración Remota se ejecuta usando servidores web externos (IIS, Apache, etc.)
Escoja esta opción cuando desee ejecutar MDaemon Administración Remota bajo Internet Information Server (IIS) u otros servidores web en lugar del servidor integrado de MDaemon. Esto previene a ciertos elementos de entorno de ser accedidos y que podría causar conflictos con sus servicios alternos.

Para más información, vea el artículo de la Base de Conocimientos: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS.

MDaemon Administración Remota utiliza este puerto TCP
Este es el puerto en el cual MDaemon Administración Remota escuchará conexiones de su navegador web. El puerto por defecto es 1000.

La sesión finaliza después de xx minutos inactivos
Cuando está identificado en MDaemon Administración Remota, esta es la cantidad de tiempo que se le permite a su sesión estar inactiva antes de que MDaemon Administración Remota la cierre. Por defecto son 15 minutos.

Ajustes de Seguridad

Nota: Las opciones en esta sección están disponibles en la interface web MDaemon Administración Remota (MDRA) 354.

Usar tokens CSRF (Cross-Site-Request-Forgery)
Por omisión, se utilizan tokens CSRF (falsificación de petición de sitios cruzados o Cross-Site-Request-Forgery) para tener transacciones más seguras y prevenir ataques CSRF.

Permitir a los usuarios visualizar sus contraseñas cuando las teclean
Por omisión, los usuarios pueden dar clic a un ícono para visualizar los caracteres de la contraseña que están tecleando a iniciar sesión el la interface web de la administración remota. Deshabilite esta casilla si no quiere permitir esto.

Permitir WebAuthn al iniciar sesión
Marque esta casilla si desea permitir que los usuarios de MDRA inicien sesión utilizando la API de Autenticación Web (también conocida como WebAuthn), que les da una experiencia segura de inicio de sesión sin contraseña, permitiendo utilizar para autenticación biométricos, llaves de seguridad USB, Bluetooth y más. WebAuthn está habilitada por omisión.

Permitir que el inicio de sesión con WebAuthn omita la página de Autenticación de Dos Factores
Dado que WebAuthn ya es una forma multi-factor de autenticación, el utilizar otra forma de Autenticación de Dos Factores (2F) al iniciar sesión se puede considerar redundante o excesivo para algunos usuarios o administradores. Por esto, puede marcar esta casilla si desea omitir 2FA cuando alguien utiliza autenticación WebAuthn al iniciar sesión. **NOTA:** Sin importar este ajuste, cuando una cuenta está configurada específicamente para *Requerir Autenticación de Dos Factores* 720, esa cuenta no podrá omitir 2FA, aún cuando esté utilizando WebAuthn.

Permitir WebAuthn para Autenticación de Dos Factores
Marque esta casilla si desea permitir que los usuarios de MDRA utilicen la API de Autenticación Web (también conocida como WebAuthn) para la autenticación de dos factores. WebAuthn permite a los usuarios utilizar para autenticación biométricos, llaves de seguridad USB, Bluetooth y más. WebAuthn está habilitada por omisión para la autenticación de dos factores.

Por seguridad, no puede utilizar el mismo método de autenticación para el inicio de sesión sin contraseña y la autenticación de dos factores. Por esto, si desea utilizar ambas opciones debe elegir un método distinto de autenticación para cada una.

> Visite: **webauthn.guide**, para más información sobre WebAuthn y como funciona.

Habilitar Recuérdame
Marque esta casilla si desea que se presente una casilla para habilitar *Recuérdame* en la página de inicio de MDaemon Administración Remota (MDRA) cuando os usuarios se conecten vía puertos https. Si los usuarios marcan esta casilla al iniciar la sesión, sus credenciales serán recordadas en ese dispositivo. Entonces, cada ve que utilicen ese dispositivo para conectarse a MDRA en el futuro, iniciarán sesión automáticamente, hasta el momento en que manualmente cierren la sesión de su cuenta o su token Recuérdame expire. La opción *Recuérdame* está deshabilitada por omisión.

Los tokens de Recuérdame expirarán luego de estos días
Utilice esta opción para definir el número de días que serán recordadas las credenciales de sus usuarios. Por omisión, las credenciales se recuerdan durante un máximo de 30 días antes de que el usuario sea obligado a iniciar sesión de nuevo. Esta opción se puede configurar a un máximo de 365 días. **Nota:** La Autentificación de Dos Factores (2FA) cuenta con su propia llave de expiración para Recuérdame (`TwoFactorAuthRememberUserExpiration=30`), localizada en la sección `[Default:Settings]` del archivo `Domains.ini`, que se ubica en la carpeta `\MDaemon\WorldClient\`. Por esta razón, 2FA se requerirá al inicio de sesión cuando expire el token Recuérdame de 2FA, aun cuando el token regular aun sea válido.

Restablecer Recuérdame
Dé clic en este botón si sospecha que una cuenta puede haber sufrido un fallo de seguridad. Así se restablecerán los tokens de Recuérdame para todos los usuarios, haciéndolos que inicien sesión de nuevo.

> Dado que *Recuérdame* permite a los usuarios tener un inicio de sesión persistente en múltiples dispositivos, se deberá desalentar a los usuarios de utilizar esta funcionalidad en redes públicas.

Ajustes Misceláneos

Usar cookies para recordar el nombre de inicio de sesión y otras propiedades
Por omisión la interface de la Administración Remota utiliza cookies de manera que el navegador del usuario pueda recordar las credenciales y otras propiedades. Deshabilite esta casilla si no desea utilizar cookies. El utilizar esta funcionalidad da a los usuarios una experiencia de inicio de sesión personalizada, pero requiere que tengan habilitadas las cookies en su navegador.

Requerir persistencia de IP en la sesión de MDaemon Administración Remota
Como una medida de seguridad adicional puede hacer clic en esta casilla para causar que MDaemon Administración Remota restrinja cada sesión a la dirección IP desde la cual se conectó cuando la inició. Así, nadie puede "robar" la sesión puesto que se requiere la persistencia de IP. Esta configuración es más segura, pero podría causar problemas si utiliza un servidor proxy o una conexión a Internet que asigne y cambie dinámicamente las direcciones IP..

Detener MDaemon Administración Remota cuando se detiene MDaemon
Haga clic en esta opción si desea que se apague MDaemon Administración Remota siempre que se apague MDaemon. De otra forma, MDaemon Administración Remota continuará ejecutándose en segundo plano.

Utilizar compresión HTTP
Dar clic en esta casilla si desea utilizar compresión HTTP en sus sesiones de Administración Remota.

Notificar de nuevas versiones en la página de Inicio de Sesión
Por omisión, en la página de inicio de sesión se notificará cuando están disponibles nuevas versiones de MDaemon. Deshabilite esta casilla si no quiere ser notificado ahí. **Nota:** Esta opción está disponible en la interface web de MDaemon Administración Remota (MDRA) 354.

Enviar datos de uso anónimo
Por omisión el cliente web de MDaemon Administración Remota envía datos anónimos, benignos de datos de uso tales como: el sistema operativo utilizado, versión del navegador, idioma y similares. Estos datos son utilizados por MDaemon Technologies para ayudar a mejorar la Administración Remota. Deshabilite esta opción si no desea enviar datos de uso anónimo.

Obtener la IP del encabezado X-Forwarded-For cuando se encuentre
De clic en esta casilla para habilitar el uso del encabezado `X-Forwarded-For`, que en ocasiones es agregado por servidores proxy. Esta opción se encuentra deshabilitada por omisión. Habilítela solo si su servidor proxy inserta este encabezado.

Habilitar Recuérdame
Marque esta casilla si desea que se presente una casilla de verificación al inicio de sesión de la Administración Remota, para habilitar la función *Recuérdame* cuando los usuarios se conecten vía puertos https 361. Si los usuarios marcan esta casilla al iniciar sesión, las credenciales serán recordadas para ese dispositivo. Entonces, cada vez que utilice ese dispositivo para conectarse en el futuro, su sesión iniciará automáticamente, hasta el momento en que cierre sesión manualmente o su token de Recuérdame expire.

Por omisión, las credenciales de usuario serán recordadas por un máximo de 30 días antes de que el usuario sea obligado a iniciar sesión de nuevo. Si desea incrementar el tiempo de expiración, lo puede hacer modificando el valor de la opción *Los tokens Recuérdame expiran luego de estos días* en la interface web de MDaemon Administración Remota (MDRA). Puede modificarlo manualmente editando la llave `RememberUserExpiration=30` en la sección `[Default:Settings]` del archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. El valor de expiración se puede configurar a un máximo de 365 días. **Nota:** La Autentificación de Dos Factores 720 (2FA) cuenta con su propia llave de expiración para Recuérdame (`TwoFactorAuthRememberUserExpiration=30`), localizada en la sección `[Default:Settings]` del archivo `Domains.ini`, localizado en la carpeta `\MDaemon\WorldClient\`. Por esto, 2FA será requerido nuevamente al iniciar sesión cuando el token 2FA expire, aun cuando el token regular aun sea válido.

La opción *Recuérdame* se encuentra deshabilitada por omisión.

Dado que *Recuérdame* permite a los usuarios contar con un inicio de sesión persistente en múltiples dispositivos, los usuarios deberán ser desalentados de utilizarlo en redes públicas. Más aun, si llega a sospechar que una cuenta ha tenido un fallo de seguridad, en MDRA se cuenta con un botón *Restablecer Recuérdame* que puede utilizar para restablecer los tokens Recuérdame para todos los usuarios. Esto requerirá que todos los usuarios inicien sesión de nuevo.

URL de MDaemon Administración Remota
Esta es la URL que MDaemon Administración Remota utilizará internamente cuando los usuarios hagan clic en la Configuración Avanzada para editar sus configuraciones de cuenta a través de MDaemon Administración Remota. Si está ejecutando MDaemon Administración Remota en un servidor integrado, deje este campo en blanco. Si está utilizando un servidor web alternativo como IIS, y ha configurado MDaemon Administración Remota para ejecutarse en una URL o IP alternativa, entonces especifique la URL aquí.

Enlazar el servidor de red de MDaemon Administración Remota sólo a estas direcciones IP
Si desea restringir el servidor MDaemon Administración Remota sólo a ciertas direcciones IP, especifique aquellas direcciones aquí separadas por comas. Si deja este campo en blanco entonces MDaemon Administración Remota monitoreará todas las direcciones IP que haya designado para sus Dominios 190.

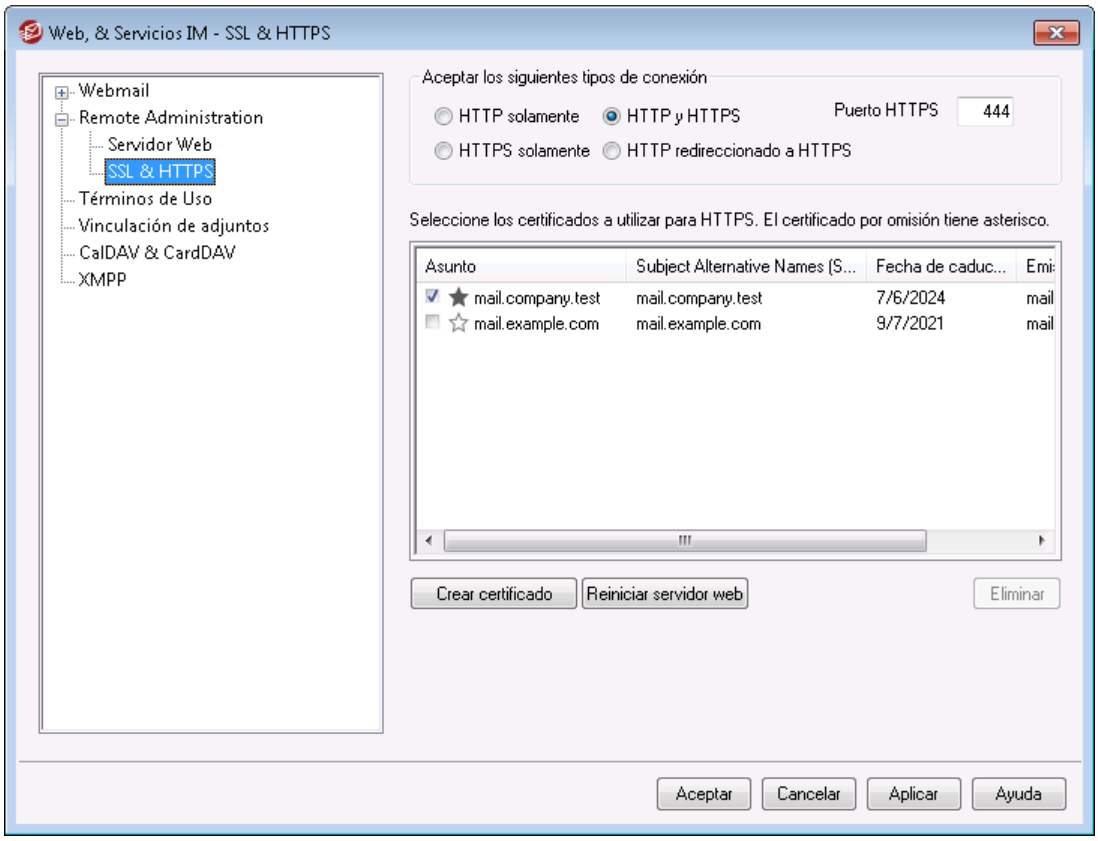
Reiniciar MDaemon Administración Remota (requerido cuando se cambia el puerto o el valor de IIS)
Haga clic en este botón si desea reiniciar el servidor MDaemon Administración Remota. Nota: cuando cambie la configuración de puerto debe reiniciar MDaemon Administración Remota para que las nuevas configuraciones sean reconocidas.

Editar Administradores de Listas de Distribución
Dé clic en este botón si desea abrir el archivo de la lista de Administradores de Listas de Distribución para visualizarlo o editarlo.

Ver:

MDaemon Administración Remota (configuración web) 354
MDaemon Administración Remota » HTTPS 361
Ejecutar MDaemon Administración Remota bajo IIS
Administrador de Plantillas » Servicios Web 798
Editor de Cuentas » Servicios Web 720
Artículo de la Base de Conocimientos: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS

3.6.2.2 SSL & HTTPS



El servidor web integrado en MDaemon soporta el protocolo Secure Sockets Layer (SSL). SSL es el método estándar de asegurar las comunicaciones web servidor/cliente. Proporciona autentificación de servidor, encripción de datos y autentificación opcional de cliente para conexiones TCP/IP. Más aun, dado que el soporte HTTPS (i.e. HTTP sobre SSL) está integrado en todos los principales navegadores, al instalar simplemente un certificado digital en su servidor, se activarán las capacidades de conexión SSL de los clientes.

Las opciones para habilitar y configurar la Administración Remota para utilizar HTTPS se localizan en la pantalla SSL & HTTPS bajo Configuración » Web & Servicios IM » Administración Remota". Para su conveniencia, sin embargo, estas opciones también se encuentran bajo "Seguridad » Ajustes de Seguridad » SSL & TLS » Administración Remota".

Para más información sobre el protocolo SSL y Certificados ver: **SSL & Certificados** 575

Esta pantalla solamente aplica para la Administración Remota al utilizar el servidor web integrado de MDaemon. Si configura la Administración Remota para utilizar algún otro servidor web tal como IIS, estas opciones no se utilizarán — el soporte a SSL/HTTPS tendrá que ser configurado

utilizando las herramientas del otro servidor web.

Aceptar los siguientes tipos de conexión

Solo HTTP
Seleccione esta opción si no desea permitir conexiones HTTPS para la Administración Remota. Solo se aceptarán conexiones HTTP.

HTTP y HTTPS
Seleccione esta opción si desea habilitar soporte SSL para la Administración Remota, pero no desea forzar a los usuarios de la Administración Remota a utilizar HTTPS. Administración Remota escuchará conexiones en el puerto HTTPS definido abajo, pero de todas maneras responderá a conexiones HTTP normales en el puerto TCP asignado para la Administración Remota en la pantalla Servidor Web 356.

Solo HTTPS
Seleccione esta opción si desea requerir HTTPS al conectarse a la Administración Remota. Esta responderá solo a conexiones HTTPS cuando esta opción esté habilitada — no responderá a peticiones HTTP.

HTTP redirigido a HTTPS
Seleccione esta opción si desea redirigir todas las conexiones HTTP a HTTPS en el puerto HTTPS.

Puerto HTTPS
Este es el puerto TCP en el que la Administración Remota escuchará las conexiones SSL. El puerto SSL por omisión es el 443. Si se utiliza este puerto, no tendrá que incluir el número de puerto en la URL de la Administración Remota al conectarse vía HTTPS (ej. "https://example.com" es equivalente a "https://example.com:443").

Este no es el mismo puerto para Administración Remota que se define en la pantalla Servidor Web 356. Si está permitiendo conexiones HTTP para la Administración Remota entonces esas conexiones deben utilizar ese otro puerto para conectarse exitosamente. Las conexiones HTTPS deben utilizar el puerto HTTPS.

Seleccionar certificado a utilizar para HTTPS/SSL

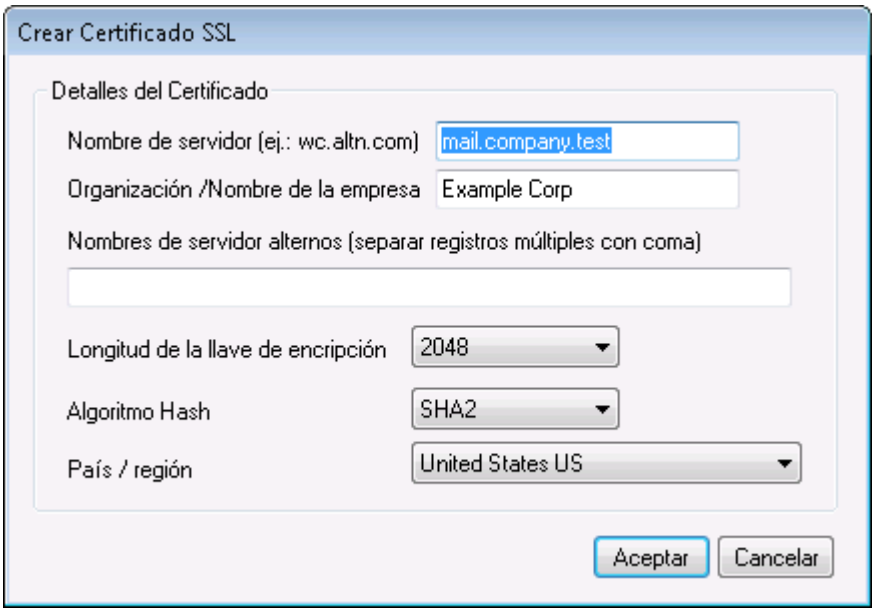
Esta caja muestra sus certificados SSL. Marque la casilla al lado de cualquier certificado que desee activar. Dé clic en la estrella al lado del que desea que se considere el certificado por omisión. MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite que se utilice un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará los certificados activos y elegirá el que contenga el nombre de host solicitado en el campo Subject Alternative Names (puede especificar los nombres alternos al crear el certificado). Si el cliente no solicita un nombre de host o si no se encuentra un certificado coincidente, se utilizará el certificado por omisión. Dé doble clic en cualquier certificado para abrirlo en el diálogo de Certificados de Windows, para revisarlo (solo disponible en la interface de escritorio, no en la administración remota

vía web).

Eliminar
Seleccione un certificado en la lista y dé clic en este botón para eliminarlo. Se abrirá una caja de conformación que le preguntará si está seguro de que desea eliminar ese certificado.

Crear Certificado

Dé clic en este botón para abrir el diálogo Crear Certificado .



Detalles del Certificado

Nombre de Servidor
Al crear un certificado, registre qué usuarios se conectarán (por ejemplo "wc.example.com").

Organización/nombre de empresa
Registre aquí la organización o empresa "propietaria" del certificado.

Nombres de servidor alternativos (separe múltiples registros con una coma)
Si se tienen nombres de host alternativos a los que se puedan conectar los usuarios y desea que este certificado aplique también para esos nombres, entonces registre aquí los nombres de dominio separados por comas. Se permiten comodines, de manera que "`*.example.com`" aplicará para todos los subdominios de `example.com` (por ejemplo, "`wc.example.com`", "`mail.example.com`"y demás).

MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite utilizar un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon revisará los certificados activos y elegirá el que contenga el nombre de host solicitado en el campo Subject Alternative Names. Si el cliente no solicita un nombre de host o no se encuentra un certificado

correspondiente, se utilizará el certificado por omisión.

Longitud de la llave de Encripción
Seleccione la longitud de bit deseada para la llave de encripción de este certificado. Mientras más larga sea más segura será la transferencia de datos. Note, sin embargo, que no todas las aplicaciones soportan longitudes de llave mayores de 512.

País/región
Elija el país o región en que reside su servidor.

Algoritmo Hash
Elija el algoritmo hash que desea utilizar: SHA1 o SHA2. El ajuste por omisión es SHA2.

Reiniciar el servidor web

Dé clic en este botón para reiniciar el servidor web. Este se debe reiniciar antes de utilizar el nuevo certificado.

Utilizar Let's Encrypt para Administrar su Certificado

Let's Encrypt es una autoridad de Certificación (Certificate Authority - CA) que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los procesos completos de creación, validación, firma y renovación manuales de certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se cuenta con la pantalla Let's Encrypt 594 para ayudarle a configurar y ejecutar fácilmente el script de PowerShell incluido en la carpeta "`MDaemon\LetsEncrypt`". Al ejecutar el script se configurará todo lo necesario para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta HTTP de Webmail para completar la validación http-01. Utiliza el Nombre de host SMTP 192 del dominio por omisión 190 como dominio para el certificado, incluye cualesquiera *Nombres de host Alternos* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para utilizar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" , denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora del inicio de ejecución del script. También, se envían mensajes de notificación de la ocurrencia de errores, si se especifica una *Cuenta de correo de Admin para notificaciones*. Vea el tema Let's Encrypt 594 para más información.

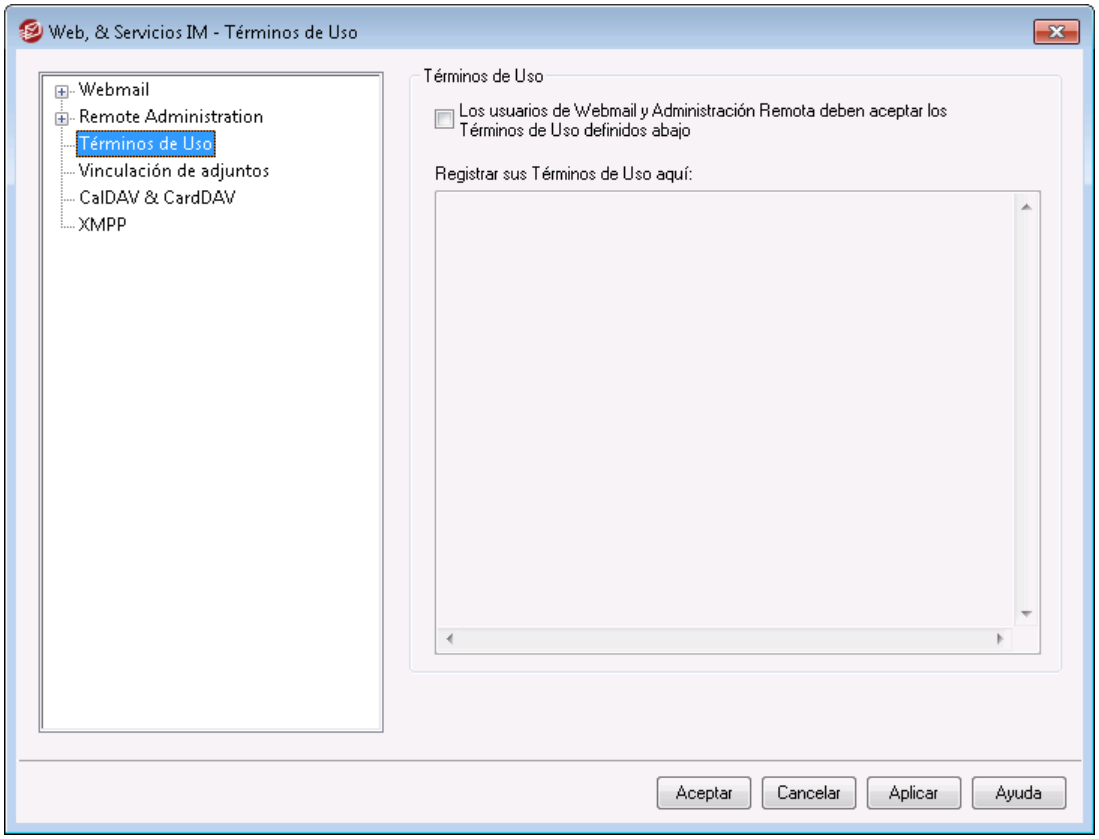
Para más información sobre SSL y Certificados ver:

SSL y Certificados 575
Crear y Utilizar Certificados SSL 912

Para más información sobre Administración Remota ver:

Configuración Remota 354
Administración Remota » Servidor Web 356
Valores por Omisión de Acceso Web 798
Editor de Cuentas » Web 720
Artículo de la Base de Conocimientos: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS

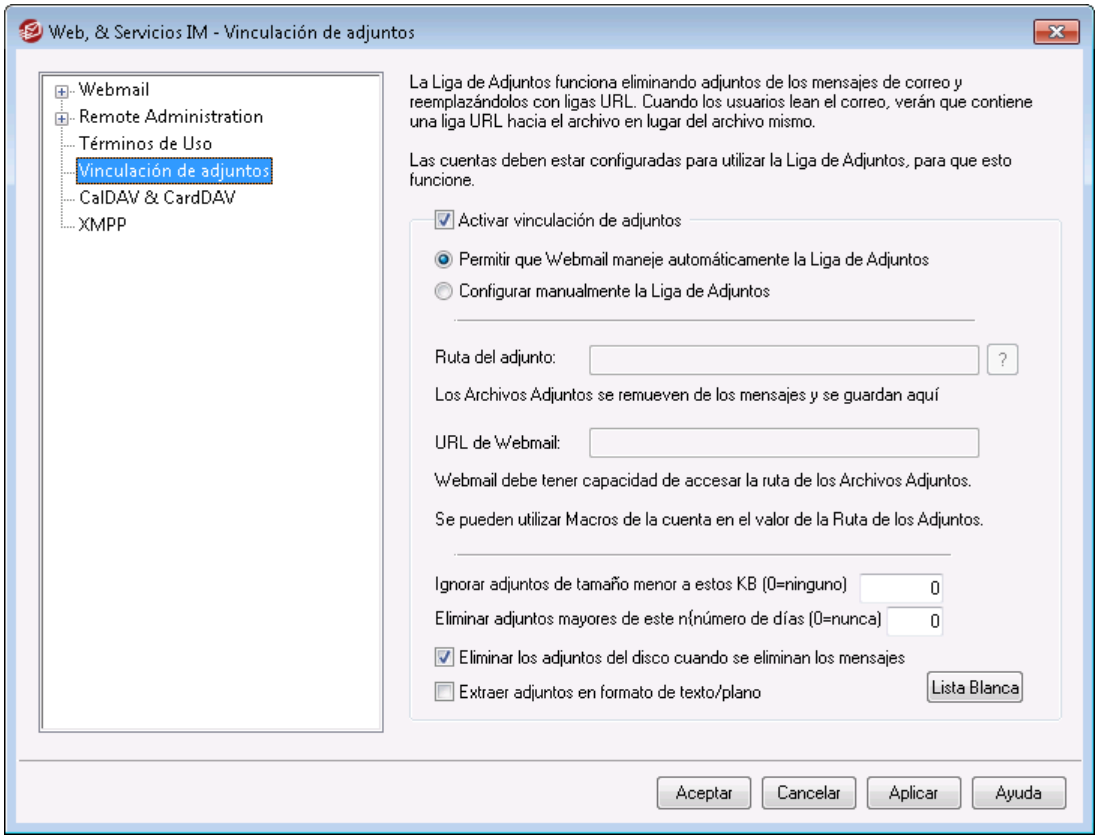
3.6.3 Términos de Uso



Los usuarios de Webmail y Administración Remota deben aceptar los Términos de Uso establecidos a continuación

Marque esta casilla y registre su declaración de Términos de Uso si desea requerir que los usuarios de Webmail y Administración Remota acepten la declaración de Términos de Uso cada vez que inicien sesión.

3.6.4 Vinculación de Adjuntos



La Vinculación de Adjuntos (Configuración » Web & Servicios IM » Vinculación de Adjuntos) es una opción que habilita que MDaemon remueva los archivos adjuntos del correo entrante, los guarde en una ubicación determinada y coloque una liga URL hacia esos archivos en cada uno de los mensajes de donde los extrajo. Los destinatarios pueden entonces dar clic a esas ligas para descargar los archivos. Esto puede acelerar de manera importante el procesamiento de correo cuando los usuarios reciben sus mensajes o sincronizan sus carpetas de correo, dado que los mensajes no llevarán archivos adjuntos que en ocasiones pueden ser muy grandes. También puede proporcionar seguridad mejorada y un mayor nivel de protección a los usuarios, dado que los adjuntos pueden guardarse en una ubicación centralizada para monitoreo por el administrador y no serán descargados en automático a los clientes de correo donde podrían ejecutarse en forma automática. Más aun, si selecciona la opción "*Dejar que Webmail administre automáticamente la Vinculación de Adjuntos*", la definición de las ubicaciones de los archivos y la URL de Webmail se manejan automáticamente. Si decide administrar la Vinculación de Adjuntos manualmente, puede especificar la ubicación donde se guardarán los archivos y puede utilizar macros especiales para hacer que la ubicación sea dinámica. Para que la Vinculación de Adjuntos funcione, debe estar habilitada globalmente utilizando la opción en esta pantalla y cada Cuenta que desee que la utilice debe estar

configurada específicamente para hacerlo en la pantalla Adjuntos[735] en el Editor de Cuentas. Finalmente, las ligas a los adjuntos que MDaemon colocará en los mensajes no contienen rutas directas de archivo. En lugar de esto contienen un identificador único (GUID) que el servidor utiliza para mapear el archivo a su ruta física. Este mapeo GUID se guarda en el archivo `AttachmentLinking.dat` .

La Vinculación de Adjuntos intentará utilizar el nombre de archivo proporcionado por los encabezados MIME (si existen). Si el nombre de archivo es mayor de 50 caracteres solo se utilizarán los últimos 50 caracteres. Si al nombre del archivo le falta la extensión, se agregará ".att".

Por omisión, la funcionalidad Vinculación de Adjuntos coloca el texto "MDaemon reemplazó los siguientes archivos con estas ligas:" en ciertos mensajes de correo. Si desea modificar ese texto, agregue la llave siguiente a su archivo `MDaemon.ini`, localizado en la carpeta \app\, después reinicie MDaemon:

```
[AttachmentLinking]
HeaderText=Este es mi texto.
```

Habilitar la Vinculación de Adjuntos
Dé clic en esta casilla para habilitar la Vinculación de Adjuntos para todas las cuentas que hayan sido específicamente configuradas para utilizarlo en la pantalla Adjuntos[735] en el Editor de Cuentas. Cuando habilite la opción global, se le preguntará si también desea habilitar la opción por cuenta específica para todas las cuentas de MDaemon. Si selecciona "Si", la vinculación de adjuntos se habilitará para todas las cuentas y las opciones correspondientes bajo la plantilla Cuentas Nuevas[815] también se habilitará. Si selecciona "No", entonces la funcionalidad de Vinculación de Adjuntos estará disponible pero no así la opción por cuenta específica—deberá activarla anualmente para cada cuenta que requiera utilizarla. Cuando se habilita la Vinculación de Adjuntos, el servidor de Webmail debe permanecer activo.

Dejar que Webmail administre automáticamente la Vinculación de Adjuntos
Este es la opción por omisión cuando se habilita la Vinculación de Adjuntos. Utilícela si desea permitir que Webmail maneje la Vinculación de Adjuntos automáticamente. Los archivos extraídos se guardarán en:". . . `\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\`".

Configurar manualmente la Vinculación de Adjuntos
Seleccione esta opción si desea definir la carpeta en la que se guardarán los archivos adjuntos extraídos. Deberá definir tanto la ruta del adjunto como la URL de Webmail cuando elija esta opción.

Ruta del Adjunto
Use esta caja de texto para definir la carpeta en la que se guardarán los archivos adjuntos extraídos. Puede establecer una ruta estática o utilizar una plantilla[795] y scripts[843] con macros para generar la ruta dinámicamente. Por ejemplo, "`$ROOTDIR$\Attachments\$DOMAIN$\`" agrupará todos los adjuntos en una subcarpeta nombrada con el nombre del dominio al que pertenece el usuario, bajo la subcarpeta "`Attachments`" contenida en el directorio raíz de MDaemon (usualmente `C:\MDaemon\`).

Así, para "usuario@ejemplo.com" el ejemplo haría que los adjuntos extraídos se colocaran en la subcarpeta: "C:\MDaemon\Attachments\ejemplo.com\." Puede subdividir el archivo de adjuntos agregando la macro "$MAILBOX$" al ejemplo. Esto haría que los archivos de Juan se guardaran en una subcarpeta bajo "\ejemplo.com\" llamada "juan.". Así, la nueva ruta sería: "C:\MDaemon\Attachments\example.com\Frank\."

URL de Webmail
Ingrese la URL de Webmail aquí (i.e. "http://correo.ejemplo.com:3000/WorldClient.dll"). MDaemon utilizará esta URL al insertar en los mensajes las ligas hacia los archivos extraídos.

Ignorar adjuntos de tamaño menos a estos KB (0 = ninguno)
Este es el tamaño mínimo requerido antes de que se extraiga un adjunto de un mensaje. Utilice esta opción si no desea extraer adjuntos pequeños. Si la configura a "0" entonces la Vinculación de Adjuntos extraerá todos los adjuntos sin importar su tamaño.

Eliminar adjuntos mayores de este número de días (0 = nunca)
Utilice esta opción si desea establecer un límite al número de días que se almacenarán los archivos adjuntos. Como parte del evento diario de mantenimiento, MDaemon eliminará los archivos adjuntos almacenados que sean mayores del tiempo límite definido, si se encuentran en la carpeta por omisión de adjuntos o en una de sus subcarpetas. La carpeta por omisión es: "<MDaemonRoot>\Attachments\...". Los adjuntos no se eliminarán si se personaliza la carpeta hacia otra ubicación. Esta opción se encuentra deshabilitada por omisión (configurada en "0").

Eliminar adjuntos del disco cuando los mensajes sean eliminados
Dé clic en esta opción si desea que los adjuntos extraídos sean eliminados del servidor siempre que el mensaje al que estaban ligados haya sido eliminado.

Cuando se habilita esta opción y algún usuario descarga correo vía un cliente POP3 que no está configurado para dejar mensajes en el servidor, entonces todos los adjuntos extraídos se perderán irremediablemente. Si esta opción no se habilita entonces no se perderán los adjuntos, pero puede llegar a ocuparse una gran cantidad de espacio en disco, por archivos inútiles u obsoletos que su destinatario original ya no desea o requiere. Virtualmente todos los clientes POP tienen la capacidad de dejar mensajes en el servidor.

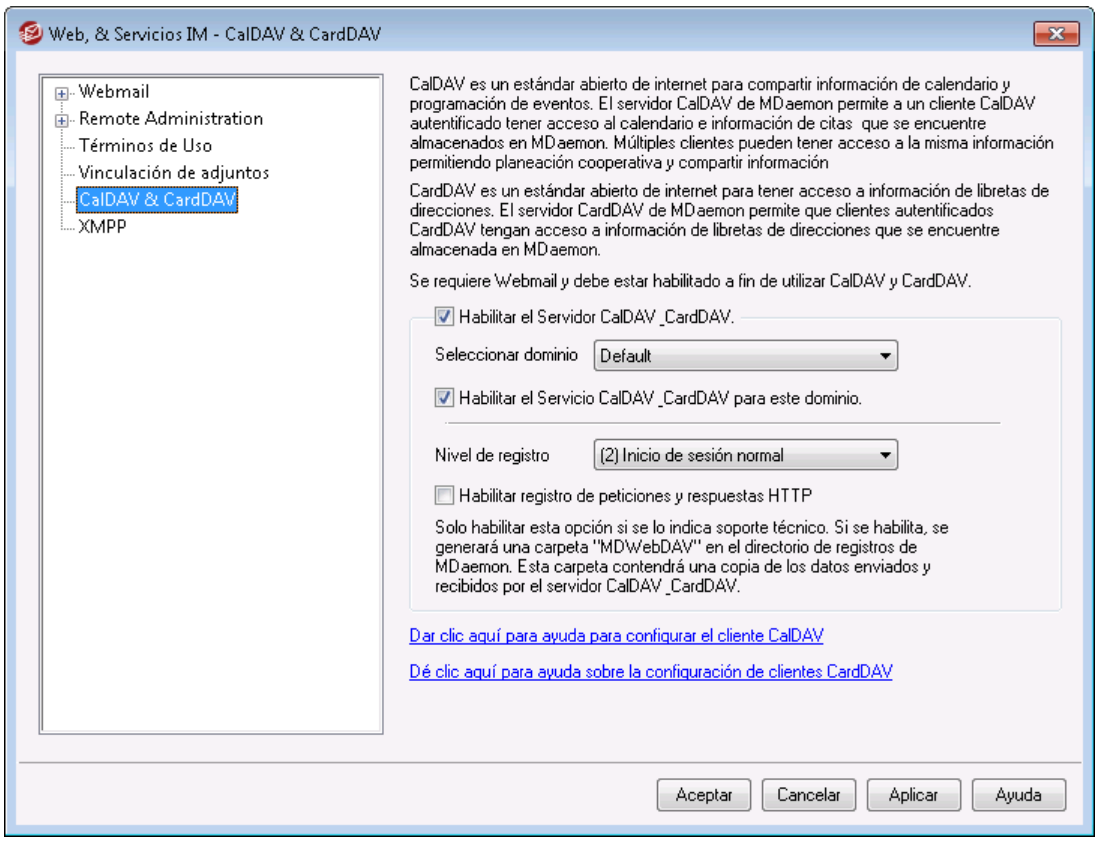
Extraer adjuntos tipo "texto/plano"
Por omisión, los adjuntos de tipo texto/plano no serán extraídos. Dé clic en esta casilla si desea incluir esos tipos en la extracción automática.

Lista de Exentos
Dé clic en este botón para abrir la lista de Exentos de Vinculación de Adjuntos. Incluya cualquier nombre de archivo que no desee que se extraiga de los mensajes. Winmail.dat se incluye en esta lista por omisión.

Ver:

Plantillas de Cuentas Nuevas 793
Editor de Cuentas » Adjuntos 735
Macros de Plantillas 795
Scripts de Macros 843

3.6.5 CalDAV & CardDAV



CalDAV es un estándar de Internet para administrar y compartir calendarios e información de programación de eventos. El soporte de MDaemon a CalDAV permite que sus cuentas utilicen cualquier cliente que soporte CalDAV para tener acceso y administrar sus calendarios y tareas personales. También pueden accesar calendarios públicos 314 o compartidos 743 dependiendo de sus permisos de acceso 316 . CardDAV es un estándar para tener acceso a la información de contactos/libreta de direcciones. El servidor CardDAV de MDaemon permite que clientes CardDAV autentificados tengan acceso a la información de contactos almacenada en MDaemon.

Habilitar el servidor CalDAV & CardDAV
El soporte a CalDAV está habilitado por omisión. Sin embargo, se requiere Webmail para CalDAV y por esto debe estar habilitado 326 para ser utilizado. Deshabilite esta opción si no desea soportar CalDAV. Para habilitar CalDAV para dominios individuales, utilice las opciones siguientes.

Modificar los Ajustes por Omisión de CalDAV & CardDAV por Dominio
Inicialmente, todos los dominios de MDaemon tendrán habilitado o deshabilitado CalDAV con base en la selección *Por omisión* en el menú desplegable *Seleccionar dominio*. Para modificar el ajuste por omisión:

1. En el menú desplegable *Seleccionar Dominio* seleccione **Por Omisión.**
2. Marque la casilla al lado de **Habilitar servicio CalDAV & CardDAV para este dominio** si desea que CalDAV esté habilitado para todos los dominios por omisión, o deshabilite la casilla si desea deshabilitarlo por omisión.
3. Dé clic en **OK**.

Habilitar/Deshabilitar CalDAV & CardDAV para Dominios Específicos
Para anular el ajuste *Por omisión* de CalDAV para dominios individuales:

1. En la lista desplegable *Seleccionar Dominio*, seleccione un dominio específico,
2. Marque la casilla al lado de **Habilitar servicio CalDAV & CardDAV para este dominio** si desea que CalDAV esté habilitado para este dominio o limpie la casilla si desea deshabilitarlo.
3. Dé clic en **OK**.

Registro

Nivel de registro
Utilice esta lista desplegable para definir el grado en que se registrarán las actividades CalDAV & CardDAV. Existen seis niveles posibles de registro: 1-Depuración, 2-Normal (por omisión), 3-Solo advertencias y errores, 4- Solo Errores, 5-Solo Errores Críticos y 6-Sin registro. Este es un ajuste global—no se puede aplicar a dominios específicos.

Habilitar registro de peticiones y respuestas HTTP
Si se habilita, esto creará una carpeta `MDWebDAV` en la carpeta de registros de MDaemon. Todos los datos enviados y recibidos por el servidor CalDAV & CardDAV serán registrados en esa carpeta. Normalmente esta opción solo se utilizará para diagnósticos y no debe habilitarse a menos de que se lo indique Soporte Técnico.

Configurar clientes CalDAV

Para configurar clientes que soporten RFC 6764 (Localizando Servicios para extensiones de Calendario a WebDAV (CalDAV)), solo se requiere el servidor, nombre de usuario y contraseña. Puede configurar sus registros DNS para apuntar el cliente a la URL correcta. Cuando no se ha configurado un registro DNS, el usuario puede registrar una URL ".well-known" en el cliente: "nombre de servidor/.well-known/caldav". Por ejemplo: `http://example.com:3000/.well-known/caldav` . El servidor web integrado de Webmail soporta la URL well-known.

Los clientes que no soportan en automático la localización del servicio CalDAV, tales como Mozilla Thunderbird vía el complemento Lightning, requerirán una URL completa para cada Calendario y Lista de Tareas. Las URLs CalDAV de MDaemon se construyen así:

Calendarios y Tareas
Calendario o lista de tareas por omisión del usuario:

`http://[host]/webdav/calendar`
(ej. `http://example.com:3000/webdav/calendar`)

`http://[host]/webdav/tasklist`
(ej. `http://example.com/webdav/tasklist`)

Calendario o lista de tareas personalizado del usuario:

`http://[host]/webdav/calendar/[calendar-name]`
(ej. `http://example.com/webdav/calendar/personal`)

`http://[host]/webdav/tasklist/[tasklist-name]`
(ej. `http://example.com/webdav/tasklist/todo`)

Calendario o lista de tareas del usuario en una subcarpeta:

http://[host]/webdav/calendar/[folder]/[calendar-name]
(ej. `http://example.com/webdav/calendar/my-stuff/personal`)

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(ej. `http://example.com/webdav/tasklist/my-stuff/todo`)

Calendarios y Tareas Compartidos
Calendario y lista de tareas de otro usuario:

`http://[host]/webdav/calendars/[domain]/[usuario]`
(ej. `http://example.com/webdav/calendars/example.net/frank`)

`http://[host]/webdav/tasks/[domain]/[user]`
(ej. `http://example.com/webdav/tasks/example.net/frank`)

Calendario o lista de tareas personalizados de otro usuario:

`http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]`
(ej.
`http://example.com/webdav/calendars/example.net/frank/personal`)

`http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]`
(ej. `http://example.com/webdav/tasks/example.net/frank/todo`)

Calendarios y Tareas Públicos
Calendario o lista de tareas del Dominio por Omisión:

`http://[host]/webdav/public-calendars/[domain]`
(ej. `http://example.com/webdav/public-calendars/example.com`)

`http://[host]/webdav/public-tasks/[domain]`
(ej. `http://example.com/webdav/public-tasks/example.com`)

Calendario o lista de tareas en la raíz de la jerarquía de Carpetas Públicas:

`http://[host]/webdav/public-calendars/[calendar-name]`
(ej. `http://example.com/webdav/public-calendars/holidays`)

`http://[host]/webdav/public-tasks/[tasklist-name]`
(ej. `http://example.com/webdav/public-tasks/projects`)

Se debe tener cuidado especial al probar el cliente OutlookDAV. Si existen múltiples perfiles MAPI, hemos visto que el cliente emite comandos al servidor para todos los elementos del calendario devueltos por el servidor. OutlookDAV solo soporta el perfil MAPI por omisión.

Para más información sobre la configuración de clientes CalDAV, busque "CalDav" en la Base de Conocimientos de MDaemon.

Configurar cliente CardDAV

Para configurar clientes que soporten el estándar RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV)), solo se requiere la dirección del servidor, el nombre de usuario y la contraseña. La libreta de direcciones de Apple y iOS soportan este estándar. Los registros en el DNS se pueden configurar para apuntar el cliente a la URL correcta. Cuando un registro DNS no se ha configurado, los clientes consultan una "URL conocida", que en el caso de CardDAV es `/.well-known/carddav`. El servidor web integrado de Webmail soporta esta url conocida. Los clientes que no soportan la localización automática del servicio CardDAV requerirán la URL completa.

Los clientes CardDAV más notables son Contactos de Apple (incluido en Mac OS X), Apple iOS (iPhone) y Mozilla Thunderbird vía el complemento SOGO.

A partir de OS X 10.11 (EL Capitán), la aplicación Contactos de Apple solamente soporta una única carpeta/colección. Cuando el servidor CardDAV detecta la aplicación Contactos de Apple, solo devuelve la carpeta por omisión de contactos del usuario autentificado. Adicionalmente, OS X 10.11 (EL Capitán) tiene un problema conocido que impide que la cuenta CardDAV se agregue utilizando la vista "Avanzada" del diálogo.

Accesando la libreta de direcciones

La ruta "addressbook" es un atajo a su propia libreta de direcciones.

`http://[host]/webdav/addressbook` - su carpeta de contactos por omisión.

`http://[host]/webdav/addressbook/friends` - la carpeta de contactos "friends".

`http://[host]/webdav/addressbook/myfolder/personal` - su carpeta de contactos "personal" en una subcarpeta denominada "myfolder".

Accesando carpetas compartidas de otro usuario a las que tenga acceso
La ruta "contacts" es un atajo a carpetas de contactos compartidas

`http://[host]/webdav/contacts/example.com/user2` - carpeta de contactos por omisión del usuario user2@example.com

`http://[host]/webdav/contacts/example.com/user2/myfolder` - carpeta de contactos "myfolder" del usuario user2@example.com

Acceso a carpetas públicas sobre las que tiene permisos

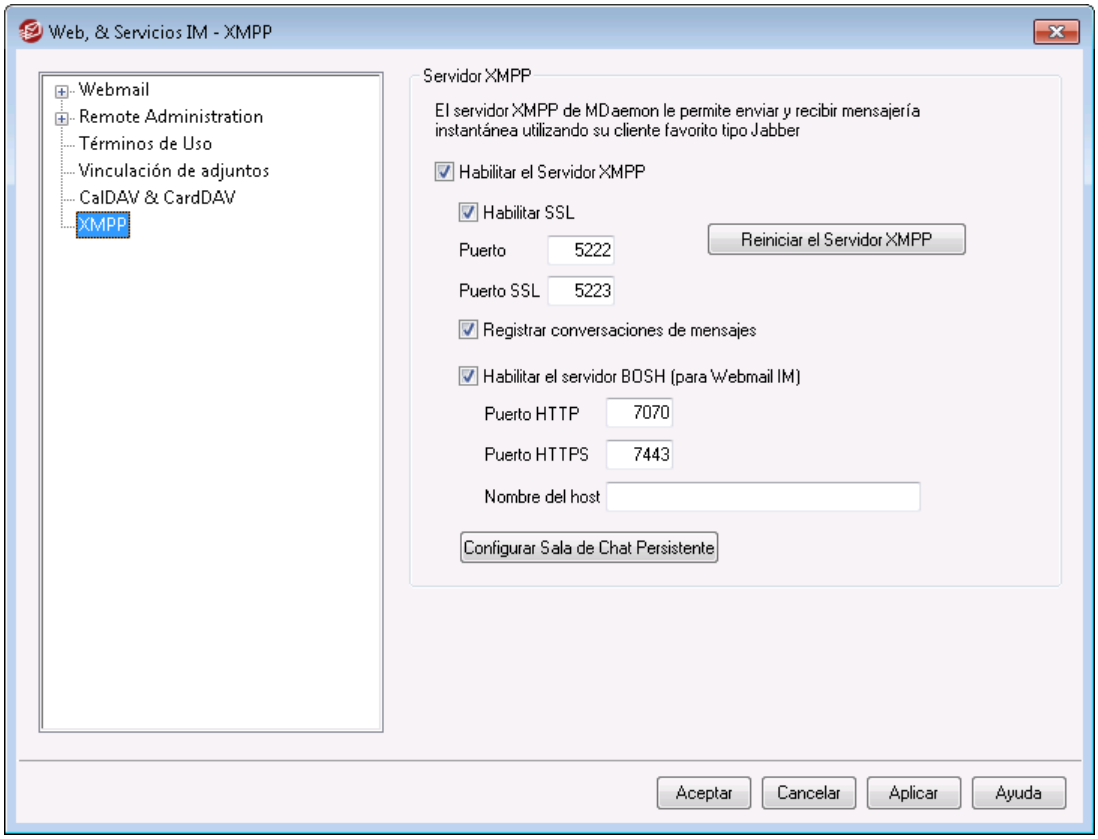
La ruta "public-contacts" es un atajo a la carpeta pública de contactos.
`http://[host]/webdav/public-contacts/example.com` - carpeta de contactos por omisión de example.com

`http://[host]/webdav/public-contacts/foldername` - carpeta de contactos "foldername" en la raíz de la jerarquía de la carpeta pública de contactos.

Se debe tener cuidado especial al probar el cliente OutlookDAV. Si existen múltiples perfiles MAPI, hemos visto que el cliente emite comandos al servidor para todos los elementos del calendario devueltos por el servidor. OutlookDAV solo soporta el perfil MAPI por omisión.

Para más información para configurar clientes CardDAV, busque "CardDav" en la Base de Conocimientos de MDaemon.

3.6.6 XMPP



MDaemon está equipado con un servidor XMPP (Extensible Messaging and Presence Protocol), denominado en ocasiones servidor Jabber. Esto permite a los usuarios enviar y recibir mensajería instantánea utilizando MDaemon Mensajería Instantánea 322 y clientes XMPP de terceros como Pidgin, Gajim, Swift y muchos otros. Los clientes están disponibles en la mayoría de los sistemas operativos y en las plataformas de dispositivos móviles.

El servidor XMPP se instala como servicio de Windows y sus puertos por omisión son el 5222 (SSL vía STARTTLS) y 5223 (SSL dedicado). El servidor XMPP utilizará la configuración SSL de MDaemon si se encuentra habilitada en éste. Así mismo, algunos clientes XMPP utilizan registros DNS SRV para autodescubrimiento de nombres de host. Por favor consulte http://wiki.xmpp.org/web/SRV_Records para más información.

Los usuarios se firman a través del cliente XMPP seleccionado utilizando su dirección de correo y contraseña. Sin embargo, algunos clientes requieren que la dirección de correo se divida en componentes separados para iniciar sesión. Por ejemplo, en lugar de "`frank@example.com`," algunos clientes requieren que se utilice "`frank`" como nombre de inicio de sesión y "`example.com`" como Dominio.

Para servicio multiusuario/grupos, los clientes típicamente los despliegan como "cuartos" o "conferencias". Cuando desee iniciar una sesión de conversación en grupo, genere un cuarto/conferencia (dándole un nombre) y luego invite a los otros usuarios a ese cuarto. La mayoría de los clientes no requieren que registre la ubicación del servidor para la conferencia; solo necesita darle un nombre. Cuando se le pide hacerlo, sin embargo, utilice "`conference.<your domain>`" como ubicación (ej. `conference.example.com`). Algunos clientes solicitan que registre el

nombre y ubicación juntos con la forma: "room@conference.<your domain>" (ej. Room01@conference.example.com).

Algunos clientes (como Pidgin), soportan el servicio de búsqueda de usuarios, permitiéndole buscar el servidor de los usuarios por nombre o dirección de correo, lo que facilita agregar contactos. Usualmente no tendrá que proporcionar la ubicación de búsqueda, pero si se le solicita utilice "search.<your domain>" (ej. search.example.com). Al hacer la consulta, se puede utilizar el símbolo % como comodín. Por esto, podría utilizar "%@example.com" en el campo de dirección de correo para desplegar una lista de todos los usuarios con una dirección de correo que termine en "@example.com."

Servidor XMPP

Habilitar Servidor XMPP
Dé clic en esta opción para habilitar el servidor XMPP. Para permitir la mensajería instantánea también debe asegurarse de que está habilitada la opción **Habilitar mensajería instantánea** en la pantalla MDIM 332.

Habilitar SSL
Dé clic en esta opción si desea soportar SSL para el servidor XMPP, utilizando el *Puerto SSL Port* especificado abajo. **Nota:** Esto también aplica a la opción siguiente para definir un *puerto HTTPS Port* para el servidor BOSH.

Puerto
El Puerto XMPP por omisión es el 5222, que soporta SSL vía STARTTLS.

Puerto SSL
El puerto SSL dedicado para XMPP es el 5223.

Reiniciar el servidor XMPP
Dé clic en este botón para reiniciar el servidor XMPP.

Registrar conversaciones
Por omisión todas las conversaciones de mensajería instantánea se registrar en un archivo denominado XMPPServer-<date>.log, localizado en la carpeta MDaemon\Logs\. Deshabilite esta casilla si no desea registrar las conversaciones.

Habilitar el Servidor BOSH (para Webmail IM)
Dé clic en esta opción para habilitar el servidor BOSH, permitiendo mensajería instantánea dentro de MDaemon Webmail.

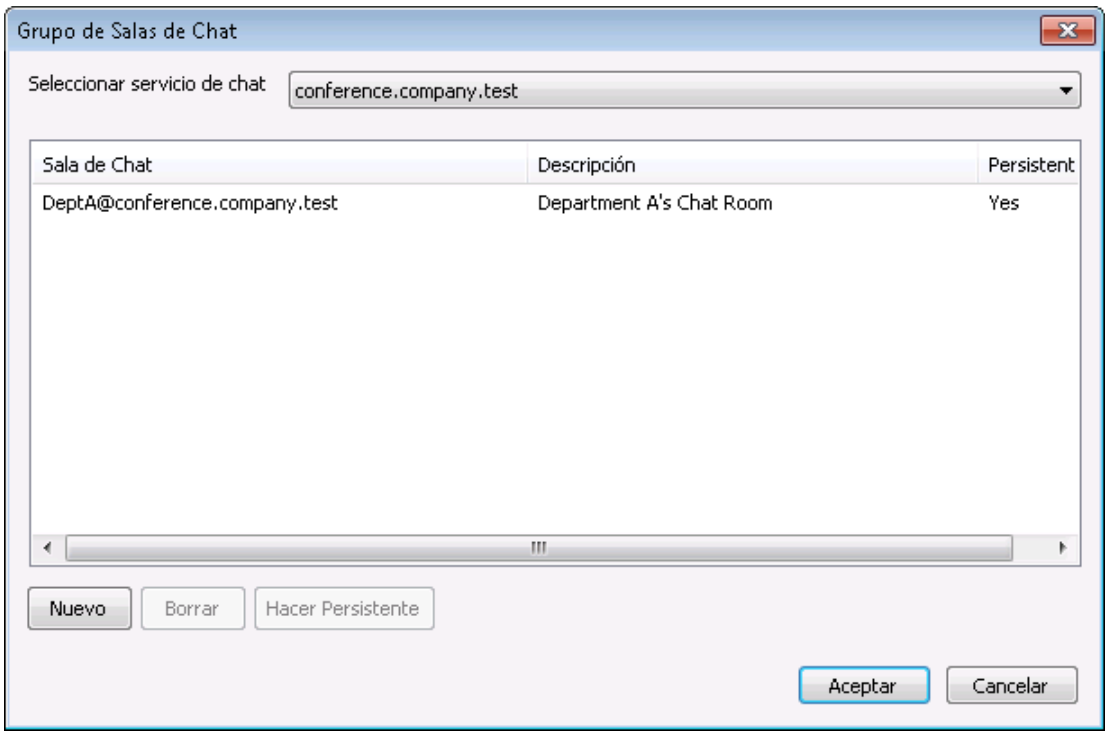
Puerto HTTP
Por omisión el servidor BOSH utiliza el puerto 7070 para HTTP.

Puerto HTTPS
El servidor BOSH utiliza este puerto HTTPS cuando se activa la opción que se presenta arriba *Habilitar SSL*. El puerto por omisión es el 7443.

Nombre de Host
Utilice esta opción para especificar un nombre de Host si es necesario.

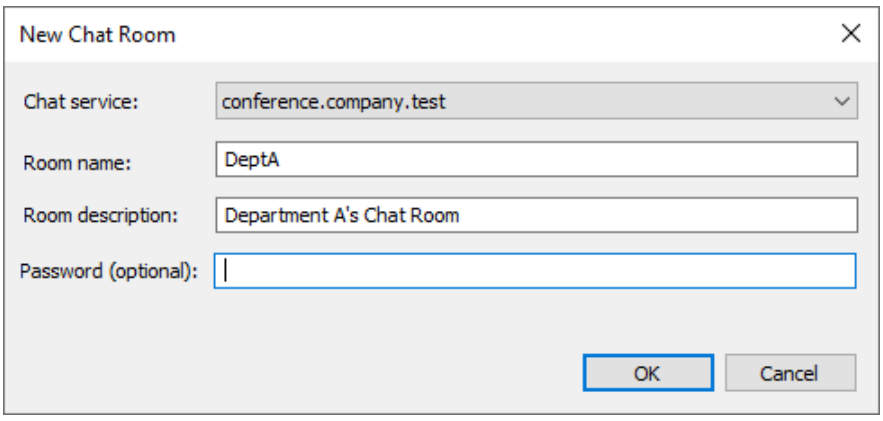
Configurar Salas de Chat Persistentes

Dar clic en este botón para abrir el diálogo Grupo de Salas de Chat. Normalmente, cuando un usuario utiliza una sala de chat, esta desaparecerá cuando la última persona salga de la sala, sin embargo puede utilizar estas opciones para crear salas de chat persistentes que seguirán existiendo aunque estén vacías. También puede eliminar salas y convertir las salas temporales existentes en salas persistentes.



Seleccionar servicio de chat
Seleccione el servicio de chat para desplegar las salas de chat de ese dominio.

Nuevo
Dé clic en este botón para agregar una sala de chat persistente.



Seleccionar servicio de chat
Seleccione el servicio de chat para la sala.

Nombre de la Sala
Teclee un nombre para la sala de chat, sin espacios.

Descripción de la Sala
Incluir aquí una descripción de la sala. Los usuarios observarán esto al seleccionar la sala a la que van a ingresar.

Contraseña (opcional)
Si deseas solicitar contraseña para poder ingresar a la sala, registre una contraseña aquí.

Borrar
Si desea eliminar una sala, selecciónela y dé clic en este botón para borrarla.

Convertir en Persistente
Cuando se encuentra en la lista una sala de chat temporal, puede seleccionarla y dar clic en este botón si desea hacerla persistente.

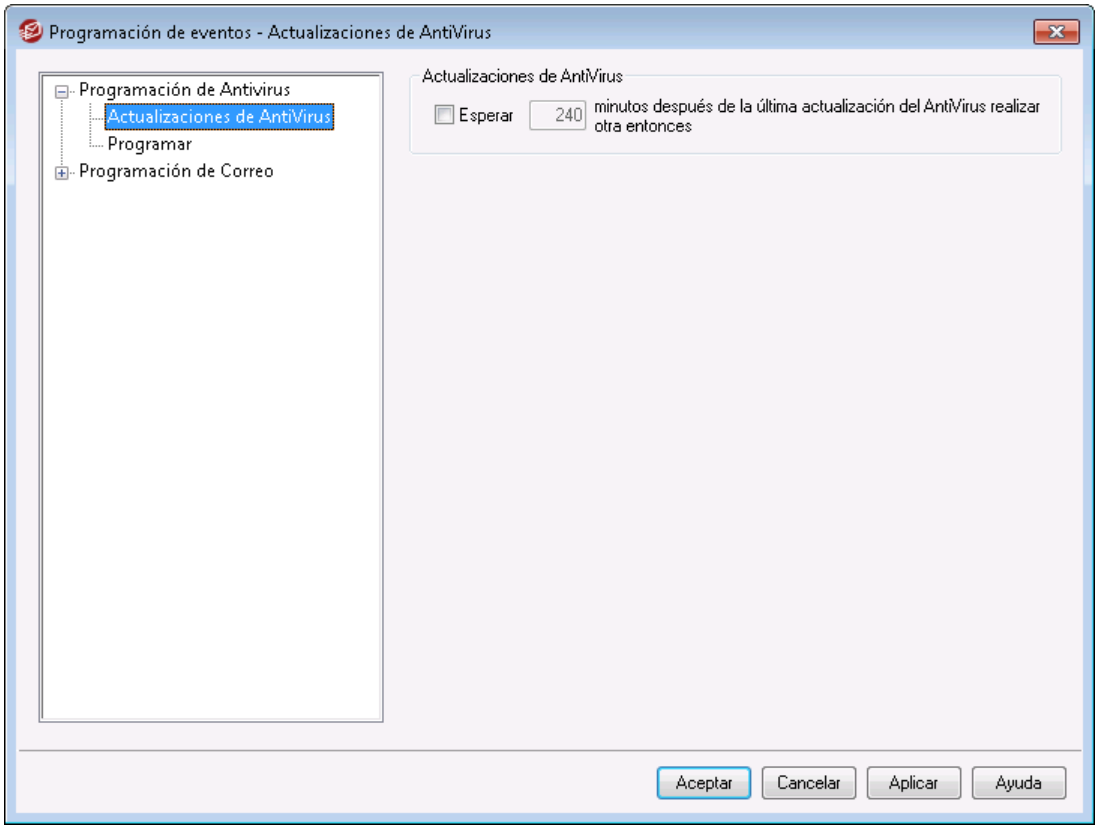
Ver:

Webmail » MDIM 332

3.7 Programación de Eventos

3.7.1 Programación de Antivirus

3.7.1.1 Actualizaciones de AntiVirus



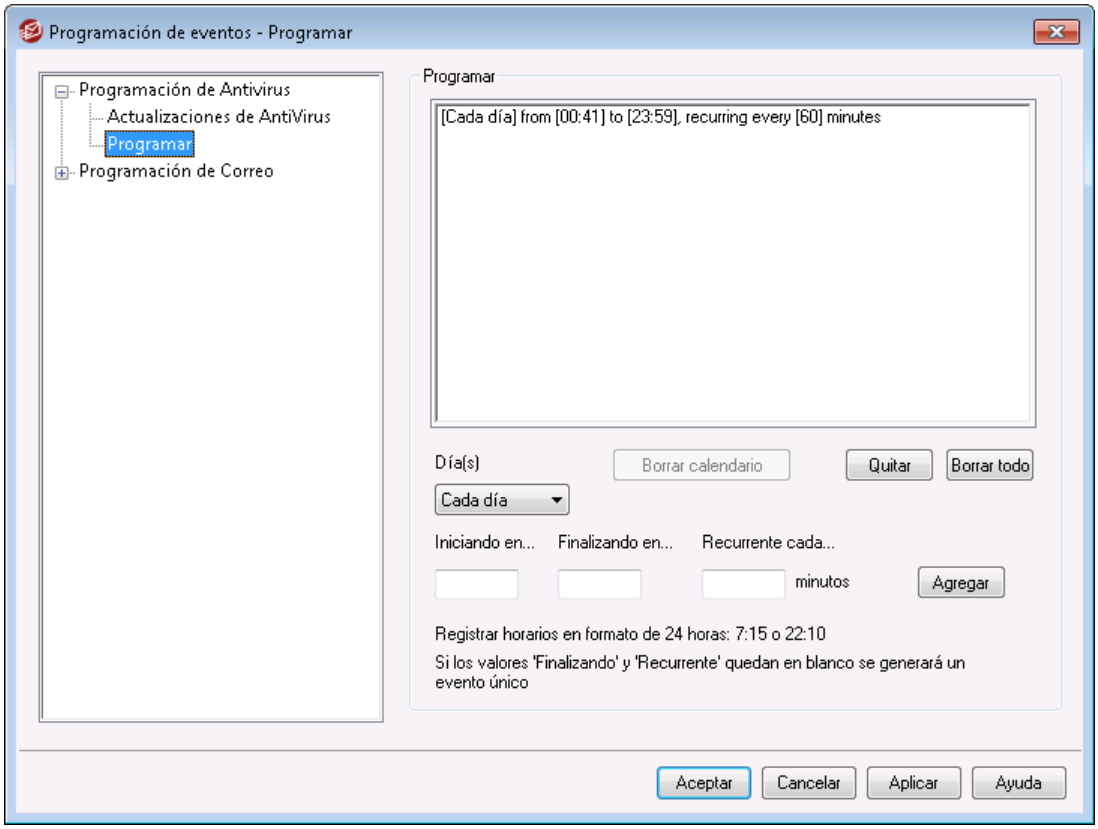
Actualizaciones de Antivirus

Esperar XX minutos después de la última actualización de Antivirus para ejecutar otra
Haga clic en esta casilla y especifique el número de minutos que desea que el AntiVirus espere antes de comprobar actualizaciones de firmas de virus nuevas. Note que, este es en realidad el número de minutos que el AntiVirus *intentará* esperar después de la última vez que se comprobaron actualizaciones, tanto si ésta fue desencadenada por el programador como manualmente. El programador y las actualizaciones desencadenadas son precedentes de esta configuración y por lo tanto restablecerán este contador si un evento de actualización del AntiVirus se desencadena por uno de dichos métodos. Así, por ejemplo, si tiene esta opción configurada para comprobar las actualizaciones cada 240 minutos y comprueba manualmente una actualización después de 100 minutos, este contador se restablecerá a 240.

Ver:

Programación de Actualizaciones de Antivirus 378
Antivirus 668
Actualizador del Antivirus 673

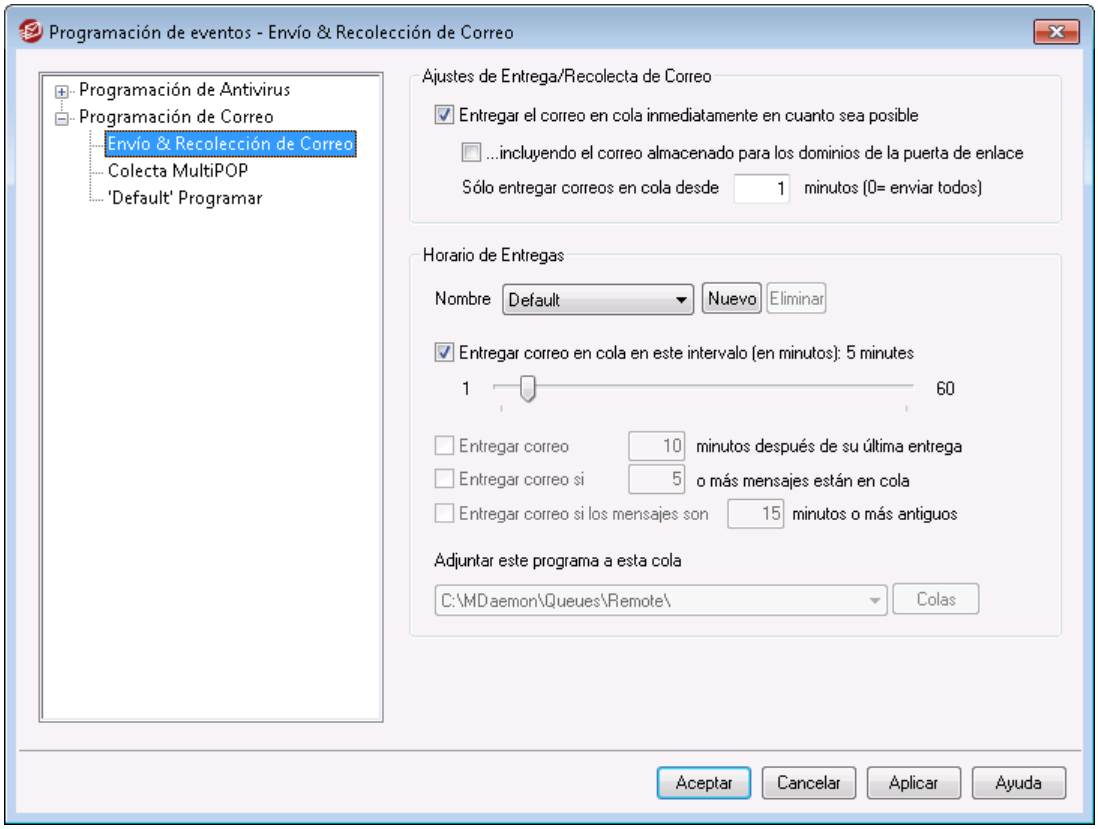
3.7.1.2 Programar



Utilice el programador de Actualizaciones de Antivirus para definir las horas específicas en las que Antivirus[645] comprobará las actualizaciones. El programador está ubicado en: Configurar » Programador de Eventos » Programación de Antivirus » Programar.

3.7.2 Programación de Correo

3.7.2.1 Envío & Recolección de Correo



Haga clic en Configuración » Programación de Eventos para abrir el Programador de Eventos de MDaemon. Al utilizar esta pantalla puede programar los eventos de procesamiento de correo remoto de MDaemon tan detallada o simplemente como prefiera. Puede utilizar un contador para procesar correo a intervalos regulares o puede programar la hora exacta para la entrega y recolección de correo utilizando las pantallas Programación de Correo 384. También puede definir las condiciones que detonarán el procesamiento de correo en horarios no programados tales como cuando se alcance cierto número de mensajes en espera de ser enviados o cuando un mensaje ha estado esperando durante un tiempo específico. Más aun, puede crear programaciones personalizadas que puede asignar a colas remotas particulares. Los calendarios particulares le permiten establecer diferentes horarios para diferentes tipos de mensajes. Por ejemplo, puede crear programaciones para mensaje grandes, para mensajes de listas de distribución, para ciertos dominios y más.

Utilice la sección Actualizaciones de Antivirus 377 del Programador de Eventos para programar la frecuencia con que MDaemon verificará las actualizaciones de Antivirus.

Ajustes Globales de la Entrega/Recolección de Correo

Entregar el correo en cola inmediatamente en cuanto sea posible
Cuando se activa esta opción y un mensaje llega y se pone en cola para envío remoto, en lugar de esperar para el siguiente intervalo de procesamiento o algún otro evento para ejecutar el proceso de correo, MDaemon lo procesará

inmediatamente y enviará todo el correo remoto que haya sido puesto en cola dentro del número de minutos designado en la opción siguiente de *Sólo entregar correos en cola desde [xx] minutos.*

...incluyendo el correo almacenado para los dominios de puerta de enlace
Haga clic en esta casilla si también quiere que los mensajes de los Dominios de Puerta de Enlace se envíen inmediatamente. Sin embargo, esto sólo aplica a las puertas de enlace con la opción *Entregar mensajes almacenados cada vez que MDaemon procese el correo remoto* activada en la pantalla Puerta de Enlace 262 del Editor de Puertas de Enlace.

Sólo entregar correos en cola desde [xx] minutos (0=enviar todos)
Esta opción gobierna cómo los mensajes recientes deben haber sido puestos en cola antes de que la opción anterior de *Entregar el correo en cola inmediatamente en cuanto sea posible* los marque para envío. Cuando esta opción ejecuta procesamiento de cola remoto, en lugar de intentar el envío de todo lo que haya en cola, MDaemon procesará sólo aquellos mensajes que están puestos en cola dentro del número de minutos designados. La cola entera se seguirá procesando, sin embargo, cuando el botón de barra de menú de *Procesar...cola* se pulse o cualquier otra programación normal de eventos ejecute el procesamiento de cola remoto. Por defecto, esta opción se establece en un minuto. Puede establecerlo a "0" si desea que se procese la cola por completo cada vez que el procesamiento de correo remoto se ejecute, pero no está recomendado puesto que es mucho menos eficiente.

Las opciones anteriores sólo aplican a la programación por Defecto. No están disponibles para las programaciones personalizadas (ver la siguiente opción de *Nombre...*).

Horarios de Entregas

Nombre...
Utilice esta lista desplegable para seleccionar un programador a editar. El programador por defecto siempre se usará para la cola remota normal y para el correo recolectado por DomainPOP y MultiPOP. Para configuraciones utilizando los servicios de marcación, el programador por defecto también se utilizará para dominios de la LAN, los cuales son dominios remotos que se han designado como residentes de su área local y que por tanto no requieren marcación RAS. Otros programadores pueden ser asignados a colas de correo remoto personalizadas, y los mensajes pueden ser enrutados a dichas colas personalizadas 877 automáticamente utilizando el Filtro de Contenido 645. Cuando haya acabado de editar unas opciones de programación, haya clic en el botón Aceptar para seleccionar otro programador a editar. Si realiza cambios a un programador y luego selecciona otro programador, un cuadro de confirmación se abrirá preguntando si desea guardar o descartar los cambios realizados al programador actualmente seleccionado antes de cambiar a otro programador.

Nuevo
Haga clic en esta opción para crear un nuevo programador. Un cuadro se abrirá para que pueda designar un nombre. Después de que el nombre del programador haya sido designado, una pantalla de Programación del Correo 384 correspondiente será creada en el menú de la izquierda. Use dicha pantalla para asignar los tiempos de dicho programador.

Eliminar
Para eliminar un programador personalizado, primero selecciónelo en la lista desplegable *Nombre...* y luego haga clic en Eliminar. Aparecerá un mensaje de confirmación preguntando si está seguro de que desea eliminarlo. Eliminar un programador personalizado no eliminará ninguna cola remota personalizada o regla de Filtro de Contenidos asociada a éste. Sin embargo, si elimina una cola personalizada entonces las programaciones asociadas a esa cola también se eliminarán, y todas las reglas de filtro de contenido también.

Entregar correo en cola en este intervalo (en minutos)
Haga clic en la casilla de verificación y mueva esta barra de izquierda a derecha para especificar el intervalo de tiempo entre las sesiones de procesamiento de correo. Puede configurarse para contar con un rango de 1 a 60 minutos. Después de dicha cantidad de tiempo, MDaemon procesará el correo remoto antes de empezar nuevamente con la cuenta. Cuando se desmarque esta casilla, los intervalos de procesamiento de *Correo Remoto* serán determinados por las otras opciones de programación.

Entregar correo [xx] minutos después de su última entrega
Use esta opción cuando quiera que una sesión de procesamiento de correo remoto ocurra en un intervalo regular de tiempo después de que haya ocurrido la última sesión, independientemente de la programación que iniciara la sesión. A diferencia de los rígidos intervalos que se usan cuando se establece un tiempo específico o cuando se usa la barra de desplazamiento *Entregar correo en cola en este intervalo*, el intervalo de tiempo de esta opción se restablecerá cada vez que el correo sea procesado.

Entregar correo si [xx] o más mensajes están en cola
Cuando se habilite esta opción, MDaemon ejecutará una sesión de correo siempre que la cola remota cumpla o exceda el número que se especifique aquí. Estas sesiones de correo son adicionales a otras que se programen de manera habitual.

Entregar correo si los mensajes son [xx] minutos o más antiguos
Cuando se seleccione esta opción, MDaemon ejecutará una sesión de correo siempre que un mensaje haya estado esperando en la cola durante el número de minutos especificado. Estas sesiones son adicionales a otras cualesquiera que se programen de manera habitual.

Colas

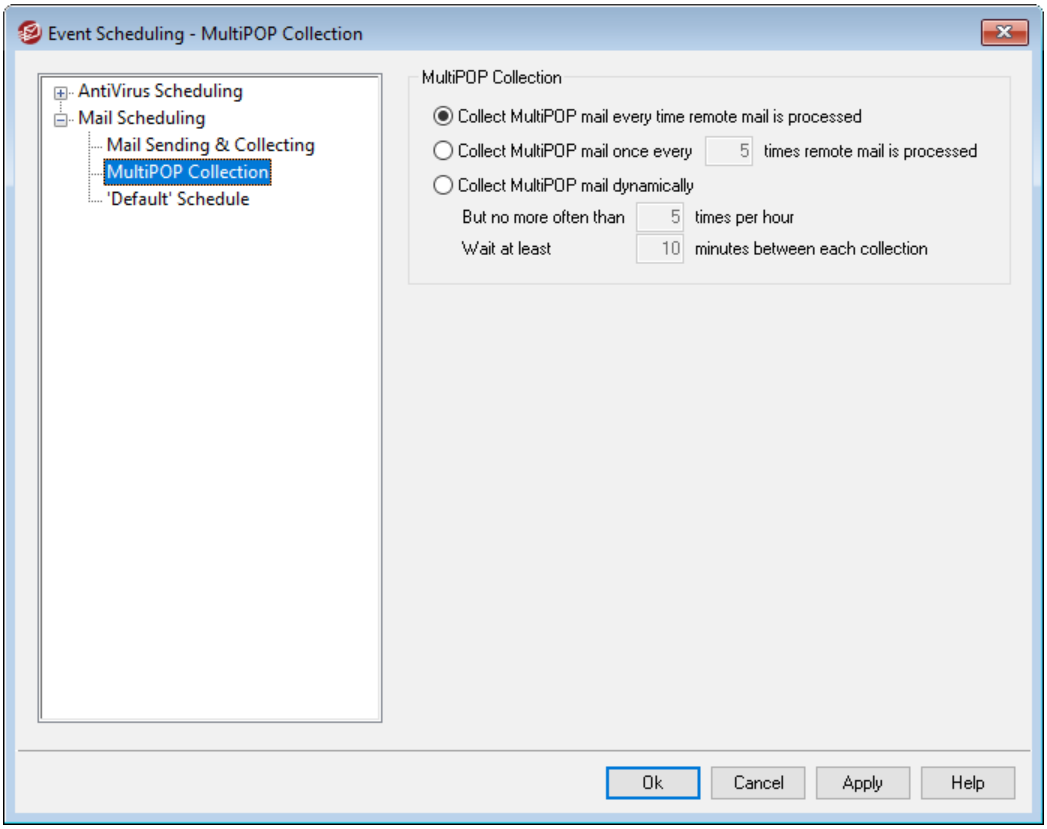
Agregar esta programación a esta cola
Utilice esta opción para asociar la programación seleccionada con una cola específica de correo remoto personalizada. Entonces puede utilizar el filtro de contenido para crear reglas que colocarán ciertos mensajes en esa cola. Por ejemplo, si desea programar el envío de mensajes de listas destinados a direcciones remotas, para que se realice en un horario específico, puede crear una cola personalizada para esos mensajes, crear una regla que los coloque en esa cola y luego crear la programación personalizada y asignarla a esa cola.

Colas
Dé clic en el botón para abrir la pantalla Colas Personalizadas 877, en la que puede crear colas remotas personalizadas para ser utilizadas con el Programador de Eventos.

Ver:

[Programación de Correo](#) 384
[Actualizaciones de Antivirus](#) 377

3.7.2.2 Recolección MultiPOP



Recolección de MultiPOP

Recolectar el correo MultiPOP cada vez que se procesa un correo remoto
Escoja esta opción si quiere que MDaemon recolecte todo el correo MultiPOP 739 cada vez que se procese el correo remoto.

Recolectar el correo MultiPOP una vez cada XX veces que se procesa el correo remoto
Escoja esta opción y especifique un numeral en el cuadro si desea que el correo MultiPOP se recolecte con menos frecuencia que la recolección de correo remoto. Este numeral denota cuántas veces debe ser procesado el correo remoto antes de que se recolecte el correo MultiPOP.

Recolectar el correo MultiPOP dinámicamente
Escoja esta opción si desea recolectar mensajes MultiPOP dinámicamente. Normalmente, MultiPOP se recolecta para todos los usuarios en el mismo

momento cada vez que se procesa un intervalo remoto, o una vez cada x intervalos remotos. Cuando se recolecta dinámicamente, los mensajes MultiPOP se recolectan para cada usuario individual cuando ese usuario comprueba su correo local vía POP, IMAP o Webmail en lugar de todos los usuarios a la vez. Aun así, dado que la recolección MultiPOP se desencadena a partir de que un usuario comprueba su correo, los mensajes nuevos MultiPOP recolectados no serán visibles al usuario hasta que compruebe *nuevamente* su correo. Así, necesitará comprobar su correo dos veces para poder ver los nuevos mensajes MultiPOP. La primera vez para detonar MultiPOP y la segunda para ver el correo que se ha recolectado.

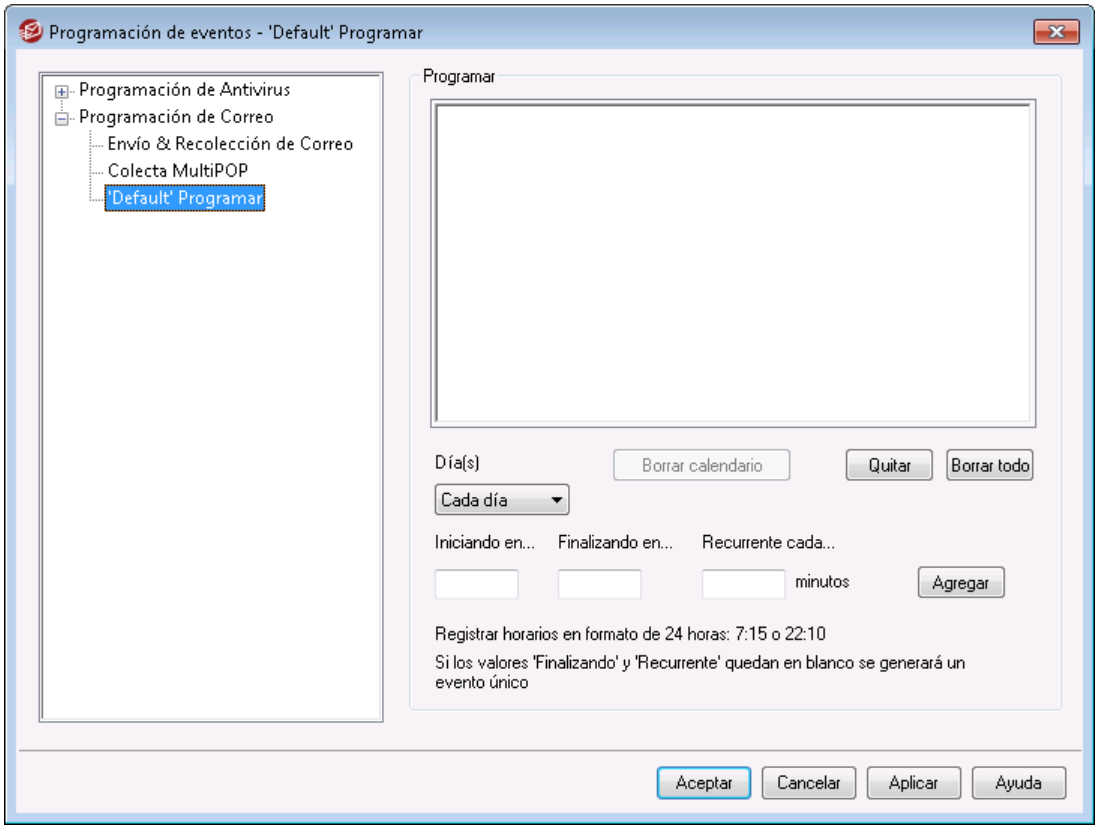
Pero no más de XX veces por hora
Para poder reducir la carga que el uso extensivo de MultiPOP puede potencialmente ejecutar en su MDaemon, puede usar este control para especificar un número máximo de veces por hora que se puede recolectar MultiPOP para cada usuario.

Esperar al menos XX minutos entre cada recolección
Esta opción puede ayudar a reducir la carga en el servidor de correo limitando la frecuencia con la que los mensajes MultiPOP pueden ser recolectados por cada usuario. Restringirá la recolección de correo MultiPOP a una sola vez cada varios minutos por usuario. Especifique el número de minutos que desea requerir que esperen los usuarios antes de permitir comprobar nuevamente el correo MultiPOP.

Ver:

MultiPOP
Editor de Cuentas | MultiPOP 739

3.7.2.3 Programación del Correo



Cada Programación de Correo corresponde a la programación del mismo nombre listado en la lista desplegable *Nombre* en la pantalla de Envío & Recolección de Correo 380. Use cada Programación de Correo para designar tiempos específicos en los que el procesamiento de correo remoto ocurrirá para dicha programación. Los Programadores de Correo están localizados en Configurar » Programación de Eventos » Programación de Correo » 'Nombre' del Programador.

Programar

Borrar programación

Este botón eliminará la Programación de Correo Personalizada. La programación se eliminará y su entrada correspondiente será eliminada de la lista desplegable en de la pantalla de Envío & Recolección de Correo 380. Después de que haga clic en este botón, un cuadro de confirmación se abrirá preguntando si está seguro de que quiere borrar la programación. Esta opción sólo está disponible para programaciones personalizadas — la Programación por Defecto no se pueden eliminar.

Eliminar

Para eliminar una entrada de la lista, seleccione la entrada y luego haga clic en este botón.

Borrar todo

Este botón eliminar todas las entradas del programador anterior.

Crear Programación de Eventos

Día(s)
Cuando se crea un nuevo evento para el programador, primero se selecciona el día o días en los que se establecerá este evento. Puede seleccionar: cada día, laborables (Lunes a Viernes), Fines de semana (Sábado y Domingo), o días específicos de la semana.

Empezando a las...
Introduzca la hora en la que desea que empiece el evento. El valor de hora debe ser en formato 25 horas, desde las 00:00 a las 23:59. Si desea que sea un sólo evento en lugar de un evento recurrente, este es el único valor de tiempo que deberá introducir (deje las opciones *Acabando a las...* y *Recurrir cada...* en blanco).

Acabando a las...
Introduzca la hora a la que desea que finalice el evento. El valor de tiempo debe ser en formato 24 horas, desde las 00:01 a las 23:59, y debe ser mayor al valor de *Empezando a las...* Por ejemplo, si el valor *Empezar a las...* fuera "10:00" entonces este valor puede ser desde las "10:01" a las "23:59". Deje esta opción en blanco si desea que sea un único evento en lugar de un evento recurrente.

Recurrir cada [xx] minutos
Este es el intervalo de tiempo en el que el correo será procesado entre los valores de *Empezando a las...* y *Acabando a las...* Deje esta opción en blanco si desea que sea un evento único en lugar de un evento recurrente.

Agregar
Una vez haya designado el valor de *Empezando a las* y *Día(s)* y el valor opcional *Acabando a las...* y *Recurrir cada...,* haga clic en este botón para agregar el evento al programador.

Dependiendo de sus necesidades, puede ser suficiente con utilizar las opciones simples de programación que se presentan en la pantalla Envío y Recolección de Correo 380 para controlar los intervalos de procesamiento del correo. Por ejemplo, no tiene sentido generar una programación específica con eventos cada minuto de cada día cuando simplemente puede configurar la barra deslizable en Envío & Recolección de Correo a intervalos de un minuto y lograr lo mismo. Por otro lado, si desea que los intervalos de procesamiento estén separados más de una hora o solo ciertos días, entonces puede utilizar alguna combinación de las opciones de programación, en horarios específicos.

Ver:

Envío & Recolección de Correo 380
Actualizaciones de Antivirus 377
Actualizaciones de AntiSpam 696

3.8 MDaemon Connector

El soporte de MDaemon Private Cloud a MDaemon Connector (MC) permite a cualquiera de sus usuarios utilizar Microsoft Outlook como cliente preferido de correo cuando se instala MC en su computadora. MC proporciona funcionalidad de trabajo en grupo y colaboración conectando a los usuarios del cliente de Outlook al servidor MDaemon, para utilizar el correo, el calendario con funcionalidad libre/ocupado, la libreta de direcciones, listas de distribución, tareas y notas.

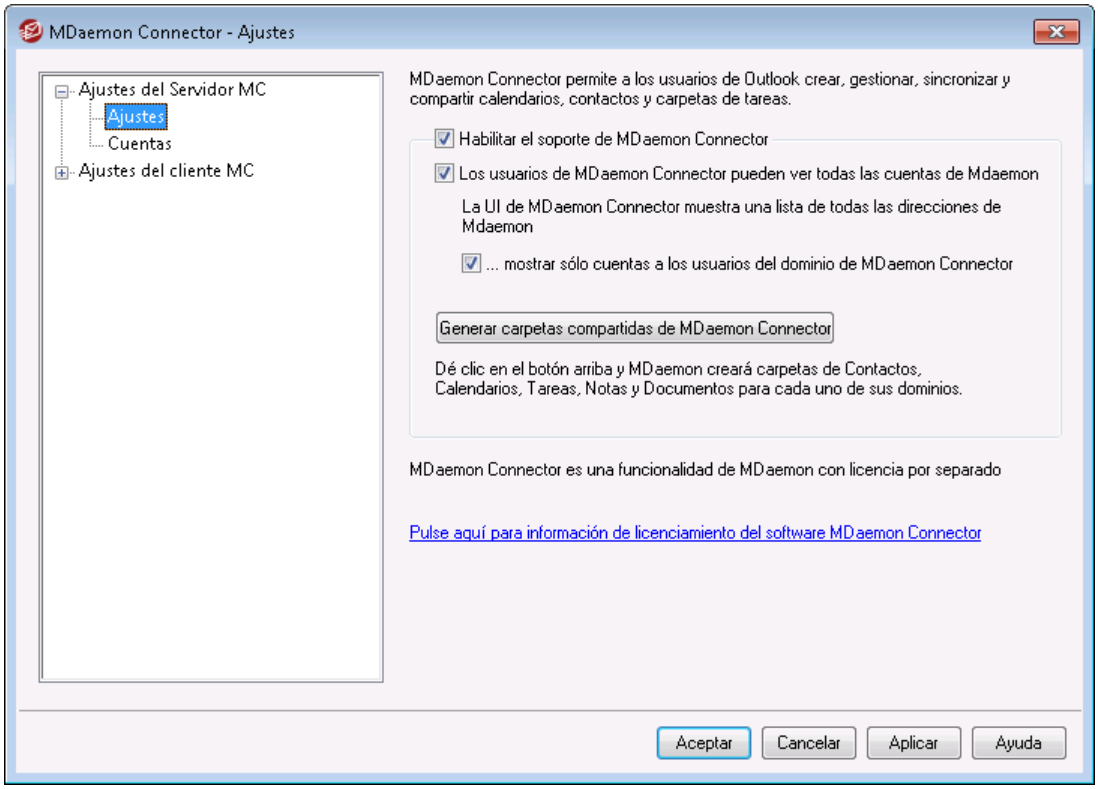
Localizado en Inicio » MDaemon Connector, este diálogo se utiliza para activar y configurar MDaemon Connector y para autorizar a utilizarlo a cuentas específicas.

Ver:

Ajustes del Servidor MC » Ajustes 387
Ajustes del Servidor MC » Cuentas 389
Ajustes del Cliente MC 390

3.8.1 Ajustes del Servidor MC

3.8.1.1 Ajustes



MDaemon Connector

Habilitar el soporte de MDaemon Connector
Haga clic en esta casilla para activar MDaemon Connector (MC). Sus usuarios no podrán utilizar las funcionalidades de MC a menos que esta opción esté habilitada.

Los usuarios de MDaemon Connector pueden ver todas las cuentas de MDaemon
Haga clic en esta opción si quiere que todas las cuentas de MDaemon que hayan sido autorizadas a conectarse vía MDaemon Connector sean visibles en la lista de *Permisos* que aparece en MDaemon Connector en los clientes de los usuarios. Desde esa lista, los usuarios de MC pueden elegir las cuentas a las que desean otorgar permisos para compartir sus elementos de Outlook. Cuando esta opción está des habilitada, la lista Permisos de MDaemon Connector aparecerá en blanco y los usuarios tendrán que ingresar las direcciones de correo manualmente. Solo podrán compartir elementos de Outlook las direcciones pertenecientes a cuentas autorizadas a conectarse vía MC. Si un usuario captura una dirección no autorizada, los elementos no serán compartidos a menos que se le autorice posteriormente a conectarse vía MC.

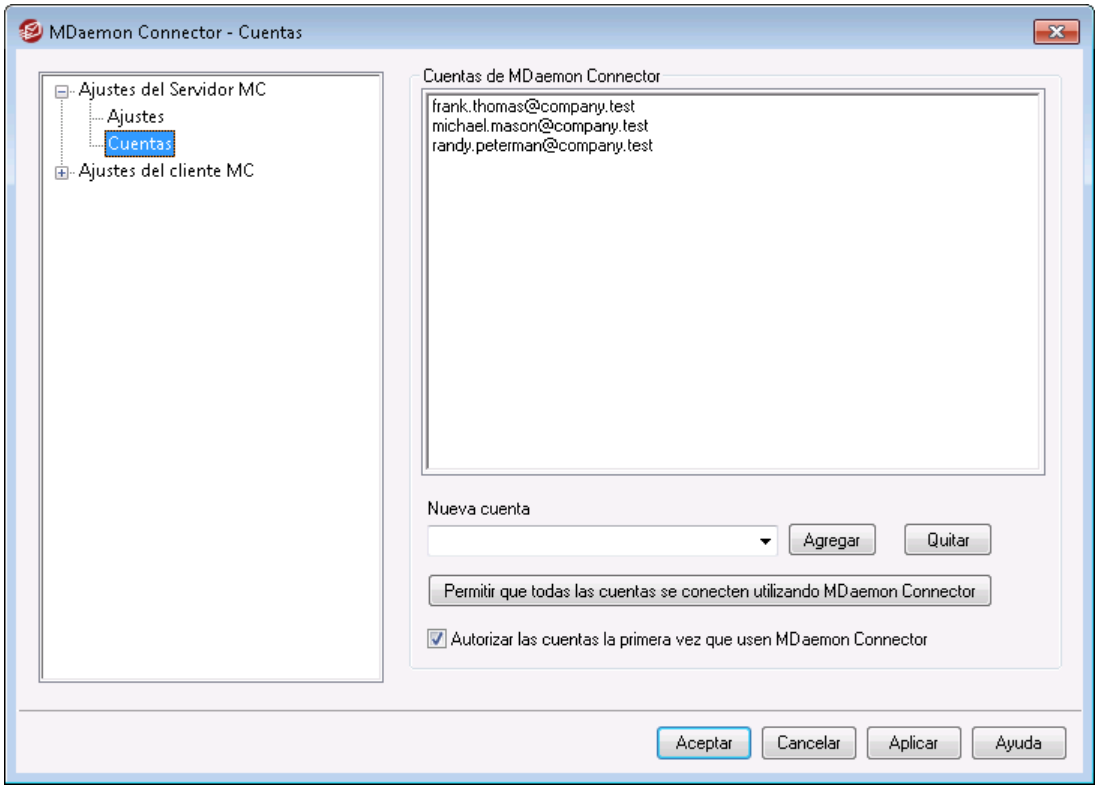
...mostrar sólo cuentas a los usuarios del dominio de Outlook Connector
Esta opción sólo está disponible cuando está habilitada la opción anterior *Los usuarios de MDaemon Connector pueden ver todas las cuentas de MDaemon*. Marque esta casilla si quiere que sólo los usuarios autorizados a conectar vía Outlook Connector, y que pertenezcan al mismo dominio, aparezcan en la lista de *Permisos* en MDaemon Connector. Las cuentas que pertenezcan a diferentes dominios no se listarán, aunque estén autorizadas a conectarse a vía MDaemon Connector.

Generar carpetas compartidas de MDaemon Connector
Haga clic en este botón para generar un conjunto de carpetas de MC para cada dominio. Generará las siguientes carpetas: Contactos, Calendario, Agenda, Tareas y Notas.

Ver:

Ajustes de Servidor MC » Cuentas 389
Ajustes de Cliente MC 390

3.8.1.2 Cuentas



Cuentas de MDaemon Connector

Esta es la lista de usuarios de MDaemon que están autorizados a compartir sus carpetas de Outlook, Contactos, Calendarios, Notas, y demás, a través de MDaemon Connector. Puede añadir usuarios a la lista usando las opciones definidas a continuación.

Cuentas nuevas
Para añadir una cuenta de MDaemon a la lista de cuentas autorizadas de MDaemon Connector, seleccione la cuenta deseada de esta lista desplegable y luego haga clic en *Agregar.* Para eliminar la cuenta, selecciónela y dé clic en *Eliminar.*

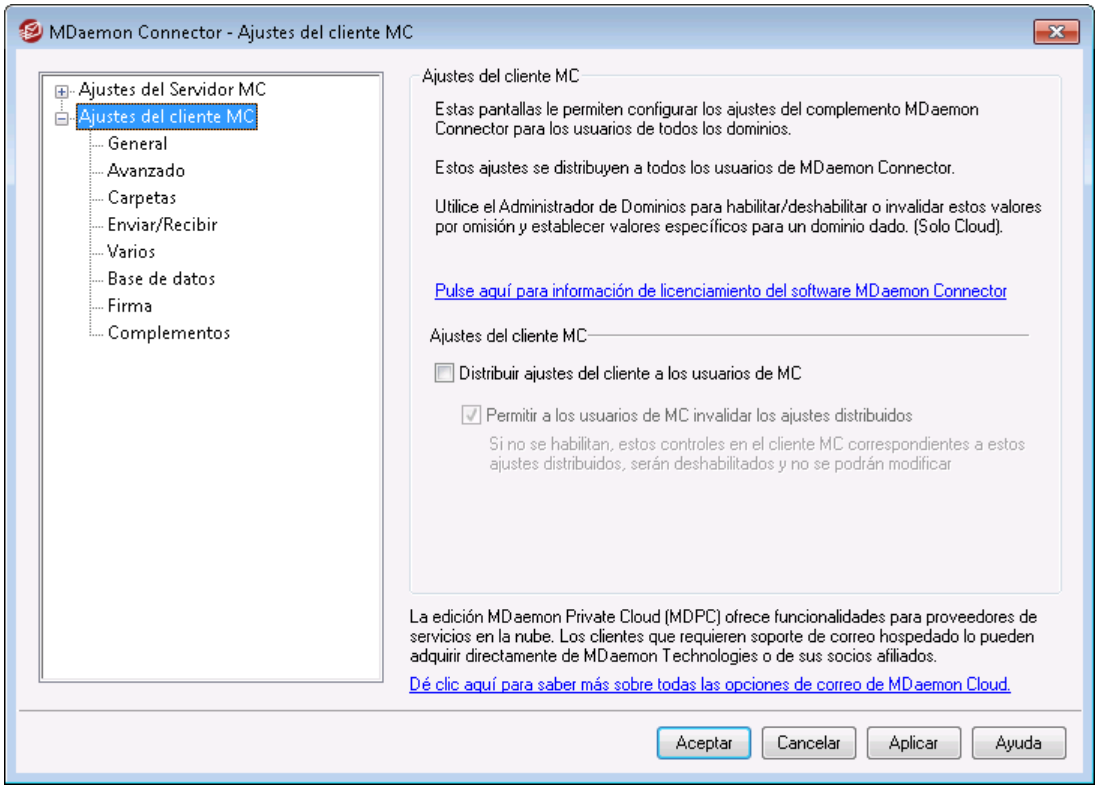
Permitir que todas las cuentas utilicen MDaemon Connector
Para autorizar automáticamente a todas las cuentas de MDaemon para que se conecten vía MDaemon Connector, haga clic en este botón y todas las cuentas de MDaemon serán añadidas a la lista de *Cuentas de MDaemon Connector.*

Autorizar las cuentas la primera vez que usen MDaemon Connector
Haga clic en esta casilla si quiere que las cuentas individuales sean añadidas a la lista de *Cuentas de MDaemon Connector* la primera vez que cada una conecte con MDaemon Connector. **Nota:** si habilita esta opción, estará efectivamente autorizando a todas las cuentas de MDaemon a utilizar MDaemon Connector. Las cuentas simplemente no se añadirán a la lista hasta que se hayan conectado por primera vez.

Ver:

Ajustes del Servidor OC » Ajustes 387
Ajustes del Cliente OC 390

3.8.2 Ajustes del Cliente MC



Utilice el diálogo Ajustes del Cliente MC para administrar centralizadamente los ajustes de cliente de sus usuarios de MDaemon Connector. Configure cada pantalla con los ajustes que considere y MDaemon los entregará a las pantallas correspondientes de los clientes conforme sea necesario, cada vez que los usuarios de MDaemon Connector se conecten al servidor. Los Ajustes del Cliente MC solo se envían a los clientes cuando uno de los valores haya sido modificado desde la última ocasión que el cliente se haya conectado y los haya recibido. Si está habilitada la opción "*Permitir a los usuarios de MC omitir los ajustes entregados*", los usuarios pueden modificar en su cliente individual cualquier ajuste que haya sido determinado en el servidor. Si esta opción está deshabilitada, entonces todas las pantallas en el cliente estarán bloqueadas; los usuarios de MDaemon Connector no podrán hacer modificaciones.

Para permitir ciertos ajustes que deben ser diferentes para cada usuario o dominio, los Ajustes de Cliente MC soportan macros tales como `$USERNAME$`, `$EMAIL$` y `$DOMAIN$`. Estas macros se convertirán en datos específicos para el usuario o

dominio cuando los ajustes se entreguen al cliente. Tenga cuidado de no colocar valores estáticos en ninguno de los campos que utilizarán una macro, tal como colocar algo así como "Frank Thomas" en el campo Su Nombre. Si lo hace, todos los usuarios de Outlook Connector que se conecten a MDaemon, verán su nombre configurado como "Frank Thomas." Para su conveniencia, se colocó el botón Referencia de Macros en la pantalla General 392 que despliega una lista de las macros soportadas.

Para aquellos que utilizan MDaemon Private Cloud (MDPC), existe otro diálogo Ajustes de Cliente de MC en el Administrador de Dominios 190, para controlar los ajustes de cliente de MDaemon Connector con base en el dominio.

Esta funcionalidad se encuentra deshabilitada por omisión y solo es soportada por el cliente de MDaemon Connector versión 4.0.0 o superior.

Ajustes de Cliente MC

Entregar ajustes de cliente a usuarios de MC
Habilite esta opción si desea entregar los ajustes preconfigurados en la pantalla Ajustes de Cliente MC hacia sus usuarios de MDaemon Connector siempre que se conecten. Los Ajustes de Cliente MC solo se envían a los clientes cuando uno de los ajustes ha sido modificado desde la última ocasión en que el cliente se conectó y los recibió. Esta opción se encuentra deshabilitada por omisión.

Permitir a los usuarios de MC omitir los ajustes entregados
Si se habilita esta opción, los usuarios pueden omitir cualquiera de los ajustes entregados en sus clientes individuales. Si se encuentra deshabilitada, todas las pantallas de cliente estarán bloqueadas; los usuarios de MDaemon Connector no podrán hacer modificaciones.

Permitir a los usuarios omitir los ajustes entregados, no impide que el servidor entregue cambios futuros a los clientes. Por ejemplo, si un usuario modifica alguno de los ajustes de MDaemon Connector y luego el administrador realiza un cambio en alguna de las pantallas de Ajustes del Cliente MC en el servidor, todos los Ajustes de Cliente serán entregados al cliente de ese usuario la siguiente ocasión que se conecte al servidor. Por esto, el ajuste establecido previamente por el usuario será modificado para coincidir con los ajustes del servidor.

Descubrimiento Automático de Ajustes de MC

Cuando se configura inicialmente MDaemon Connector en el cliente, lo usuarios pueden dar clic en el botón "*Probar & Obtener Ajustes de Cuenta*" en la pantalla General luego de registrar el *Nombre de Usuario* y la *Contraseña*. Esto hace que MDaemon Connector intente validar las credenciales y recuperar automáticamente la Información del Servidor para la cuenta.

Para conectarse al servidor, primero el cliente probará los valores FQDN más comunes. Para IMAP, intenta autenticarse en `mail.<domain>` (ej. `mail.example.com`) utilizando el puerto SSL dedicado, luego el puerto no SSL con TLS. Si no tiene éxito entonces repetirá el mismo proceso con `imap.<domain>`,

luego `<domain>` y finalmente con `imap.mail.<domain>`. Si todos los intentos fallan entonces se intenta el inicio de sesión no encriptado para esas mismas direcciones.

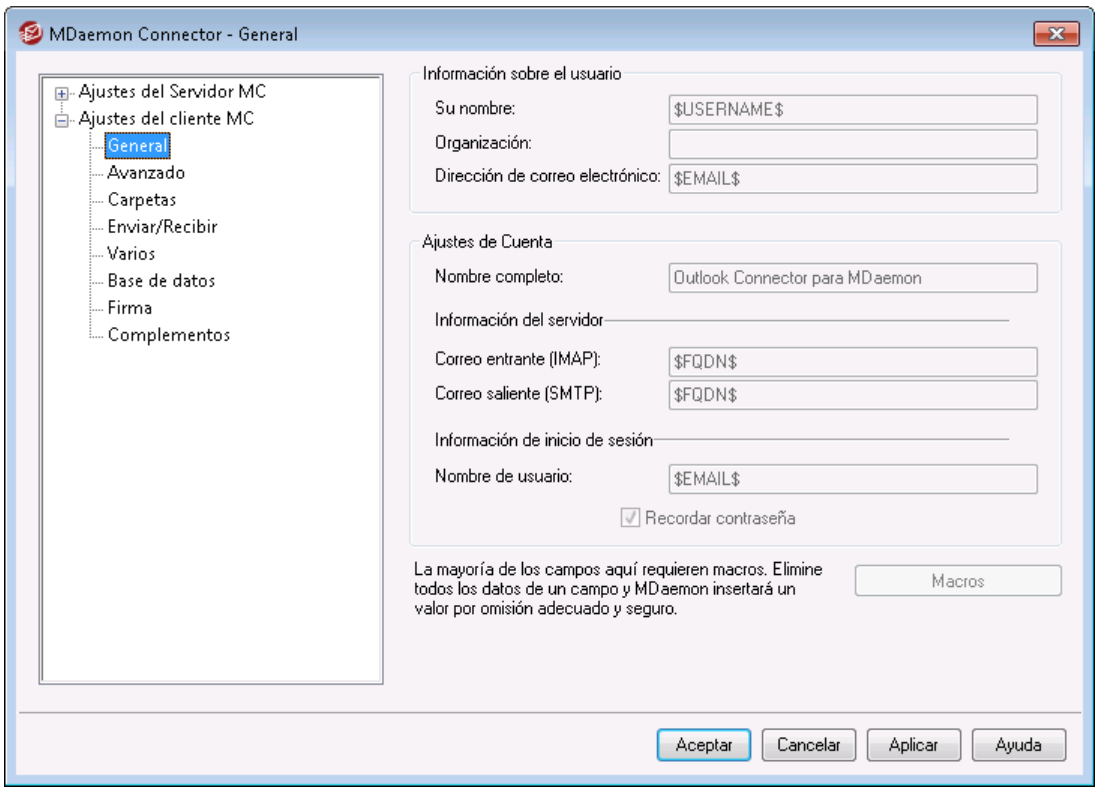
Para SMTP, prueba en `mail.<domain>` utilizando los puertos 587, 25 y luego 465, utilizando primero SSL y luego TLS. Esto se repite para `smtp.<domain>`, `<domain>` y luego `smtp.mail.<domain>`. Si todos los intentos fallan entonces se intenta el inicio de sesión no encriptado para esas mismas direcciones.

Si MDaemon Connector se puede autentificar exitosamente, la información entrante y saliente del servidor junto con la información SSL/TLS se configura automáticamente.

Ver:

Ajustes de Cliente MC » Ajustes 387
Ajustes de Cliente MC » Cuentas 389
Ajustes de Cliente MC » General 392

3.8.2.1 General



Cuando ha habilitado la opción "*Entregar ajustes de cliente MC a los usuarios*" en la pantalla Ajustes de Cliente MC 390, los ajustes en esta pantalla se entregarán a la pantalla correspondiente en el cliente de MDaemon Connector siempre que un usuario de MDaemon Connector se conecte al servidor. Los Ajustes de Cliente MC solo se envían a los clientes cuando uno de los valores ha sido modificado desde la última ocasión en que se conectó el cliente y los recibió. La mayoría de los campos

en esta pantalla deben contener macros en lugar de valores estáticos. Ver abajo Referencia de Macros 394.

Información de Usuario

Su Nombre
Por omisión esta opción utiliza la macro $USERNAME$ que inserta el nombre y apellido del usuario. Este aparece en el encabezado From en los mensajes del usuario.

Organización
Este es un espacio opcional para el nombre de su negocio u organización.

Dirección de Correo Electrónico
Por omisión esta opción utiliza la macro $EMAIL$, que inserta la dirección de correo electrónico del usuario. Esta aparece en el encabezado From en los mensajes del usuario.

Ajustes de Cuenta

Nombre de Despliegue
Este nombre se despliega en Outlook de manera que el usuario puede identificar qué cuenta está utilizando. Esto es útil para usuarios que tienen múltiples cuentas en su perfil. Solo el usuario ve esta información. Esta se configura por omisión como "MDaemon Connector".

Información del Servidor

Correo Entrante (IMAP)
Este es el servidor al que tienen acceso los clientes de MDaemon Connector para recolectar y administrar el correo de cada usuario. Se define por omisión como $FQDN$.

Correo Saliente (SMTP)
Este es el servidor al que se conectan los clientes de MDaemon Connector para enviar los mensajes salientes del usuario. Con frecuencia es el mismo que el Servidor Entrante (IMAP) anterior. Se define por omisión como $FQDN$.

Información de Inicio de Sesión

Nombre de Usuario
Este es el nombre de usuario requerido para accesar y administrar cada cuenta de correo de los usuarios de MDaemon. Este es típicamente el nombre de la *Dirección de Correo* mencionada arriba. Se define por omisión como $EMAIL$.

Recordar contraseña
Por omisión los clientes de MDaemon Connector se configuran para grabar la contraseña de usuario, de manera que cuando Outlook inicia automáticamente inicia sesión con la cuenta de correo sin pedir las credenciales. Deshabilite esta opción si desea requerir a los usuarios que ingresen su contraseña al iniciar Outlook.

Referencia de Macros

Para permitir que ciertos ajustes sean diferentes para cada usuario o dominio, los Ajustes de Cliente MC soportan macros tales como `$USERNAME$`, `$EMAIL$` y `$DOMAIN$`. Estas macros se convertirán en datos específicos por usuario o dominio al entregar los ajustes al cliente. Tenga cuidado de no colocar valores estáticos en ningún campo que utilice una macro, como colocar "Frank Thomas" en el campo *Su Nombre*. El hacerlo originará que todo usuario de MDaemon Connector que se conecte a MDaemon tenga registrado su nombre como "Frank Thomas." Dé clic en el botón Referencia de Macros para visualizar la lista de macros disponibles:

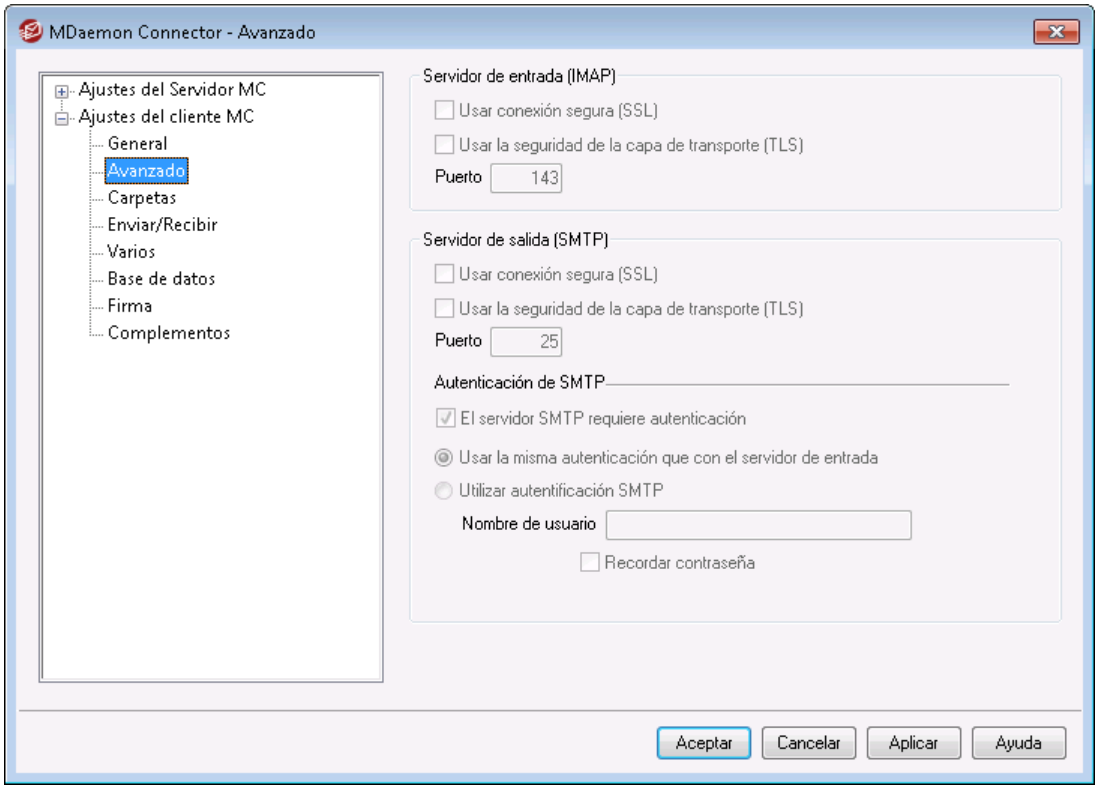
`$USERNAME$`	Esta macro inserta el valor de la opción "*Nombre y Apellido*" en la pantalla Detalles de Cuenta[715] del usuario. Es equivalente a: "$USERFIRSTNAME$ $USERLASTNAME$"
`$EMAIL$`	Inserta la dirección de correo del usuario. Es equivalente a: $MAILBOX$@$DOMAIN$.
`$MAILBOX$`	Esta macro inserta el Nombre de Buzón[715] de la cuenta.
`$USERFIRSTNAME$`	Esta macro resuelve el nombre del propietario de la cuenta.
`$USERFIRSTNAMELC$`	Esta macro resuelve el nombre del propietario de la cuenta, en minúsculas.
`$USERLASTNAME$`	Esta macro resuelve el apellido del propietario de la cuenta.
`$USERLASTNAMELC$`	Esta macro resuelve el apellido del propietario de la cuenta, en minúsculas.
`$USERFIRSTINITIAL$`	Esta macro resuelve la inicial del nombre del propietario de la cuenta.
`$USERFIRSTINITIALLC$`	Esta macro resuelve la inicial del nombre del propietario de la cuenta, en minúsculas.
`$USERLASTINITIAL$`	Esta macro resuelve la inicial del apellido del propietario de la cuenta.
`$USERLASTINITIALLC$`	Esta macro resuelve la inicial del apellido del propietario de la cuenta, en minúsculas.
`$MAILBOXFIRSTCHARSn$`	Donde "n" es un número entre 1 y 10. Se expandirá a los primeros "n" caracteres del nombre del buzón.

$DOMAIN$	Inserta el Dominio del Buzón[715] de la cuenta.
$DOMAINIP$	Esta macro resuelve a la Dirección IPv4[192] asociada con el dominio al que pertenece la cuenta.
$DOMAINIP6$	Esta macro resuelve a la Dirección IPv6[192] asociada con el dominio al que pertenece la cuenta.
$FQDN$	Inserta el valor Fully Qualified Domain Name, o Nombre del Servidor SMTP[192], del dominio a que pertenece la cuenta.
$PRIMARYDOMAIN$	Esta macro resuelve al nombre del dominio por omisión[190].
$PRIMARYIP$	Esta macro resuelve a la Dirección IPv4[192] asociada con el dominio por omisión[190] de MDaemon.
$PRIMARYIP6$	Esta macro resuelve a la Dirección IPv6[192] asociada con el dominio por omisión[190] de MDaemon.

Ver:

Ajustes de Cliente MC[390]
Ajustes de Cliente MC » Ajustes[387]
Ajustes de Cliente MC » Cuentas[389]

3.8.2.2 Avanzado



Cuando tiene habilitada la opción "*Entregar ajustes de cliente a usuarios de MC*" en la pantalla Ajustes de Cliente MC 390, los ajustes en esta pantalla se entregarán a la pantalla correspondiente en el cliente de MDaemon Connector siempre que un usuario de MC se conecte al servidor. Los Ajustes de Cliente MC solo se envían a los clientes cuando uno de los valores se ha modificado desde la última ocasión en que el cliente se conectó y los recibió.

Servidor Entrante (IMAP)

Utilizar conexión segura (SSL)
Habilite esta casilla si desea que los clientes utilicen una conexión SSL segura al conectarse al servidor de Correo Entrante (IMAP). Al habilitar esta opción se modifica en automático el puerto al "993" que es el puerto SSL por omisión.

Utilizar TLS (Transport Layer Security)
Marque esta casilla si desea que los clientes MC utilicen una conexión TLS segura al conectarse al servidor de Correo Entrante (IMAP).

Puerto
Este es el puerto al que se conectarán los clientes de MDaemon Connector hacia el servidor de Correo Entrante (IMAP). Por omisión este es el 143 para conexiones IMAP o 993 para conexiones encriptadas SSL.

Servidor Saliente (SMTP)

Utilizar conexión segura (SSL)
Habilite esta casilla si desea que los clientes utilicen una conexión SSL segura al conectarse al servidor de Correo Saliente (SMTP). Al habilitar esta opción se modifica en automático el puerto al "465," que es el puerto SSL por omisión.

Utilizar TLS (Transport Layer Security)
Marque esta casilla si desea que los clientes MC utilicen una conexión TLS segura al conectarse al servidor de Correo Saliente (SMTP).

Puerto
Este es el puerto al que se conectarán los clientes de MDaemon Connector hacia el servidor de Correo Saliente (SMTP). Por omisión este es el 25 para conexiones SMTP o 465 para conexiones SMTP encriptadas SSL.

Autentificación SMTP

El servidor SMTP requiere autentificación
Por omisión los usuarios deben validar las credenciales de inicio de sesión para autentificarse al conectarse al servidor Saliente (SMTP) para enviar un mensaje de correo electrónico.

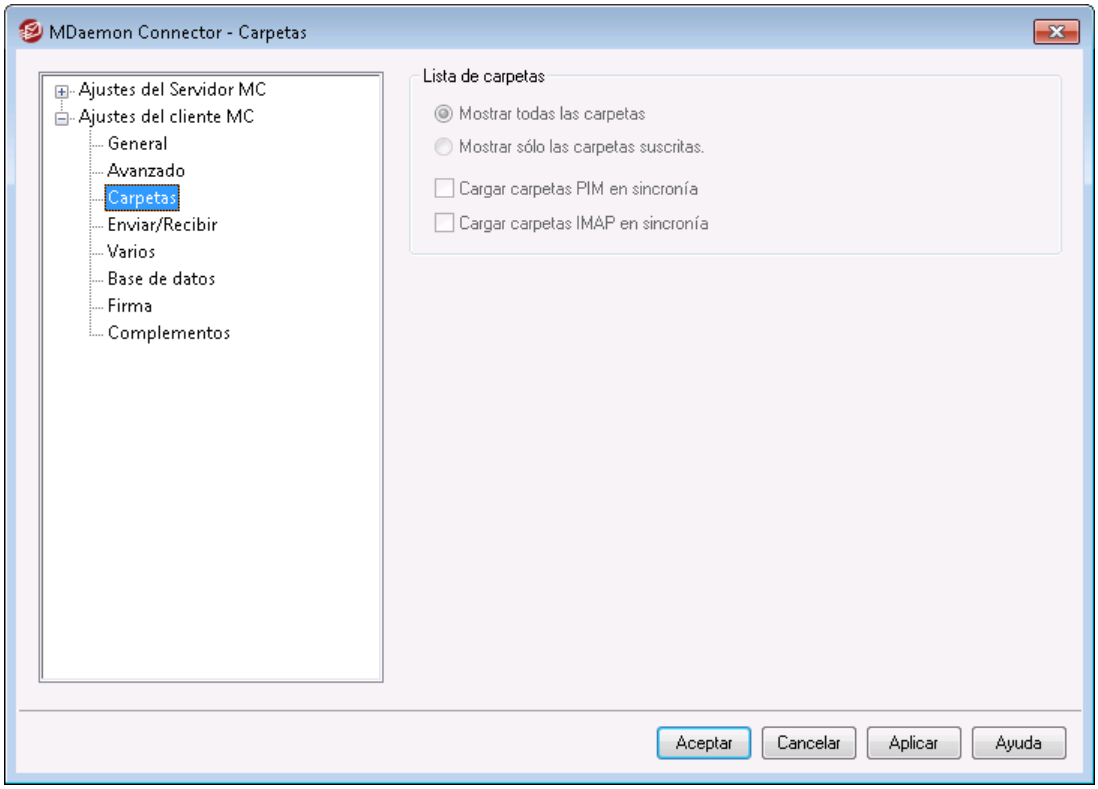
Utilice la misma Autentificación para el Servidor Entrante
Por omisión los clientes de MDaemon Connector se autentificarán utilizando las mismas credenciales en el servidor de Correo Saliente (SMTP) que las que utilizan para el servidor de Correo Entrante (IMAP).

Utilizar autentificación SMTP
Utilice esta opción si desea requerir que los usuarios de MDaemon Connector utilicen diferentes credenciales de autentificación al enviar mensajes, esto puede ser necesario al utilizar un servidor distinto para el correo saliente.

Ver:

Ajustes de Cliente OC 390
Ajustes de Servidor MC » Ajustes 387
Ajustes de Servidor MC » Cuentas 389

3.8.2.3 Carpetas



Cuando tiene habilitada la opción "*Entregar ajustes de cliente a usuarios de MC*" en la pantalla Ajustes de Cliente MC, los ajustes en esta pantalla se entregarán a la pantalla correspondiente en el cliente de MDaemon Connector siempre que un usuario de MC se conecte al servidor. Los Ajustes del Cliente de MC solo se envían a los clientes cuando uno de los valores se ha modificado desde la última ocasión en que el cliente se conectó y los recibió.

Lista de Carpetas

Mostrar todas las Carpetas
Por omisión la lista de carpetas en Outlook desplegará todas las carpetas a las que tiene acceso el usuario de MDaemon Connector en el servidor de correo.

Mostrar solo las Carpetas Suscritas
Seleccione esta opción si desea que la lista de carpetas en Outlook despliegue solo aquellas carpetas a las que el usuario se ha suscrito.

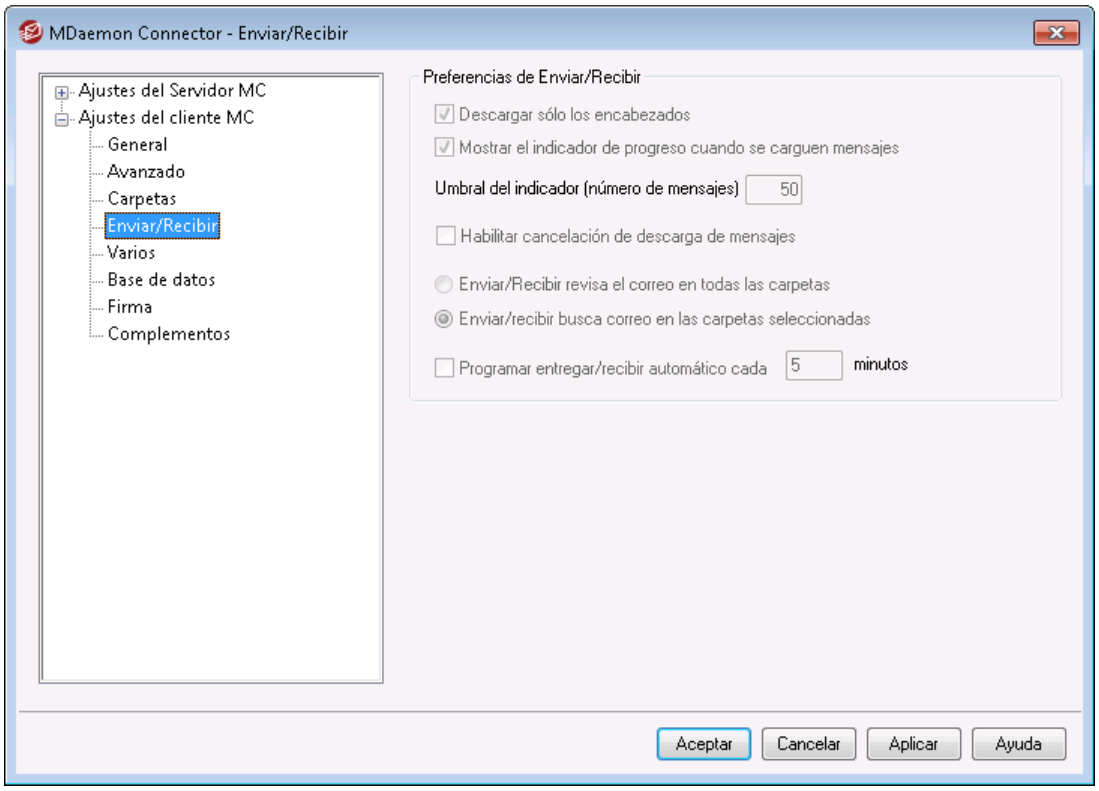
Cargar carpetas PIM de manera síncrona
En la mayoría de los casos esta opción no debería estar marcada, lo que significa que un usuario de MDaemon Connector puede continuar utilizando Outlook mientras MDaemon Connector carga los contenidos de las carpetas PIM (esto es, carpetas no de correo tales como: Contactos, Calendarios y Tareas). Si selecciona esta casilla, Outlook efectivamente quedará bloqueado hasta que se hayan cargado todos los datos. En general esta opción puede requerirse solo cuando el usuario cuenta con aplicaciones de terceros que intentan tener acceso al contenido de las carpetas PIM.

Cargar carpetas IMAP de manera síncrona
En la mayoría de los casos esta opción no debería estar marcada, lo que significa que un usuario de MDaemon Connector puede continuar utilizando Outlook mientras MDaemon Connector carga los contenidos de las carpetas IMAP del usuario. Si marca esta casilla entonces Outlook efectivamente quedará bloqueado hasta que se hayan cargado todos los datos. En general esta opción puede requerirse solo cuando el usuario cuenta con aplicaciones de terceros que intentan tener acceso al contenido de las carpetas de correo.

Ver:

Ajustes de Cliente MC 390
Ajustes de Cliente MC» Ajustes 387
Ajustes de Servidor MC» Cuentas 389

3.8.2.4 Enviar/Recibir



Cuando ha habilitado la opción "*Entregar ajustes de cliente MC a los usuarios*" en la pantalla Ajustes de Cliente MC 390, los ajustes en esta pantalla se entregarán en la pantalla correspondiente del Cliente de MDaemon Connector siempre que el usuario de MC se conecte al servidor. Los Ajustes de Cliente MC solo se envían a los clientes cuando uno de esos valores se ha modificado desde la última ocasión en que el cliente se conectó y los recibió.

Preferencias de Envío/Recepción

Descargar solo encabezados
Por omisión cuando MDaemon Connector Envía/Recibe y encuentra mensajes nuevos, solo descargará los encabezados de los mensajes (i.e. To, From, Subject y similares) para despliegue en la lista de mensajes. El mensaje completo no se descarga hasta que se visualiza.

Mostrar indicador de avance al descargar mensajes
MDaemon Connector despliega un indicador de avance al descargar un gran número de mensajes. Deshabilite esta casilla si no desea que despliegue el indicador de avance.

Umbral del Indicador (número de mensajes)
Cuando se habilita la opción *Mostrar indicador de avance...,* el indicador de avance se despliega al descargar una cantidad igual o mayor a este número de mensajes.

Habilitar cancelación de descarga de mensajes
Marque esta casilla si desea que los usuarios de MDaemon Connector puedan cancelar la descarga cuando MDaemon Connector está descargando un mensaje grande.

Enviar/Recibir verifica correo en todas las carpetas
Seleccione esta opción si desea que MDaemon Connector verifique si existen mensajes nuevos en todas las carpetas de correo cuando ejecuta la acción Enviar/Recibir en la cuenta del usuario.

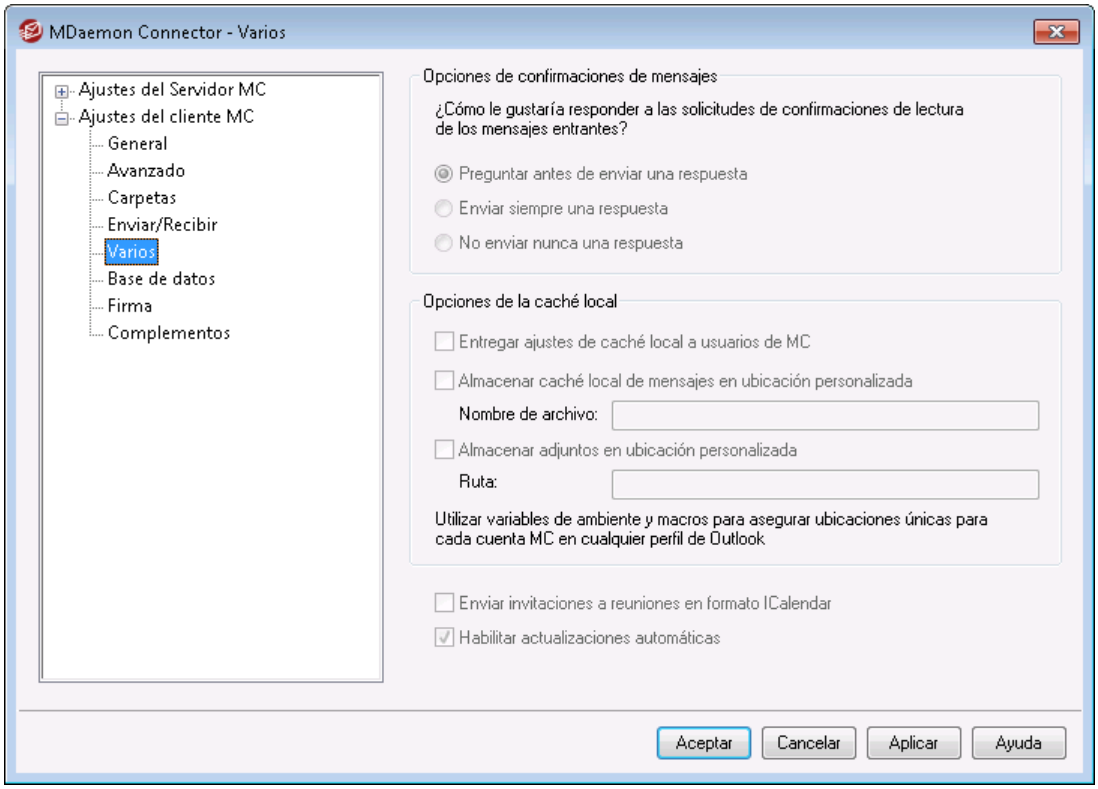
Enviar/Recibir verifica correo en las carpetas seleccionadas
Seleccione esta opción si desea que MDaemon Connector verifique si existen mensajes nuevos en las carpetas definidas por el usuario, al enviar/recibir con la cuenta.

Programar Enviar/Recibir automáticamente cada [xx] minutos
Utilice esta opción si desea enviar/recibir en intervalos determinados.

Ver:

Ajustes de Cliente MC 390
Ajustes de Cliente MC » Ajustes 387
Ajustes de Servidor MC » Cuentas 389

3.8.2.5 Misceláneos



Cuando ha habilitado la opción "*Entregar ajustes de cliente MD a los usuarios*" en la pantalla Ajustes de Cliente MD 390, los ajustes en esta pantalla se entregarán a la pantalla correspondiente en el cliente de MDaemon Connector siempre que el usuario de MDaemon Connector se conecte al servidor. Los Ajustes de cliente MD solo se envían a cliente cuando uno de los ajustes se ha modificado desde la última ocasión en que el cliente se conectó y los recibió.

Administrar Opciones de Recepción

En ocasiones los mensajes entrantes contienen encabezados especiales que solicitan se envíe una respuesta automática al remitente para que sepa cuando ha leído usted el mensaje. Configure esta opción para especificar como quiere que MDaemon Connector maneje los mensajes que solicitan confirmación de lectura.

Preguntarme antes de enviar respuesta
Seleccione esta opción si desea que se les pregunte a los usuarios si se envía o no la confirmación de lectura del mensaje cuando abran el mensaje que lo solicita.

Enviar respuesta siempre
Seleccione esta opción si desea enviar un mensaje de confirmación de lectura siempre que el usuario abra el mensaje que lo solicita.

Nunca enviar respuesta
Seleccione esta opción si no desea que MDaemon Connector responda a las peticiones de confirmación de lectura.

Opciones en caché local

Las opciones en esta sección controlan la ubicación específica en que se crea el caché local de mensajes del usuario, así como la ubicación donde se guardan los archivos adjuntos.

Estas opciones requieren que el usuario tenga instalada la versión de MDaemon Connector 4.5.0 o superior.

Entregar los ajustes de caché local a usuarios de MD
Por omisión, MDaemon no entrega los ajustes al cliente de MDaemon Connector. Habilite esta casilla si desea que se entreguen. El cliente de MDaemon Connector moverá los archivos locales de su ubicación actual a la ubicación por omisión o la ubicación personalizada si especifica una en las opciones siguientes.

Almacenar el archivo local de caché en una ubicación personalizada | Nombre de Archivo
Especifique una ruta local y nombre de archivo para el caché si desea que el cliente de MDaemon Connector mueva los archivos locales a una ubicación personalizada. Se deberán utilizar variables de ambientes y macros para asegurar que se define una ubicación única para cada usuario. Por ejemplo:

```
%APPDATA%\Alt-N\MDaemon Connector 2.0\Accounts\%OUTLOOKPROFILE%\
  %OUTLOOKEMAIL%\LocalCache.db
```

Almacenar archivos adjuntos en una ubicación personalizada | Ruta
Si desea personalizar la ubicación de la carpeta en que el cliente de MDaemon Connector almacena los archivos adjuntos, especifique esa ruta aquí. Se deberán utilizar variables de ambiente y macros para asegurar que se define una ubicación única para cada usuario.

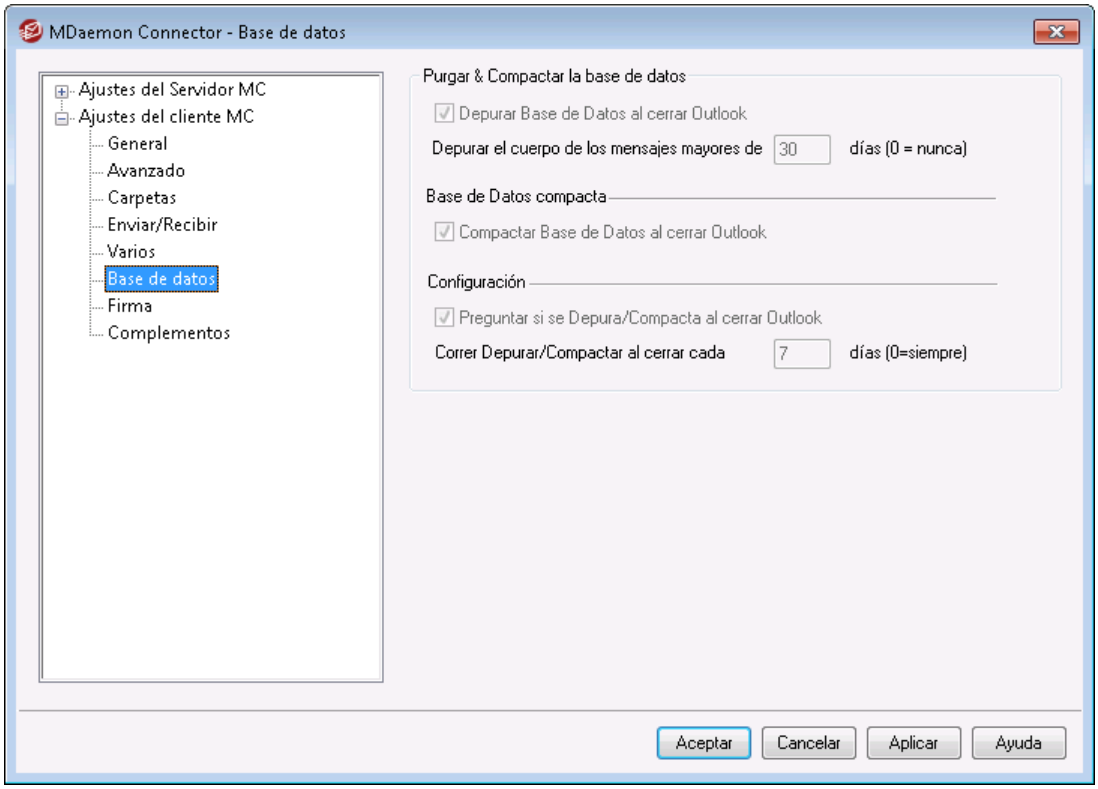
Enviar solicitudes de reuniones en formato iCalendar
Marque esta caja si desea que MDaemon Connector envíe las solicitudes de reuniones en formato iCalendar (iCal).

Habilitar actualizaciones automáticas
Por omisión MDaemon Connector se actualizará en automático siempre que se encuentre disponible una nueva versión. Deshabilite esta casilla si no desea que se actualice en automático.

Ver:

Ajustes de Cliente MD 390
Ajustes de Cliente MD » Ajustes 387
Ajustes de Servidor MD » Cuentas 389

3.8.2.6 Base de Datos



Cuando ha habilitado la opción "*Entregar ajustes de cliente MD a los usuarios*" en la pantalla Ajustes de Cliente MD 390, los ajustes en esta pantalla se entregarán a la pantalla correspondiente en el cliente de MDaemon Connector siempre que el usuario de MDaemon Connector se conecte al servidor. Los Ajustes de cliente MD solo se envían a cliente cuando uno de los ajustes se ha modificado desde la última ocasión en que el cliente se conectó y los recibió.

Purgar & Compactar la Base de Datos

Purgar la base de datos al cerrar Outlook
Para conservar espacio en disco y mejorar el rendimiento, por omisión MDaemon Connector se configura para purgar/eliminar el cuerpo de mensajes viejos al cierre de Outlook. Esto no elimina los encabezados de los mensajes ni afecta los mensajes originales almacenados en el servidor; simplemente elimina el cuerpo de los mensajes viejos grabado en el caché local. Siempre que abra un mensaje viejo que haya sido purgado en el pasado, el cuerpo del mensaje se descargará de nuevo a su computadora. Más aun, solo se purgan los cuerpos de mensajes de correo; no se afecta a Contactos, Calendarios, Tareas, Diarios o Notas. Deshabilite esta opción si no desea purgar la base de datos al cierre.

Purgue el cuerpo de mensajes mayores de XX días (0¨= nunca)

Utilice esta opción para definir qué tan viejos deben ser los mensajes para que su cuerpo se purgue al cerrarse Outlook. Por omisión un mensaje debe tener más de 30 días para que sea purgado. Su edad se basa en la fecha de modificación del mensaje. utilice "0" en esta opción si no desea que se purguen.

Compactar Base de Datos

Compactar base de datos al cerrar Outlook
Para conservar espacio en disco y mejorar el rendimiento, por omisión MDaemon Connector está configurado para compactar y defragmentar la base de datos del caché local de mensajes siempre que el usuario cierre Outlook. Sin embargo, Outlook debe cerrar limpiamente para que la acción de compartir ocurra; si Outlook se cierra inesperadamente o usted utiliza el Administrador de Tareas para "Finalizar la Tarea", la base de datos no será compactada. Puede utilizar las opciones en la sección Configuración abajo para definir con qué frecuencia debe ocurrir esto y si se le pregunta o no antes de que ocurra.

Configuración

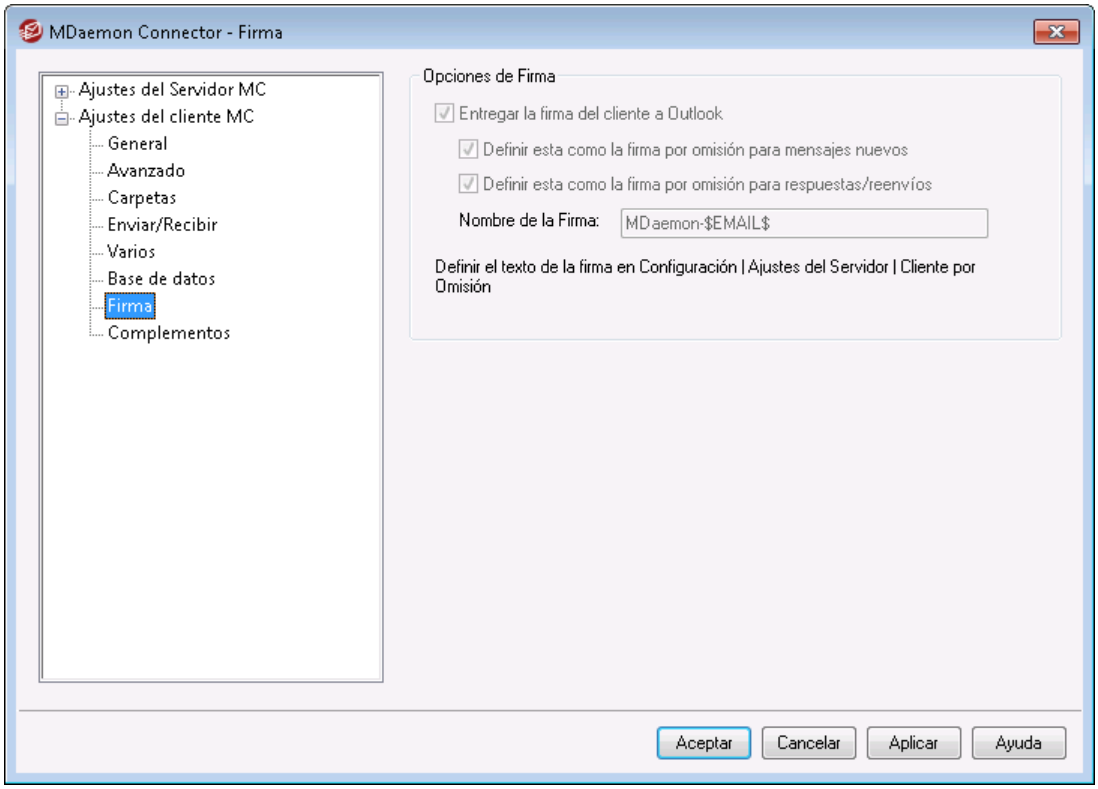
Preguntarme si se Purga/Compacta al cierre de Outlook
Utilice esta opción si desea que se pregunte a los usuarios antes de que MDaemon Connector purgue o compacte el archivo de la base de datos al cierre. Si el usuario da clic en **SI**, entonces se realizarán las acciones de compactación o purga, desplegando un indicador de avance mientras esto ocurre. Deshabilite esta casilla si no desea que se pregunte a los usuarios; al cierre de MDaemon Connector se purgará o compactará la base de datos automáticamente, desplegando un indicador de avance al hacerlo.

Ejecutar Purgar/Compactar al cierre de Outlook cada XX días (0=siempre)
Esta opción controla la frecuencia con que MDaemon Connector purga o compacta la base de datos al cierre. Por omisión esta opción está configurada en 7 días, lo que significa que ejecutará Purgar/Compactar al cierre una vez cada siete días. Configure esta opción en "0" si desea purgar/compactar la base de datos cada vez que Outlook se cierre.

Ver:

Ajustes de Cliente MD 390
Ajustes de Cliente MD » Ajustes 387
Ajustes de Servidor MD » Cuentas 389

3.8.2.7 Firma



Cuando ha habilitado la opción "*Entregar ajustes de cliente a los usuarios de MC*" en la pantalla Ajustes de Cliente MC 390, los ajustes seleccionados en esta pantalla serán entregados en la pantalla Firmas (localizada en Outlook bajo **Archivo » Opciones » Correo » Firmas**) siempre que un usuario de MDaemon Connector se conecte al servidor. Esta funcionalidad requiere de MDaemon Connector 6.5.0 o superior.

Opciones de Firma

Entregar firma de cliente a Outlook
Habilite esta opción si desea entregar la firma por omisión del cliente 147 (o la firma del cliente 215 específica para el dominio, si se ha creado alguna) a sus usuarios de MDaemon Connector. Designe un nombre para la firma en la opción que se describe abajo *Nombre de la firma*.

Firma por omisión para mensajes nuevos
Marque esta casilla si desea hacer que la firma del cliente sea la de omisión a utilizar para mensajes nuevos.

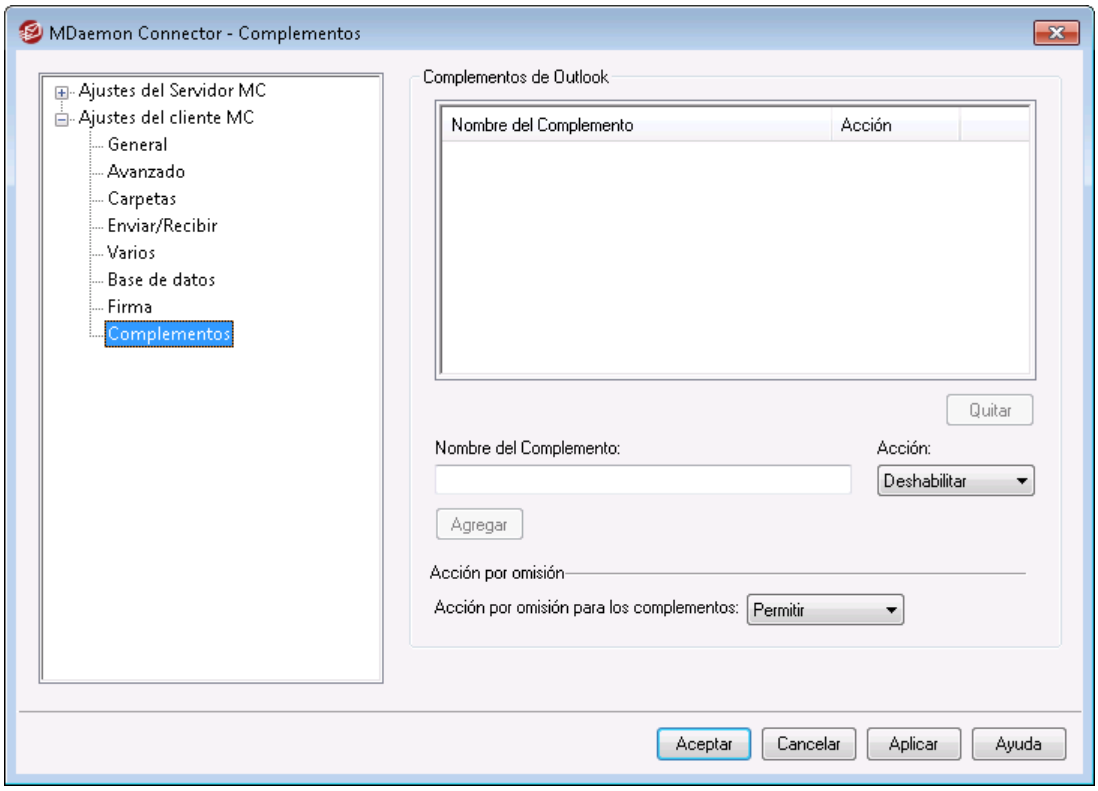
Firma por omisión para respuestas/reenvíos
Marque esta casilla si desea hacer que la firma del cliente sea la de omisión a utilizar al responder o reenviar mensajes.

Nombre de la firma:
Este es el nombre definido a la firma entregada a la cuenta de correo en Outlook de los usuarios de MDaemon Connector. Por omisión el nombre de la firma se define como: "`MDaemon-$EMAIL$`". La macro $EMAIL$ se convertirá en la dirección de correo del usuario. Por ejemplo, "`MDaemon-Frank.Thomas@company.test`"

Ver:

MC Ajustes de Cliente 390
MC Ajustes de Servidor » Ajustes 387
MC Ajustes de Servidor » Cuentas 389
Firmas de Cliente por Omisión 147
Administrador de Dominios » Firmas de Cliente 215

3.8.2.8 Complementos



Utilizando la pantalla Complementos, puede administrar el estado de los complementos de Outlook utilizados por sus usuarios de MDaemon Connector. Puede permitir que se utilicen normalmente cualquiera o todos los complementos o puede deshabilitar el que usted elija. Esta funcionalidad puede ser útil específicamente en los casos en que usted sabe de un complemento específico que entra en conflicto con MDaemon Connector, permitiéndole deshabilitar ese complemento para evitar problemas. La funcionalidad Complementos requiere de MDaemon Connector 5.0 o superior.

Complementos de Outlook

Esta caja contiene la lista de los complementos de Outlook utilizados por sus usuarios y la Acción asignada a cada uno: *Deshabilitar*, *Permitir*, *Por Omisión*. Cuando un usuario de MC inicia sesión en Outlook, el cliente de MC envía la lista de los complementos del usuario a MDaemon y luego deshabilita cualquiera que se haya definido como *Deshabilitado*. Cualquier que esté configurado como "*Permitir*" no se modificará. Aquellos configurados como "*Por Omisión*" utilizarán la *Acción por Omisión para complementos* asignada abajo.

MDaemon Connector solo puede administrar los Complementos de Outlook para aquellos usuarios que han configurado su cuenta de MDaemon Connector como la cuenta por omisión en Microsoft Outlook.

Agregar, Eliminar y Modificar Complementos

Agregar un Complemento

Para agregar un complemento a la lista, teclee el *Nombre del Complemento* tal como aparece en Outlook, defina la *Acción* y dé clic en **Agregar**. Esta opción es útil si usted sabe de algún complemento que desea administrar, pero aún no se ha conectado ningún usuario que lo tenga instalado.

Eliminar un Complemento

Para eliminar de la lista un complemento, selecciónelo y dé clic en *Eliminar*.

Definir la Acción de un Complemento

Para modificar un complemento, selecciónelo, utilice la lista desplegable para configurar su *Acción* y dé clic en **Agregar**.

Acción Por Omisión

Acción por Omisión para Complementos

Configure esta opción como *Permitir* o *Deshabilitar*. Cuando se configura como *Permitir*, por omisión MDaemon Connector solo deshabilitará los complementos que usted haya definido específicamente como "*Deshabilitar.*" No se tocarán todos los demás Complementos. Cuando se configura como *Deshabilitar*, MDaemon Connector deshabilitará automáticamente todos los complementos excepto aquellos que haya configurado específicamente como "*Permitir*." Esta opción está configurada como *Permitir* por omisión.

Ver:

Ajustes del Cliente MC 390
Ajustes del Cliente MC » Ajustes 387
Ajustes del Cliente MC » Cuentas 389

3.9 Servicio de Clúster

El servicio de Clúster de MDaemon está diseñado para compartir su configuración entre dos o más servidores de MDaemon en su red. Esto le permite utilizar hardware o software para balanceo de carga para distribuir la carga del servicio de correo a lo largo de múltiples servidores de MDaemon, lo que puede mejorar la velocidad y eficiencia al reducir congestión y sobrecarga en la red y maximizar sus recursos de correo. También ayuda a asegurar redundancia en su sistema de correo en caso de que alguno de sus servidores sufriera una falla de hardware o software.

A continuación una serie de elementos a considerar para decidir configurar o no un clúster de MDaemon en su red:

Nodos

Un Clúster de MDaemon estará compuesto por un nodo primario y nodos secundarios. Un servidor MDaemon será definido como Primario y el resto como Secundarios.

- El servidor MDaemon que actúa como nodo primario tiene su configuración replicada en todos los otros nodos. Por esto el nodo primario es el único que puede ser utilizado para hacer cambios de configuración; si tiene acceso a un nodo secundario y hace cambios de configuración, estos serán sobrescritos. Consecuentemente, la mayoría de las opciones de configuración no están disponibles en la interface de usuario de los nodos secundarios.
- El servicio de clúster no replica en los nodos las carpetas de correo o las carpetas públicas; todos los nodos comparten el mismo conjunto de carpetas de mensajes. Las carpetas de correo de usuario y las carpetas públicas deben encontrarse en una ubicación en su red accesible a todos los nodos.
- Cualquier modificación al correo que ocurra en un nodo secundario, se enviará al nodo primario y luego los demás nodos son notificados de la modificación.
- XML-API en los nodos secundarios es de solo lectura.
- Cada nodo en el clúster debe estar en la misma red. No recomendamos utilizar el servicio de clúster para agrupar servidores que se encuentran en ubicaciones distintas.
- Cada nodo en el clúster necesita ejecutar la misma versión de MDaemon.
- Cada nodo en el clúster requiere su propia llave de MDaemon.

Enrutamiento

MDaemon no maneja el enrutamiento de tráfico hacia o desde nodos específicos. Recomendamos utilizar alguna solución de balanceo de carga de terceros para manejar el enrutamiento del tráfico.

Se requiere que su balanceador de carga maneje sesiones sticky para que todo el tráfico de la misma IP se enrute al mismo host. Sesiones Sticky es muy importante para el tráfico de MDRA, Webmail y XMPP ya que ellos no están conscientes del clúster, lo que significa que la información de sesiones no se comunica entre nodos. Para manejar esta limitación:

- Todas las conexiones MDRA deben enrutarse al nodo primario.
- Cuando alguien inicia sesión en Webmail en un servidor específico, todo el tráfico de esa sesión se debe enrutar al mismo servidor.
- El tráfico de Webmail y XMPP requiere ser enrutado al mismo servidor a fin de que funcione el chat integrado de Webmail.
- Todo el tráfico XMPP debe enrutarse al mismo nodo, de otra manera los usuarios conectados a distintos servidores no podrán chatear entre sí.
- Considerando los puntos arriba mencionados, recomendamos que todo el tráfico HTTP y XMPP se enrute al nodo primario, ya que es la configuración

más sencilla y la que tiene menor probabilidad de dar problemas. Sin embargo, si no utiliza estas funcionalidades, puede alterar su configuración (aunque se requieren de todas maneras las sesiones sticky).

Buzones y Carpetas

Buzones, Carpetas Públicas y algunas otras carpetas deben almacenarse en una ruta compartida que sea accesible a cada nodo en el clúster. Recuerde que si está utilizando rutas UNC, requerirá ejecutar el servicio MDaemon como usuario con acceso a la ubicación en la red.

- Debe actualizar manualmente las rutas de buzón y carpetas y mover los contenidos de las carpetas a la ubicación accesible al clúster. Esto no es una función automatizada que pueda ejecutar MDaemon por usted al configurar el clúster. El servicio de clúster actualizará el archivo MDaemon.ini con las rutas de carpetas de la red para Buzones y Carpetas Públicas que usted proporcione en la configuración del servicio de clúster.
- El directorio de Lockfiles debe colocarse en una ubicación compartida. Puede permitir que el Servicio de Clúster lo haga automáticamente o lo puede hacer manual, editando el registro `LockFiles` en la sección `[Directories]` del archivo `MDaemon.ini`. Si permite que lo haga el servicio de clúster, el directorio LockFiles se ubicará bajo la ruta de buzones de la red.
- También debe moverse el directorio PEM a una ubicación compartida. Para hacerlo, copie la carpeta `MDaemon\PEM\` a la nueva ubicación compartida, edite el registro `PEM` en la sección `[Directories]` del archivo `MDaemon.ini` y reinicie MDaemon.
- La plantilla de cuentas nuevas se actualizará con la ruta de carpetas proporcionada en la configuración del servicio de clúster.

Monitoreo Dinámico

- Monitoreo Dinámico 610 envía todas las peticiones al servidor nodo primario y los datos de ese nodo se replican a los nodos secundarios.
- Si el nodo primario está fuera de línea, los nodos secundarios utilizan su propia configuración de monitoreo dinámico, que debe ser idéntica a la configuración del nodo primario al momento en que salió de línea. Cuando el primario entra en línea de nuevo, cualquier modificación hecha al Monitoreo Dinámico por los nodos secundarios, será reescrita.

Certificados

- Los Certificados SSL se replican automáticamente del nodo Primario a los Secundarios.
- MDaemon también replica los ajustes de certificados 577, de manera que cada nodo/servidor en el clúster intentará utilizar el mismo certificado. Si un nodo no cuenta con el certificado correcto, todo el tráfico SSL/TLS/HTTPS fallará en ese nodo.
- Las opciones de LetsEncrypt de MDaemon no soportan nodos secundarios en este momento.

Otros

- La Vinculación de Adjuntos 366 no se puede utilizar en un clúster y por esto se deshabilita cuando se habilita la funcionalidad de clústeres.

- La Instalación Automática de Actualizaciones[501] debe estar deshabilitada.
- La Vinculación de Nombre de Dominio a dirección IP[192] debe estar deshabilitada.
- Todos los nodos en un clúster deben configurarse en la misma zona horaria y con la misma hora. Si la zona horaria no es igual o si el horario está desfasado por más de un segundo, se enviará una advertencia al registro del Clúster.

Configurar el Servicio de Clúster

Siga los pasos siguientes para configurar el servicio de clúster:

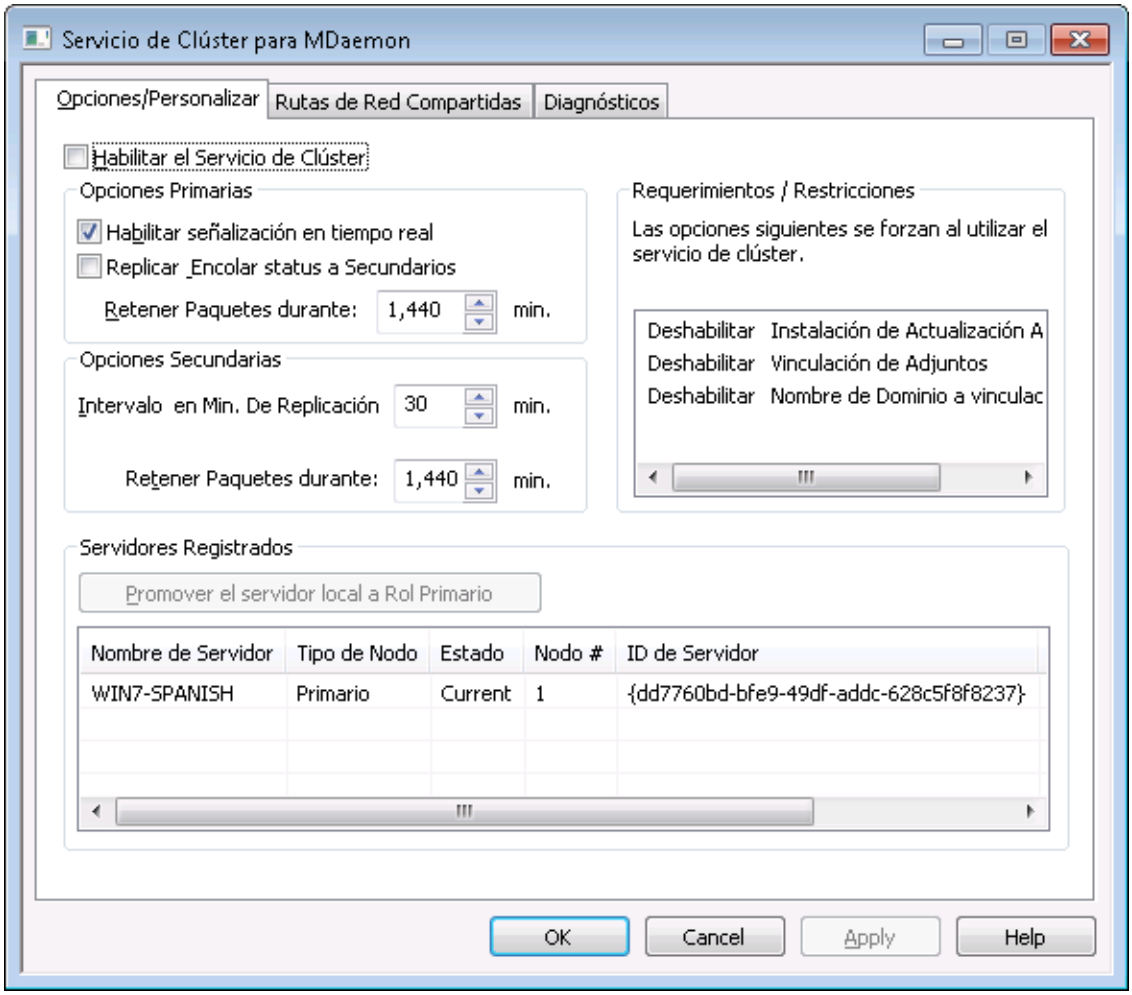
1. Asegúrese de que ha actualizado todas las rutas de buzones y de las carpetas públicas. El servidor primario deberá estar utilizando una ubicación de almacenamiento en la red para alojar estos datos y deberá tener acceso a los datos sin problemas antes de proceder.
2. Deberán estar instalados todos los certificados correctos en cada nodo.
3. Instalar MDaemon en un nodo secundario utilizando una llave única.
4. En el nodo primario, vaya a **Configuración » Servicio de Clúster**
5. Dé clic derecho en la lista de Servidores Registrados y clic en **Agregar nuevo servidor de MDaemon al Clúster** (esto puede ser lento porque busca los servidores disponibles en la red).
6. En *Nombre del Servidor*, registre el nombre NETBIOS, la dirección IP o nombre DNS del nodo secundario donde está instalado MDaemon o seleccione el servidor de la lista desplegable - puede haber un retardo ya que busca en la red los servidores disponibles.
7. Dé clic en **OK**.
8. Revise los logs de Complementos y Clúster para asegurarse que los dos servidores están conectados y la replicación está ocurriendo.
9. Vaya a **Configuración » Servicio de Clúster** en el nodo secundario para confirmar que ahora enlista el nodo primario y los secundarios bajo Servidores Registrados.
10. Configure su solución (hardware o software) de balanceo de carga para enrutar tráfico al clúster como se discutió arriba.

Ver:

Servicio de Clúster | Opciones/Personalizar[410]
Servicio de Clúster | Rutas de Red Compartidas[412]
Servicio de Clúster | Diagnósticos[414]

3.9.1 Opciones/Personalizar

Opciones/Personalizar



Habilitar el Servicio de Clúster

Dé clic para habilitar el Servicio de Clúster.

Opciones Primarias

Habilitar señales en tiempo real
Por omisión, siempre que ocurre un cambio en el nodo Primario, envía una señal de replicación a los nodos Secundarios, para notificarles que necesitan hacer una petición de replicación para sincronizar los ajustes entre nodos.

Replicar estados de Colas a los Secundarios
Marque esta casilla si desea estar seguro de que si hay cambios en el estado de las colas de correo (ej. que estén congeladas o descongeladas) en el nodo Primario, ese estado se modificará también en los nodos Secundarios.

Opciones Secundarias

Intervalo de Replicación [xx] minutos
Esta opción determina cuanto tiempo esperará el nodo Secundario la señal de replicación del nodo Primario antes de realizar la petición de replicación de todas formas. Por omisión esto se configura a 30 minutos.

Servidores Registrados

Aquí se despliegan todos los nodos en su clúster de servidores MDaemon.

Promover el servidor local al rol Primario
Para cambiar un nodo Secundario a Primario, en el Secundario que desea promover, seleccione el nodo en la lista y dé clic en **Promover**. El nuevo Primario deberá informar al Primario anterior para que se vuelva a asociar al clúster como secundario. Para configuraciones con múltiples nodos secundarios, los nodos secundarios adicionales necesitarán ser eliminados y agregados de nuevo al clúster.

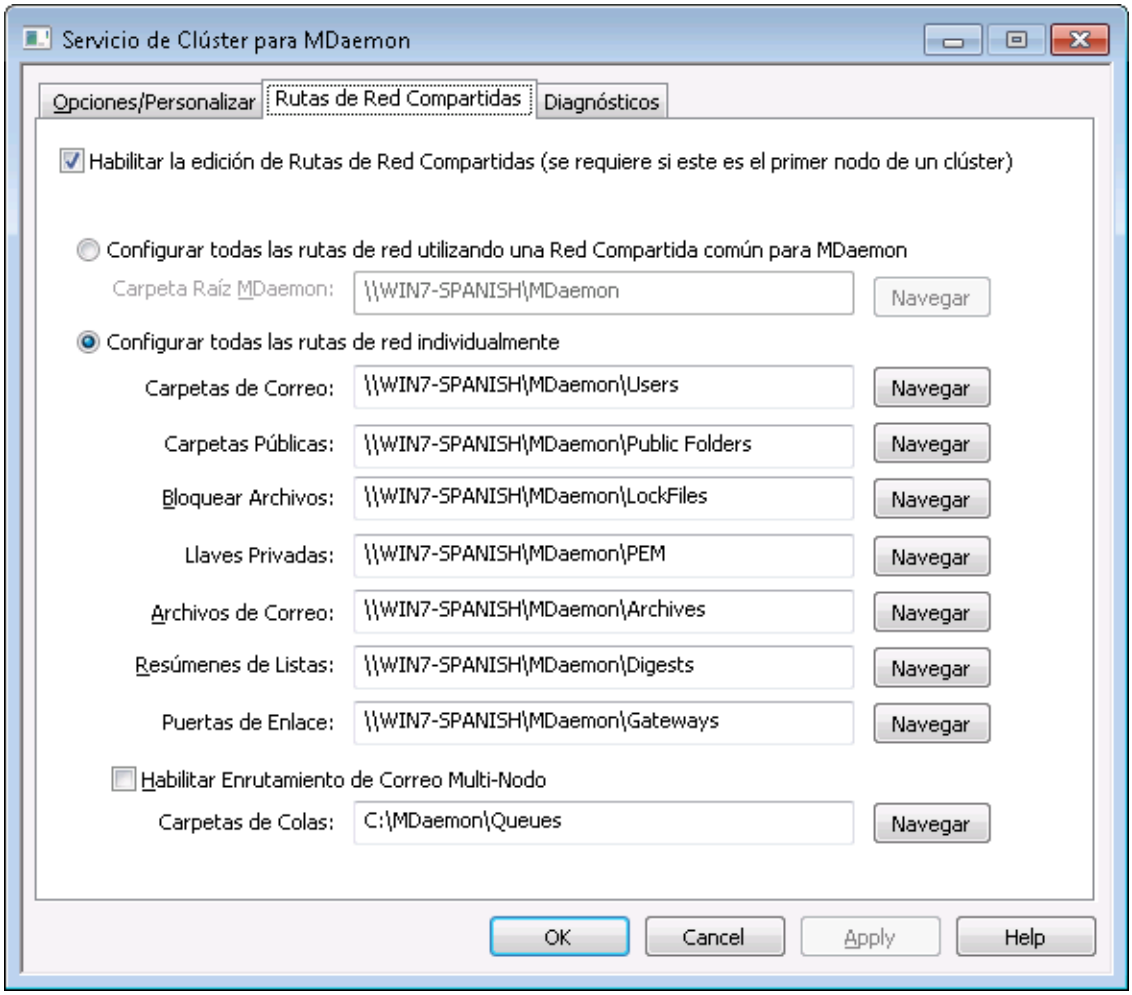
Agregar un nuevo servidor MDaemon al clúster
Para agregar un nuevo servidor MDaemon a un clúster, dé clic derecho en la lista de servidores y luego clic en **Agregar nuevo servidor MDaemon al clúster**. En la pantalla que se abre, registre el nombre NETBIOS, la dirección IP o nombre de DNS del servidor en que está instalado en MDaemon, o seleccione el servidor desde la lista desplegable. Puede haber un retraso ya que hace una búsqueda en la red de los servidores disponibles.

Ver:

Servicio de Clúster 407
Servicio de Clúster | Rutas de Red Compartidas 412
Servicio de Clúster | Diagnósticos 414

3.9.2 Rutas de Red Compartidas

Rutas de Red Compartidas



Habilitar la edición de Rutas de Red Compartidas (requerido si este es el primer nodo del Clúster)

Utilice las opciones en esta pantalla para establecer las rutas de red compartidas que se utilizará el clúster de MDaemon. Esto se requiere en el primer nodo del clúster de manera que las rutas de red compartidas puedan ser replicadas en los otros nodos.

Definir todas las rutas de red utilizando un Recurso Compartido de MDaemon
Elija esta opción si desea localizar todas las rutas de red compartidas bajo un único recurso compartido de red. Esta opción hace que todas las rutas se configuran a valores por omisión y todos los controles de ruta serán de solo lectura.

Definir las rutas de red individualmente
Elija esta opción si desea definir cada ruta compartida de red individualmente. Por ejemplo, si desea almacenar carpetas de correo y archivos de correo en diferentes ubicaciones de red.

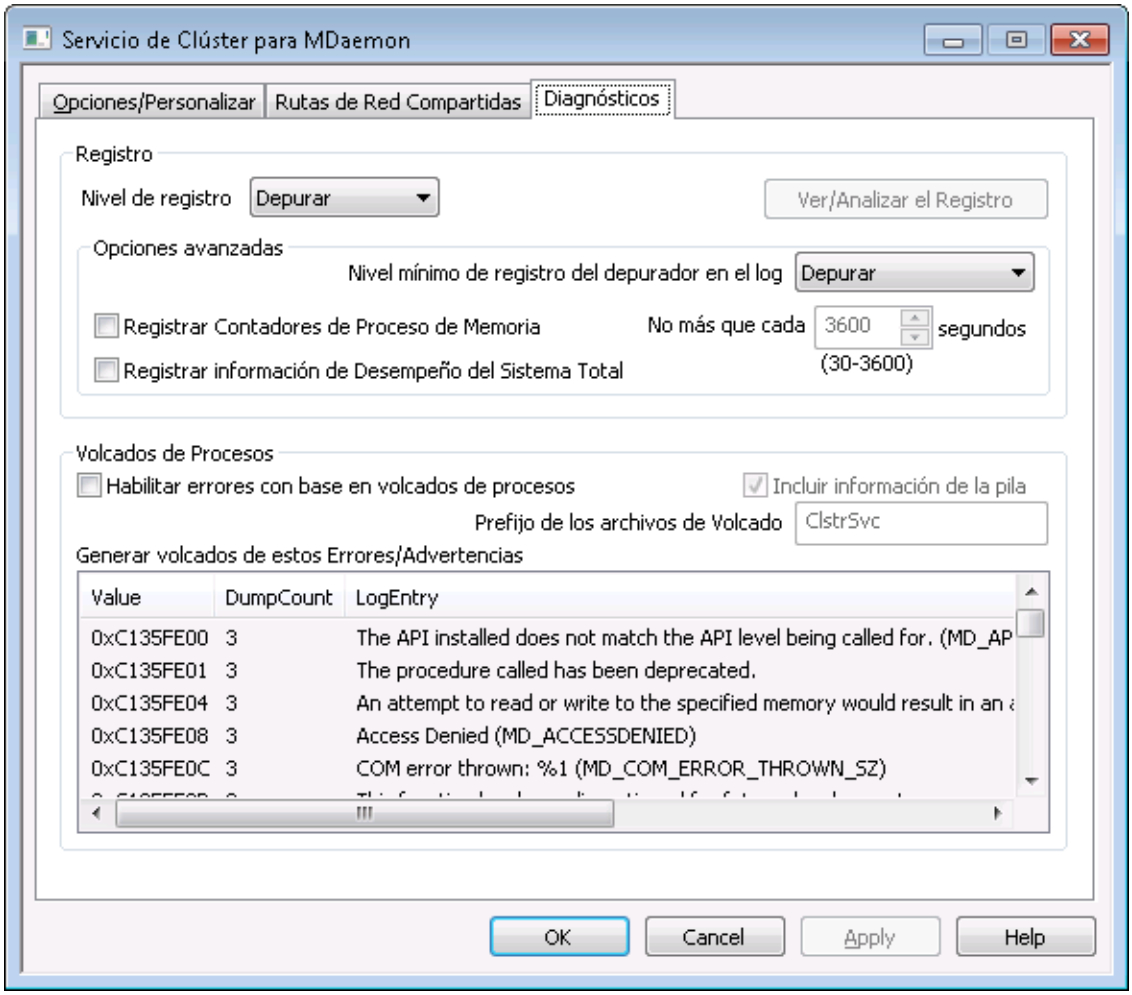
Habilitar Enrutamiento de Correo Multi-Nodo
Utilice Enrutamiento de Correo Multi-Nodo si desea compartir colas de correo entre nodos del clúster. Si múltiples servidores procesan y entregan los mensajes, se puede repartir el trabajo de manera más equilibrada y prevenir que los mensajes se atoren en las colas de los servidores que salgan de servicio.

Ver:

Servicio de Clúster 407
Servicio de Clúster | Rutas de Red Compartidas 412
Servicio de Clúster | Diagnósticos 414

3.9.3 Diagnósticos

Diagnósticos



Registro

Nivel de Registro
Se soportan seis niveles de registro dependiendo de la más alta a más baja cantidad de datos registrados:

Depurar Es el nivel de registro más detallado. Incluye todas las entradas disponibles y típicamente solo se utiliza al diagnosticar un problema o cuando el administrador requiere información detallada.

Info Registro Moderado. Incluye operaciones generales sin detalle. Es el nivel de registro por omisión.

Advertencia Incluye advertencias, errores, errores críticos y eventos de inicio/cierre de la aplicación.

Error Se registran errores, errores críticos y eventos de inicio/cierre de la aplicación.

Críticos Se incluyen errores críticos y eventos de inicio/cierre de la aplicación.

Ninguno Solo se registran eventos de inicio/cierre de la aplicación.

Ver/Analizar el Registro
Dé clic en este botón para abrir el Sistema de Visor Avanzado de Registros de MDaemon. Por omisión, los registros se almacenan en: "..\MDaemon\Logs\"

Opciones Avanzadas

Nivel mínimo de registros para el depurador
Este es el nivel mínimo de registros a emitir al depurador. Los niveles disponibles de registro son los mismos descritos previamente.

Registrar contadores de procesamiento de memoria
Marque esta casilla para incluir en el archivo de registro información específica de procesos de Memoria, Identificadores e Hilos. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos. Las entradas al registro solo se emiten si los datos se han modificado desde la última vez que se registraron.

Registrar información del desempeño general del sistema
Marque esta casilla si desea incluir en el registro información del desempeño general del sistema. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos.

No más de cada [xx] segundos
Utilice esta opción para establecer el límite de la frecuencia con que se registrará la información de procesos y desempeño.

Volcados de Proceso

Habilitar volcados de procesos con base en errores
Habilite esta opción si desea generar volcados de proceso siempre que ocurran advertencias o errores específicos que usted determine abajo.

Incluir información de la pila en los volcados
Por omisión, se incluye información de la pila en los volcados de procesos. Deshabilite esta casilla si no desea que se incluya esta información.

Prefijo para los archivos de volcado
Los nombres de archivos de volados de procesos inician con este texto.

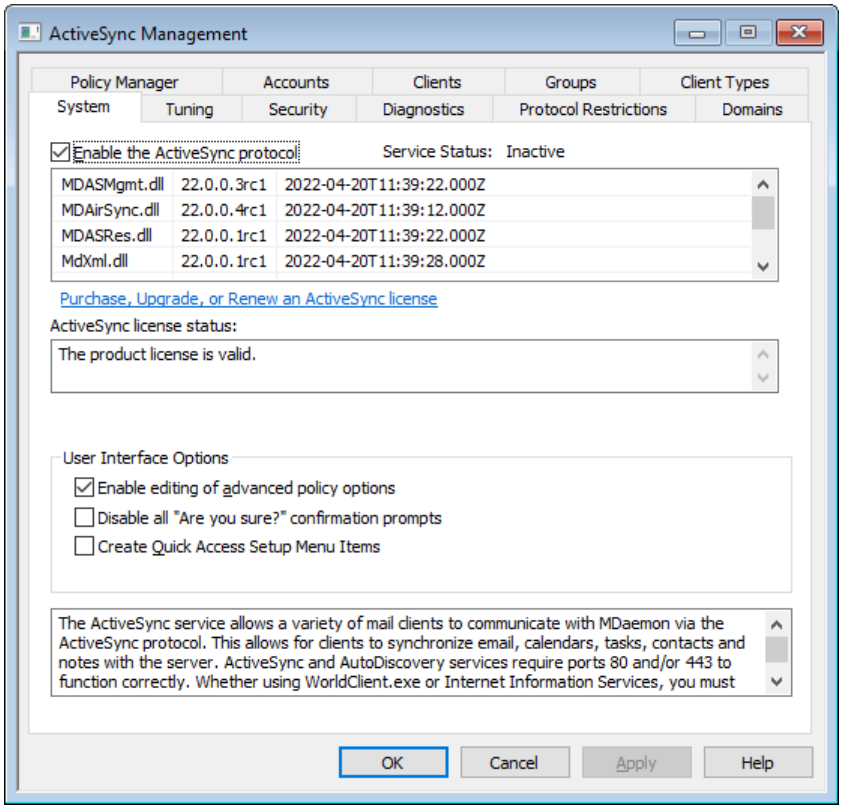
Errores/Advertencias para genera volcados
Dé clic derecho en esta área y utilice las opciones *Agregar/Editar/Eliminar Registro...* para administrar la lista de errores o advertencias que detonarán volcados de procesos. Por cada entrada puede definir el número de volcados de proceso permitidos antes de que se desactive.

Ver:

Servicio de Clúster 407
Servicio de Clúster | Rutas de Red Compartidas 412
Servicio de Clúster | Diagnósticos 414

3.10 ActiveSync

3.10.1 Sistema ActiveSync



MDaemon incluye soporte para "ActiveSync para MDaemon" que es un servidor ActiveSync para conexión inalámbrica (over-the-air OTA), complemento opcional para MDaemon Private Cloud. Este servidor es capaz de sincronizar el correo y datos PIM del usuario (i.e. Contactos, Calendario y Tareas) entre su cuenta MDaemon/Webmail y un dispositivo con capacidades ActiveSync.

ActiveSync es una extensión de servicio web que funciona solamente en los puertos **80** (para http) y **443** (para https). Este es un requerimiento de la implementación de ActiveSync. Si se habilita ActiveSync y usted utiliza el servidor web 326 integrado

en Webmail, pero este no está corriendo en el puerto 80 o el 443, entonces empezará a correr automáticamente en el puerto 80 en adición a cualesquiera otros puertos donde lo tenga configurado en las pantallas Servidor Web 326 y SSL & HTTPS 328. Si está utilizando otro servidor para Webmail tal como IIS, entonces debe configurar manualmente el uso del puerto 80 o el 443.

Si tiene la intención de ejecutar ActiveSync bajo IIS debe llamar a la DLL de ActiveSync (`MDAirSync.dll`) cuando se solicita "`/Microsoft-Server-ActiveSync`". Esta es la petición que utilizan todos los clientes de ActiveSync. Algunas versiones de IIS no tienen esta capacidad sin descargar, instalar y configurar software de terceros.

Todas las sincronizaciones de primera vez con ActiveSync son una sincronización de una vía desde el servidor hacia el dispositivo. Perderá datos en el dispositivo al sincronizar con ActiveSync por primera vez. Este es un requerimiento de la implementación de ActiveSync. Por esto, respalde los datos del dispositivo antes de utilizar ActiveSync por primera vez. La mayoría de los dispositivos que soportan ActiveSync advierten al usuario que "**todos los datos del dispositivo se perderán**" pero algunos no lo hacen. Por favor maneje ActiveSync con precaución.

Habilitar/Deshabilitar ActiveSync

Dé clic en *Habilitar el Protocolo ActiveSync* para iniciar ActiveSync para MDaemon. Entonces podrá utilizar las opciones Dominios 434 para controlar si estará o no disponible para todos o algunos de sus dominios.

Opciones de Interface de Usuario

Habilitar la edición de opciones avanzadas de políticas
Habilite esta opción si desea que sea visible la pestaña Ajustes Avanzados en el Editor de Políticas ActiveSync 443. Contiene varios ajustes avanzados de política que en la mayoría de los casos no requerirán ser modificados. Esta opción se encuentra deshabilitada por omisión.

Deshabilitar todas las peticiones de confirmación "¿Está Seguro?"
Por omisión cuando modifica ciertos ajustes de ActiveSync, se le pregunta si está seguro de que desea hacer el cambio. Dé clic en esta casilla si desea deshabilitar esas preguntas.

Crear elementos de acceso rápido en el menú de configuración
Si habilita esta opción, se modificará el menú en Configuración » ActiveSync en la interface de MDaemon, agregando ligas al monitor de Conexiones de ActiveSync y el Visor/Analizador de Registros. **Nota:** cuando se deshabilita esta opción, esas herramientas se pueden encontrar dando clic derecho en **ActiveSync** bajo Servidores en el panel de Estadísticas en la interface de la aplicación.

Servicio Autodiscover de ActiveSync

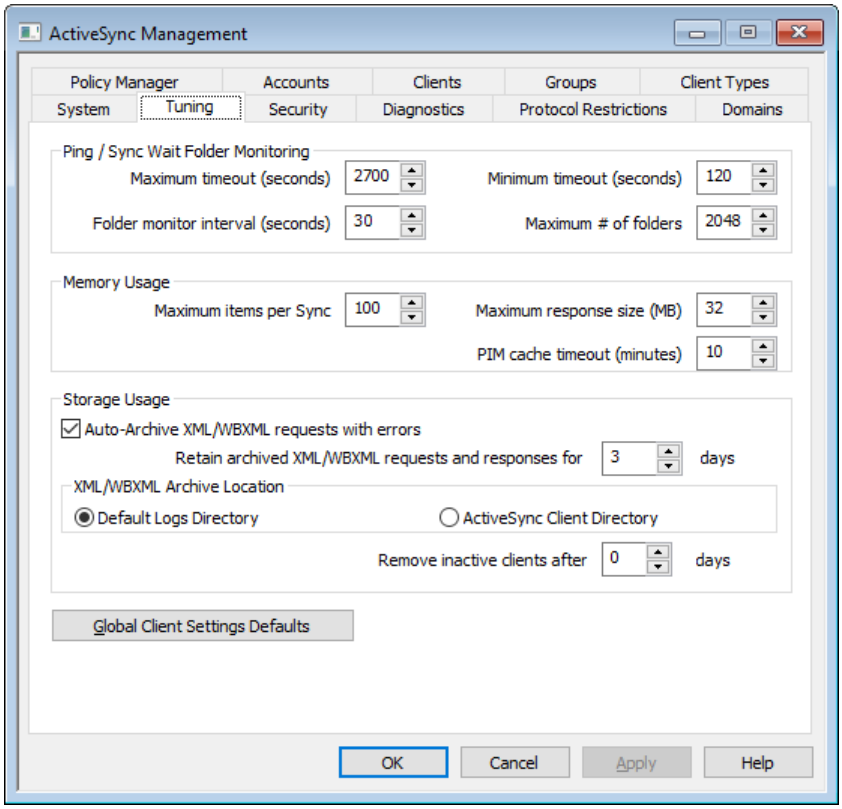
MDaemon soporta el servicio Autodiscover de ActiveSync, que permite a los usuarios configurar una cuenta ActiveSync con solo su dirección de correo y

contraseña, sin necesidad de saber el nombre del servidor donde se encuentra el servicio ActiveSync. Autodiscover requiere que HTTPS 328 esté habilitado.

Ver:

Editor de Cuentas » ActiveSync 764
ActiveSync » Dominios 434
SSL & HTTPS 328
Servidor Web 326

3.10.2 Ajustes



Esta pantalla contiene opciones avanzadas que en la mayoría de los casos no requerirán ajustes, y contiene el botón Ajustes Globales de Clientes 421, para ajustar los valores por omisión utilizados para los clientes ActiveSync.

Monitoreo de la carpeta de espera Ping/Sync

Tiempo de espera Máximo (1200-7200 segundos)
Este es el tiempo máximo que el Servicio ActiveSync de MDaemon (MDAS) esperará mientras monitorea una carpeta antes de devolver la respuesta al cliente. El valor por omisión es 2700 segundos (i.e. 45 minutos).

Tiempo de espera Mínimo (120-480 segundos)
Este es el tiempo mínimo que MDAS esperará mientras monitorea una carpeta antes de devolver una respuesta al cliente. El valor por omisión es de 120 segundos. Si es necesario, puede reducir el número de conexiones que se hacen al servidor incrementando este valor, dado que esto haría que el cliente se conecte con menor frecuencia debido a que el tiempo de espera involucrado sería mayor.

Intervalo de monitoreo de Carpetas (30-120 segundos)
Este es el número de segundos que esperará el servicio ActiveSync entre ocurrencias de monitoreo de carpetas. Por omisión está configurado a 30 segundos.

Máximo # de carpetas
Este es el número máximo de carpetas que se permite a cada cliente ActiveSync monitorear para detectar cambios. El valor por omisión es 2048.

Uso de Memoria

Máximos elementos por Sync
Este es el número máximo de elementos que devolverá al cliente el servicio ActiveSync en respuesta a una petición Sync. Si se utiliza un valor bajo en esta opción se puede reducir el uso de memoria en un servidor muy ocupado, pero esto requerirá más conexiones y ancho de banda. También puede decrementar la vida de la batería porque los dispositivos pueden requerir hacer más peticiones para obtener todos los cambios durante un sync. Valores altos en esta opción incrementan el uso de memoria y son más susceptibles de generar errores de comunicación. El valor por omisión es 100 y en general es una cantidad aceptable. Vale la pena notar, sin embargo, que los clientes especificarán el valor que prefieran, lo que podría efectivamente disminuir este valor para algunos clientes. Si u cliente solicita un valor mayor al máximo, entonces se utilizará el máximo.

Máximo tamaño de respuesta (MB)
Este es el tamaño máximo permisible de una respuesta a una petición Sync de un cliente. Antes de procesar un elemento dado para una sincronización servidor a cliente, se verifica el valor actual de la respuesta y si es mayor o igual que este valor, la colección se marca indicando que hay más modificaciones disponibles y no se agregarán más elementos a la respuesta. Esto es útil para servidores que regularmente contienen muchos adjuntos grandes en el correo.

Tiempo de espera de caché PIM (5-60 minutos)
Dado que los Contactos, Documentos, Eventos y otros datos PIM con frecuencia son estáticos y se obtienen solo actualizaciones ocasionales de los clientes, MDAS guarda en caché estos datos para reducir actividad del disco. Esta información, sin embargo, se carga en automático siempre que los datos cambian en el disco. Este valor controla cuanto tiempo se guardarán en caché los datos del usuario desde la última vez en que se accesaron.

Uso de Almacenamiento

Auto-Archivar peticiones XML/WBXML con errores
En el caso de que haya deshabilitado las opciones para *Archivar peticiones y respuestas [XML | WBXML]* en la pantalla Ajustes de Cliente 421, esta opción aún

archivará peticiones XML o WBXML problemáticas. Solo se archivarán las peticiones que generen errores. Esta opción está habilitada por omisión.

Retener peticiones y respuestas XML/WBXML archivadas durante [xx] días
Este es el número de días en que se guardarán las respuestas auto-archivadas. Por omisión se conservan 3 días.

Localización del Archivo XML/WBXML

Directorio de Registros por omisión
Los archivos de peticiones y errores XML/WBXML se almacenarán en el directorio por omisión de los registros de MDaemon.

Directorio de Cliente ActiveSync
Elija esta opción si alternativamente desea almacenar los archivos en el directorio Depurar Cliente ActiveSync del usuario.

Eliminar clientes inactivos luego de [xx] días
Este es el número de días que un Dispositivo ActiveSync 460 puede seguir conectándose a MDAS antes de que sea eliminado. Cuando el dispositivo se elimine, se descartan sus ajustes de configuración y acceso. Si alguna vez se vuelve a conectar el dispositivo, MDaemon responderá como si fuera un dispositivo nuevo que nunca se ha utilizado en el servidor. Se le forzará a reaprovisionarse si está definida una política para el dominio 434 o cuenta 451, se ejecutará una sincronización inicial de carpetas y se resincronizarán todas las carpetas suscritas. Esta opción puede ayudar a su servidor a liberarse de mantener información vieja y dispositivos en desuso. Esta opción se configura a 31 días por omisión. Cuando se configura en "0", los dispositivos no se eliminarán, sin importar cuanto tiempo hayan estado inactivos.

Ajustes Globales de Cliente por Omisión

Dé clic en este botón para abrir el diálogo Ajustes Globales de Cliente ActiveSync 421, para configurar los ajustes por omisión a utilizar para los clientes ActiveSync.

Notificaciones ActiveSync

Notificaciones de RollBack de Sincronizaciones

El Servicio ActiveSync puede notificar a los administradores si un cliente ha estado enviado repetida/frecuentemente llaves de sincronización expiradas en operaciones Sync.

Esto meramente informa al admin que el servidor emitió un rollback para una colección dada de llaves porque el cliente hizo una petición sync con la llave Sync más recientemente expirada. El asunto dice "Cliente ActiveSync utiliza llave Sync Expirada". Esto puede ocurrir por problemas de red o alguna otra cosa sobre el contenido enviado previamente al cliente en esa colección. En algunos casos, el item ID estará ahí, depende meramente de si la sincronización anterior en esa colección envió cualquier elemento.

Los avisos de Rollback no significan que el cliente esté fuera de sincronización, significa que el cliente tiene el potencial de salir de sincronización y nuestro sistema interno lo ha detectado. Los avisos de RollBack se emiten para una colección no más de una vez por cada periodo de 24 horas. Las siguientes llaves

se pueden editar en el encabezado [System] en el archivo `\MDaemon\Data\AirSync.ini`:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (Por omisión está deshabilitado)
- [System] RollbackNotificationThreshhold=[1-254] : Número de rollbacks que deben ocurrir para una colección dada antes de que se envíe una notificación al administrador. Recomendamos un valor de por lo menos 5 ya que posibles problemas de red pueden tener parte en esto. (El valor por omisión es 10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Define si se generará CC al usuario cuyo cliente envió el aviso de llave Sync expirada. (Deshabilitada por omisión)

Notificaciones de Mensajes Corruptos de ActiveSync

El Servicio ActiveSync puede notificar a los administradores si algún mensaje en particular no puede ser procesado. Estos avisos se envían en tiempo real para informar al admin que un elemento de correo no puede ser segmentado y que no es posible realizar más acciones para este elemento. El asunto dice "Corrupt message notification". Estos elementos, en versiones previas, podían llevar a un cierre inesperado de MDaemon. En la mayoría de los casos, el contenido del archivo msg no se encontrará en formato MIME. Si contiene datos MIME, es posible que esté corrupto. Puede seleccionar enviar copia de estas notificaciones al usuario con la llave CMNCCUser para que estén enterados de que ha llegado un mensaje ilegible a su buzón. La acción adecuada para esto es eliminar el archivo msg del mensaje del buzón del usuario y analizarlo para determinar por qué no fue posible ser segmentado y como llego al estado en que se encuentra. Las llaves siguientes se pueden editar bajo el encabezado [System] en el archivo `\MDaemon\Data\AirSync.ini`:

- [System] SendCorruptMessageNotifications=[Yes|No|1|0|True|False] (Habilitado por Omisión)
- [System] CMNCCUser==[0|1|Yes|No|True|False] (Habilitado por Omisión)

Ver:

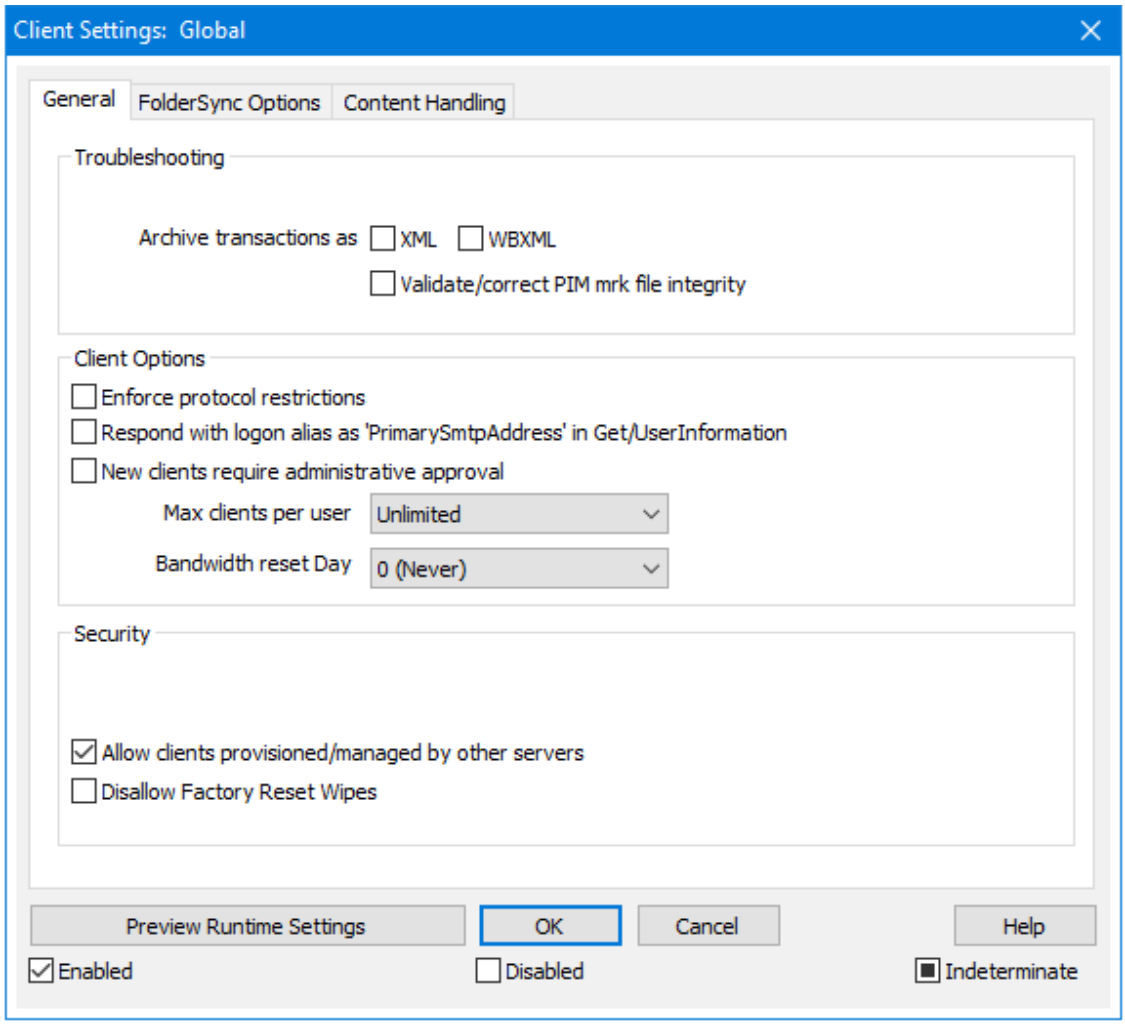
ActiveSync » Diagnósticos 430

3.10.2.1 Ajustes de Cliente

La pantalla de Ajustes de Cliente enlista los perfiles de ajustes por omisión de ActiveSync que se han configurado para este servicio. Puede crear y editar los perfiles de ajustes de cliente: Global, Dominios 215, Grupos 468, Cuentas 451, Tipos de Cliente 475 y Clientes 460 (i.e. dispositivos) en sus respectivas opciones.

Dé clic en **Agregar...** para agregar un grupo de seguridad nuevo o un perfil de dispositivo o seleccione una entrada y de clic en **Editar...** o en **Eliminar** para editar o eliminar el perfil.

Ajustes Globales de Cliente



Esta pantalla contiene los ajustes globales para administrar clientes ActiveSync. Existen ajustes de cliente equivalentes bajo las otras pantallas de ActiveSync, tales como Dominios 434, Cuentas 451 y Clientes 460, para ajustar estas opciones por dominio, por cuenta y por cliente respectivamente. Los ajustes globales se configuran a valores específicos, pero los ajustes de dominio, cuenta, cliente y otros ajustes se establecen por omisión para *Heredar* el valor de su respectiva opción padre. Por esto, al modificar cualquier ajuste en esta pantalla se cambiará efectivamente la misma opción en todas las pantallas hijo, permitiéndole por omisión administrar todos los clientes en el servidor al modificar solamente los valores en esta pantalla. Alternativamente, al modificar un valor en una pantalla hijo omitirá su ajuste padre, permitiéndole alterar los valores a nivel dominio, cuenta u otro nivel, si fuera necesario.

Al igual que en Políticas 442, que se asignan al dispositivo y generalmente controlan lo que hace el dispositivo, los Ajustes de Cliente controlan lo que hará el servidor con respecto a varias opciones relacionadas con los clientes, tales como: controlar cuantos clientes ActiveSync puede utilizar una cuenta, si se sincronizarán o no las Carpetas Públicas a un dispositivo junto con las carpetas personales de la cuenta, si se incluirá o no la carpeta de lista de permitidos del usuario y demás.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el

cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas[314] a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta[316] para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas[314] padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas[128] a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas[743] a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes[460] y tipos de clientes[475] que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

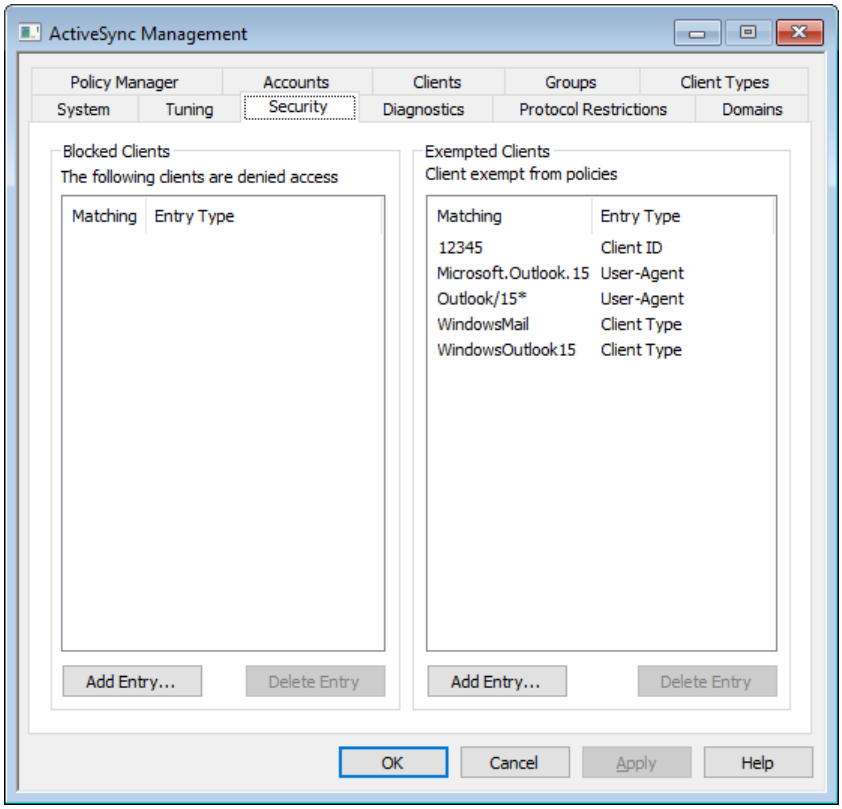
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Dominios 434
ActiveSync » Cuentas 451
ActiveSync » Clientes 460

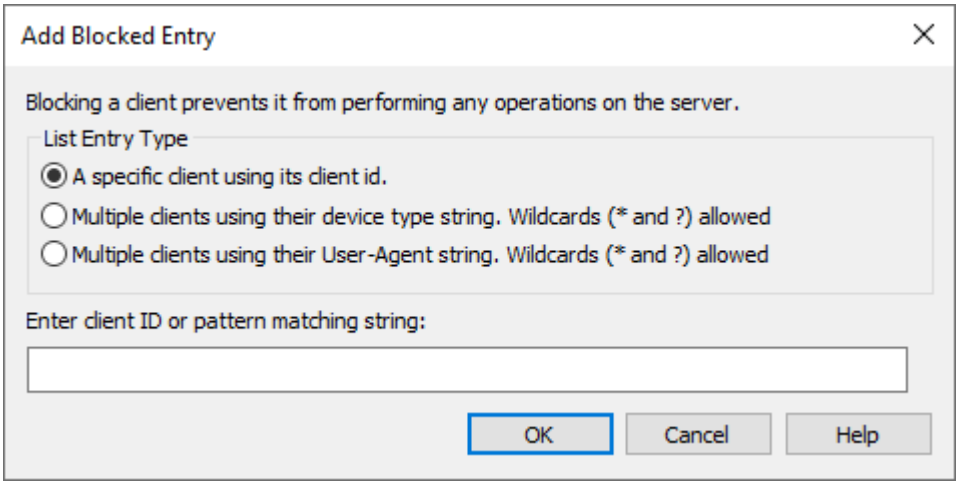
3.10.3 Seguridad



Clientes Bloqueados

Utilice esta opción para impedir que un tipo específico de Dispositivo, ID de Dispositivo o Agente de Usuario tenga acceso al servidor ActiveSync de MDaemon.

Agregar un registro Bloqueado
Para agregar una entrada a la lista, dé clic en **Agregar Registro**, especifique la información del dispositivo y dé clic en **OK**. Puede obtener la información del dispositivo mismo o de los archivos de registro de ActiveSync si el dispositivo se ha conectado al Servidor ActiveSync de MDaemon.



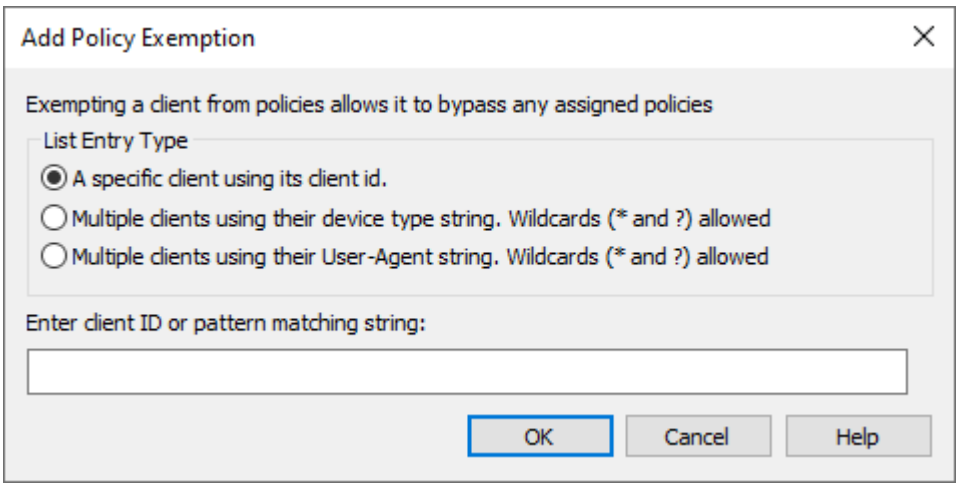
Puede bloquear un dispositivo fácilmente desde el diálogo Clientes 460. Dé clic derecho en un cliente en la lista y luego clic en **Bloquear este cliente**.

Eliminar un Registro de Bloqueado
Para eliminar entradas, seleccione una o más de ellas de la lista y dé clic en **Eliminar Registro**. Se le pedirá que confirme la acción antes de que se elimine.

Clientes Exentos

Utilice esta opción para exentar a un Tipo específico de Dispositivo, ID de Dispositivo o Agente de Usuario de aprovisionarse o de las restricciones de política 442.

Agregar un cliente exento
Para agregar una entrada a la lista, dé clic en **Agregar Registro**, especifique la información del dispositivo y dé clic en **OK**. Puede obtener la información del dispositivo mismo o de los archivos de registro de ActiveSync si el dispositivo se ha conectado al Servidor ActiveSync de MDaemon.



Puede exentar fácilmente un dispositivo desde el diálogo Clientes 460. Dé clic derecho sobre un cliente en la lista y luego clic en **Exentar**

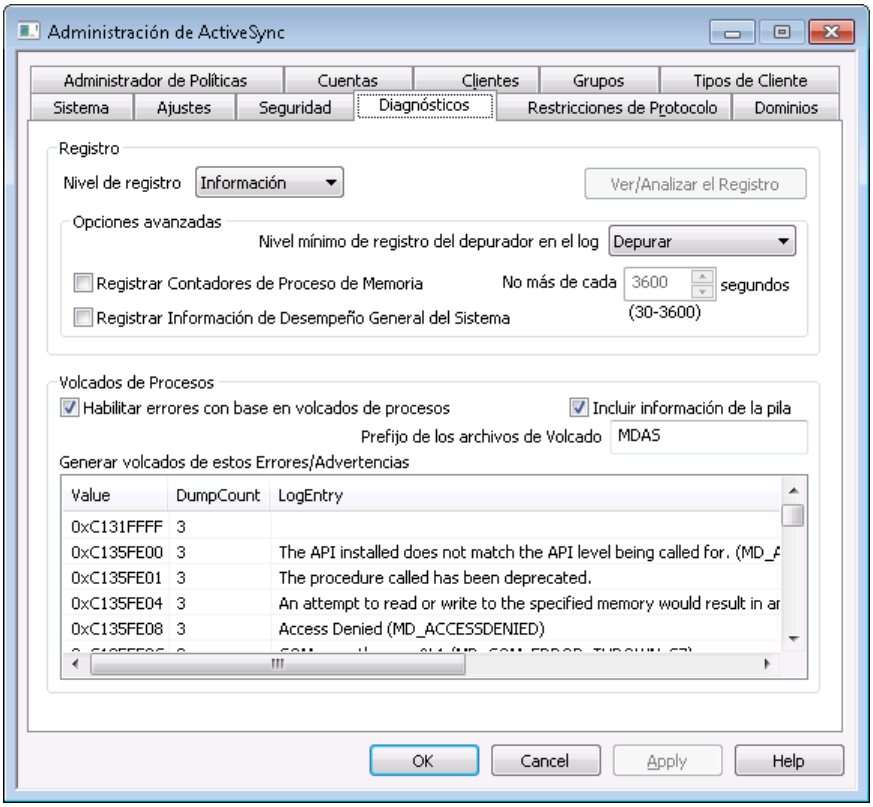
este cliente de las políticas.

Eliminar un registro exento
Para eliminar entradas, seleccione una o más de ellas de la lista y dé clic en **Eliminar Registro**. Se le pedirá que confirme la acción antes de que se elimine.

Ver:

ActiveSync » Clientes 247

3.10.4 Diagnósticos



Esta pantalla contiene opciones avanzadas que en la mayoría de los casos no necesitan ser utilizadas a menos que esté intentando diagnosticar un problema o tratando algún tema con soporte técnico.

Registro y Archivo

Esta sección contiene los ajustes globales de nivel de registro de ActiveSync. Ajustes de Cliente de Dominio 223 con el nivel de registro establecido en "Utilizar valor heredado o el de omisión" heredará el ajuste configurado aquí.

Nivel de Registro
Se soportan seis niveles de registro dependiendo de la más alta a más baja cantidad de datos registrados:

Depurar Es el nivel de registro más detallado. Incluye todas las entradas disponibles y típicamente solo se utiliza al diagnosticar un problema o cuando el administrador requiere información detallada.

Info Registro Moderado. Incluye operaciones generales sin detalle. Es el nivel de registro por omisión.

Advertencia Incluye advertencias, errores, errores críticos y eventos de inicio/cierre de la aplicación.

Error Se registran errores, errores críticos y eventos de inicio/cierre de la aplicación.

Críticos Se incluyen errores críticos y eventos de inicio/cierre de la aplicación.

Ninguno Solo se registran eventos de inicio/cierre de la aplicación.

Ver/Analizar el Registro
Dé clic en este botón para abrir el Sistema de Visor Avanzado de Registros de MDaemon. Por omisión, los registros se almacenan en: "..\MDaemon\Logs\"

Opciones Avanzadas

Nivel mínimo de registros para el depurador
Este es el nivel mínimo de registros a emitir al depurador. Los niveles disponibles de registro son los mismos descritos previamente.

Registrar contadores de procesamiento de memoria
Marque esta casilla para incluir en el archivo de registro información específica de procesos de Memoria, Identificadores e Hilos. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos. Las entradas al registro solo se emiten si los datos se han modificado desde la última vez que se registraron.

Registrar información del desempeño general del sistema
Marque esta casilla si desea incluir en el registro información del desempeño general del sistema. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos.

No más de cada [xx] segundos
Utilice esta opción para establecer el límite de la frecuencia con que se registrará la información de procesos y desempeño.

Volcados de Proceso

Habilitar volcados de procesos con base en errores
Habilite esta opción si desea generar volcados de proceso siempre que ocurran advertencias o errores específicos que usted determine abajo.

Incluir información de la pila en los volcados
Por omisión, se incluye información de la pila en los volcados de procesos.

Deshabilite esta casilla si no desea que se incluya esta información.

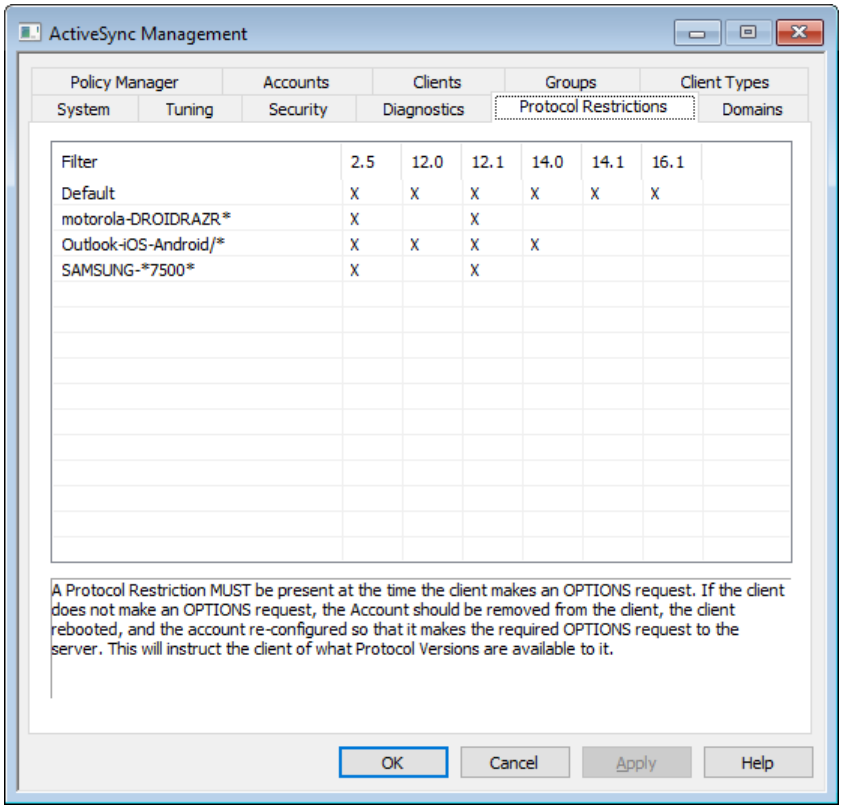
Prefijo para los archivos de volcado
Los nombres de archivos de volados de procesos inician con este texto.

Errores/Advertencias para genera volcados
Dé clic derecho en esta área y utilice las opciones *Agregar/Editar/Eliminar Registro...* para administrar la lista de errores o advertencias que detonarán volcados de procesos. Por cada entrada puede definir el número de volcados de proceso permitidos antes de que se desactive.

Ver:

ActiveSync » Ajustes 418

3.10.5 Restricciones de Protocolo



Restricciones de Protocolo por Dispositivo

Utilice esta opción localizada bajo "ActiveSync » Restricciones de Protocolo" para decirle a ciertos clientes y dispositivos que están restringidos a protocolos ActiveSync específicos. Esto es útil cuando, por ejemplo, un cierto tipo de dispositivo soporta de manera inestable alguna de las versiones del protocolo, pero funciona correctamente con otra. Al utilizar el diálogo Crear/Editar Restricciones de Protocolo 433, puede definir restricciones con base en el Agente de Usuario o el Tipo

de Dispositivo y restringir los dispositivos a cualquiera de las siguientes versiones del protocolo ActiveSync: 2.5, 12.0, 12.1, 14.0, 14.1. y 16.1

> Por omisión, las restricciones de protocolo no impiden que un cliente intente utilizar un protocolo diferente, le dicen al cliente cuales protocolos utilizar. Si un cliente intenta utilizar de cualquier manera un protocolo restringido, MDaemon permitirá la conexión. Si desea negar conexiones que intenten utilizar protocolos restringidos, utilice la opción siguiente *Forzar todas las restricciones de protocolo* en el diálogo Ajustes de Cliente 421.

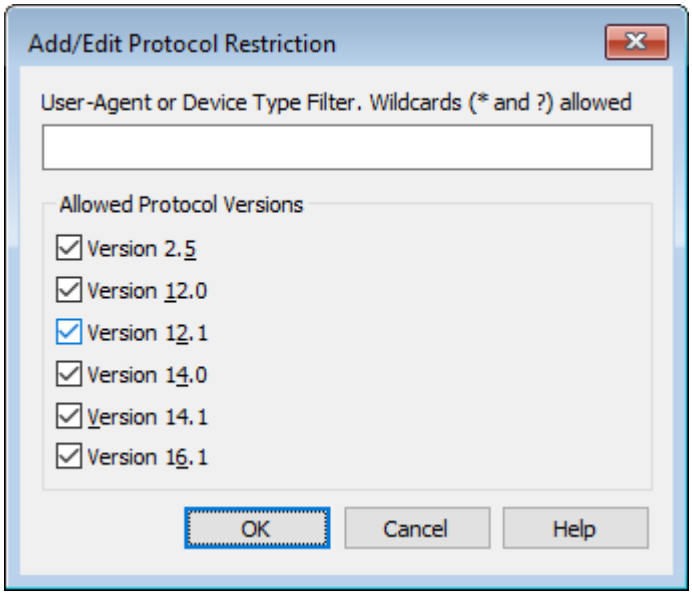
Dé clic derecho en una entrada en la lista para abrir un menú con las opciones siguientes:

Crear Restricción de Protocolo
Dé clic en esta opción para abrir el diálogo Agregar/Editar Restricción de Protocolo 433 (ver abajo), utilizado para agregar sus restricciones de protocolo.

Editar Restricciones de Protocolo
Para editar una restricción de protocolo, dé doble clic en una entrada en la lista (o clic derecho y seleccione **Editar Restricción de Protocolo**). Luego de realizar los cambios deseados en el editor de restricciones, dé clic en **OK**.

Eliminar Restricción de Protocolo
Para eliminar una restricción de protocolo, dé doble clic en una entrada en la lista (o clic derecho y seleccione **Eliminar Restricción de Protocolo**). Dé clic en **Sí** para confirmar su decisión de eliminar la restricción.

Agregar/Editar Restricciones de Protocolo

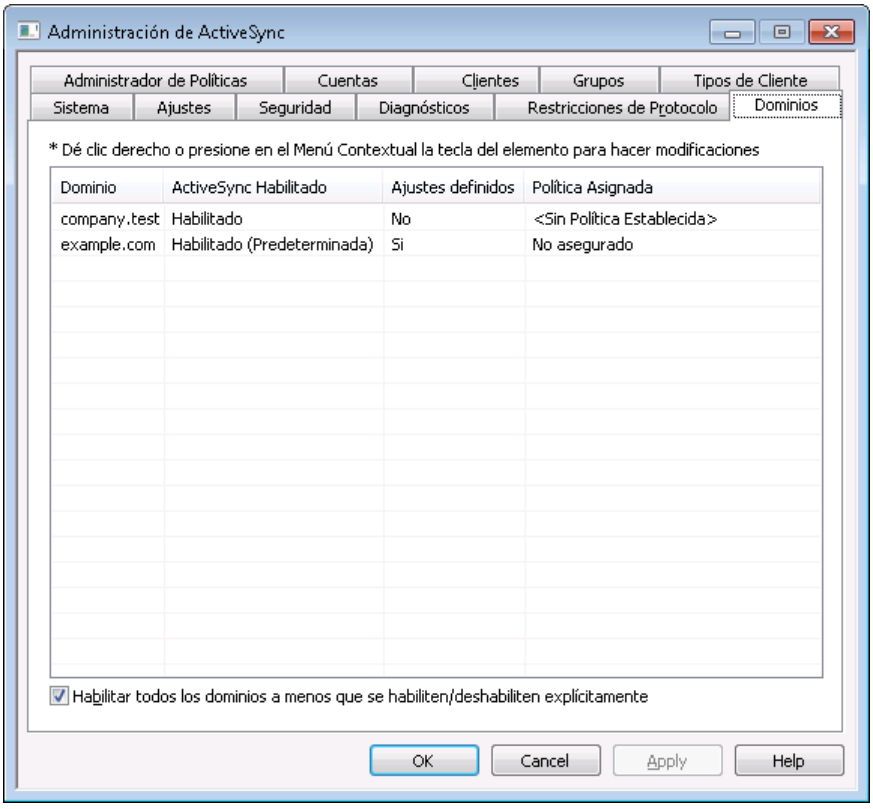


Filtro de Agente de Usuario o Tipo de Dispositivo
Ingrese el Agente de Usuario o Tipo de Dispositivo al que desea aplicar la restricción. Al identificar el agente, MDaemon utiliza e incluye el primer carácter "/" en la cadena, si está presente. Si no lo está, entonces se utiliza la cadena

completa. Si no conoce el nombre exacto del Agente de Usuario o Tipo de Dispositivo, una vez que se ha conectado el cliente a MDaemon ActiveSync (MDAS), puede ir a la pantalla Clientes 460, seleccione el cliente de la lista y dé clic en Detalles. También puede encontrar esta información examinando directamente el archivo de registro MDAS.

Versiones de Protocolo Permitidas
Dé clic en cada protocolo que desea soportar por el dispositivo o agente. Cuando se conecta el cliente especificado a MDaemon, se le dirá que utilice solo los protocolos que usted ha seleccionado.

3.10.6 Dominios



Utilice esta pantalla para administrar los Ajustes de ActiveSync para sus dominios 190. Puede habilitar o deshabilitar ActiveSync para cada dominio, asignar una Política ActiveSync 442 por omisión, administrar los ajustes por omisión de clientes y administrar dispositivos asociados con el dominio.

Habilitar/Deshabilitar ActiveSync para Dominios específicos

Para establecer el estado de ActiveSync para un dominio específico:

1. Dé clic en un dominio en la lista.
2. Dé clic en **Habilitar/Deshabilitar o Por Omisión.** Si selecciona "*Por Omisión*" entonces la opción abajo para "*Habilitar todos los dominios a menos que explícitamente se habiliten o deshabiliten*" determinará si ActiveSync está o no activo para el dominio.

A fin de utilizar ActiveSync requerirá configurar correctamente un cliente ActiveSync en el dispositivo del usuario. Para obtener instrucciones sobre cómo hacer esto, siga la liga *Comprar, Actualizar o Evaluar ActiveSync para MDaemon* en la pantalla ActiveSync para MDaemon 416 y desplácese hacia abajo a las instrucciones de configuración del dispositivo.

Configurar el Estado por Omisión de ActiveSync

Los Dominios con la columna *ActiveSync Habilitado* definida en **Habilitado/Deshabilitado (Por Omisión)** obtienen su ajuste de ActiveSync del estado de la opción: **Habilitar todos los dominios a menos que se habiliten/deshabiliten explícitamente.** Cuando esta opción se habilita, todos los dominios tendrán a ActiveSync habilitado por omisión. Cuando se deshabilita, ActiveSync será deshabilitado por omisión. Si se ajusta el valor de un dominio específicamente a **Habilitado** o **Deshabilitado**, no se considerará el valor del ajuste por omisión.

Si modifica el ajuste *ActiveSync Habilitado* para un dominio a **Deshabilitado**, se abrirá una caja de confirmación para preguntarle si desea revocar el acceso a ActiveSync a todos los usuarios de ese dominio. Seleccione **No** si desea permitir que cualquier usuario del dominio que actualmente utiliza ActiveSync continúe utilizándolo. Si selecciona **Si**, entonces ActiveSync se deshabilitará para todos los usuarios del dominio.

Modificar los Ajustes de Cliente de Dominio

Dé clic derecho en un dominio para administrar los Ajustes de Cliente por Dominio. Por omisión estos ajustes se heredan de la pantalla Ajustes Globales de Cliente 421. Vea Administrando los Ajustes de Cliente por Dominio 436 abajo.

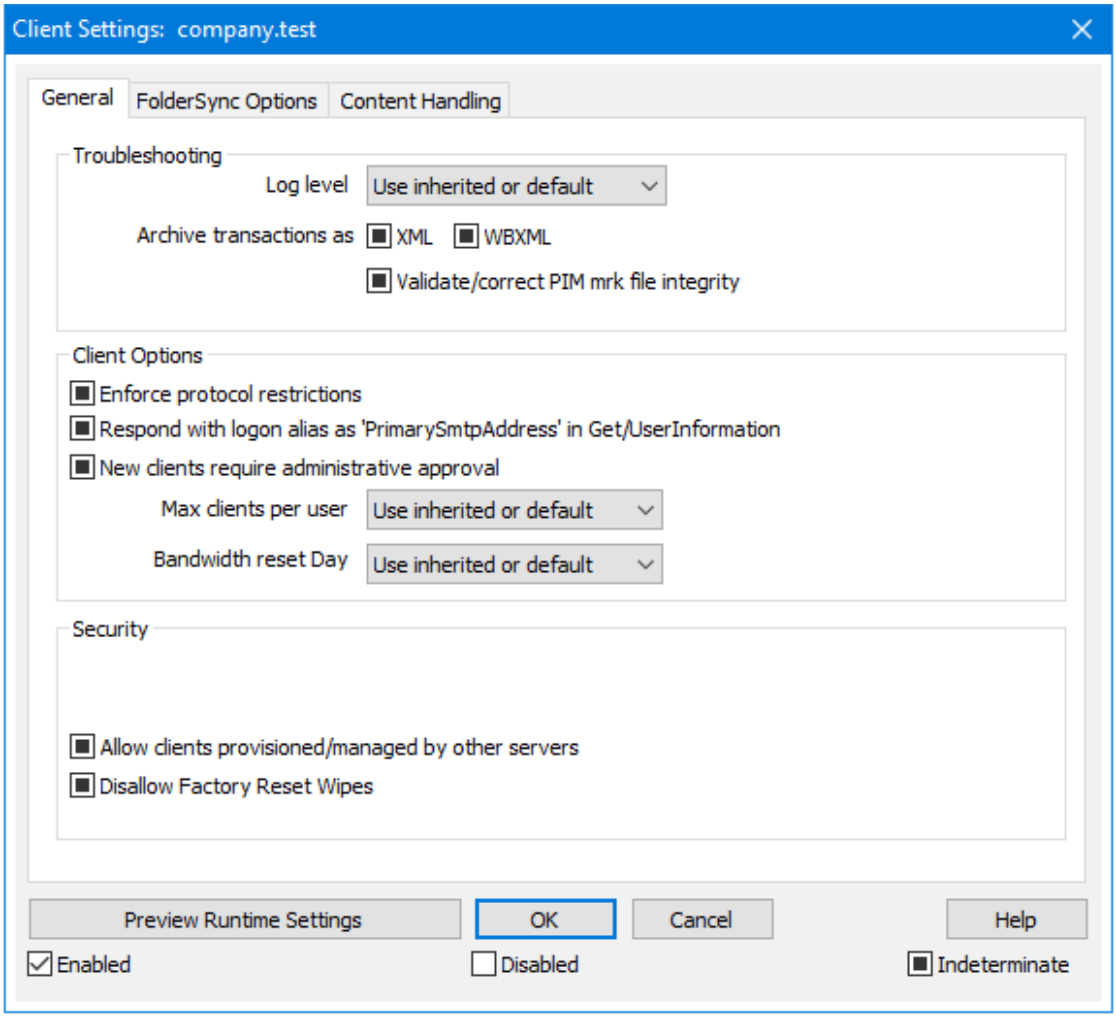
Asignar una Política ActiveSync por Omisión

Para asignar una política ActiveSync por omisión a un dominio:

1. Dé clic derecho en un dominio de la lista.
2. Dé clic en **Aplicar Política**.
3. Bajo "Política a Asignar" seleccione la política deseada en la lista desplegable (para administras las políticas disponibles vea el Administrador de Políticas 442).
4. Dé clic en **OK**.

Administrar los Ajustes de Cliente por Dominio

La pantalla de Ajustes de Cliente del Dominio le permite administrar los ajustes por omisión para cuentas y clientes asociados con el dominio.



Por omisión todas las opciones en esta pantalla se configuran a "Utilizar valore heredado o el de omisión" lo que significa que cada opción tomará su valor de la opción correspondiente en la pantalla Ajustes Globales de Cliente 421. Similarmente, las pantallas ajustes de cliente para las Cuentas 451 de este dominio heredarán sus ajustes de esta pantalla, dado que la pantalla Ajustes de Cliente del Dominio es su pantalla padre. Cualquier cambio hecho en las opciones en esta pantalla se reflejará en aquellas pantallas. Debajo de eso, los Tipos de Cliente tienen pantallas de ajuste que heredan sus valores de los ajustes a nivel cuenta y finalmente los clientes 460 individuales también cuenta con sus propios ajustes . Esta configuración permite hacer cambios para todas las cuentas y clientes de un dominio simplemente modificando los valores en esta pantalla y se le permite omitir estos ajustes para cualquier cuenta o cliente como lo requiera.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que

el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas[314] a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta[316] para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas[314] padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas[128] a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas[743] a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes[460] y tipos de clientes[475] que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura

para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

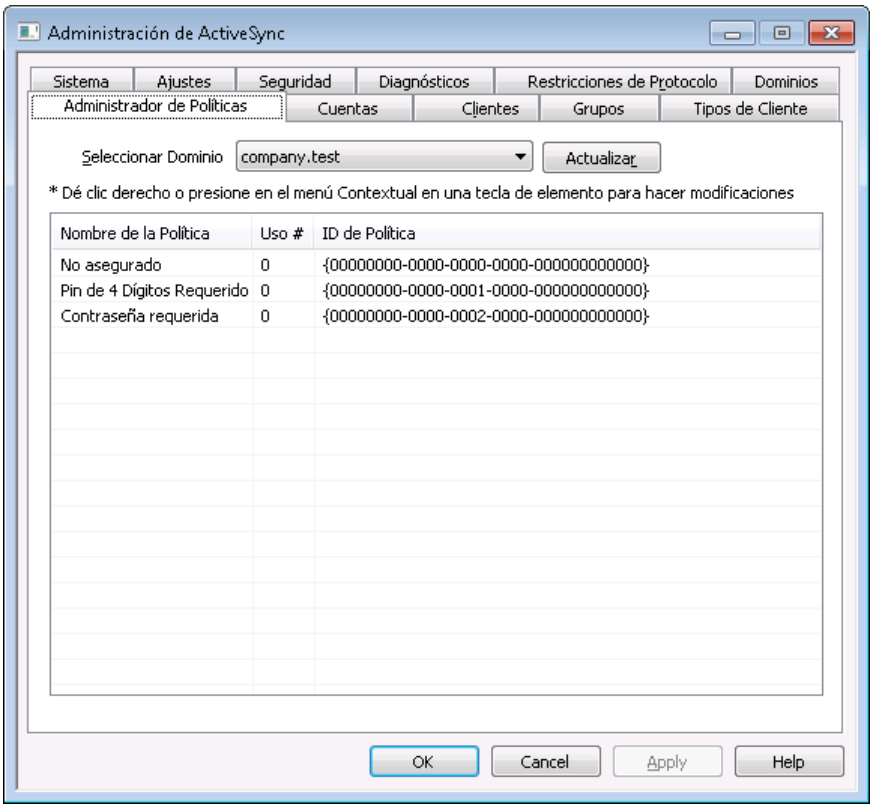
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

Administrador de Dominios » Ajustes de Cliente ActiveSync 223
Administrador de Dominios » Clientes ActiveSync 247
ActiveSync » Administrador de Políticas 442
ActiveSync » Clientes 460

3.10.7 Administrador de Políticas



Utilice esta pantalla para administrar las Políticas ActiveSync que se pueden asignar a dispositivos de usuario para controlar varias opciones. Se proporcionan políticas predeterminadas y puede crear editar y eliminar las suyas propias. Las políticas por omisión se pueden asignar por domino 434 y por cuenta 451 y las políticas se pueden asignar a clientes específicos 247.

No todos los dispositivos ActiveSync reconocen o aplican políticas consistentemente. Algunos pueden ignorar políticas o ciertos elementos de política y otro pueden

> requerir un reinicio de dispositivo antes de que tengan efecto los cambios. Más aun, cuando se intenta asignar una política nueva a un dispositivo, no se aplicará hasta la siguiente ocasión en que el dispositivo se conecte por sí mismo al servidor ActiveSync; las políticas no se pueden "entregar" a los dispositivos hasta que se conecten.

Políticas ActiveSync

Dé clic derecho en la lista para abrir un menú de acceso rápido a las opciones siguientes:

Crear Política
Dé clic en esta opción para abrir el Editor de Políticas ActiveSync, que se utiliza para crear y editar políticas.

Eliminar
Para eliminar una política, seleccione una política personalizada de la lista y de clic en **Eliminar**. Dé clic en **Sí** para confirmar la acción. Las políticas predeterminadas no se pueden eliminar.

Editar Política
Para editar una política, dé clic derecho en una política personalizada en la lista y luego clic en **Editar Política**. Luego de hacer las modificaciones deseadas en el editor de políticas, dé clic en **OK**. Las políticas predeterminadas no se pueden editar.

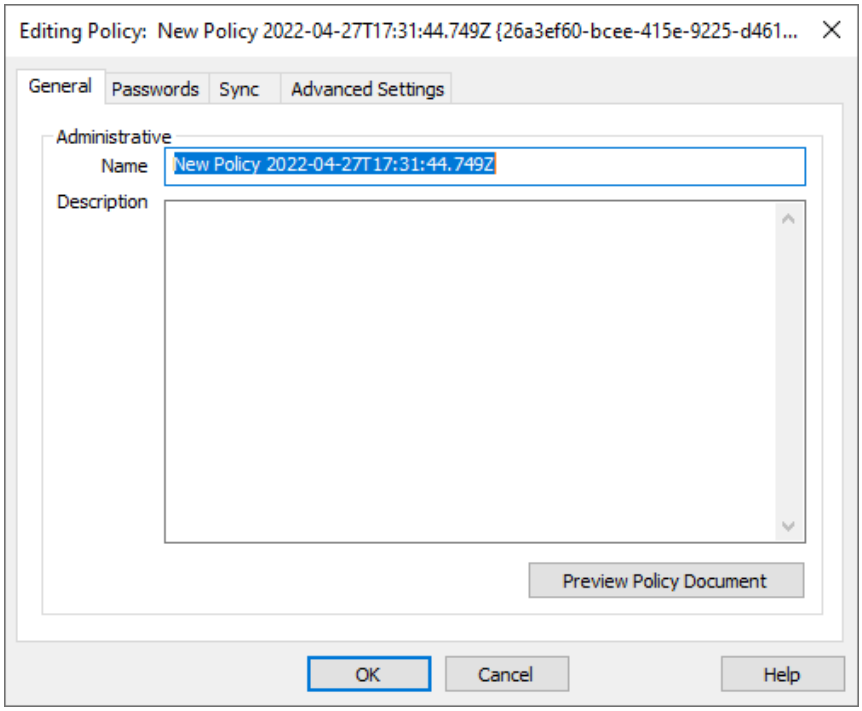
Visualizar Uso de Políticas
Dé clic derecho en una política y luego seleccione esta opción para visualizar una lista de todos los dominios, cuentas y clientes que están configurados para utilizar esta política.

Editor de Políticas ActiveSync

El Editor de Políticas ActiveSync cuenta con 4 pestañas: General, Contraseñas, Sync y Ajustes Avanzados. La pestaña de Ajustes Avanzados está oculta a menos que active *Habilitar la edición de opciones avanzadas de políticas* 416, localizada en la pantalla ActiveSync Sistema.

General

Utilice esta pantalla para definir un nombre y descripción para su política. También puede tener una vista previa del documento XML de la política.



Administrativo

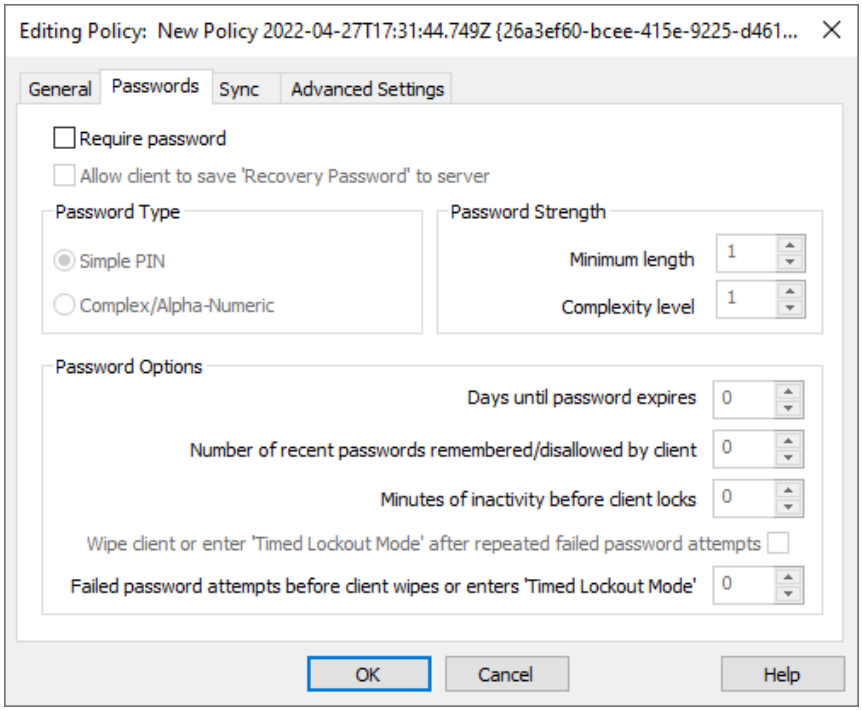
Nombre
Especifique aquí un nombre para su política personalizada.

Descripción
Utilice esta área para describir su política personalizada. Esta descripción aparece en el diálogo Aplicar Política al seleccionar una política para aplicarla a un dominio, cuenta o cliente.

Vista Previa del Documento de Política
Dé clic en este botón para una vista previa del documento XML de esta política.

Contraseñas

Las opciones de Contraseña y requerimientos para esta política se definen en esta pestaña.



Requerir contraseña
Marque esta caja si desea requerir contraseña en el dispositivo. Está deshabilitada por omisión.

Permitir al dispositivo grabar "Contraseña de Recuperación" en el servidor.
Habilite esta opción si desea permitir a los clientes utilizar la opción de Recuperación de Contraseña ActiveSync, que le permite al dispositivo grabar una contraseña temporal de recuperación en el servidor para desbloquear el dispositivo si la contraseña se olvida. El administrador puede encontrar esta contraseña de recuperación bajo los Detalles[460] del cliente. La mayoría de los dispositivos no soportan esta funcionalidad.

Tipo de Contraseña

PIN Simple
La manera en que se implementa es opción depende principalmente del dispositivo, pero seleccionar *PIN Simple PIN* como tipo de contraseña generalmente significa que no hay restricciones o requerimientos de complejidad para la contraseña del dispositivo, más que la opción siguiente *Longitud Mínima de Contraseña.* Esta permite contraseñas simples tales como: "111," "aaa," "1234," "ABCD" y similares.

Compleja Alfa/Numérica
Utilice esta opción de política si desea requerir contraseñas más complejas y seguras en el dispositivo en lugar de la opción *PIN Simple*. Utilice la opción siguiente *Nivel de Complejidad* para definir exactamente qué tan compleja debe ser la contraseña. Esta es la selección por omisión cuando se requiere una contraseña con esta política.

Seguridad de la Contraseña

Longitud Mínima
Utilice esta opción para definir el número de caracteres mínimo que debe contener la contraseña del dispositivo, de 1 a 16. Esta opción está configurada como "1" por omisión.

Nivel de Complejidad
Utilice esta opción para establecer el requerimiento de nivel de complejidad de las contraseñas como *Compleja/Alfanumérica*. El nivel es el número de tipos diferentes de caracteres que debe contener la contraseña: mayúsculas, minúsculas, números y caracteres no-alfanuméricos (tales como signos de puntuación o caracteres especiales). Puede requerir de 1 a 4 tipos de caracteres. Por ejemplo, si esta opción se configura en "2", entonces la contraseña debe contener por lo menos dos de los cuatro tipos de caracteres: mayúsculas y números, mayúsculas y minúsculas, números y símbolos, etc. Esta opción se configura como "1" por omisión.

Opciones de Contraseña

Días para que expire la contraseña (0=nunca)
Este es el número de días permitido antes de que la contraseña del dispositivo deba ser modificada. La opción se encuentra deshabilitada por omisión (configurada en "0").

Número de contraseñas recientes a recordar/deshabilitar por dispositivo (0=ninguna)
Utilice esta opción si desea prevenir que el dispositivo reutilice un número específico de contraseñas anteriores. Por ejemplo, si esta opción se configura como "2" y usted modifica la contraseña del dispositivo, no podrá cambiarla a ninguna de las últimas dos contraseñas que haya utilizado. Esta opción está deshabilitada por omisión (configurada en "0").

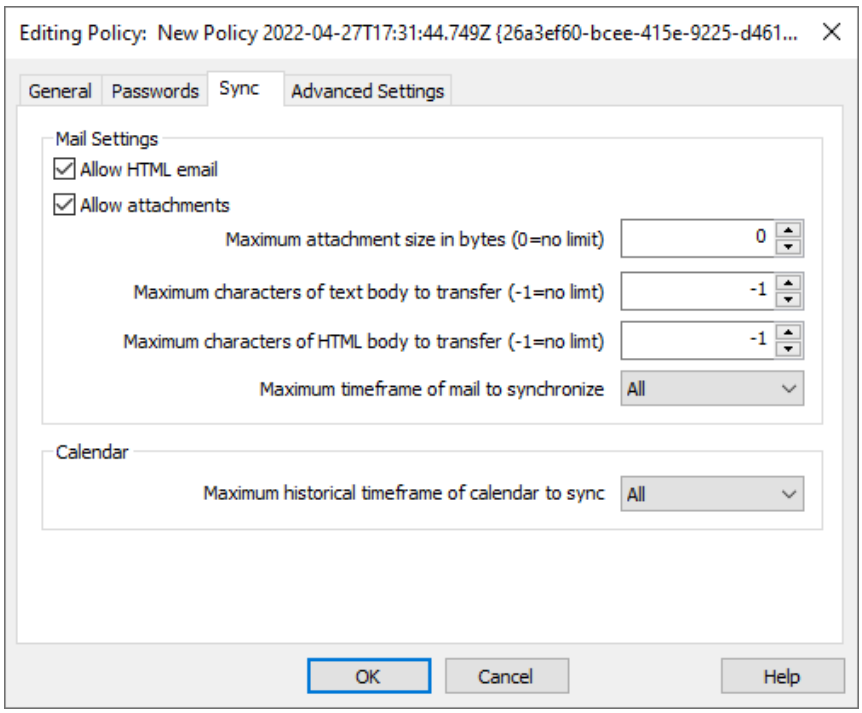
Minutos de inactividad antes de que se bloquee el dispositivo (0=nunca)
Esta es la cantidad de minutos que puede funcionar un dispositivo sin interacción del usuario antes de que se bloquee. Esta opción de contraseña se encuentra deshabilitada por omisión (configurada en "0").

Borrar el dispositivo o pasarlo a 'Modo de Bloqueo' luego de intentos fallidos de contraseña
Cuando esta opción está habilitada y el usuario falla el número determinado de intentos de contraseña, el dispositivo se bloqueará durante cierto tiempo o ejecutará un borrado de todos los datos, dependiendo del dispositivo. Esta opción está deshabilitada por omisión.

Intentos fallidos de contraseña antes de que el dispositivo se borre o entre en "Modo Bloqueo"
Cuando la opción "*Borrar el Dispositivo...*" descrita arriba está habilitada y el usuario falla este número de intentos de contraseña, el dispositivo será borrado o se detonará el 'Modo de Bloqueo' dependiendo del dispositivo.

Sync

Esta pantalla contiene varios ajustes que administran el correo HTML, permitiendo adjuntos, limitando el número de caracteres a transferir y el rango de tiempo máximo de correo y calendario a sincronizar.



Ajustes de Correo

Permitir correo HTML
Por omisión, se puede sincronizar/enviar correo con formato HTML a los clientes ActiveSync. Deshabilite esta caja si desea enviar solo texto plano.

Permitir adjuntos
Permite al dispositivo descargar archivos adjuntos. La opción está habilitada por omisión.

Max tamaño de adjuntos en bytes (0=sin límite)
Este es el tamaño máximo de adjunto que se puede descargar en automático al dispositivo. Por omisión el tamaño de adjunto no tiene límite (configurado a "0").

Máximo de caracteres a transferir en el cuerpo del mensaje en texto plano (-1=sin límite)
Este es el número máximo de caracteres en el cuerpo de mensajes con formato en texto plano que se enviará al cliente. Si el cuerpo del mensaje contiene más caracteres de los permitidos, será truncado al límite especificado. Por omisión no está configurado ningún límite (la opción está configurada a "-1"). Si establece la opción a "0" solo se enviará el encabezado del mensaje.

Máximo de caracteres a transferir en el cuerpo del mensaje HTML (-1=sin límite)
Este es el número máximo de caracteres en el cuerpo de mensajes con formato HTML que se enviará al cliente. Si el cuerpo del mensaje contiene más caracteres de los permitidos, será truncado al límite especificado. Por omisión no está configurado ningún límite (la opción está configurada a "-1"). Si establece la opción a "0" solo se enviará el encabezado del mensaje.

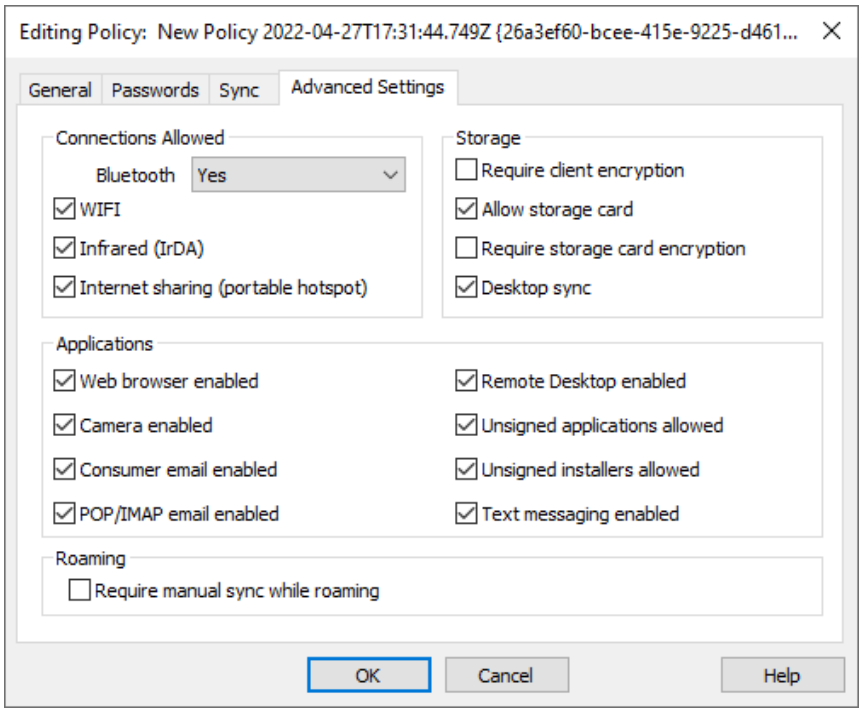
Máximo lapso para sincronizar correo
Esta es la cantidad de correo anterior por rango de fecha desde hoy, que puede sincronizarse al dispositivo. Por omisión está configurado a "Todo", lo que significa que todo el correo se puede sincronizar sin importar su antigüedad.

Calendario

Máximo lapso para sincronizar calendario
Esto es que tan atrás a partir de hoy se sincronizarán registros del calendario al dispositivo. Por omisión está configurado como "Todo", lo que significa que todos los registros pasados serán sincronizados sin importar su antigüedad.

Ajustes Avanzados

La pestaña de Ajustes Avanzados contiene opciones que controlan los tipos de conexiones permitidas y si ciertas aplicaciones pueden ser habilitadas, el almacenamiento, encripción y roaming.



Esta pestaña está oculta a menos que active *Habilitar la edición de*

políticas avanzadas 416, localizada en la pantalla ActiveSync para MDaemon.

Conexiones Permitidas

Bluetooth
Utilice esta opción para definir si se permiten conexiones Bluetooth en el dispositivo. Puede seleccionar **Si** para permitir conexiones Bluetooth, **No** para impedirlas o **Manos Libres** para restringir Bluetooth solo a Manos Libres. Esta opción está configurada a **Si** por omisión.

WIFI
Permite conexiones WIFI. Habilitada por omisión.

Infrarrojo (IrDA)
Permite conexiones infrarrojas (IrDA). Habilitada por omisión.

Compartir Internet (Punto de acceso portátil)
Esta opción permite al dispositivo utilizar el Internet compartido (punto de acceso portátil). Se encuentra habilitada por omisión.

Almacenamiento

Requerir encripción del dispositivo
Dé clic en esta opción si desea requerir encripción en el dispositivo. No todos los dispositivos soportan la encripción. Está deshabilitada por omisión.

Permitir tarjeta de almacenamiento
Permite que el dispositivo utilice una tarjeta de almacenamiento. Se encuentra habilitada por omisión.

Requerir encripción en la tarjeta de almacenamiento
Utilice esta opción si desea requerir encripción en la tarjeta de almacenamiento. Está deshabilitada por omisión.

Sincronización con el Escritorio
Permite ActiveSync en el Escritorio en el dispositivo. Está habilidad por omisión.

Aplicaciones

Navegador habilitado
Permite el uso el navegador en el dispositivo. No todos los dispositivos soportan esta opción y puede no aplicar a navegadores de terceros. Está habilitada por omisión.

Cámara habilitada
Permite utilizar la cámara en el dispositivo. Esta opción se encuentra habilitada por omisión.

Correo del consumidor habilitado
El dispositivo permite al usuario configurar una cuenta de correo personal. Cuando se deshabilita, los tipos de cuentas de correo o servicios que están prohibidos dependen por entero del cliente

ActiveSync en particular. Esta opción está habilitada por omisión.

Correo POP/IMAP habilitado
Permite el acceso a correo POP o IMAP. Se encuentra habilitada por omisión.

Escritorio Remoto habilitado
Permite al cliente utilizar el Escritorio Remoto. Está habilitada por omisión.

Permitir aplicaciones no firmadas
Esta opción permite que se utilicen aplicaciones no firmadas en el dispositivo. Está habilitada por omisión.

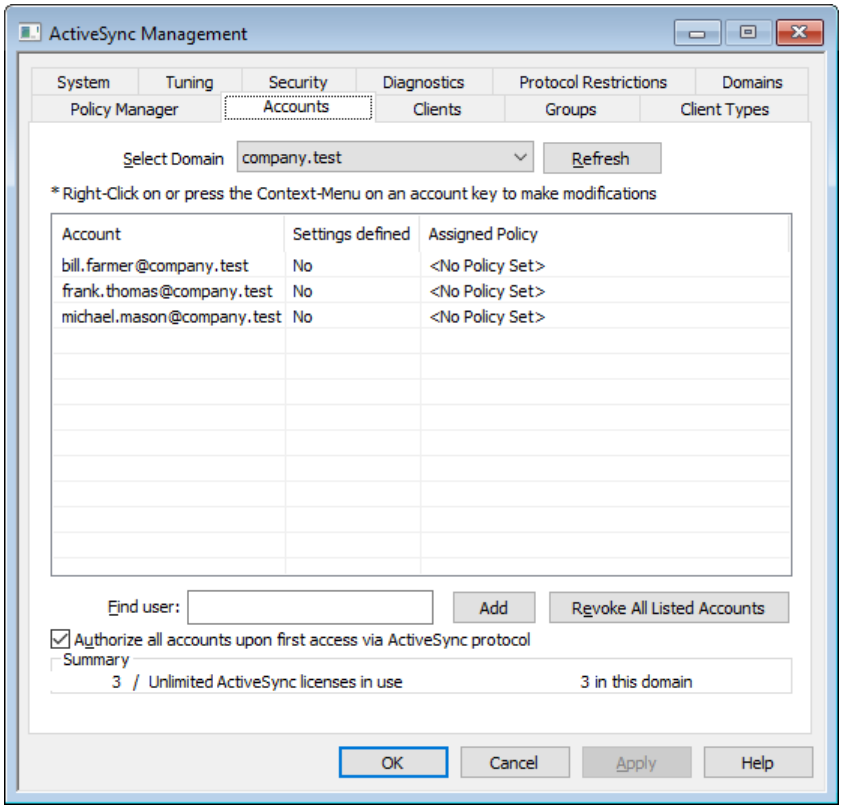
Permitir instaladores no firmados
Esta opción permite que se ejecuten instaladores no firmados en el dispositivo. Está habilitada por omisión.

Mensajería de texto habilitada
Esta opción permite la mensajería de texto en el dispositivo. Se encuentra habilitada por omisión.

Roaming

Requerir sincronización manual cuando se encuentra en roaming
Utilice esta opción de política si desea requerir que el dispositivo se sincronice manualmente cuando se encuentra en roaming. El permitir la sincronización automática en roaming puede incrementar los costos de datos para el dispositivo, dependiendo de su carrier y su plan de datos. Esta opción está deshabilitada por omisión.

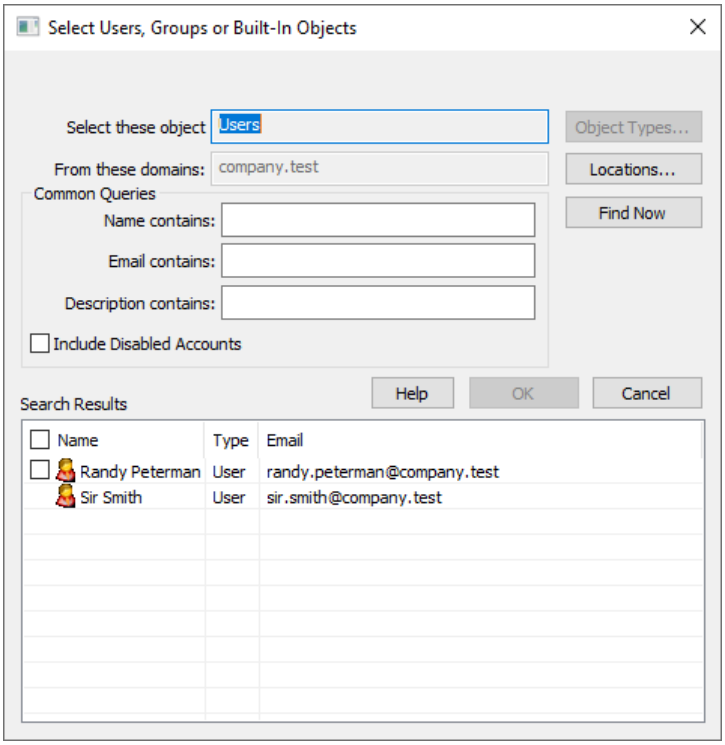
3.10.8 Cuentas



Utilice esta pantalla para definir las cuentas autorizadas para utilizar ActiveSync. Puede autorizar o revocar cuentas manualmente, o configurar a MDaemon para autorizarlas en automática al momento que cada cuenta se conecte utilizando ActiveSync.

Autorizar Cuentas Manualmente

En la pantalla Cuentas, seleccione un dominio en la lista desplegable *Seleccionar Dominio* y dé clic en **Agregar** para autorizar manualmente a una o más cuentas para utilizar ActiveSync. Esto abre el diálogo Selección de Usuarios para encontrar y seleccionar las cuentas.



De estos Dominios
Aquí se enlista el dominio que seleccionó en la opción *Seleccionar Dominio* en la pantalla cuentas. Puede consultar los usuarios de este Dominio.

Consultas comunes
Utilice las opciones en esta sección para reducir la búsqueda especificando todo o parte del nombre del usuario, su dirección de correo u otro contenido de la Descripción[715] de la cuenta. Deje estos campos en blanco si desea que los resultados de las búsquedas contengan todos los usuarios que coincidan con los dominios seleccionados.

Incluir Cuentas Deshabilitadas
Marque esta caja si desea incluir cuentas deshabilitadas[715] en su búsqueda.

Encontrar Ahora
Luego que haya especificado todos sus criterios de búsqueda, dé clic en **Encontrar Ahora** para ejecutar la búsqueda.

Resultados de la Búsqueda
Luego de ejecutar la búsqueda, seleccione los usuarios deseados en los Resultados de la Búsqueda y de clic en OK para agregarlos a la lista de cuentas autorizadas.

Revocar cuentas

Para revocar la autorización de la cuenta para utilizar ActiveSync, dé clic derecho en una cuenta en la lista y clic en **Revocar Permisos ActiveSync**. Si desea revocar los permisos de todas las cuentas, dé clic en el botón **Revocar todas las cuentas en la lista**.

Si ha habilitado la opción *Autorizar todas las cuentas cuando acceden el protocolo ActiveSync por primera vez,* al revocar el acceso de la cuenta se le eliminará de la lista, pero la siguiente ocasión en que se conecte se le autorizará a conectarse de nuevo.

Autorizar todas las cuentas en su primer acceso vía ActiveSync

Marque esta caja si desea autorizar automáticamente las cuentas, una a la vez, en cuento se conecten a MDaemon utilizando ActiveSync.

Asignar una Política ActiveSync

Para asignar una Política 442 a la cuenta:

1. Dé clic derecho en una cuenta en la lista.
2. Dé clic en **Aplicar Política**.
3. Bajo "Asignar Política" seleccione la política deseada en la lista desplegable (para administrar sus políticas disponibles, vea el Administrador de Políticas 442).
4. Dé clic en **OK**.

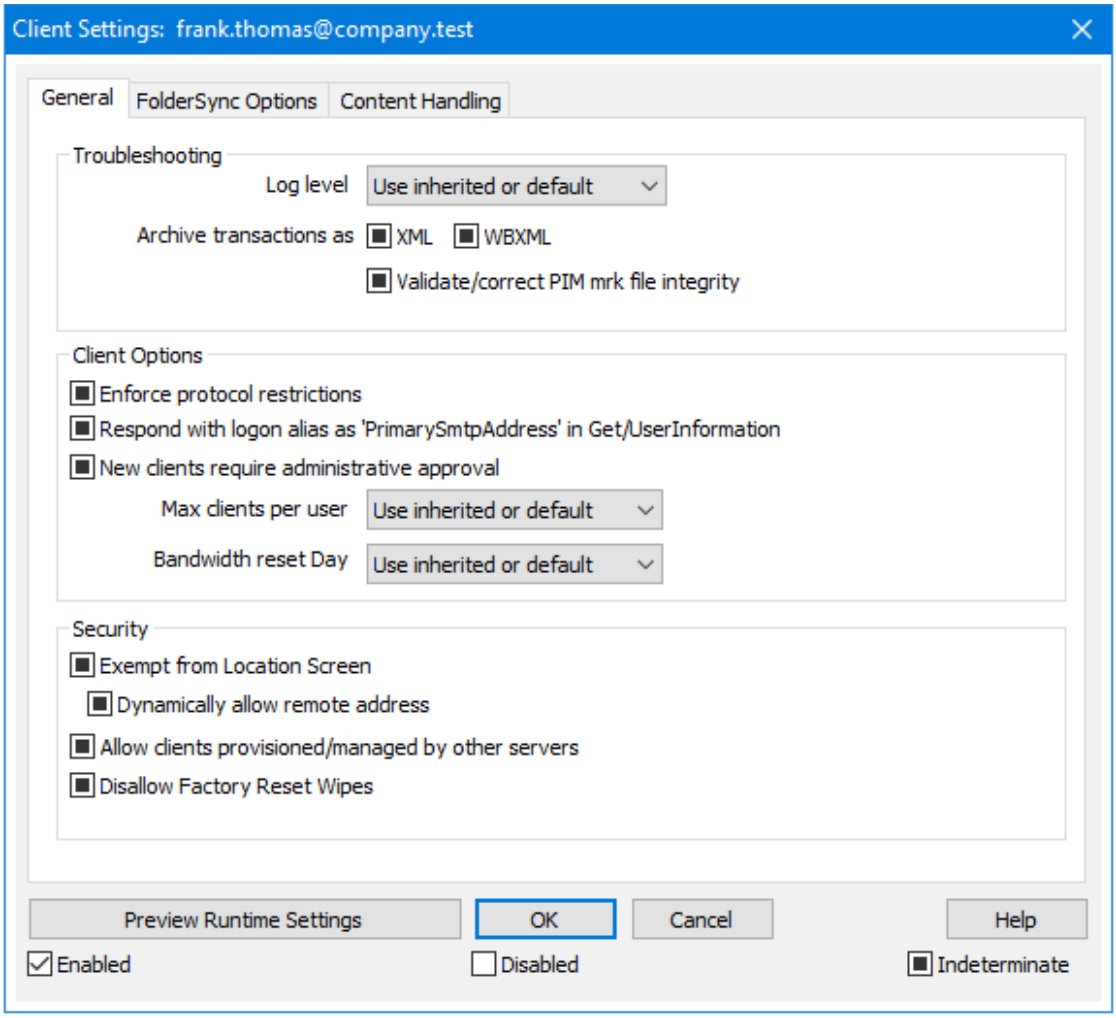
Esta política se asignará a cualquier dispositivo nuevo que se conecte para esta cuenta.

Buscando en la Lista de Cuentas Autorizadas

Si tiene un gran número de cuentas autorizadas para utilizar ActiveSync, puede utilizar la caja Encontrar usuario para buscar en la lista una cuenta en particular. Simplemente teclee las primeras letras de la dirección de correo de la cuenta para seleccionar el usuario.

Ajustes de Cliente de Cuenta

Dé clic derecho en una cuenta y luego clic en **Personalizar Ajustes de Cliente** para administrar los Ajustes de Cliente para la cuenta. Estos ajustes se aplicarán a cualquier cliente ActiveSync que se conecte para la cuenta.



Por omisión todas las opciones en esta pantalla están configuradas a "Utilizar el valor heredado o el de omisión", lo que significa que si la cuenta es miembro de un Grupo[468], entonces el ajuste de cada opción se tomará de los Ajustes de Cliente de ese grupo. Si la cuenta no está en un grupo o si no hay Ajustes de Cliente configurados para ese grupo, entonces cada opción tomará su valor de la opción correspondiente en la pantalla Ajustes de Cliente de Dominio[223]. Cualquier modificación hecha a los ajustes en esa pantalla se reflejará en esta. Alternativamente, cualquier cambio que se realice en esta pantalla tendrá prioridad sobre los ajustes a nivel grupo o dominio para esta cuenta.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes[460] indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones[572]. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días[418] localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado**

Completo en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción

necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432

16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

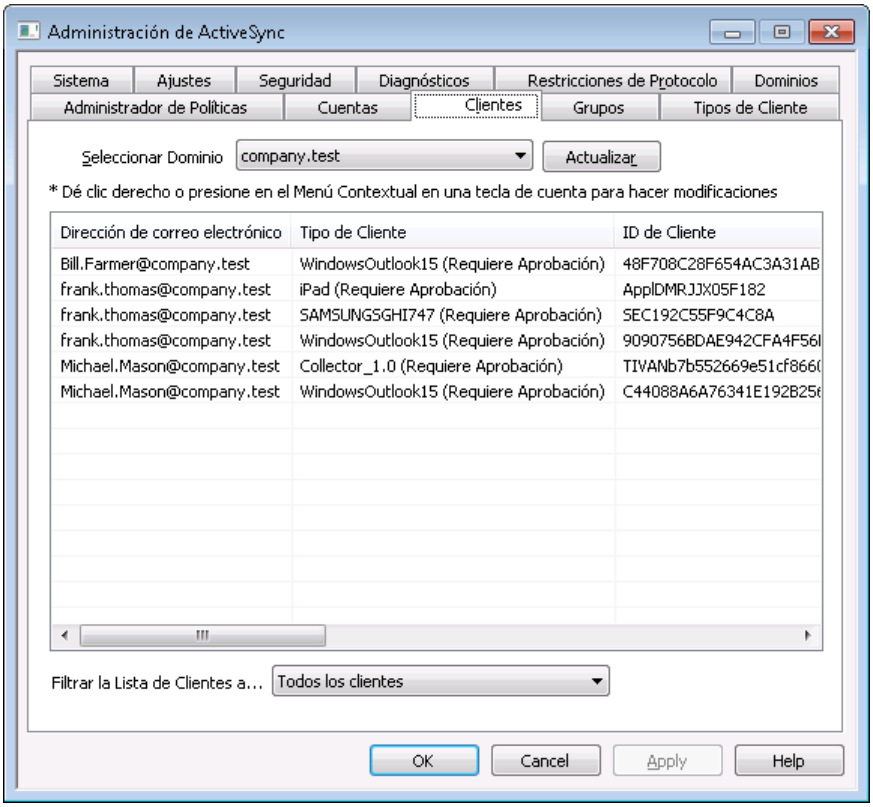
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

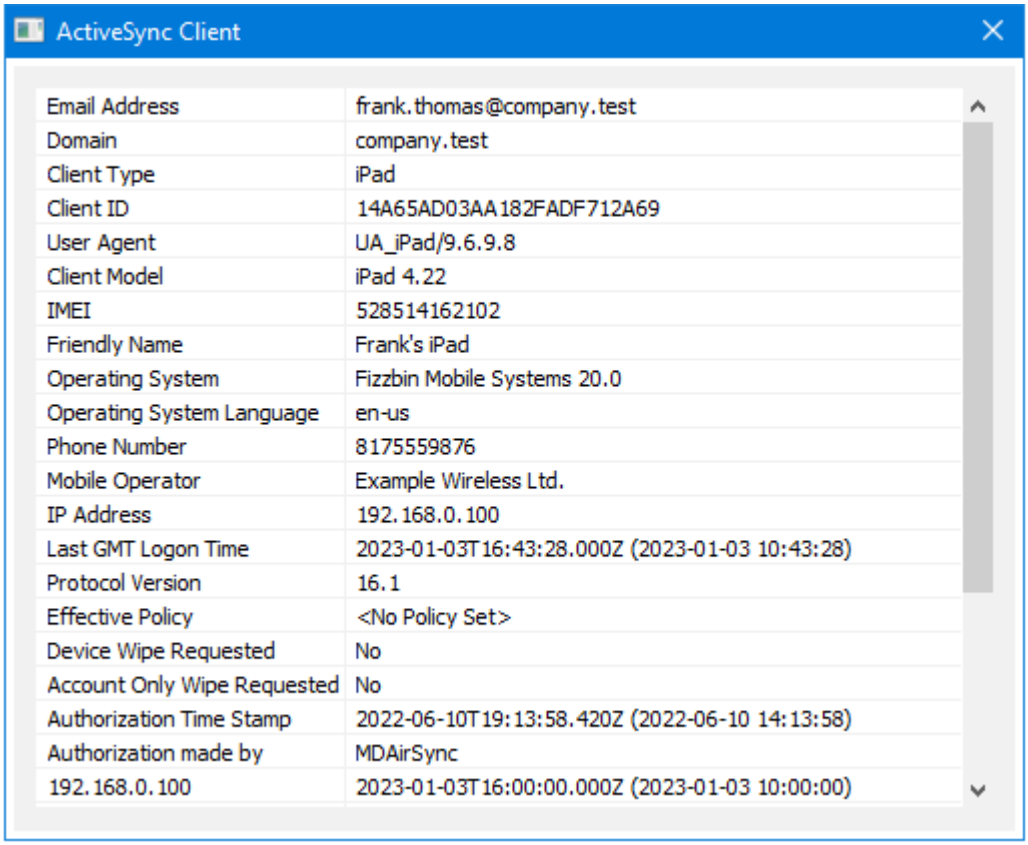
ActiveSync » Ajustes de Cliente 421
ActiveSync » Dominios 434
ActiveSync » Clientes 460
Cuentas » Ajustes de Cliente ActiveSync 765
Cuentas » Clientes ActiveSync 772

3.10.9 Clientes



Esta pantalla contiene un registro por cada cliente ActiveSync asociado con un dominio seleccionado. Dé doble clic en cualquier registro para ver más detalles sobre el cliente. Dé clic derecho en una entrada para abrir un acceso directo desde el cual puede personalizar sus ajustes de cliente, visualizar estadísticas y realizar varias funciones más.

Detalles del Cliente ActiveSync



Seleccione una entrada y dé clic en **Ver Detalles del Cliente** para abrir el diálogo de Detalles del Cliente. Esta pantalla contiene información sobre el cliente, tal como su Tipo de Cliente, ID de Cliente, último inicio de sesión y más.

Ajustes de Cliente

dé clic derecho en un cliente y clic en **Personalizar Ajustes de Cliente** para administrar sus Ajustes de Cliente. Por omisión estos ajustes se heredan de la pantalla de Ajustes de Tipo de Cliente, pero se pueden ajustar si lo desea . Vea Administrar Ajustes del Cliente del Dispositivo abajo.

Asignar una Política ActiveSync

Para asignar una Política 442 al dispositivo:

1. Dé clic derecho en un dispositivo en la lista.
2. Dé clic en **Aplicar Política**. Esto abre el diálogo Aplicar Política.
3. Dé clic en **Política a Asignar** en la lista desplegable y seleccione la política deseada.
4. Dé clic en **OK**.

Estadísticas

Dé clic derecho en una entrada y luego clic en **Ver Estadísticas** para abrir el diálogo Estadísticas del Cliente, que contiene varias estadísticas de uso para el cliente.

Restablecer Estadísticas

Si desea restablecer las estadísticas del cliente, dé clic derecho en el cliente, luego clic en **Restablecer Estadísticas** y **OK** para confirmar la acción.

Remover un Cliente ActiveSync

Para remover un cliente ActiveSync, dé clic derecho en el cliente y clic en **Eliminar**, y luego en **Si**. Esto eliminará el cliente de la lista así como toda la información de sincronización relativa al cliente, en MDaemon. Por esto, si en el futuro la cuenta utiliza ActiveSync para sincronizar el mismo cliente, MDaemon lo tratará como si nunca antes hubiera sido utilizado en el servidor: todos los datos del cliente tendrán que resincronizarse con MDaemon.

Borrar por completo un Cliente ActiveSync

Cuando se ha aplicado una política 442 a un cliente ActiveSync seleccionado y el cliente la ha aplicado y respondido, entonces se dispondrá con una opción de Borrado Completo para ese cliente. Para hacer un Borrado completo, dé clic derecho en el cliente (o selecciónelo si está utilizado MDRA) y dé clic en **Borrado Completo**. La próxima vez que se conecte ese cliente, MDaemon le dirá que borre todos los datos o se restaure a sí mismo a sus valores de fábrica. Dependiendo del cliente, esto puede eliminar todo en el dispositivo incluyendo apps descargadas. Más aún, en tanto exista el registro en ActiveSync de ese cliente, MDaemon continuará enviando peticiones de borrado siempre que el dispositivo se conecte en el futuro. Si en algún momento desea eliminar el cliente, asegúrese de agregarlo primero a la Lista de Bloqueados 428, de manera que no se pueda conectar en el futuro. Finalmente, si un dispositivo borrado es recuperado y desea permitirle que se conecte de nuevo, deberá seleccionar el dispositivo y dar clic en **Cancelar Acciones de Borrado**. También deberá eliminarlo de la Lista de Bloqueados.

Borrado de Cuenta de un Cliente ActiveSync

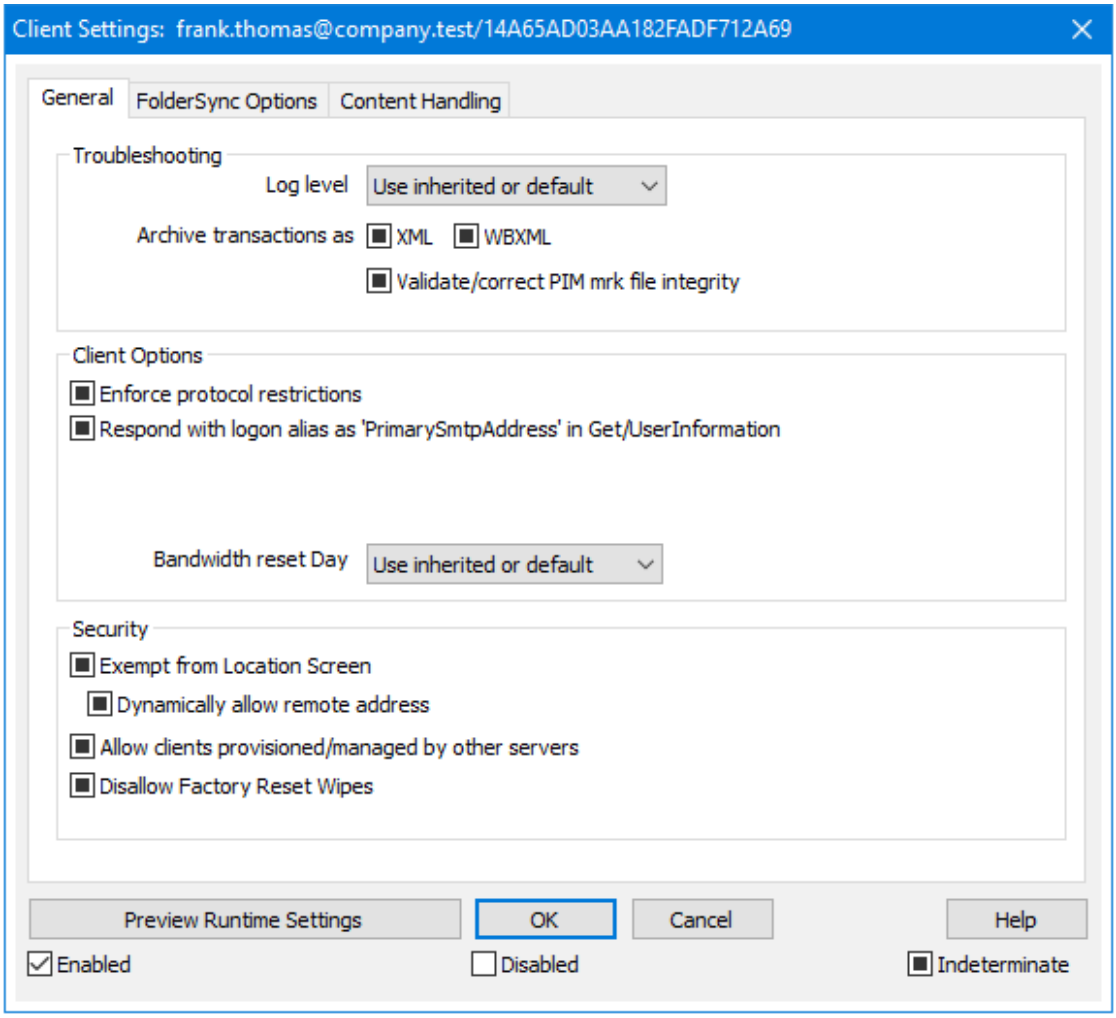
Para borrar la cuenta de correo y datos PIM de un cliente o dispositivo, dé clic derecho y clic en **Borrar Cuenta de Correo y datos PIM del Cliente.** La opción *Borrar Cuenta* es similar a la opción **Borrado Completo** explicada arriba, pero en lugar de borrar todos los datos, solo borrará los datos de la cuenta tales como correos, registros del calendario, contactos y demás. El resto, como son las apps, fotos o música quedarán intactos.

Autorizar un Cliente

Si está habilitada la opción "*Clientes nuevos requiere aprobación administrativa*" en la pantalla Ajustes de Cliente ActiveSync 421, seleccione un cliente y de clic en Aprobar cliente para sync, en este botón para autorizar su sincronización con el servidor.

Administrar los Ajustes del Cliente de un Dispositivo

La pantalla de Ajustes de Cliente a nivel dispositivo le permite administrar los ajustes para un dispositivo en particular.



Por omisión todas las opciones en esta pantalla se establecen como "Usar heredado o el de omisión", lo que significa que cada opción tomará sus ajustes de la opción correspondiente en la pantalla Ajustes de Cliente de la cuenta 451. Cualquier cambio hecho a los ajustes en esa pantalla se verá reflejado en esta pantalla. En correspondencia, cualquier cambio que realice en esta pantalla omitirá el ajuste a nivel de cuenta para este dispositivo.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk

Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo

Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation

Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa

Habilite esta opción si desea requerir que los clientes nuevos sean autorizados

por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar

esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por

omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una

dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido[834] para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

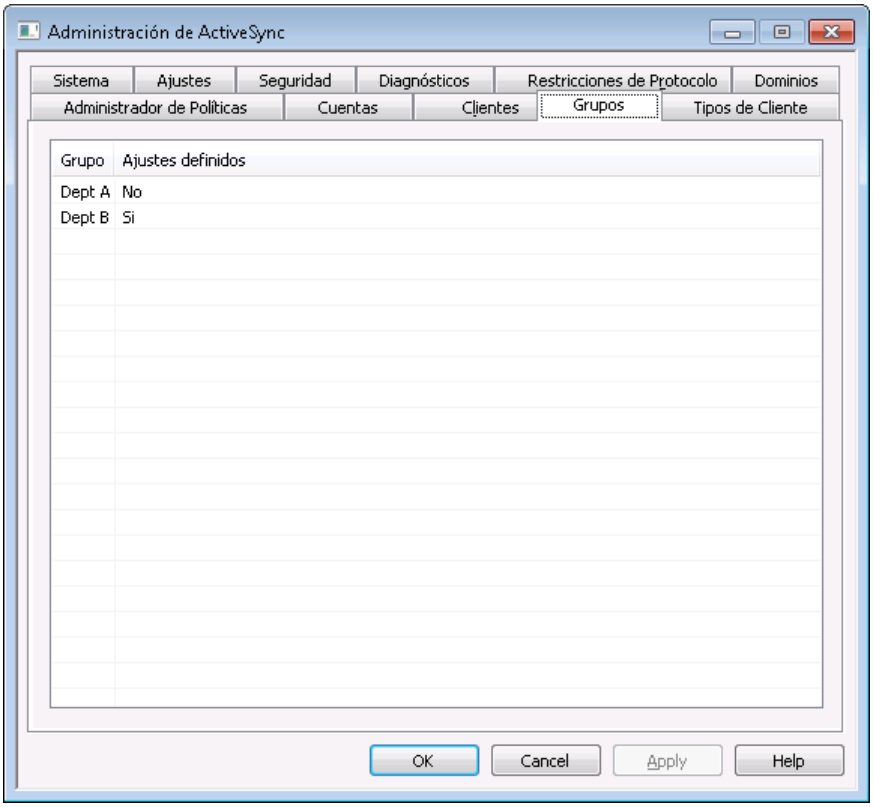
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios[434], cuentas[451] y clientes[460]). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

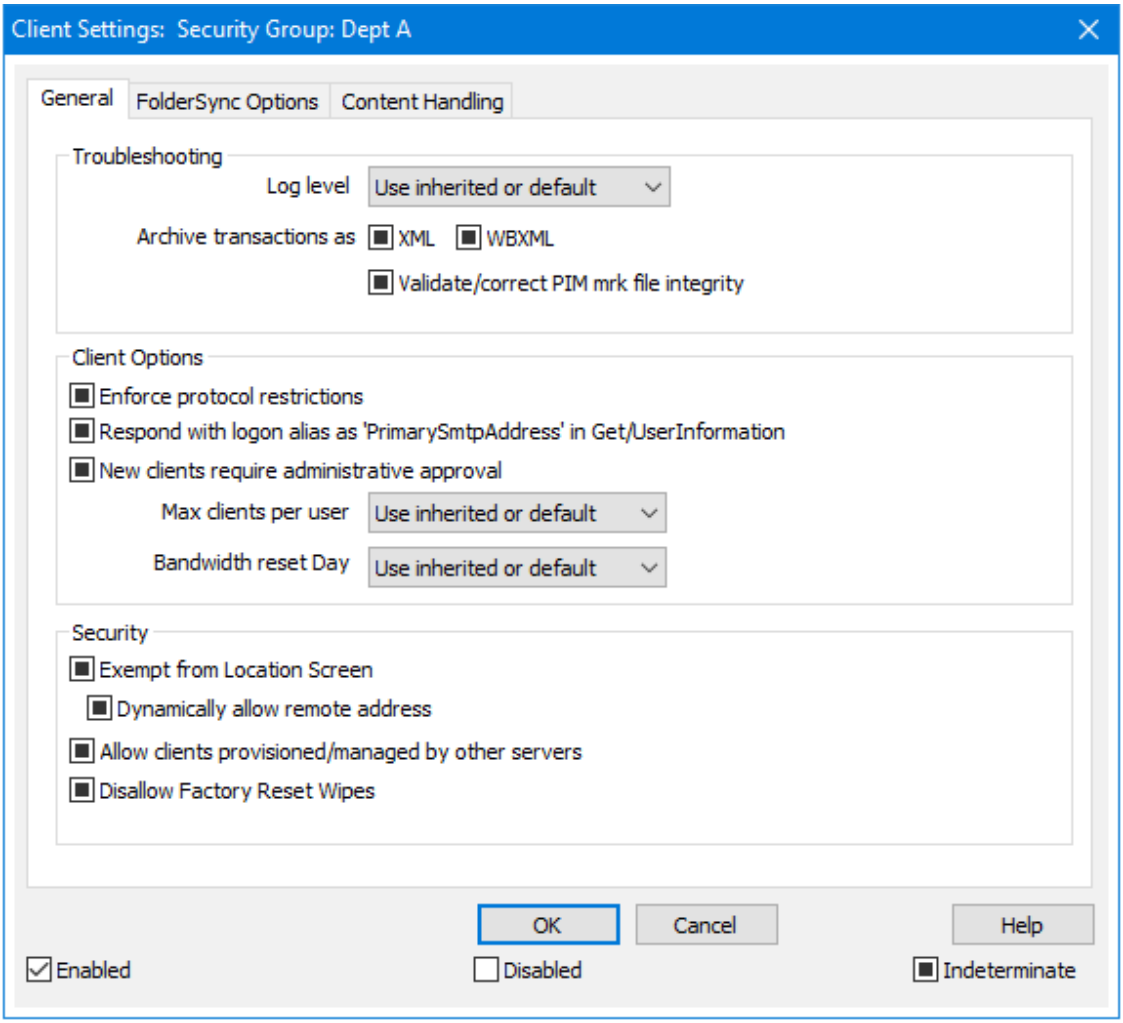
ActiveSync » Ajustes de Cliente[421]
ActiveSync » Dominios[434]
ActiveSync » Cuentas[451]

3.10.10 Grupos



Si desea asignar Ajustes de Cliente ActiveSync personalizados a un Grupo 781 de cuentas, utilice esta pantalla para administrar esos ajustes. Todos los grupos se enlistan aquí y cada registro de grupo indica si sus ajustes han sido personalizados o no. Para editar los Ajustes de Cliente de un Grupo, dé doble clic en el Grupo o clic derecho en el Grupo y luego clic en **Personalizar Ajustes de Cliente**.

Ajustes de Cliente por Grupo



Por omisión los ajustes de cliente de Grupos se configuran para heredar su estado de los Ajustes de Cliente de Dominio 223 del usuario. Si se modifica el ajuste del grupo, se anula el ajuste del dominio para cualquier cuenta que sea miembro del grupo. Si no desea que los Ajustes de Cliente del Grupo se apliquen a un miembro o dispositivo específico del grupo, entonces puede omitir los ajustes de grupo editando los Ajustes de Cliente para la Cuenta 451, Tipo de Cliente 475 o Cliente 460.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados

por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes[460] indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones[572]. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días[418] localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más

información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para

ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

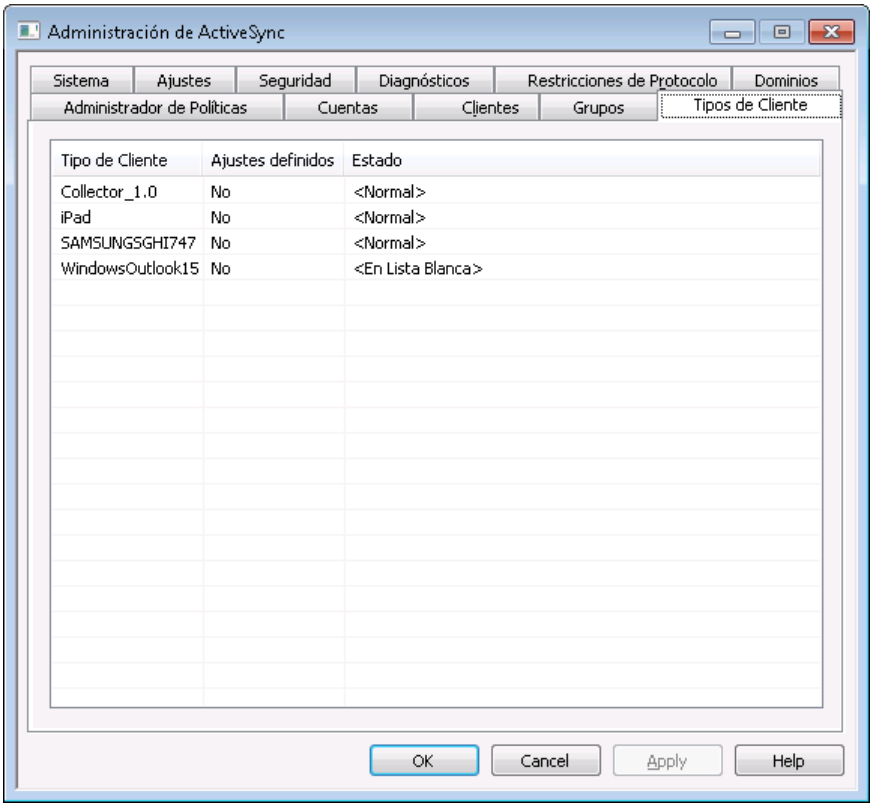
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

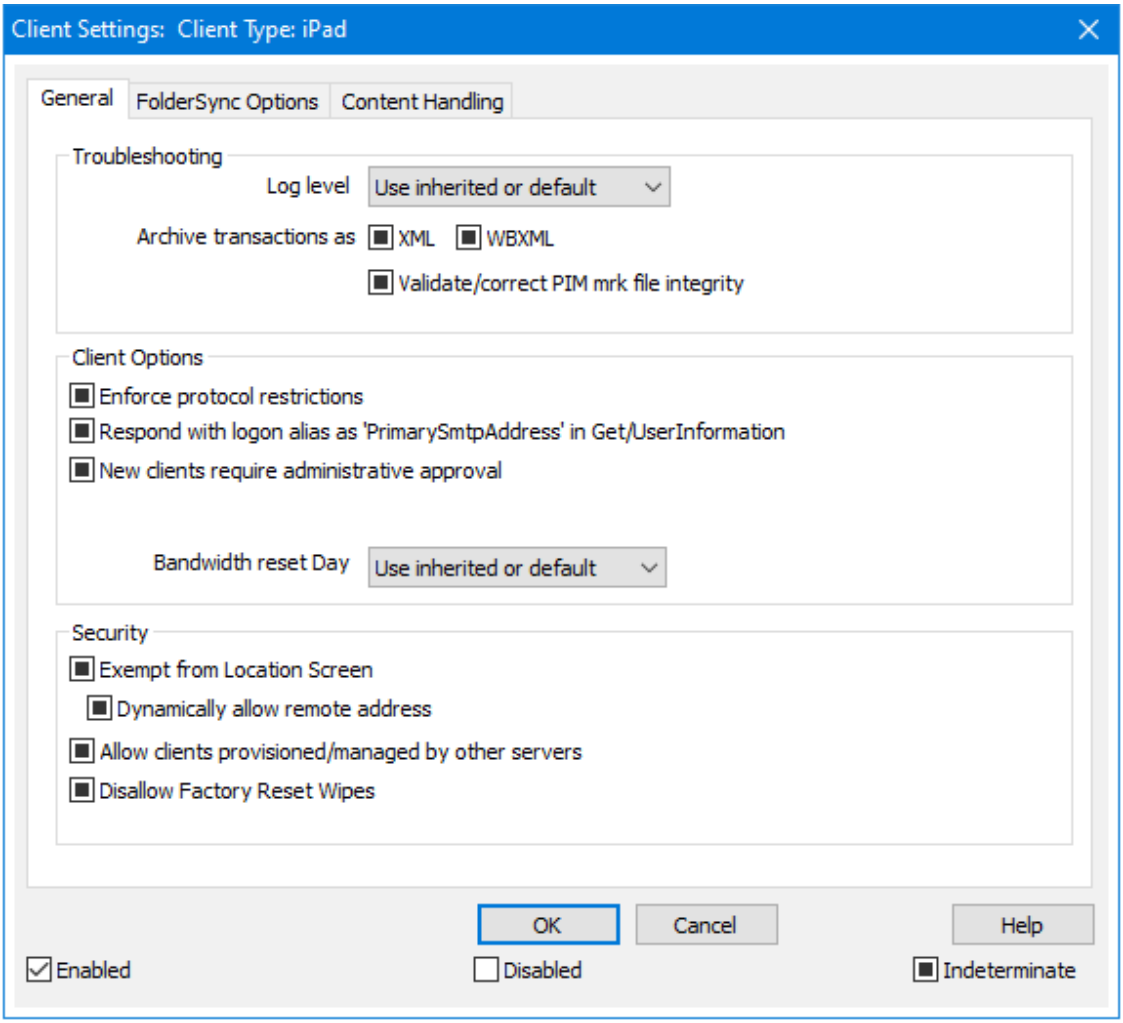
ActiveSync » Dominios 434
ActiveSync » Cuentas 451
ActiveSync » Clientes 460

3.10.11 Tipos de Cliente



Si desea asignar Ajustes de Cliente ActiveSync personalizados a un tipo específico de cliente ActiveSync, utilice esta pantalla para administrar esos ajustes. El Tipo de Cliente de todos los clientes autorizados actualmente 460 para utilizar ActiveSync están enlistados aquí y cada entrada de Tipo de Cliente indica si sus ajustes han sido personalizados o no. Para editar los Ajustes de Cliente por Tipo de Cliente dé doble clic en la entrada o clic derecho y luego clic en **Personalizar Ajustes de Cliente**. También puede dar clic derecho en una entrada para eliminar los ajustes personalizados o para agregar o eliminar un Tipo de Cliente de la Lista de Permitidos o de Exentos 428 de ActiveSync.

Ajustes de cliente por Tipo de Cliente



Por omisión cada ajuste de cliente por Tipo de Cliente se configura para heredar su estado de los Ajustes de Cliente por Cuenta 765. Si se modifica el ajuste por Tipo de Cliente, se omitirá el ajuste de cuenta para cualquier cuenta utilizando un cliente de ese tipo. Si no desea que se apliquen los ajustes de Cliente por Tipo de Cliente a un cliente específico, entonces puede omitir los ajustes editando sus Ajustes de Cliente 460.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados

por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes[460] indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones[572]. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días[418] localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más

información, vea: **Borrar por Completo un Cliente ActiveSync**[460] en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas[314] a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas[314] a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta[316] para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas[314] padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido 834 para

ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

Vista Previa de Ajustes Efectivos

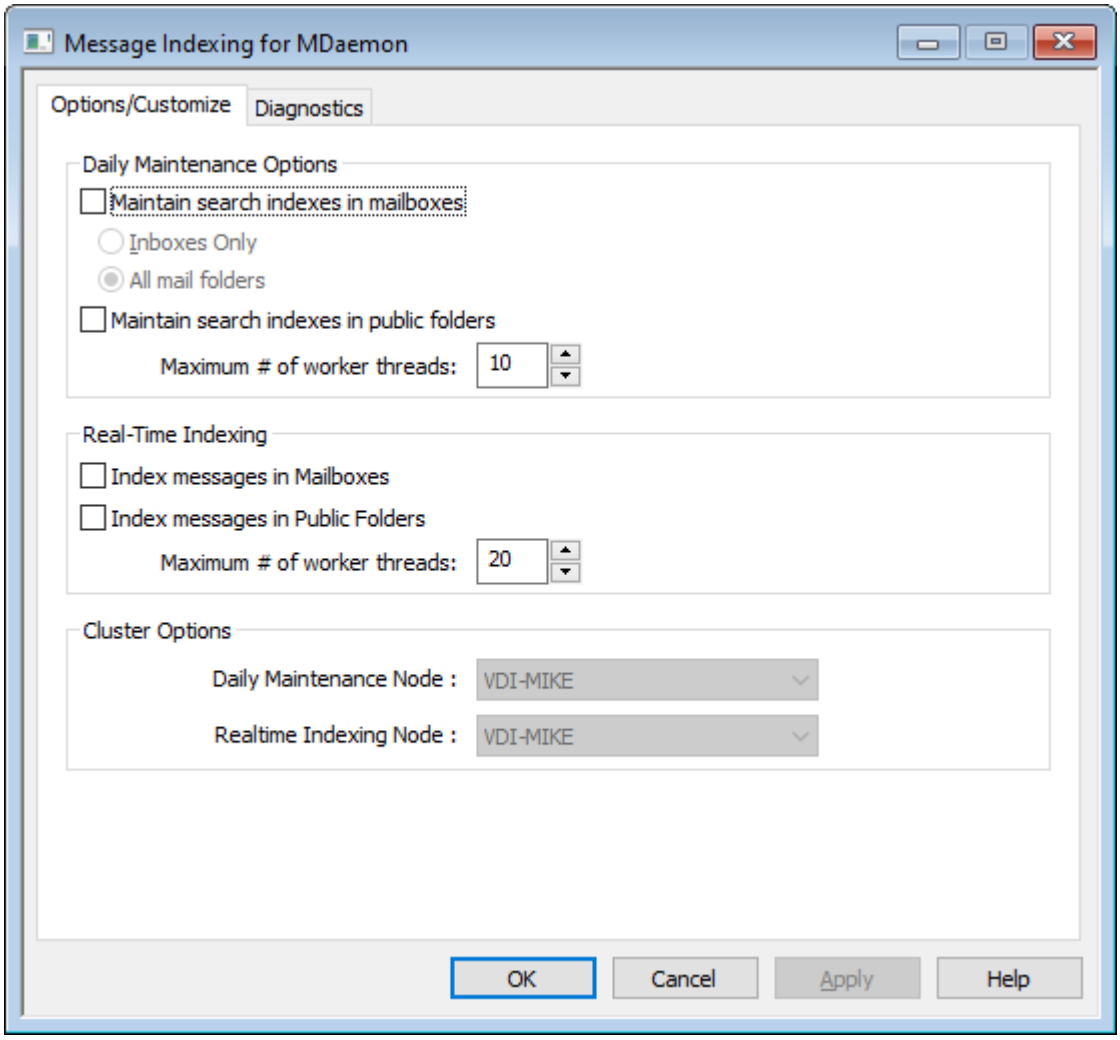
Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Cuentas 451
ActiveSync » Clientes 460
ActiveSync » Seguridad 428

3.11 Indexación de Mensajes

3.11.1 Opciones/Personalizar



El diálogo de Indexación de Mensajes es utilizado para la configuración de mantenimiento en tiempo real y nocturno para los índices de consultas utilizados por Webmail, ActiveSync y Administración Remota.

Opciones de Mantenimiento Diario

Las opciones en esta sección administran la Indexación nocturna de búsquedas.

Índices principales de búsquedas en buzones
Marque esta casilla si desea mantener los índices de búsqueda en sus carpetas de correo. Puede elegir hacer esto ya sea para la Bandeja de entrada o para todas las carpetas de correo.

Mantener índices de búsqueda en carpetas públicas
Habilite esta opción si desea mantener los índices de búsqueda en sus carpetas públicas 314. También puede especificar un número máximo de hilos que se permitirá operar en esto simultáneamente.

Indexación en Tiempo Real

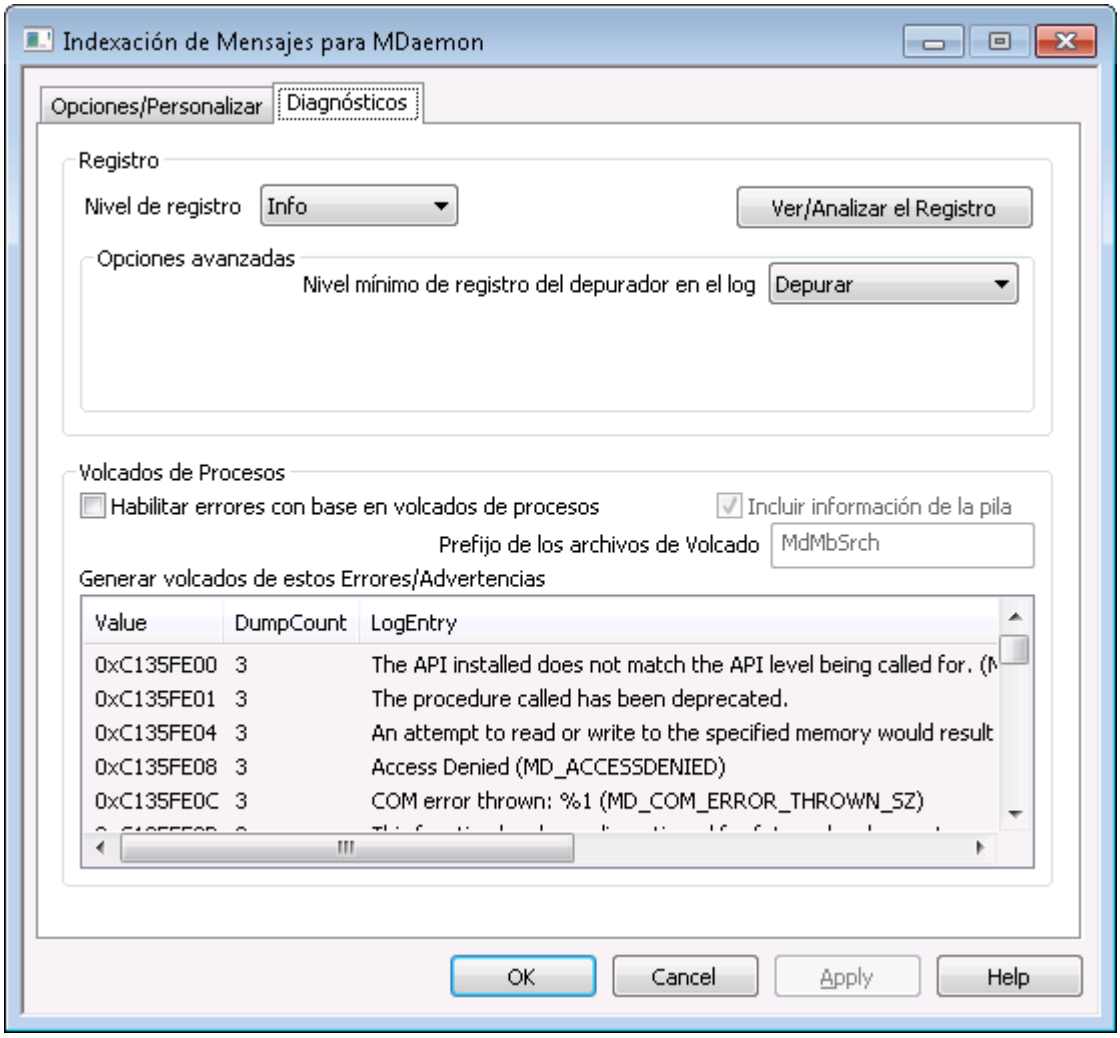
Indexar mensajes en Buzones
Habilite esta opción si desea ejecutar la Indexación de búsquedas en tiempo real sobre Buzones de manera que los índices de consulta estén actualizados.

Indexar mensajes en Carpetas Públicas
Marque esta casilla si desea realizar Indexación en tiempo real de las Carpetas Públicas 314.

Opciones de Clúster

Si utiliza el servicio de Clúster, utilice las opciones en esta sección para asignar los nodos del clúster que estarán dedicados al mantenimiento diario de indexado y a la Indexación en tiempo real.

3.11.2 Diagnósticos



Esta pantalla contiene opciones avanzadas que en la mayoría de los casos no necesitas utilizarse a menos que usted intente diagnosticar un problema con Indexación de Mensajes o se lo indique Soporte técnico.

Registro

Nivel de Registro
Se soportan seis niveles de registro dependiendo de la más alta a más baja cantidad de datos registrados:

Depurar Es el nivel de registro más detallado. Incluye todas las entradas disponibles y típicamente solo se utiliza al diagnosticar un problema o cuando el administrador requiere información detallada.

Info Registro Moderado. Incluye operaciones generales sin detalle. Es el nivel de registro por omisión.

Advertencia Incluye advertencias, errores, errores críticos y eventos de inicio/cierre de la aplicación.

Error Se registran errores, errores críticos y eventos de inicio/cierre de la aplicación.

Críticos Se incluyen errores críticos y eventos de inicio/cierre de la aplicación.

Ninguno Solo se registran eventos de inicio/cierre de la aplicación.

Ver/Analizar el Registro
Dé clic en este botón para abrir el Sistema de Visor Avanzado de Registros de MDaemon. Por omisión, los registros se almacenan en: "..\MDaemon\Logs\"

Opciones Avanzadas

Mínimo nivel de registro para depuración
Este es el nivel mínimo de registro a emitir para depuración. Los niveles de registro disponibles son los mismos descritos arriba.

Volcados de Proceso

Habilitar volcados de procesos con base en errores
Habilite esta opción si desea generar volcados de proceso siempre que ocurran advertencias o errores específicos que usted determine abajo.

Incluir información de la pila en los volcados
Por omisión, se incluye información de la pila en los volcados de procesos. Deshabilite esta casilla si no desea que se incluya esta información.

Prefijo para los archivos de volcado
Los nombres de archivos de volados de procesos inician con este texto.

Errores/Advertencias para genera volcados
Dé clic derecho en esta área y utilice las opciones *Agregar/Editar/Eliminar Registro...* para administrar la lista de errores o advertencias que detonarán volcados de procesos. Por cada entrada puede definir el número de volcados de proceso permitidos antes de que se desactive.

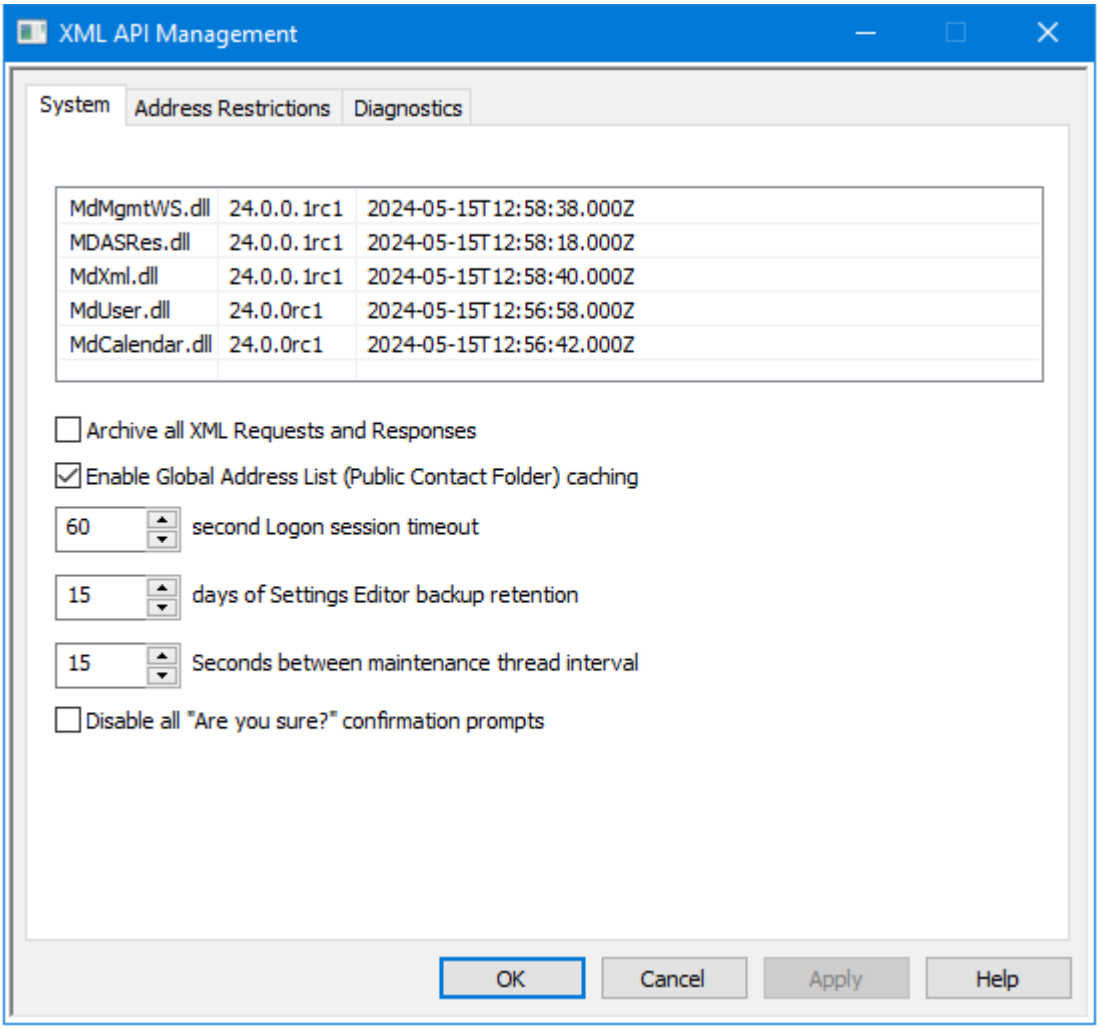
Ver:

Monitoreo Dinámico » Opciones/Personalizar 610

3.12 XML API Service

Este diálogo contiene varios ajustes de administración para el servicio de la API XML de MDaemon. Para más información sobre la librería de la API de MDaemon e integrar sus aplicaciones personalizadas con MDaemon vea: **MD-API.html** (ubicado en la carpeta `\..\MDaemon\Docs\API`).

Sistema



Archivar todas las peticiones y respuestas XML
Habilite esta opción si desea grabar todas las peticiones y respuestas XML de manera que pueda diagnosticar posibles problemas que pudieran surgir.

Habilitar caché de la Lista Global de Direcciones (Carpeta Pública de Contactos)
Utilice esta opción si desea permitir que la API mantenga en caché la Lista Global de Direcciones (carpetas públicas de contactos) para dominios, a fin de mejorar el rendimiento. Esta opción está habilitada por omisión.

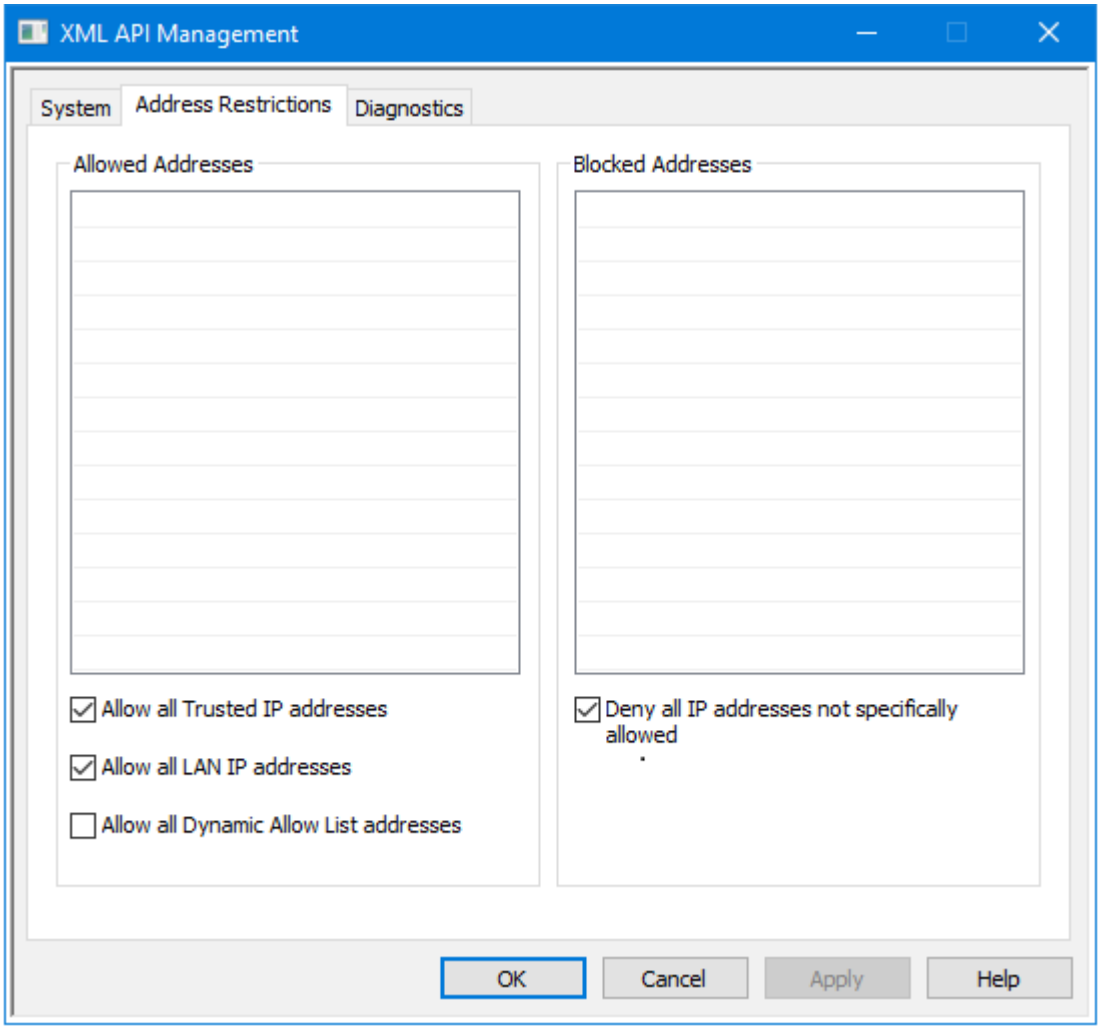
[xx] segundos de tiempo de espera para una sesión
Esta opción determina el número de segundos antes de que un token de inicio de sesión de la API expire si no es utilizado.

[xx] días de retención de respaldo de los Ajustes del Editor
Esta opción determina el número de días para retener respaldos de los archivos Editor/INIfile y Editor/HiWater, de manera que los cambios se puedan deshacer o revertir vía la acción 'recuperar'.

[xx] Segundos entre el intervalo del hilo de mantenimiento
Este es el número de segundos que el hilo de mantenimiento duerme antes de verificar si hay nuevas tareas de mantenimiento como limpiar directorios y archivos antiguos.

Deshabilitar todas las peticiones de confirmación "¿Está seguro?"
Marque esta casilla si desea deshabilitar todas las peticiones de confirmación 'Está seguro?' para agilizar las acciones de la IU.

Restricciones de Direcciones



Direcciones Permitidas

Dé clic derecho para agregar una dirección/máscara IP a la lista de direcciones permitidas. Estas direcciones tienen permiso para conectarse a la API.

Permitir todas las direcciones IP Confiables
Marque esta casilla si desea permitir que todas las Direcciones Ip Confiables 520 se conecten a la API.

Permitir todas las direcciones IP de la LAN
Marque esta casilla si desea permitir que se conecten a la API todas las direcciones IP de la LAN 608.

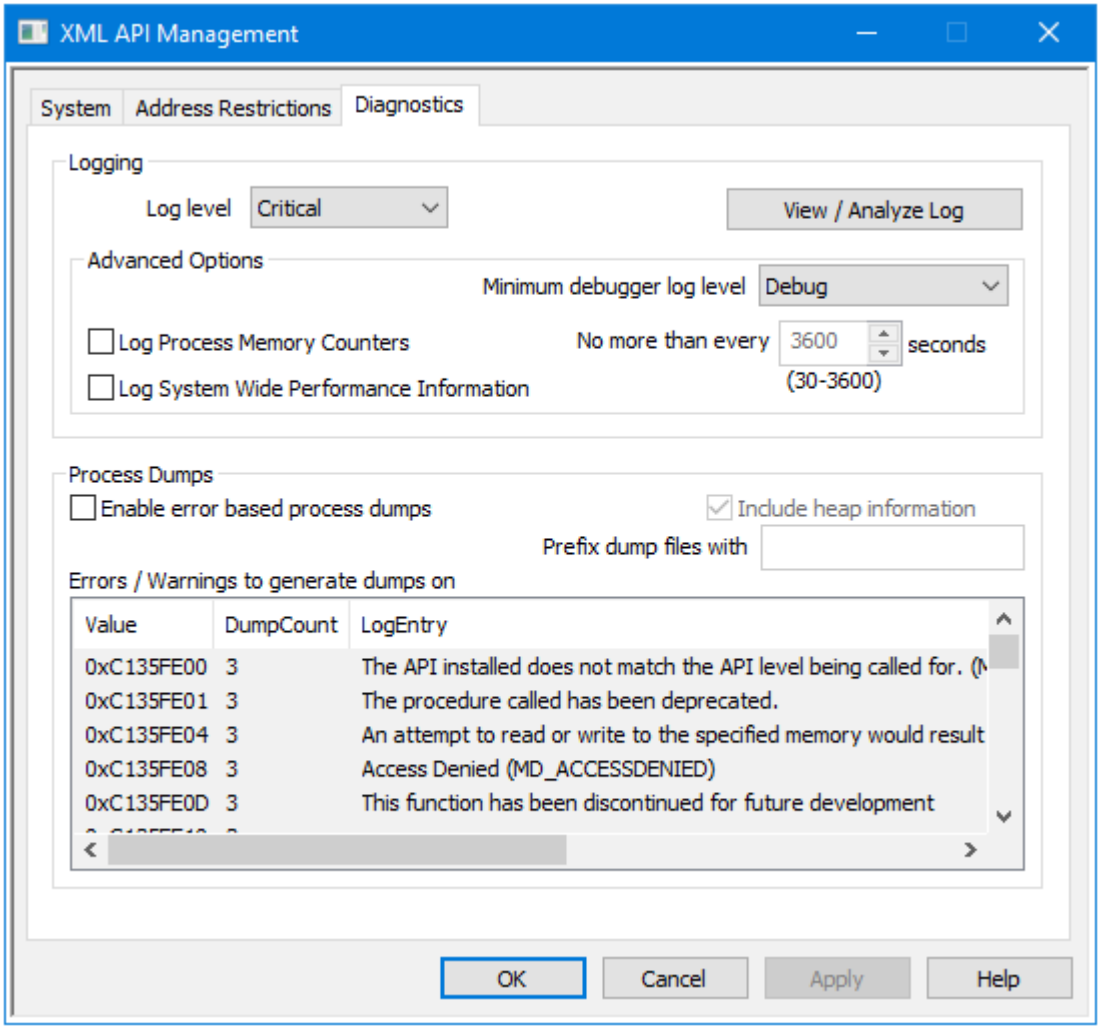
Permitir todas las direcciones de la Lista Dinámica de Permitidas
Utilice esta opción si desea permitir que se conecten a la API todas las direcciones Permitidas Dinámicamente 624.

Direcciones Bloqueadas

Dé clic derecho para agregar o modificar direcciones IP en esta lista. Estas direcciones IP no pueden conectarse a la API.

Denegar acceso a todas las direcciones IP que no están permitidas específicamente
Cuando se marca esta casilla, las únicas direcciones IP que se pueden conectar a la API son las permitidas específicamente vía los ajustes de Direcciones Permitidas.

Diagnósticos



Logging

Nivel de Registro
Se soportan seis niveles de registro dependiendo de la más alta a más baja cantidad de datos registrados:

Depurar Es el nivel de registro más detallado. Incluye todas las entradas disponibles y típicamente solo se utiliza al diagnosticar un problema o cuando el administrador requiere información detallada.

Info Registro Moderado. Incluye operaciones generales sin detalle. Es el nivel de registro por omisión.

Advertencia Incluye advertencias, errores, errores críticos y eventos de inicio/cierre de la aplicación.

Error Se registran errores, errores críticos y eventos de inicio/cierre de la aplicación.

Críticos Se incluyen errores críticos y eventos de inicio/cierre de la aplicación.

Ninguno Solo se registran eventos de inicio/cierre de la aplicación.

Ver/Analizar el Registro
Dé clic en este botón para abrir el Sistema de Visor Avanzado de Registros de MDaemon. Por omisión, los registros se almacenan en: "..\MDaemon\Logs\"

Opciones Avanzadas

Nivel mínimo de registros para el depurador
Este es el nivel mínimo de registros a emitir al depurador. Los niveles disponibles de registro son los mismos descritos previamente.

Registrar contadores de procesamiento de memoria
Marque esta casilla para incluir en el archivo de registro información específica de procesos de Memoria, Identificadores e Hilos. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos. Las entradas al registro solo se emiten si los datos se han modificado desde la última vez que se registraron.

Registrar información del desempeño general del sistema
Marque esta casilla si desea incluir en el registro información del desempeño general del sistema. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos.

No más de cada [xx] segundos
Utilice esta opción para establecer el límite de la frecuencia con que se registrará la información de procesos y desempeño.

Volcados de Proceso

Habilitar volcados de procesos con base en errores
Habilite esta opción si desea generar volcados de proceso siempre que ocurran advertencias o errores específicos que usted determine abajo.

Incluir información de la pila en los volcados
Por omisión, se incluye información de la pila en los volcados de procesos. Deshabilite esta casilla si no desea que se incluya esta información.

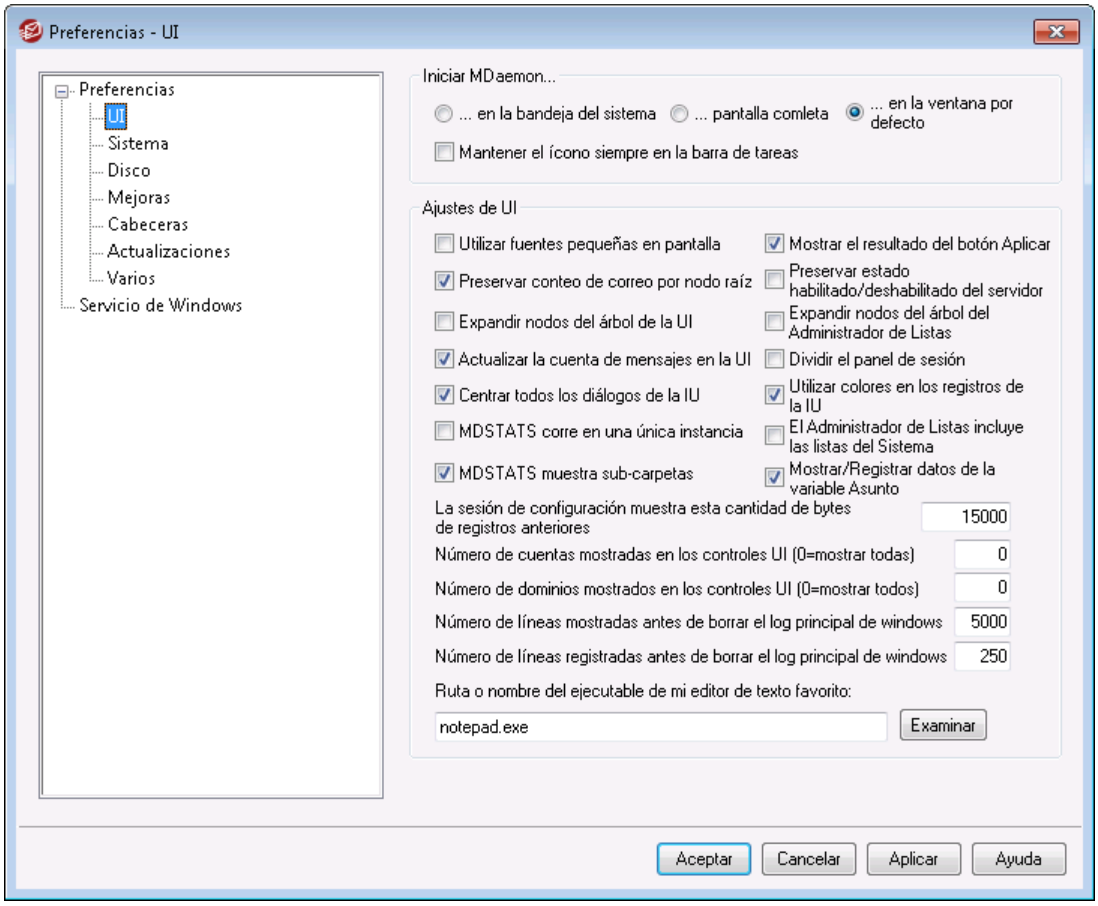
Prefijo para los archivos de volcado
Los nombres de archivos de volados de procesos inician con este texto.

Errores/Advertencias para genera volcados
Dé clic derecho en esta área y utilice las opciones *Agregar/Editar/Eliminar Registro...* para administrar la lista de errores o advertencias que detonarán volcados de procesos. Por cada entrada puede definir el número de volcados de proceso permitidos antes de que se desactive.

3.13 Preferencias

3.13.1 Preferencias

3.13.1.1 UI



Iniciar MDaemon...

...en la bandeja del sistema
Escoja esta opción si no desea mostrar la interfaz de MDaemon al inicio. El icono de MDaemon seguirá apareciendo en la bandeja de sistema.

...pantalla completa
Escoja esta opción si desea que la interfaz de MDaemon se maximice al inicio.

...en la ventana por defecto
Escoja esta opción si desea que la interfaz de MDaemon aparezca en la ventana por defecto al inicio.

Mantener siempre el ícono en la barra de tareas
Cuando se habilita esta opción, MDaemon empezará minimizado a la barra de tareas, y luego aparecerá tanto en la barra de tareas como en la bandeja de sistema cuando esté minimizado. Despeje esta casilla si no quiere que MDaemon aparezca en la barra de tareas de Windows cuando se minimice; sólo el icono de sistema estará visible.

Ajustes de UI

Usar fuente pequeña en las pantallas
Habilita las fuentes pequeñas en las ventanas de Sesión y Registro de Eventos.

Mostrar resultados del botón Aplicar
Por omisión, siempre que se dé clic en el botón Aplicar en alguna pantalla, se presentará un mensaje confirmando que los cambios que realizó han sido guardados. Deshabilite esta opción si desea aplicar los cambios sin que se despliegue el mensaje.

Preservar los contadores de nodos raíz
Active esta opción si desea guardar los contadores de nodos raíz en los reinicios. Los contadores de nodos raíz se listan en la sección "Estadísticas" del panel de Estados en la interfaz UI de MDaemon.

Preservar el estado del servidor habilitado/deshabilitado en los reinicios
Si se habilita este control, MDaemon se asegurará que el estado de sus servidores (habilitado o deshabilitado) permanece igual después del reinicio.

Expandir los nodos del árbol en la UI
Dé clic en esta caja si desea que los nodos de árbol de navegación en el panel de la izquierda se expandan automáticamente. Esto no aplica al Administrador de Listas de Distribución. 274 Si desea expandir en automático los nodos de árbol de las listas de distribución, utilice la opción siguiente *Expandir los nodos de árbol de las Listas de Distribución*.

Expandir los nodos de árbol de las Listas de Distribución
Dé clic en esta casilla si desea que los nodos de árbol de navegación del Administrador de Listas de Distribución 274 en el panel izquierdo se expandan automáticamente.

Actualizar la UI con los conteos de mensajes
Esta opción controla si MDaemon comprobará o no el disco para contar los mensajes en las colas de mensajes.

Dividir el panel de sesión
Habilite esta opción si desea que la pestaña de Sesiones en la UI se divida de las otras pestañas a su propio panel. Para modificar este ajuste se requiere reiniciar la UI de MDaemon y la opción en el menú para cambiar paneles ya no estará disponible.

Centrar todo el diálogo en la UI
Por omisión todos los diálogos se centran en la pantalla cuando se abren, en lugar de traslaparlos. Deshabilite esta casilla si desea que los diálogos se traslapen , esto ocasionalmente puede hacer que se salgan parcialmente de la pantalla o queden fuera del marco.

Utilizar colores en los logs de la UI
Habilite esta opción si desea que se muestre en colores el texto desplegado en las pestañas Rastreo de Eventos y Registro 81 en la interface de usuario de MDaemon. Esta opción se encuentra habilitada por omisión y para modificarla se requiere reiniciar MDaemon antes de que el cambio tenga efecto. Ver: Registro de Sesiones a colores 189 para más información.

El Administrador de Listas incluye Listas del Sistema
Habilite esta opción si desea desplegar las listas de sistema generadas por MDaemon (ej. Everyone@ y MasterEveryone@) en el Administrador de Listas de Distribución 274. Las listas generadas por el sistema cuentan con elementos limitados para configuración por el usuario. Cuando esta opción está deshabilitada, las listas del sistema estarán ocultas pero disponibles para su uso. Esta opción está deshabilitada por omisión.

MDSTATS se ejecuta en una única instancia.

Haga clic en esta casilla si no quiere que más de una copia del Administrador de cola y estadística 883 de MDaemon corra a la vez. Si se intenta ejecutar el Administrador cuando ya se está corriendo simplemente hará que la instancia que se esté ejecutando actualmente se convierta en la ventana activa

MDSTATS muestra subcarpetas
Haga clic en esta casilla si quiere que el Administrador de colas y estadística 883 muestre las subcarpetas contenidas en diversas colas y carpetas de correo de usuario.

Mostrar/Registrar datos del Asunto
Por omisión la línea Asunto: se muestra en las pestañas de la UI de MDaemon y se escribe en los archivos de registro. Note, sin embargo que la línea Asunto: puede contener información que el remitente del mensaje preferiría no se desplegara y no le agradaría que fuera rastreada en los archivos de registro y las listas de distribución pueden tener una contraseña que los usuarios coloquen en la línea Asunto:. Por esto se recomienda deshabilitar esta opción.

La sesión de Configuración muestra este número de bytes de registros previos
Al correr una sesión de configuración, este es el número máximo de cantidad de datos en bitácora que se desplegarán en las pestañas Rastreo de Eventos y Registro 81. El parámetro por omisión es 15,000 bytes.

Número de cuentas mostradas en los controles de la UI (0=mostrar todos)
Este es el número máximo de cuentas que se mostrarán en las listas desplegables de varios diálogos. Además, cuando el valor en esta opción se establezca menor al número de cuentas que existan actualmente, las opciones "Editar Cuenta" y "Eliminar Cuenta" ya no aparecerán en el menú de Cuentas; sólo podrá editar y borrar cuentas utilizando el Administrador de Cuentas 712. Debe reiniciar MDaemon antes de que tome efecto cualquier cambio en esta opción. El valor por omisión es "0" lo que hace que se muestren todas las cuentas.

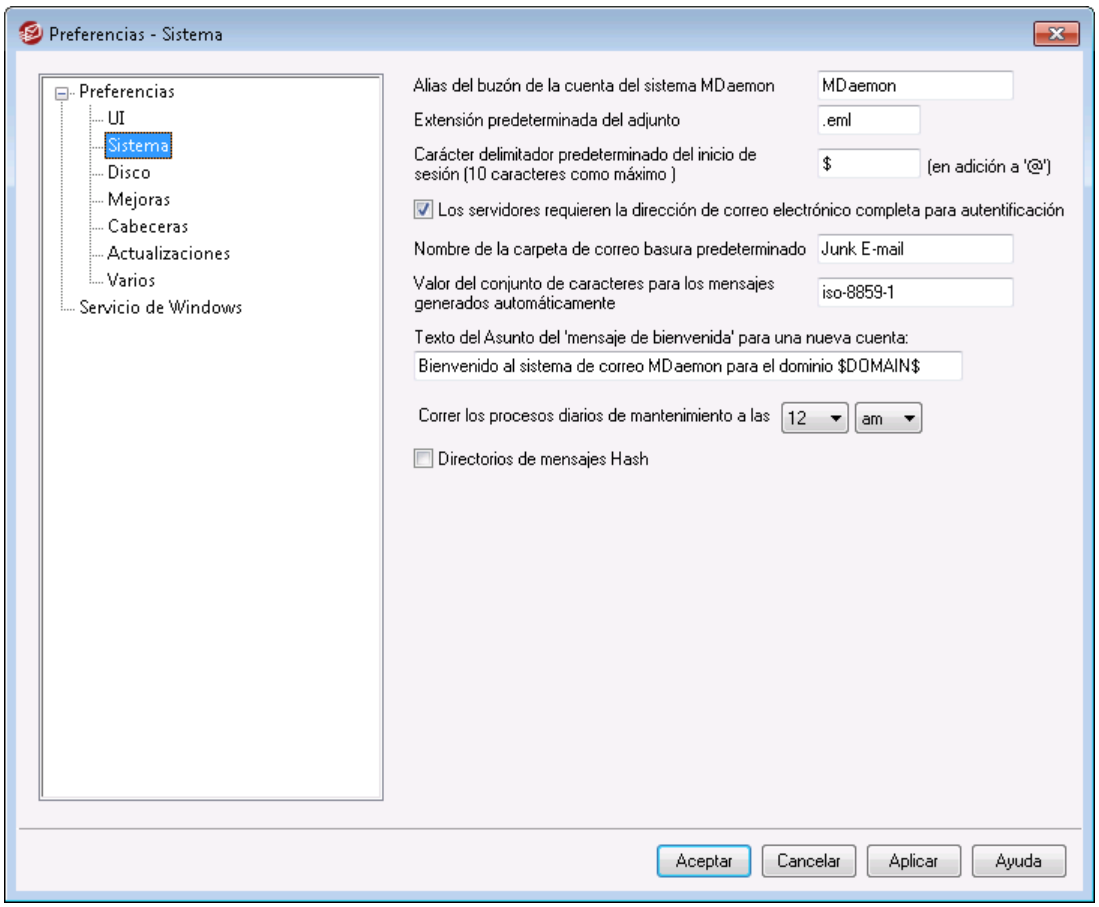
Número de dominios mostrados en los controles de la UI (0=mostrar todos)
Este es el número máximo de Dominios que se mostrarán en la GUI principal, independientemente de cuantos dominios existan actualmente. Después de cambiar este valor debe reiniciar MDaemon antes de que los cambios se hagan visibles. El valor por omisión es "0" lo que hace que se muestren todos los dominios.

Número de líneas mostradas antes de borrar el log principal de Windows
Este es el número máximo de líneas que se mostrarán en la ventana de registro de la interfaz principal. Cuando este número de líneas se alcance la ventana se limpiará. Esto no afecta al archivo de registro; sólo se limpiará la visualización.

Número de líneas registradas antes de borrar el log principal de Windows
Este es el máximo número de líneas que aparecerán en cada Ventana de Sesión[95] antes de que se limpie. Esto no afecta al archivo de registro.

Ruta o nombre del ejecutable de mi editor de texto favorito
Notepad.exe es el editor de texto que utilizará la UI de MDaemon por omisión cuando sea necesario. Si prefiere utilizar un editor distinto, registre aquí su ruta o nombre del ejecutable.

3.13.1.2 Sistema



Alias del buzón de la cuenta del sistema de MDaemon [dirección]
Esta es la dirección de correo desde la que vendrán los mensajes generados de sistema. Las confirmaciones de suscripción, mensajes de notificación de estatus de envío (DSN), otros mensajes varios de notificación, y demás mensajes de sistema.

Extensión predeterminada de adjuntos
Los mensajes generados por el sistema se crearán usando esta extensión. Esta también será la extensión asignada a los adjuntos incluidos con mensajes generados de sistema. Por ejemplo, si MDaemon genera un mensaje de

advertencia al postmaster sobre un mensaje específico, adjuntará dicho mensaje con este valor como extensión de archivo.

Carácter delimitador predeterminado del inicio de sesión (10 caracteres máximo)
Cuando se usa una dirección de correo como parámetro de acceso de cuenta, este carácter o cadena de caracteres se puede usar como alternativa a "@". Esto puede ser necesario para algunos usuarios que tienen clientes de correo que no soportan el carácter "@" en el campo de usuario. Por ejemplo, si utiliza "$" en este campo entonces los usuarios pueden acceder utilizando "usuario1@ejemplo.com" o "usuario1$dominio.com".

Los Servidores requieren la dirección de correo completa para autenticación
Los Servidores POP y IMAP de MDaemon requieren por omisión que se utilice la dirección de completa de correo para iniciar sesión en MDaemon. Si desea permitir el inicio de sesión solo con el nombre del usuario (i.e. "usuario1" en lugar de "usuario1@ejemplo.com") entonces puede deshabilitar esta opción, pero no se recomienda ya que se pueden generar situaciones ambiguas cuando MDaemon da servicio a múltiples dominios.

Nombre predeterminado de la carpeta de correo basura
Use este campo para especificar el nombre por defecto para la carpeta de Spam que MDaemon puede crear de manera automática para sus usuarios. El nombre por defecto es "Junk E-mail" para ajustarse al valor por defecto de gran variedad de otros productos distribuidos.

Nombre predeterminado de la carpeta de correo basura
Use este campo para especificar el nombre por defecto para la carpeta de Spam que MDaemon puede crear de manera automática para sus usuarios. El nombre por defecto es "Junk E-mail" para ajustarse al valor por defecto de gran variedad de otros productos distribuidos.

Valor del conjunto de caracteres para los mensajes generados automáticamente
Especifique el conjunto de caracteres que desea que se utilice para los mensajes autogenerado. La configuración por defecto es iso-8859-1.

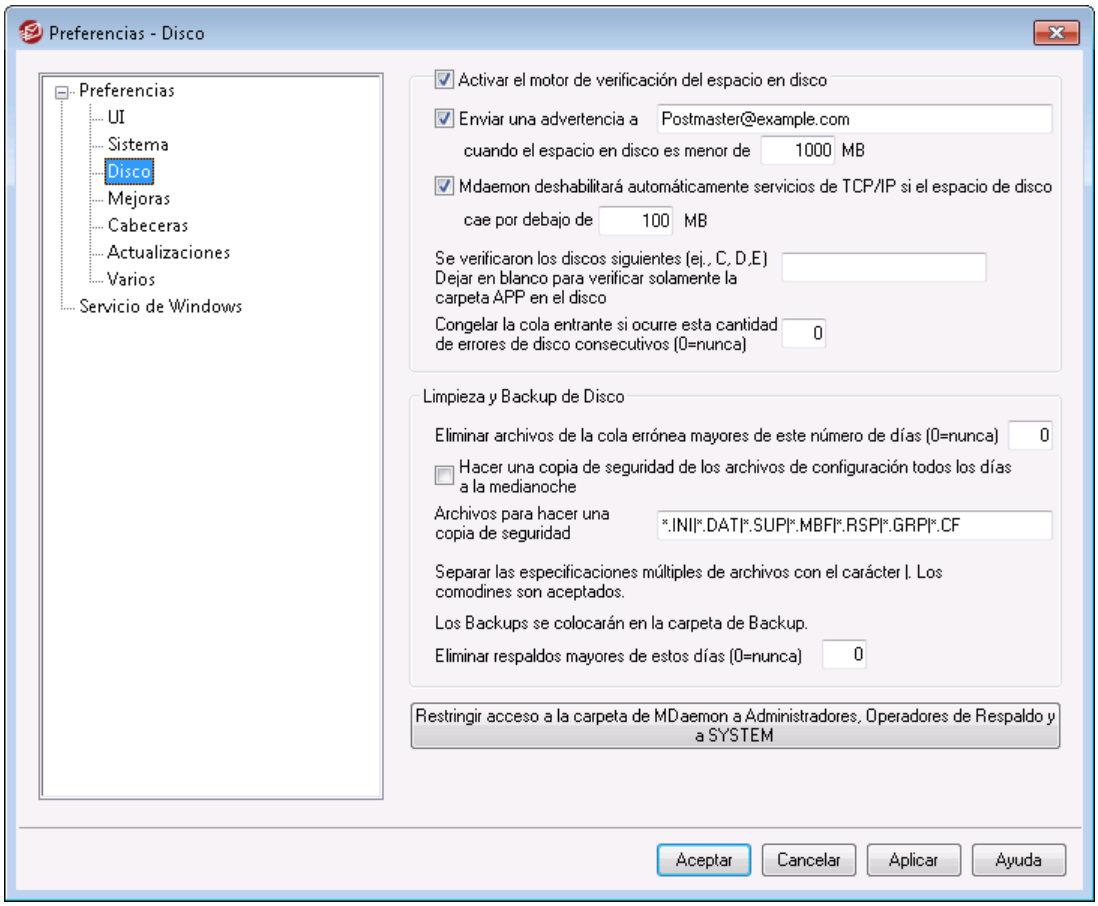
Texto del Asunto del 'mensaje de bienvenida' para una cuenta nueva:
MDaemon típicamente envía un "mensaje de bienvenida" a las cuentas nuevas. El texto aquí especificado aparecerá como "Asunto" del mensaje. El mensaje de bienvenida se construye a partir del archivo `NEWUSERHELP.DAT` ubicado en la carpeta `…\MDaemon\app\` y este encabezado de asunto puede contener cualquier macro permitida en los scripts de autorespuesta 843.

Ejecutar diariamente los procesos de mantenimiento y limpieza a las [1-12] [am/pm]
Utilice esta opción para determinar la hora en la que se realizarán los procesos diarios de mantenimiento y limpieza. El valor recomendado y por omisión es las 12am.

Sin importar la hora que configure en esta opción, existen algunos eventos diarios que ocurrirán siempre a la medianoche, tal como el mantenimiento de archivos de registro y la ejecución del archivo `midnight.bat`.

Directorios de mensajes Hash
Haga clic en esta casilla si desea habilitar el hash de directorios — MDaemon realizará un hash de algunos directorios creando hasta 65 subdirectorios. El hashing puede incrementar el rendimiento para algunos sitios de alto volumen, pero puede disminuirlo para los sitios de MDaemon habituales. Por defecto esta opción se encuentra deshabilitada.

3.13.1.3 Disco



Activar el motor de verificación del espacio en disco
Active esta casilla si desea que MDaemon monitoree la cantidad de espacio en disco disponible en la unidad donde se ubica `MDaemon.exe`.

Enviar una advertencia a [usuario o dirección] cuando el espacio de disco cae por debajo de [xx] MB
Usando esta opción puede configurar MDaemon para que envíe un mensaje de notificación al usuario o dirección de su elección cuando el espacio en disco caiga por debajo de un cierto nivel. El valor por omisión es 1000 MB.

MDaemon deshabilitará automáticamente servicios de TCP/IP si el espacio en disco cae por debajo de [xx] MB
Active esta funcionalidad si quiere que MDaemon deshabilite los servicios TCP/IP si el espacio libre en disco cae por debajo de cierto nivel. El valor por omisión es 100 MB.

Verificar los discos siguientes (ej.: C, D, E)
Utilice esta opción si desea que se monitoree el espacio en múltiples discos, especificando la unidad correspondiente a cada uno. Si deja este campo en blanco entonces solamente se verificará el disco que contiene la carpeta de MDaemon \app\folder.

Congelar la cola de entrada si ocurren este número de errores de disco consecutivos (0=nunca)
Si este número de errores de disco ocurre durante el procesamiento de la cola de entrada, MDaemon detendrá el procesamiento de la cola hasta que se resuelva la situación. Se enviará un correo al buzón del Postmaster cuando se detenga el procesamiento.

Mantenimiento y Respaldo de Disco

Eliminar los mensajes en la cola de erróneos mayores de este número de días (0=nunca)
Utilice esta opción si desea que MDaemon elimine los archivos viejos en la cola de mensajes erróneo siempre que sean mayores del número especificado de días. Si no desea eliminar esos mensajes automáticamente, utilice "0" en esta opción.

Hacer una copia de seguridad de los archivos de configuración todos los días a la medianoche
Haga clic en esta casilla si quiere que se respalden todos los archivos de configuración de MDaemon cada noche a medianoche en el directorio de Backups.

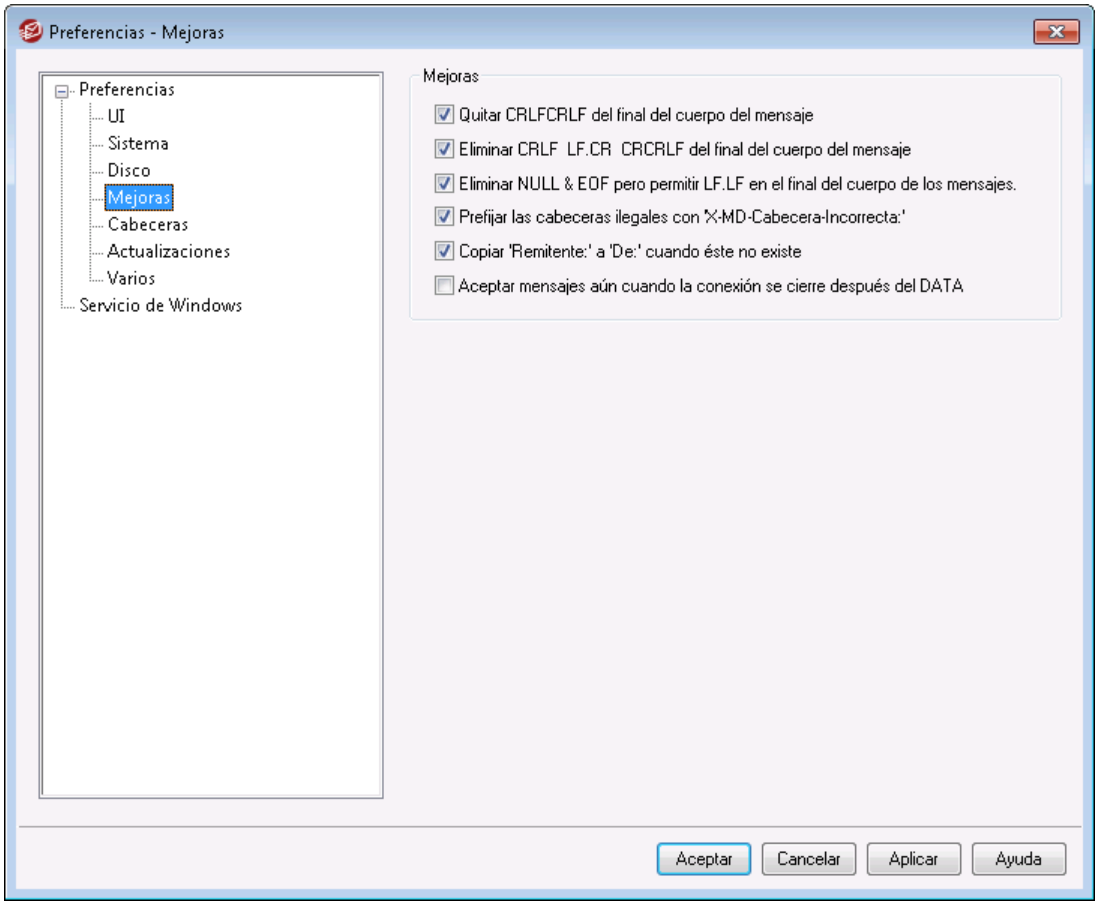
Archivos por respaldar
Use este cuadro de texto para especificar exactamente qué archivos y extensiones de archivo guardar. Los comodines están permitidos y cada nombre de archivo o extensión debe separarse por el carácter "|".

Eliminar respaldos mayores de este número de días (0=nunca)
Utilice esta opción si desea eliminar automáticamente los archivos de respaldo antiguos. Los archivos mayores del número especificado de días serán eliminados como parte del proceso nocturno de mantenimiento diario. El parámetro por omisión es "0", lo que significa que los archivos de respaldo antiguos no serán eliminados.

Restringir el acceso a carpetas de MDaemon a los grupos de Administradores, Operadores de Respaldo y SYSTEM

Dé Clic en este botón para restringir el acceso a la carpeta raíz \MDaemon\ y sus subcarpetas a las siguientes cuentas/grupos de Windows: Administradores, Operadores de Respaldo y SYSTEM.

3.13.1.4 Mejoras



Quitar CRLFCRLF del final del cuerpo del mensaje
Ciertos clientes de correo tienen problemas para mostrar mensajes que acaben con retornos de carro de línea consecutivos (p. ej. CRLFCRLF). Cuando se habilita esta casilla, MDaemon quitará las secuencias `CRLFCRLF` del final del cuerpo del mensaje. Esta opción se habilita por defecto.

Eliminar CRLF LF.CR CRCRLF del final del cuerpo del mensaje
Por defecto, MDaemon quitará esta secuencia del final de los mensajes, ya que puede causar problemas para algunos clientes de correo. Desmarque esta casilla si no quiere quitar esta secuencia de los mensajes.

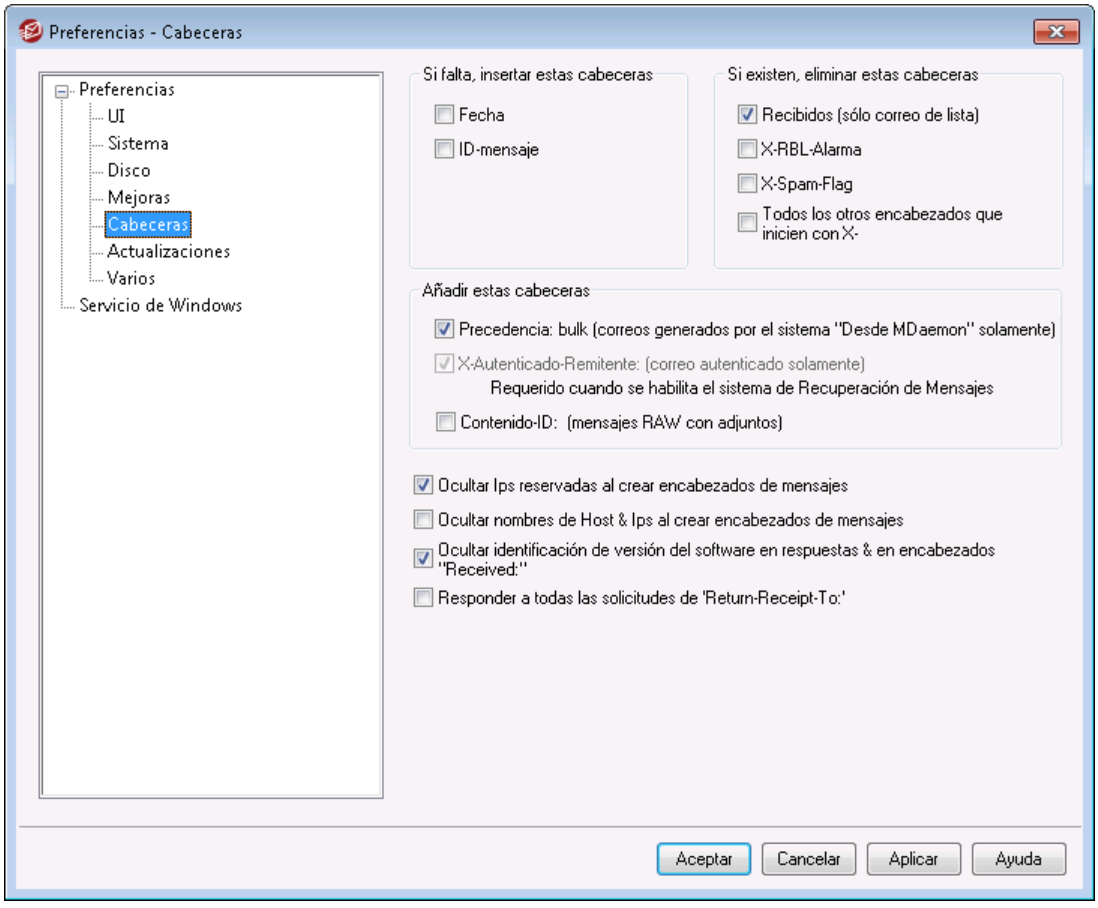
Eliminar NULL & EOF pero permitir LF.LF en el final del cuerpo de los mensajes
Cuando esta casilla está marcada MDaemon quitará los caracteres `Null` y EOF del final del cuerpo de los mensajes, pero permitirá que los mensajes acaben en `LF.LF`, así como mensajes que acaben con la secuencia normal de `CRLF.CRLF` que marca el final de un mensaje. Esta opción se habilita por defecto.

Prefijar las cabeceras ilegales con "X-MD-Bad-Header:"
Cuando esta opción se habilita y MDaemon se encuentra con una cabecera de mensaje erróneo, le prefijará el encabezado "`X-MD-Bad-Header:`" Esta opción se habilita por defecto.

Copiar 'Remitente:' a 'De:' cuando éste no existe
Algunos clientes de correo fallan al crear el encabezado `FROM:` cuando se redacta un mensaje. En su lugar, la información del encabezado `FROM:` se inserta en el encabezado `Sender:`. Esto puede causar problemas para algunos servidores de correo, así como también al destinatario del mensaje. Para ayudar a prevenir estos problemas, MDaemon creará los encabezados no existentes de `FROM:` utilizando el contenido del encabezado `Sender:` cuando se habilite esta opción. Esta opción se habilita por defecto.

Aceptar mensajes aun cuando la conexión se interrumpa durante el DATA
Cuando se habilita esta opción, MDaemon aceptará y entregará el mensaje aun y cuando aborte la conexión durante o inmediatamente después del comando DATA durante el procesamiento SMTP. Esta opción no deberá utilizarse en situaciones normales ya que puede generar mensajes duplicados.

3.13.1.5 Encabezados



Si faltan, insertar estas cabeceras

Fecha
Cuando un mensaje se encuentra que no tiene una cabecera "`Date:`", MDaemon creará una y la añadirá al archivo de mensaje si está esta opción habilitada. Será la fecha en la que MDaemon recibe por primera vez el mensaje, no la fecha de

creación por parte del remitente. Hay algunos clientes de correo que no crean esta cabecera, y algunos servidores de correo que rechazan la admisión de dichos mensajes, y esta función permite que sean enviados.

Message-ID
Cuando se encuentra que un mensaje no tiene una cabecera "`Message-ID`", MDaemon creará una y la insertará en el mensaje.

Si existen, eliminar estas cabeceras

Received (sólo correo de lista)
Marque esta casilla si desea quitar todos los encabezados "`Received:`" de los mensajes de lista de correo.

X-RBL-Warning
Haga clic en esta casilla si desea quitar todas las cabeceras "`X-RBL-Warning:`" encontradas en mensajes. Esta opción está deshabilitada por defecto.

X-Spam-Flag
Active esta opción si desea quitar las cabeceras antiguas "`X-Spam-Flag:`" de los mensajes.

Todas las cabeceras empiezan por X- (solamente correo entrante)
MDaemon y otros servidores de correo utilizan cabeceras específicas llamadas cabeceras `X-Type` para poder enrutar el correo y realizar otras funciones. Cuando se habilita esta opción, MDaemon quitará dichos encabezados de los mensajes. **Nota:** esta opción no quita los encabezados `X-RBL-Warning`. Si desea eliminar esos encabezados, utilice la opción "*X-RBL-Warning*" que se encuentra arriba

Agregar estas cabeceras

Precedence: bulk (únicamente correo generado por el sistema - 'From: MDaemon')
Cuando se marca esta casilla, a todos los mensajes generados por el sistema (mensajes de bienvenida, alarmas, mensajes de "no se pudo enviar", y demás) se les insertará la cabecera "Precedence: bulk".

X-Authenticated-Sender: (correo autenticado solamente)
Por defecto MDaemon añadirá la cabecera "X-Authenticated-Sender:" a los mensajes que lleguen en una sesión autenticada utilizando el comando `AUTH`. Desmarque esta casilla si no quiere añadir este encabezado.

Content-ID: (mensajes RAW con adjuntos)
Marque esta casilla si quiere añadir cabeceras únicas MIME `Content-ID` a los mensajes que MDaemon crea desde un fichero RAW que contiene adjuntos.

Ocultar IPs reservadas al crear encabezados de mensajes
Esta opción se encuentra habilitada por omisión e impide que las direcciones IP reservadas aparezcan en ciertos encabezados de mensaje creados por MDaemon. Las direcciones IP reservadas incluyen: `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, y `172.16.0.0/12`. Si también desea ocultar en los encabezados las IPs de su

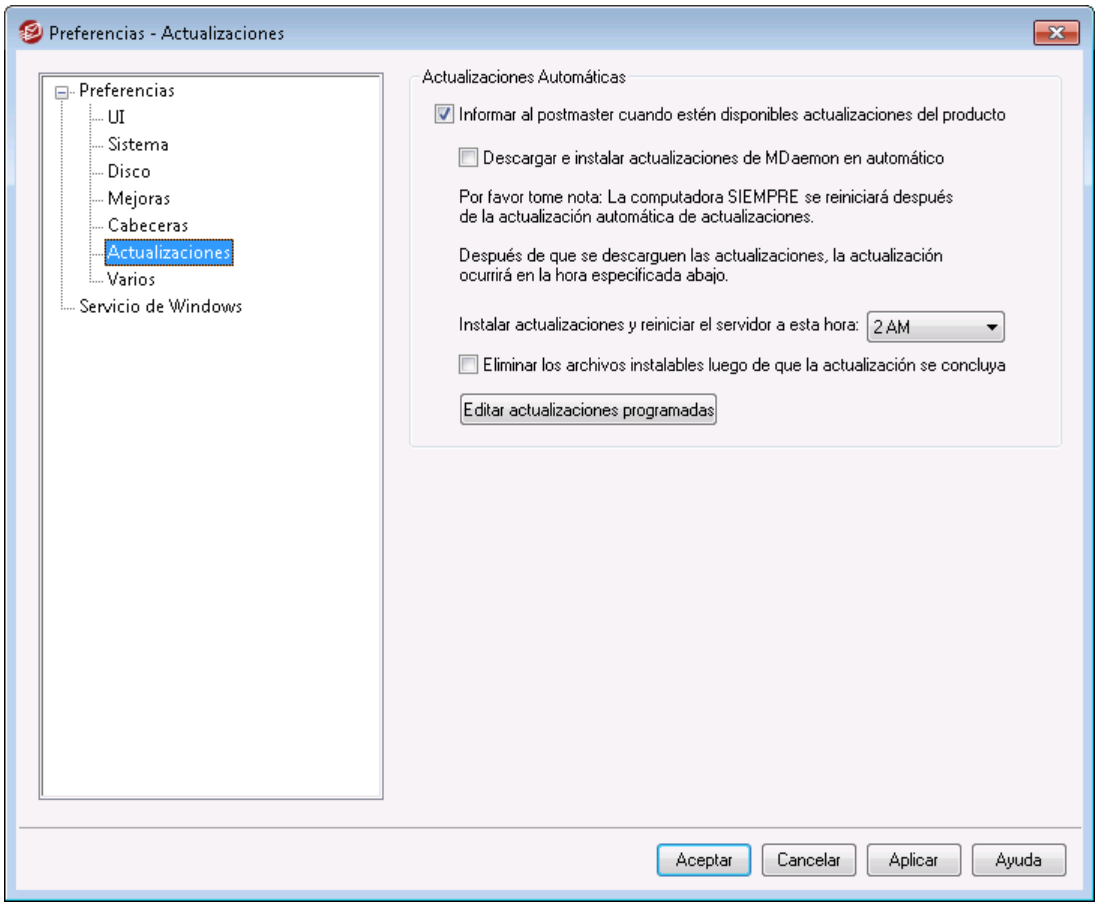
domino (incluyendo dominios LAN), puede configurar manualmente la opción en el archivo `MDaemon\app\MDaemon.ini` agregando: `[Special] HideMyIPs=Yes` (el valor por omisión es `No`).

Ocultar nombres de host e IPs al crear encabezados de mensajes
Dé clic en esta opción si desea omitir los nombres de host y direcciones IP de los encabezados "Received:" cuando se construyen. Esta opción se encuentra deshabilitada por omisión.

Ocultar la identificación de la versión de software en las respuestas y en los encabezados 'Received:'
Utilice esta opción si desea impedir que MDaemon muestre la versión de software y otra información de identificación al crear los encabezados `Received` o al responder a varias peticiones de protocolos. Esta opción se encuentra deshabilitada por omisión.

Responder a todas las solicitudes de 'Return-Receipt-To:'
Haga clic en esta casilla si desea responder las solicitudes de confirmación de envío de los mensajes entrantes y automáticamente enviar un mensaje de confirmación al remitente. Esta opción se deshabilita por defecto.

3.13.1.6 Actualizaciones



Actualizaciones Automáticas

Al utilizar la funcionalidad de Actualizaciones Automáticas, puede configurar MDaemon para informar al postmaster siempre que esté disponible una actualización y puede configurarlo para descargar e instalar las actualizaciones de manera automática. El servidor se reiniciará siempre que se instale una actualización de manera automática. Los archivos se descargan cuando se detecta la actualización, pero la instalación y el reinicio ocurren posteriormente a la hora en que usted lo haya determinado. Toda la actividad de instalación se registra en el sistema de bitácora de MDaemon y se le informa al postmaster cuando ha ocurrido alguna actualización.

Informar al postmaster siempre que estén disponibles actualizaciones de producto
Esta opción hace que MDaemon notifique al postmaster siempre que exista una actualización disponible para MDaemon. Se encuentra habilitada por omisión.

Cuando MDaemon se configura para actualizarse en automático, este mensaje no se envía. En lugar de esto, se informa al postmaster que la actualización se instaló y se le informan cualesquiera consideraciones especiales referentes a la actualización.

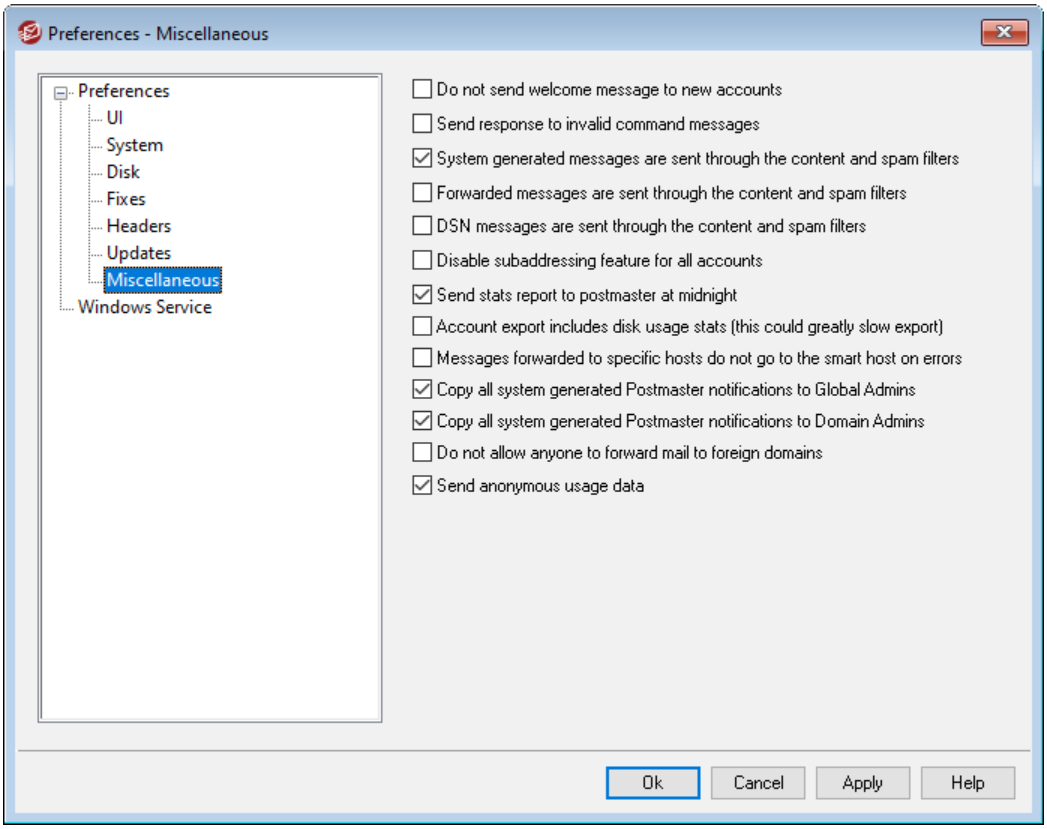
Descargar e instalar actualizaciones de MDaemon en automático
Marque esta caja si desea descargar e instalar automáticamente las actualizaciones de MDaemon. Las actualizaciones se descargan cuando se detectan y luego se instalan a la hora determinada más abajo. La opción se encuentra deshabilitada por omisión.

Instalar actualizaciones y reiniciar el servidor a esta hora:
Las actualizaciones automáticas se descargan en el momento que se detectan y se almacenan en la carpeta `\MDaemon\Updates`, pero no se instalan hasta la hora determinada aquí. El servidor en el que se encuentra instalado MDaemon se reiniciará en automático luego de cada actualización. Esta opción se encuentra configurada a las 2 AM por omisión.

Eliminar archivos instalables luego de completar la actualización
Marque esta casilla si desea eliminar los archivos instalables luego de que se complete la actualización.

Editar actualizaciones programadas
Cuando se detecta y descarga una actualización, se programa para posterior instalación. La lista de actualizaciones pendientes se guarda en el archivo `QueuedUpdates.dat`. Dé clic en este botón para revisar esa lista o eliminar alguna actualización pendiente.

3.13.1.7 Varios



No enviar mensaje de bienvenida a las cuentas nuevas
Por defecto, MDaemon generará un mensaje de Bienvenida basado en el archivo `NEWUSERHELP.DAT` y lo distribuirá a los nuevos usuarios cuando se cree una nueva cuenta. Active este control si quiere prevenir que el mensaje sea generado.

Enviar mensajes de respuesta a mensajes con comandos inválidos
Por omisión cuando alguien envía un mensaje de correo a la cuenta del sistema y este no contiene un comando válido, MDaemon no responde indicando "No se encontró comando válido". Habilite esta opción si desea enviar una respuesta a esos mensajes.

Los mensajes generados por el sistema se envían a través de los filtros de spam y contenido
Por omisión, los mensajes generados por el sistema se procesan a través de los Filtros de Contenido y de Spam. Deshabilite esta casilla si desea que sean excluidos del filtrado de contenido y de spam.

Los mensajes reenviados se envían a través de los filtros de spam y contenido
Marque esta casilla si desea que los mensajes reenviados sean procesados por el Filtro de Contenido y el Filtro de Spam. Esto se encuentra deshabilitado por omisión.

Los mensajes DSN se envían a través de los filtros de contenido y spam
Habilite esta opción si desea enviar mensajes DSN 880 a través de los filtros de spam y de contenido. Esta opción se encuentra deshabilitada por omisión.

Deshabilitar el subdireccionamiento para todas las cuentas
Haga clic en esta opción si desea deshabilitar globalmente la funcionalidad de subdireccionamiento. El subdireccionamiento no estará permitido para ninguna cuenta, independientemente de las configuraciones de cuenta individuales. Para más acerca de subdireccionamiento, vea la pantalla Filtros IMAP 737 en el Editor de Cuentas.

Enviar reporte de estadísticas al postmaster a media noche
Por omisión, el reporte de estadísticas se enviará al postmaster cada noche a media noche. Deshabilite esta casilla si no desea que se envíe el reporte. Esta opción corresponde a la pestaña Estadísticas 81 localizada en la pantalla principal de MDaemon.

La exportación de cuentas incluye estadísticas de uso de disco (eso puede alentar considerablemente la exportación)
Por omisión, la exportación de cuentas no incluye conteo de uso de disco y espacio consumido. Si desea incluir esta información en la exportación, habilite esta casilla. Esto, sin embargo, puede alentar significativamente la velocidad de exportación.

Mensajes reenviados a hosts específicos no se envían a los hosts inteligentes si ocurren errores

Al utilizar "Ajustes Avanzados de Reenvío" en la pantalla Reenvío 729 del editor de cuentas, las cuentas se pueden configurar para reenviar mensajes a un host inteligente específico en lugar de utilizar el proceso estándar de envío de MDaemon. Por defecto, cuando MDaemon encuentra un error de entrega al intentar reenviar uno de esos mensajes, lo colocará en la cola de erróneos. Habilite esta opción si en lugar de esto desea que MDaemon coloque el mensaje en la Cola de Reintentos 872 para que se reintente entregar utilizando el proceso normal de entrega de MDaemon.

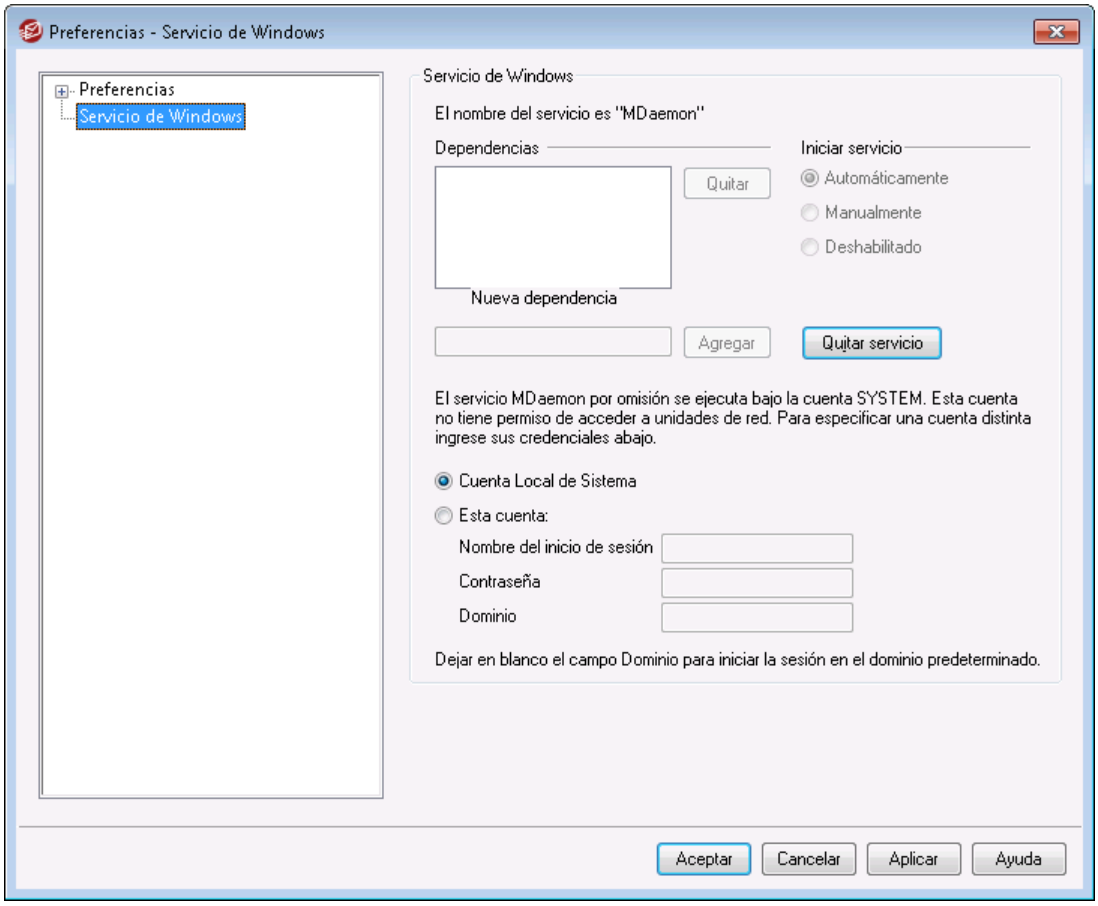
Copiar a los Admins Globales todas las notificaciones al Postmaster generadas por el sistema
Por omisión, las notificaciones generadas por el sistema que se envían al Postmaster también se enviarán a los Administradores Globales 757. Los Administradores Globales reciben todo incluyendo el reporte Resumen de Colas, Reporte Estadístico, Notas de la Versión, 'Usuario no encontrado' (para todos los dominios) y notificaciones de Errores de Disco, notificaciones de Cuenta Congelada y Deshabilitada para todos los dominios (que, como los Admins de Dominio pueden descongelar y rehabilitar), advertencias sobre licencias y versiones beta a punto de expirar, reportes de Resumen de Spam y más. Si no desea que sus administradores globales reciban esas notificaciones, deshabilite este ajuste.

Copiar a los Administradores de Dominio todas las notificaciones al Postmaster generadas por el sistema
Por omisión, las notificaciones generadas por el sistema que se envían al Postmaster también se enviarán a los Administradores de Dominio 757. Sin embargo, los Administradores de Dominio están limitados a recibir solo aquellos correos referentes a su dominio. Si no desea que sus administradores de dominio reciban estas notificaciones, deshabilite este ajuste.

No permitir que cualquiera reenvíe correo a dominios externos
Marque esta casilla si no desea permitir que las cuentas de correo reenvíen mensajes fuera del dominio. Si un usuario configura el reenvío de mensajes desde su cuenta hacia un dominio externo, las cuentas remotas a las que se reenvía serán ignoradas. Este ajuste solo aplica a mensajes reenviados utilizando las opciones de reenvío de mensajes 729 disponibles para la cuenta.

Enviar datos anónimos de uso
Por omisión, el servidor MDaemon envía datos anónimos de uso a MDaemon Technologies, para mejorar el producto y que sus funcionalidades cumplan mejor las necesidades de nuestros clientes. Deshabilite esta opción si no desea enviarnos la información anónima de uso. Para más información, vea nuestra política de privacidad.

3.13.2 Servicio de Windows



Servicio de Windows
Cuando MDaemon se ejecuta como servicio, el nombre de servicio es "MDaemon".

Dependencias
Use esta opción para designar cualquier servicio que quiere que se requiera estar ejecutando **antes** de que arranque el servicio de MDaemon.

Iniciar servicio
Este es el estado inicial del servicio: inicia automáticamente, debe ser iniciado manualmente o deshabilitado.

Instalar/Quitar Servicio
Haga clic en este botón para instalar o quitar el servicio de MDaemon.

Acceso a Recurso de Red

Cuando se ejecute MDaemon como servicio de Windows, por defecto se ejecuta bajo la cuenta SYSTEM. Dado que esta cuenta no tiene acceso a los dispositivos de red, MDaemon no podrá acceder al correo si desea almacenarlo en otros ordenadores de la LAN. Eso es así, a menos que proporcione credenciales de inicio de sesión para una cuenta que pueda ser usada por MDaemon para dar acceso a recursos compartidos. Si necesita hacer esto, puede crear un usuario de Windows designado específicamente para MDaemon con las restricciones que desee, pero que tenga acceso a los recursos de red que MDaemon pueda necesitar usar. Además, todas las aplicaciones ejecutadas por MDaemon usarán las mismas credenciales.

Nombre del inicio de sesión
Este es el nombre de inicio de sesión de la cuenta de Windows que deberá ejecutar el servicio de MDaemon.

Contraseña
Esta es la contraseña de la cuenta.

Dominio
Este es el Dominio de Windows en el que reside la cuenta. Deje este campo en blanco para acceder a través del dominio por defecto.

Sección

4 Menú Seguridad

MDaemon está equipado con un extenso conjunto de funcionalidades y controles de seguridad. Haga clic en Seguridad de la barra de menús de MDaemon para llegar a las siguientes funciones:

- **Verificación de Salud** 510 — Esta página proporciona una lista conveniente de ajustes de seguridad importantes consolidados en un solo lugar y despliega el valor actual de cada ajuste y su valor por omisión. Cuando esos valores difieren, el ajuste se resalta de manera que los Administradores Globales pueden visualizarlos. Si se desea, los administradores pueden elegir cualquiera de los ajustes y regresarlo al valor por omisión o pueden dar clic en la liga al lado de cada ajuste para ir directamente a la página donde se localiza. Adicionalmente, los administradores fácilmente pueden revertir los cambios más recientes hechos en la página de Verificación de Salud. También pueden visualizar cambios previos hechos durante la sesión actual del navegador y deshacer cambios específicos.**Nota:** Esta opción solo está disponible en la interface web MDaemon Administración Remota (MDRA) 354.
- **Antivirus** 645 — Las funcionalidades Antivirus de MDaemon Private Cloud pueden ayudarle a detener los virus que llegan en el correo electrónico, proporcionando el nivel mas alto de protección integrada disponible para los clientes de MDaemon. Interceptará, pondrá en cuarentena, reparará y/o eliminará cualquier mensaje que contenga algún virus. El componente Outbreak Protection 640 se puede utilizar para protegerlo de ciertos mensajes de Spam, phishing y dispersiones de virus que en ocasiones no son detectadas por otras medidas de seguridad tradicionales basadas en contenido y firmas antivirus.
- **Filtro de Contenido** 645 — un sistema de Filtro de Contenido multihilo y altamente versátil hace posible personalizar el comportamiento del servidor basándose en el contenido de los mensajes de correo entrantes y salientes. Puede insertar y borrar cabeceras de menaje, añadir pies de mensaje, quitar adjuntos, enrutar copias a otros usuarios, hacer que se envíe un mensaje instantáneo a alguien, ejecutar otros programas, y mucho más.
- **Filtro de Spam** 675 — usa la tecnología de filtrado de Spam para examinar heurísticamente los mensajes de correo para procesar una "puntuación". Esta puntuación se usa para determinar las posibilidades de que el mensaje sea Spam. Basándose en dicha determinación el servidor puede tomar ciertas decisiones tal como rechazar o marcar el mensaje. Vea también: Capturas de Spam. 707
- **Listas de DNS Bloqueados** 701 — le permite especificar varios servicios de lista de DNS bloqueados que serán comprobados cada vez que alguien intente enviar un mensaje a su servidor. Si la IP en conexión ha sido enlistada en cualquiera de esos hosts, el mensaje será rechazado.
- **Control de Retransmisión** 512 — se usa para controlar lo que MDaemon hará cuando un mensaje llegue a su servidor de correo siendo o no de una dirección local.
- **Protección IP** 521 — si un nombre de dominio especificado en esta lista intenta conectar a su servidor, su dirección IP debe coincidir con la que se le haya asignado.
- **Búsqueda Inversa** 514 — MDaemon puede consultar los servidores DNS para comprobar la validez de los nombres de dominio y direcciones durante los mensajes entrantes. Los controles en esta pantalla pueden usarse para

hacer que los mensajes sospechosos sean rechazados o se les inserte un encabezado especial en ellos. Los datos de búsqueda invertida también serán registrados en los archivos de MDaemon.

- **POP antes de SMTP** 518 — los controles en esta pantalla se usan para requerir a cada usuario que acceda primero a su buzón antes de que se le permita enviar un mensaje a través de MDaemon, así pues autenticando que el usuario es un propietario de cuenta válido y que tiene permiso para usar el sistema de correo.
- **Hosts Confiables** 519 — nombres de dominio y direcciones IP que serán consideradas como excepciones a las reglas de retransmisión listadas en la pantalla de Control de Retransmisión.
- **Autenticación SMTP** 523 — se usa para establecer diversas opciones que denotan cómo MDaemon se comportará cuando un usuario que envíe un mensaje a MDaemon se haya o no autenticado primero.
- **SPF** 526 — La mayoría de los dominios publican registros MX para identificar las máquinas que pueden recibir correo por ellos, pero esto no identifica las ubicaciones permitidas para enviar correo. Sender Policy Framework (SPF) es un medio por el que los dominios pueden publicar registros "MX inversos" para identificar dichas ubicaciones autorizadas para enviar mensajes.
- **DomainKeys** 529 — DomainKeys (DK) es un sistema de verificación de correo que puede usarse para prevenir la suplantación. También puede usarse para asegurar la integridad de los mensajes entrantes, asegurando que el mensaje no ha sido modificado entre el momento del envío y el de recepción. Ello se consigue usando un sistema de llaves pública/privada. Los mensajes salientes se firman usando una llave privada y los mensajes entrantes tienen verificadas sus firmadas comprobándolas con la llave pública publicada en el servidor DNS del remitente.
- **Certificación** 553 — La Certificación de Mensajes es un proceso por el que una entidad certifica la buena conducta de correo de otra entidad. La funcionalidad de Certificación es beneficiosa dado que puede ayudar a asegurarse que los mensajes no estarán innecesariamente sujetos a análisis del filtro de Spam no garantizado. También puede ayudar a reducir los recursos requeridos para procesar cada mensaje.
- **Lista de Remitentes Bloqueados** 559 — lista direcciones a las que no se les permite enviar tráfico de correo a través de su servidor.
- **Monitor IP** 562 — usado para designar direcciones IP desde las que aceptará o rechazará conexiones a su servidor.
- **Monitor Host** 564 — usado para designar hosts (nombres de dominio) para los que permitirá o rechazará conexiones a su servidor.
- **Monitoreo Dinámico** 610 — Utilizando Monitoreo Dinámico, MDaemon puede rastrear el comportamiento de las conexiones entrantes para identificar actividad sospechosa y responder en consecuencia. Puede bloquear una dirección IP 615 (o rango de direcciones) para que impedir que se conecte cuando falla la autentificación un número determinado de veces dentro de cierto rango de tiempo. También puede congelar las cuentas 615 que intentan autenticarse cuando fallan demasiadas veces demasiado rápido.
- **SSL & TLS** 575 — MDaemon soporta el protocolo Secure Sockets Layer (SSL) para SMTP, POP, e IMAP y para el servidor web de Webmail. SSL es el método estándar para proteger las comunicaciones de Internet.

- **Protección Backscatter** 597 — "Backscatter" se refiere a mensajes de respuesta que sus usuarios reciben a correos que nunca han enviado. Esto ocurre cuando un mensaje o mensajes de Spam enviados por virus contienen una dirección de respuesta falsificada. La Protección Backscatter ayudar a prevenirlo asegurando que sólo las Notificaciones de Entrega reales y las autorespuestas sean enviadas a sus cuentas, usando un método de hash de llave privada para generar e insertar un código sensible a tiempo en la dirección de respuesta de los mensajes salientes de sus usuarios.
- **Regular el Tráfico del Ancho de Banda** 600 — la Regulación de Tráfico hace que sea posible controlar el consumo de ancho de banda usado por MDaemon. Puede controlar el nivel en el que las sesiones o servicios progresan, estableciendo diferentes niveles para cada servicio prioritario de MDaemon en base a dominio, incluyendo los Dominios, así como las Puertas de Enlace.
- **Tarpitting** 602 — hace posible que haga más lenta una conexión de manera deliberada cuando se hayan recibido un número específico de comandos RCPT de un remitente de mensaje. Esto es para evitar que los spammers intenten enviar correo masivo no solicitado. El supuesto detrás de esta técnica es que a los spammers les lleva demasiado tiempo enviar cada mensaje y ello hace que dejen de intentar hacerlo en un futuro.
- **Lista Gris** 604 — La lista gris es una técnica para combatir el Spam que explota el hecho de que los servidores SMTP reintentan el envío de cualquier mensaje que reciba un código de error temporal ("inténtelo más tarde"). Usando esta técnica, cuando un mensaje llega de un remitente que no está en lista en lista de permitidos o es desconocido, su remitente, destinatario, y dirección IP del servidor de envío serán registrados y el mensaje será rechazado por la Lista Gris con un código de error temporal durante la sesión SMTP. Entonces, cuando los servidores legítimos intenten enviar los mensajes nuevamente unos minutos más tarde, éstos serán aceptados. Dado que los spammers no suelen reintentar el envío, la Lista Gris puede ayudar de manera significativa a reducir la cantidad de Spam que reciben los usuarios.
- **IPs de la LAN** 608 — use esta pantalla para listar las direcciones IP que residen en su LAN. Estas direcciones IP serán entonces tratadas como locales para los propósitos de regulación de ancho de banda, y pueden estar exentos de varias medidas y restricciones de seguridad.
- **Política del Sitio** 609 — se usa para crear una política del sitio a transmitir a los servidores de envío al principio de cada sesión SMTP. Un ejemplo de una política de sitio común es "Este servidor no retransmite".

4.1 Health Check

Esta página proporciona una lista conveniente de ajustes importantes de seguridad consolidados en una sola página y despliega el valor actual de cada ajuste y su valor por omisión. Cuando esos valores difieren, el ajuste se resalta de manera que el Administrador Global puede visualizar rápidamente esos ajustes en particular y restaurar cualquiera de ellos a los valores por omisión, si así lo desea. Cada grupo de ajustes tiene un ícono de acceso rápido, de manera que puede ir directamente a

la página donde están localizados esos ajustes. Más aún, puede también visualizar la lista de todos los cambios hechos en la Verificación de Salud durante la sesión actual del navegador y deshacerlos si es necesario. **Nota:** Esta funcionalidad solo está disponible en la interface web MDaemon Administración Remota (MDRA) 354.

Restaurar Ajustes a sus Valores por Omisión
Para restaurar uno o más ajustes a sus valores por omisión:

1. Dé clic en uno o más de los ajustes deseados.
2. Dé clic en **Restaurar a Omisión** en la barra de herramientas.

Deshacer el Último Cambio
Dé clic en **Deshacer el último** en la barra de herramientas si está utilizando la Verificación de Salud para modificar un valor e inmediatamente quiere deshacer ese cambio.

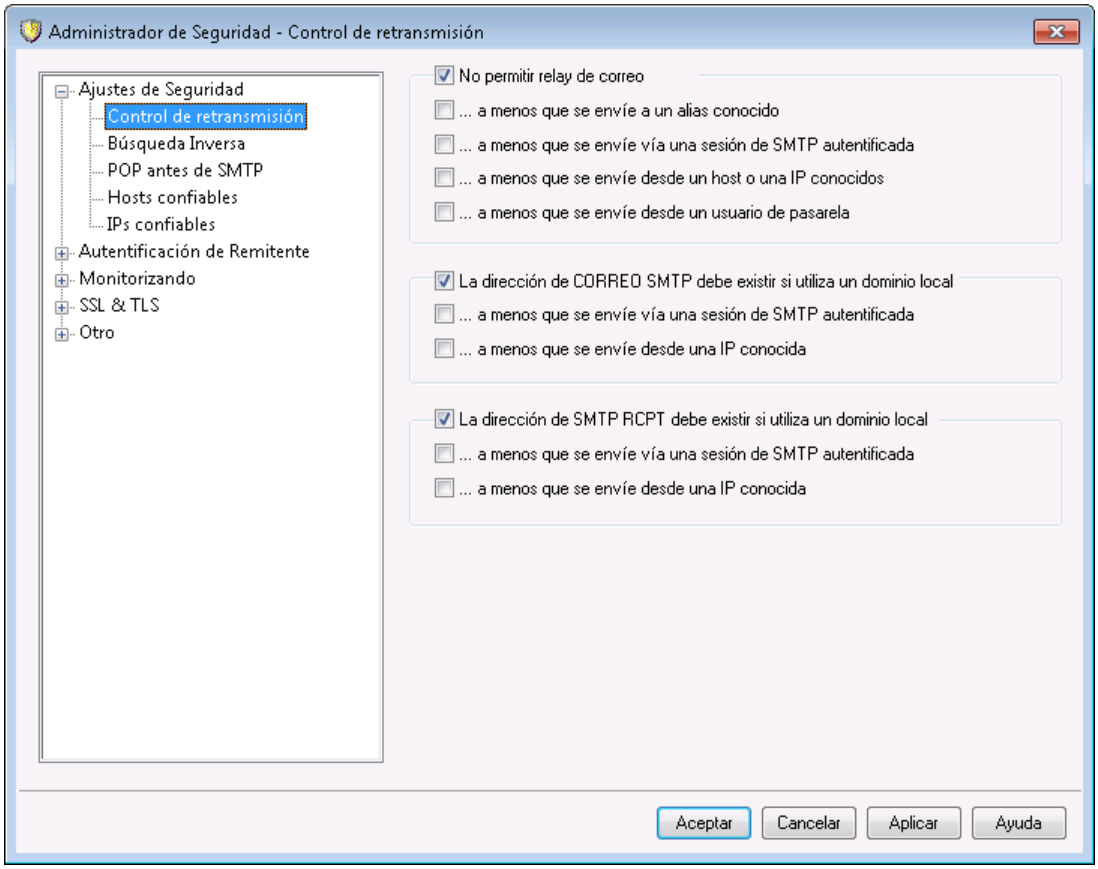
Revisar/Deshacer Cambios hechos en la Sesión
Dé clic en **Cambios en Sesión** para ver una lista de cambios hechos en la Verificación de Salud durante la sesión actual del navegador. Si desea deshacer cualquiera de los cambios enlistados, seleccione la casilla al lado de cualquiera de ellos y dé clic en **Deshacer Selección**. Dé clic en **Borrar** si desea borrar la lista de cambios en la sesión; no modificará ningún ajuste y no se puede revertir.

Los valores por omisión de estos ajustes de seguridad no necesariamente son los mejores para su instalación particular. Por favor tenga cuidado al utilizar la Verificación de Salud para hacer cualquier cambio.

4.2 Administrador de Seguridad

4.2.1 Ajustes de Seguridad

4.2.1.1 Control de retransmisión



Use el Control de Retransmisión en Seguridad » Ajustes de Seguridad » Control de Retransmisión para definir cómo reacciona su servidor a la retransmisión de correo. Cuando un mensaje llega a su servidor no dirigido a ni remitido por una dirección local, se le pedirá al servidor que retransmita (envíe) el mensaje en nombre de otro servidor. Si no quiere que el servidor pueda retransmitir correo para usuarios desconocidos, puede usar las configuraciones establecidas aquí para controlarlo.

Retransmitir correo indiscriminadamente para otros servidores puede resultar en que su dominio sea puesto en lista de bloqueados por uno o más Servicios DNS-BL[701]. Las retransmisiones abiertas no se recomiendan dado que los spammers explotan servidores abiertos para esconder sus trazas.

Retransmisión de Correo

No permitir retransmisión de correo
Cuando se habilita esta opción, MDaemon rechazará la aceptación de mensajes para envío cuando tanto el `FROM` como el `TO` son para usuarios no-locales.

...a menos que se envíe a un alias conocido
Haga clic en esta casilla si quiere que MDaemon retransmita correo para Alias 834 independientemente de las configuraciones de Retransmisión.

...a menos que se envíe vía una sesión de SMTP autentificada
Cuando se habilita esta casilla, MDaemon siempre retransmitirá correo cuando se envíe a través de una sesión SMTP autenticada.

...a menos que se envíe desde un host o una IP conocidos
Habilite esta opción si desea permitir la retransmisión cuando el correo venga de un Host Confiable o de una dirección IP Confiable.

...a menos que se envíe desde un usuario de pasarela
Habilite esta casilla si quiere que MDaemon permita la retransmisión de correo a través de dominios de puerta de enlace independientemente de sus configuraciones de Retransmisión. Esta funcionalidad está deshabilitada por defecto y no se recomienda utilizarla.

Verificación de Cuentas

La dirección de CORREO SMTP debe existir si utiliza un dominio local
Haga clic en esta opción si desea verificar que el valor MAIL pasado durante el proceso SMTP apunte a una dirección válida cuando se dirige a un dominio local o de puerta de enlace.

...a menos que se envíe vía una sesión de SMTP autentificada
Haga clic en esta opción si desea hacer exento a un mensaje de la opción *La dirección de CORREO SMTP debe existir si utiliza un dominio local...* cuando se envíe a través de una sesión SMTP de correo autenticada.

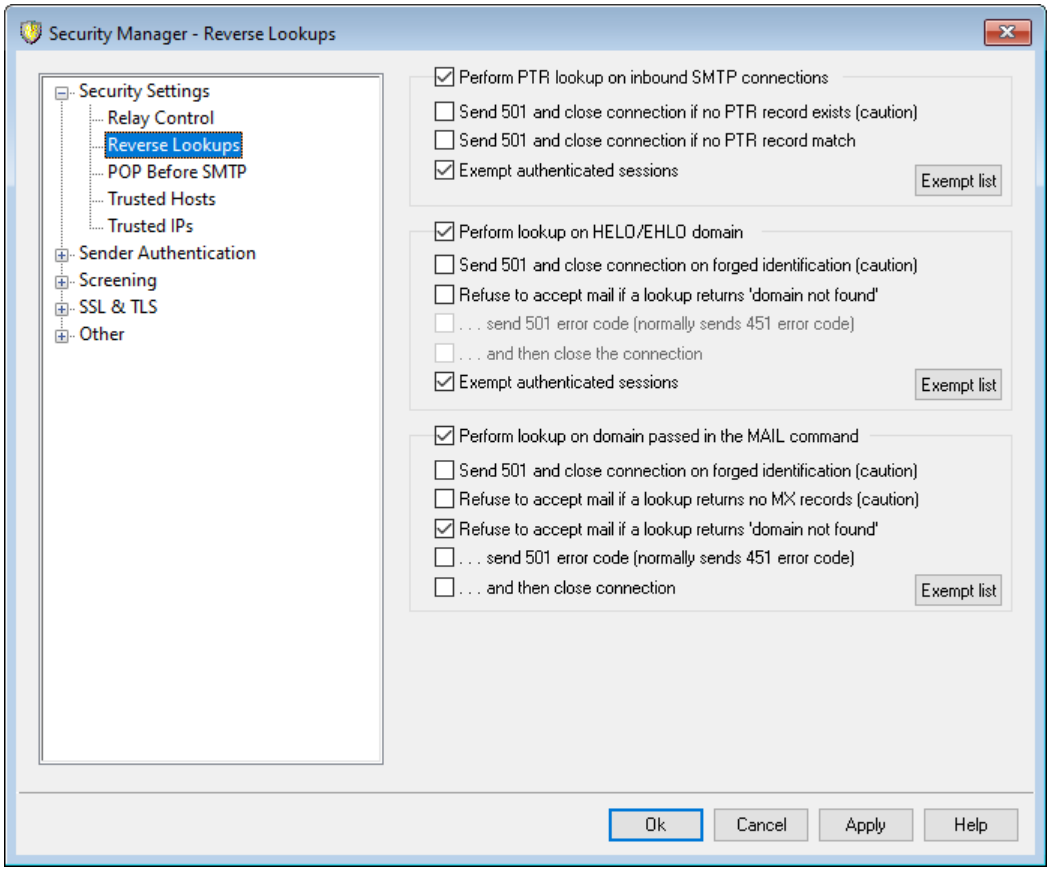
...a menos que se envíe desde una IP conocida
Haga clic en esta opción si desea hacer exento a un mensaje de la opción *La dirección de CORREO SMTP debe existir...* cuando se envíe a través de una dirección IP Confiable.

La dirección de SMTP RCPT debe existir si utiliza un dominio local
Haga clic en esta opción si desea verificar que el valor RCPT pasado durante el proceso SMTP apunte a una cuenta válida cuando se dirige a un dominio local.

...a menos que se envíe vía una sesión de SMTP autentificada
Haga clic en esta opción si desea hacer exento a un mensaje de la opción *La dirección SMTP RCPT debe existir...* cuando se envíe a través de una sesión SMTP de correo autenticada.

...a menos que se envíe desde una IP conocida
Haga clic en esta opción si desea hacer exento a un mensaje de la opción *La dirección SMTP RCPT debe existir...* cuando se envíe a través de una dirección IP Confiable.

4.2.1.2 Búsqueda Inversa



Con las opciones en esta pantalla, MDaemon puede ser configurado para realizar una búsqueda inversa en el dominio indicado en los comandos `HELO/EHLO` y `MAIL`. Cuando se realizan las búsquedas MDaemon intentará buscar todas las direcciones IP de los registros MX y A para un dominio dado. Entonces la IP del servidor que realiza la conexión se comparará con esta lista en un intento de determinar si el servidor puede estar utilizando una identidad suplantada.

También puede realizar búsquedas inversas en registros PTR (pointer records) de direcciones IP. Usando esta opción la conexión puede abortarse o puede insertarse una cabecera de aviso en el mensaje de la dirección IP entrante que no coincida con ningún registro PTR.

Finalmente, está generalmente aprobado que aceptar correo de fuentes que se identifiquen a ellas mismas usando un dominio que no exista debería ser opcional. Así pues, existe un control que hace posible que se rechacen mensajes para los que el proceso de búsqueda inversa devuelva un mensaje "dominio no encontrado" del servidor DNS. En dichos casos, MDaemon devolverá un código de error `451`, rechazará la aceptación del mensaje, y luego permitirá que la sesión SMTP progrese. Aun así, si desea devolver un código de error `501`, cerrar la conexión de socket, o ambas, otros controles se facilitan para dichos propósitos.

Las direcciones IP confiables y de localhost (127.0.0.1) siempre están exentas de las búsquedas inversas.

Realizar una búsqueda PTR en las conexiones SMTP entrantes
Habilite esta opción si quiere que MDaemon realice búsquedas PTR en todas las conexiones SMTP entrantes.

...Enviar 501 y cerrar la conexión si no hay registros PTR (precaución)
Si esta casilla está marcada MDaemon enviará un código de error `501` (error de sintaxis en los parámetros o argumentos) y cerrará la conexión si no existe registro PTR para el dominio.

...Enviar 501 y cerrar la conexión si no hay coincidencia de registros PTR
Si esta casilla está marcada MDaemon enviará un código de error `501` (error de sintaxis en los parámetros o argumentos) y cerrará la conexión si el resultado de la búsqueda PTR no coincide.

Excluir sesiones autenticadas
Haga clic en esta opción si desea diferir la búsqueda PTR en las conexiones entrantes SMTP hasta después del comando SMTP MAIL para ver si la conexión usará o no autenticación.

Lista de Exentos
Dé clic en este botón para abrir la Lista de Exentos de la búsqueda PTR, en la que puede especificar las direcciones IP que estarán exentas de búsquedas inversas PTR.

Realizar una búsqueda en el dominio HELO/EHLO
Haga clic en este cuadro si quiere que se realice una búsqueda en el nombre de dominio que se reporta durante la porción `HELO/EHLO` de la sesión. El comando `HELO/EHLO` es usado por el cliente (la máquina de envío) para identificarse a sí mismo al servidor. El nombre de dominio que pasa el cliente es usado por el servidor para completar la porción `from` del encabezado `Received`.

...Enviar 501 y finalizar la conexión cuando la identificación es falsa (precaución)
Haga clic en esta casilla si quiere que se envíe un código de error 501 y luego se cierre la conexión cuando el resultado de una búsqueda parezca ser una identificación suplantada.

Cuando el resultado de una búsqueda inversa indique el servidor está usando una identidad suplantada, el resultado puede ser frecuentemente incorrecto. Es muy común para los servidores de correo identificarse con valores que no coinciden con sus direcciones IP. Esto puede deberse a las limitaciones de los ISP y a restricciones y otras razones legítimas. Por dicha razón, debería tomar precauciones antes de activar esta opción. Lo más probable es que usar esta opción resulte en su servidor rechazando algunos correos legítimos.

No aceptar correo si la búsqueda devuelve el resultado 'dominio no encontrado'
Cuando una búsqueda resulta en "`domain not found`", si activa esta opción hará que el mensaje sea rechazado con un código de error `451` (Acción solicitada abortada: error local al procesar) y luego a la sesión se le permitirá progresar normalmente hasta su finalización.

...enviar código de error 501 (normalmente envía el código de error 451)
Habilite esta casilla si quiere que el código de error que se envíe en respuesta a "domain not found" resulte ser `501` (error de sintaxis en parámetros o argumentos) en lugar de `451`.

...y luego cerrar la conexión
Haga clic en esta casilla si quiere que la conexión se cierre inmediatamente en lugar de permitirle progresar cuando "`domain not found`" sea el resultado de la búsqueda inversa.

Exentar sesiones autentificadas
Haga clic en esta opción si desea diferir la verificación hasta después del comando SMTP MAIL con el fin de ver si la conexión utilizará autenticación o no.

Lista de Exentos
Haga clic en este botón para abrir el diálogo de Lista de Exentos de consulta HELO/EHLO, para enlistar las direcciones IP y nombres de dominio/host de sitios que desea exentar de las consultas inversas HELO/EHLO.

Realizar una búsqueda en el valor especificado en el comando MAIL
Si activa esta opción se provocará una búsqueda en el nombre de dominio pasado durante la porción del comando `MAIL` de una transacción de correo. La dirección pasada en el comando `MAIL` se supone que es la ruta invertida del mensaje, y es normalmente el buzón desde el que el mensaje se origina. A veces, sin embargo, es la dirección a la que los mensajes de error deberían dirigirse en su lugar.

...Enviar 501 y finalizar la conexión cuando la identificación es falsa (precaución)
Haga clic en esta casilla si quiere que se envíe un código de error 501 y luego se cierre la conexión cuando el resultado de una búsqueda parezca ser una identificación suplantada.

Cuando el resultado de una búsqueda inversa indique el servidor está usando una identidad suplantada, el resultado puede ser frecuentemente incorrecto. Es muy común para los servidores de correo identificarse con valores que no coinciden con sus direcciones IP. Esto puede deberse a las limitaciones de los ISP y a restricciones y otras razones legítimas. Por dicha razón, debería tomar precauciones antes de activar esta opción. Lo más probable es que usar esta opción resulte en su servidor rechazando algunos correos legítimos.

Rehusar a aceptar correo si la búsqueda no devuelve registros MX (precaución)
Habilite esta casilla si desea rehusar correo proveniente de dominios que no cuentan con registros MX. Esta opción esta deshabilitada por omisión y deberá utilizarse con precaución porque no es obligatorio que los dominios tengan registros MX para existir, ser válidos o enviar/recibir correo.

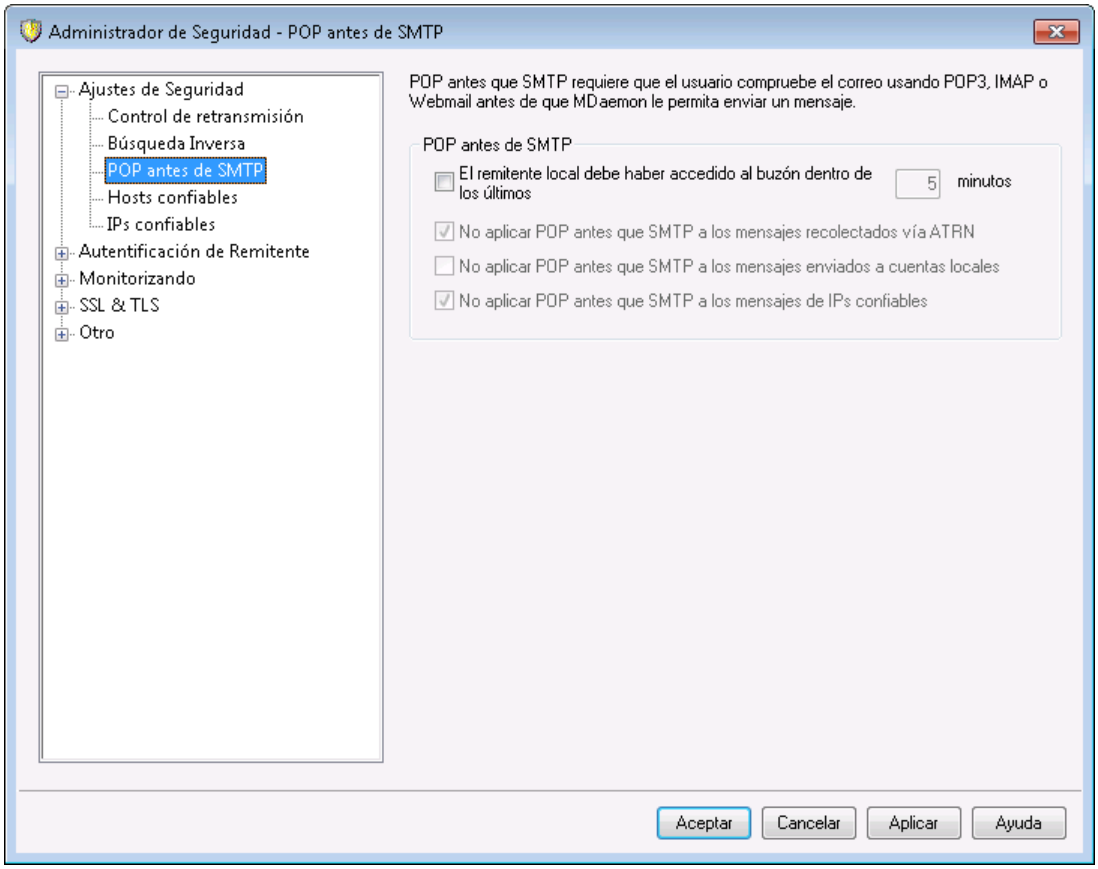
No aceptar correo si la búsqueda devuelve el resultado 'dominio no encontrado'
Cuando una búsqueda resulta en "`domain not found`", si activa esta opción hará que el mensaje sea rechazado con un código de error `451` (Acción solicitada abortada: error local al procesar) y luego a la sesión se le permitirá progresar normalmente hasta su finalización.

...enviar código de error 501 (normalmente envía el código de error 451)
Habilite esta casilla si quiere que el código de error que se envíe en respuesta a "domain not found" resulte ser `501` (error de sintaxis en parámetros o argumentos) en lugar de `451`.

...y luego cerrar la conexión
Haga clic en esta casilla si quiere que la conexión se cierre inmediatamente en lugar de permitirle progresar cuando "`domain not found`" sea el resultado de la búsqueda inversa.

Lista de Exentos
Haga clic en este botón para abrir el diálogo de Lista de Exentos de consulta MAIL. En ella puede designar las direcciones IP y dominios/host de sitios que desea exentar de consultas inversas MAIL.

4.2.1.3 POP antes de SMTP



POP antes de SMTP

El remitente local debe haber accedido al buzón dentro de los últimos [XX] minutos
Con esta funcionalidad habilitada, siempre que un mensaje sea supuestamente para un usuario local, ese usuario deberá haber accedido y comprobado su buzón local dentro del número de minutos indicado antes de que se le permita enviar correo.

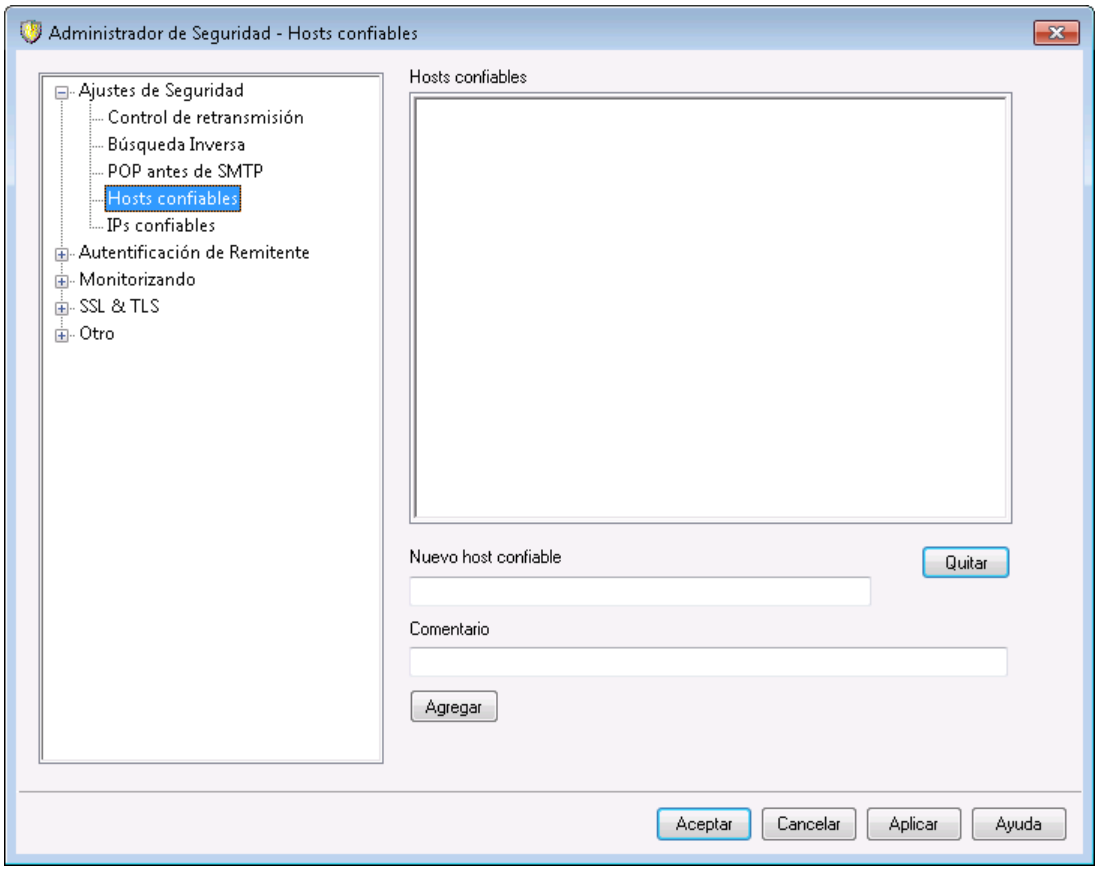
No aplicar POP Antes que SMTP a los mensajes recolectados vía ATRN
Marque esta casilla si desea que los mensajes recolectados vía ATRN 269 estén exentos de la restricción POP antes de SMTP.

No aplicar POP Antes que SMTP a los mensajes enviados a cuentas locales
Marque esta casilla si desea que los mensajes que son enviados desde un usuario local a otro estén exentos del requisito POP antes de SMTP. Normalmente, MDaemon forzará el requisito en el momento que se sepa el remitente, pero cuando este control está activado MDaemon esperará hasta que se revele el destinatario del mensaje antes de determinar si es requerido o no.

No aplicar POP Antes que SMTP a los mensajes de IPs confiables
Si esta casilla está habilitada, los mensajes que lleguen de direcciones IP listadas en la pantalla Hosts Confiables 519 estarán exentas de POP antes de SMTP.

Puede hacer exentas las sesiones autenticadas de la restricción POP antes de SMTP a través de una opción en la pantalla de Autenticación de SMTP 523.

4.2.1.4 Hosts confiables



En varios diálogos y funcionalidades de seguridad en MDaemon verá opciones que le permiten escoger si los "Hosts Confiables", "Dominios Confiables" serán o no excepciones o estarán exentos de dichas opciones. Los hosts que liste en esta pantalla son a los que se refieren dichas opciones.

Hosts confiables
Esta es la lista de los hosts que estarán exentos de ciertas opciones de seguridad designadas.

Nuevo host confiable
Introduzca un nuevo nombre de dominio para añadirlo a la lista de *Hosts Confiables*.

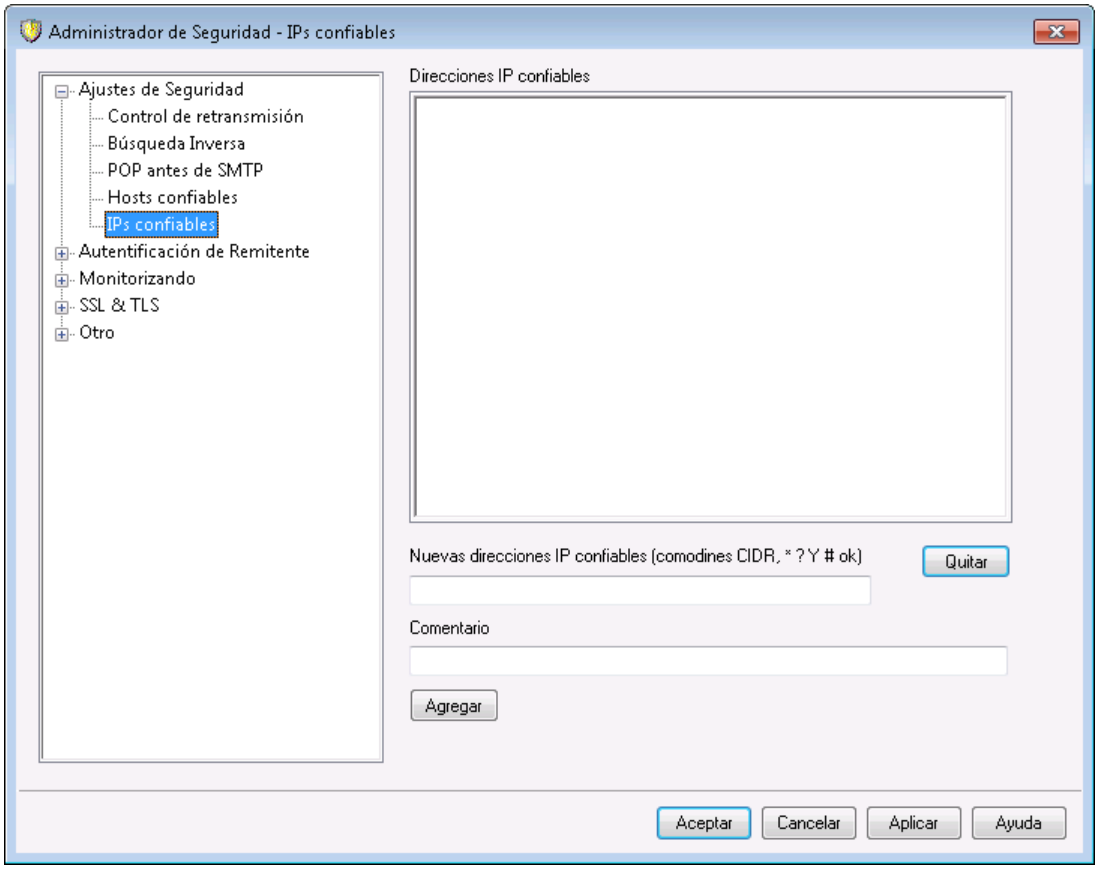
Comentario
Utilice este campo para cualquier comentario de texto sobre algún registro.

Agregar

Haga clic en este botón para añadir el nuevo dominio a la lista de *Hosts Confiables*.

Eliminar
Haga clic en este botón para eliminar las entradas seleccionadas de la lista de *Hosts Confiables*.

4.2.1.5 IPs Confiables



En varios diálogos y opciones de seguridad en MDaemon verá opciones que le permiten decidir si las "IPs Confiables" serán excepciones o estarán exentas de esas opciones. Las direcciones IP que enliste en esta pantalla son a las que se refieren esas opciones.

Direcciones IP confiables
Esta es la lista de direcciones IP que estarán exentas de ciertas opciones de seguridad determinadas.

Nueva dirección IP confiable
Registre una nueva dirección IP que será agregada a la lista de *Direcciones IP Confiables*.

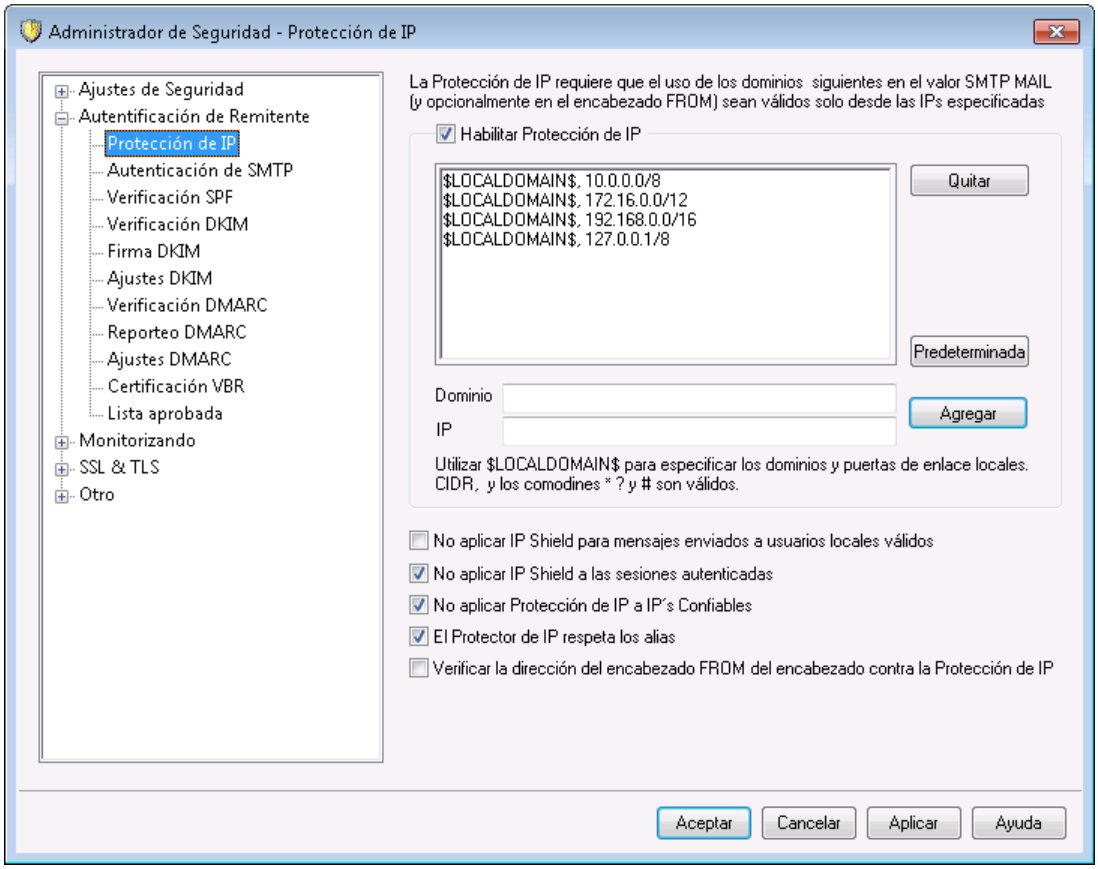
Comentario
Utilice este campo para cualquier comentario sobre este registro.

Agregar
Dé clic en este botón para agregar una dirección IP nueva a la lista de *Direcciones IP Confiables*.

Eliminar
Dé clic en este botón para eliminar los registros seleccionados de la lista de *Direcciones IP Confiables*.

4.2.2 Autenticación de Remitente

4.2.2.1 Protección IP



La Protección IP, ubicada bajo el menú Seguridad » Ajustes de Seguridad » Autenticación del Remitente, es una lista de nombres de dominios e IPs coincidentes que serán comprobados durante el comando MAIL From durante la sesión SMTP. Una sesión SMTP que diga ser de alguien en uno de los dominios listados será aceptada sólo si viene de una de las direcciones IP asociadas. Por ejemplo, suponga que su nombre de dominio es ejemplo.com y que los ordenadores de su LAN local usan direcciones IP en el rango desde 192.168.0.0 a 192.168.0.255. Con esta información puede establecer la Protección IP para asociar el nombre de dominio ejemplo.com con el rango de direcciones IP 192.168.0.* (se permiten comodines). Así pues, siempre que un ordenador se conecte a su servidor SMTP y se presente como, "`MAIL FROM <alguien@ejemplo.com>`", la sesión SMTP sólo continuará si el ordenador que se conecta tiene una dirección IP dentro del rango requerido entre 192.168.0.0 y 192.168.0.255.

Habilitar Protección IP

Desactive esta casilla si desea deshabilitar la Protección IP. Esta se habilita por omisión.

Nombre de dominio
Introduzca el nombre de dominio que desea asociar a un rango de dirección IPs específico. También puede utilizar la macro `$LOCALDOMAIN$` para cubrir todos los dominios locales (incluyendo puertas de enlace). Si utiliza esta macro no será necesario mantener actualizada la Protección IP cuando se modifiquen direcciones IP o puertas de enlace. Por omisión, se agregan registros a la Protección IP asociando todas las direcciones IP reservadas dentro de `$LOCALDOMAIN$`.

Dirección IP
Introduzca la dirección IP que desea asociar con un nombre de dominio. Debe introducir esta dirección en formato de puntos decimal.

Agregar
Haga clic en el botón *Agregar* para añadir el dominio y el rango de dirección IP al listado.

Eliminar
Haga clic en este botón para eliminar las entradas seleccionadas de la lista.

No aplicar Protección IP para mensajes enviados a usuarios locales válidos
Haga clic en esta opción si quiere que sólo aquellos mensajes dirigidos a usuarios no-locales o a usuarios locales inválidos sean validados para encontrar una coincidencia dominio/IP. Esto evitará que otros intenten pasar por usuarios locales para poder retransmitir correo a través de su servidor, pero ahorrará recursos al no comprobar mensajes que están dirigidos a sus usuarios. Si habilita tanto esta opción como la opción siguiente *La Protección protector de IP respeta los alias*, los mensajes a alias válidos también serán aceptados.

No aplicar Protección IP a sesiones autentificadas
Cuando se activa este control, las restricciones de la Protección IP no aplicarán a usuarios autentificados. Se aceptará correo de un usuario autentificado sin importar la dirección IP de la que se esté conectando. Más aun, cuando el usuario no se autentifica y se rechaza el acceso, el mensaje devuelto al cliente SMTP será "Autenticación requerida", a fin de darle al usuario una pista de que puede arreglar el problema configurando su cliente de correo para utilizar autenticación antes de enviar su mensaje. Esta opción está habilitada por omisión.

No aplicar Protección IP a IPs confiables

Cuando se activa este control, la Protección IP no se aplicará cuando la conexión venga de una Dirección IP confiable 519. Esta opción se habilita por omisión.

La Protección IP respeta los alias
Habilite esta opción si quiere que la Protección IP acepte alias de direcciones cuando compruebe las protecciones de dominio/IP. La Protección IP traducirá un alias a la verdadera cuenta a la que apunta y por lo tanto lo aceptará si pasa la comprobación. Sin esta opción habilitada, la Protección IP tratará cada alias como si fuera una dirección independiente de la cuenta a la que representa. Así,

si una dirección IP de un alias viola una Protección IP entonces el mensaje será rechazado. Esta opción se encuentra duplicada en la Pantalla de Ajustes 836 de los Alias — si cambia la configuración aquí, se verá también reflejada allí.

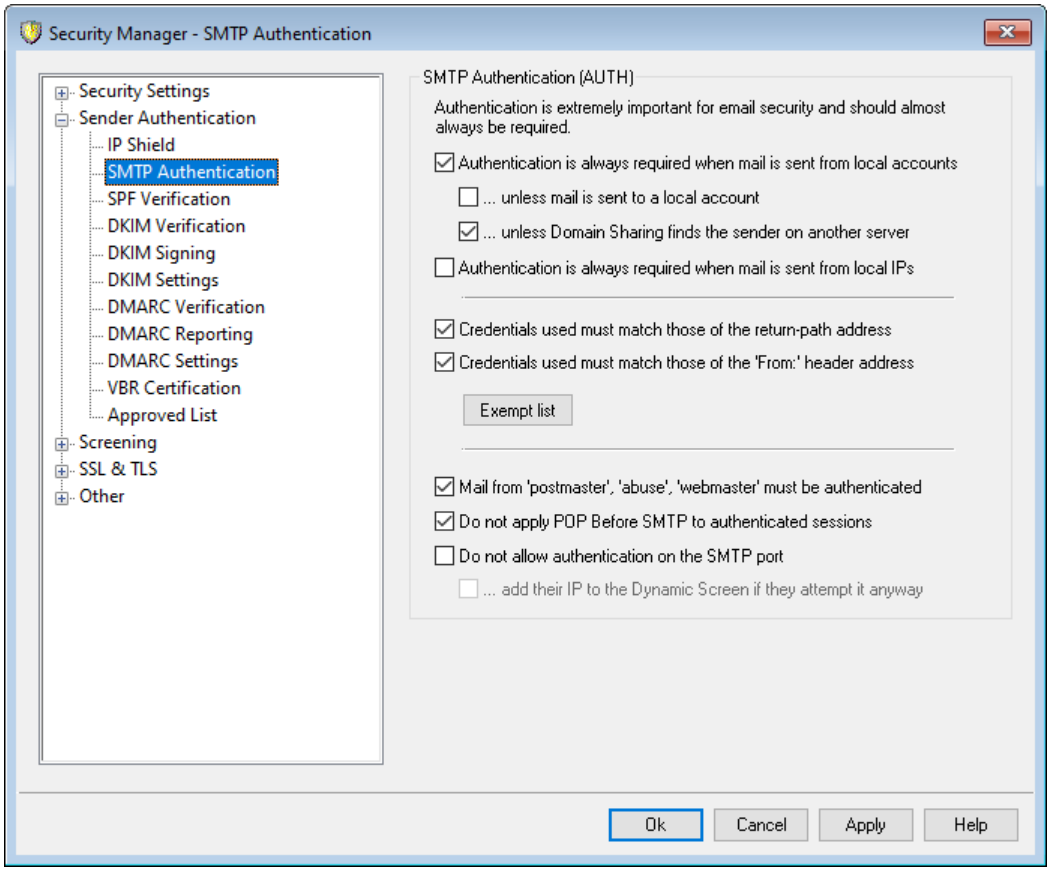
Si quiere que los mensajes entrantes dirigidos a alias válidos estén exentos de la Protección IP haga clic en esta opción y en *No aplicar Protección IP para mensajes enviados a usuarios locales no válidos*.

Verificar las direcciones en el campo FROM del encabezado con la Protección IP

Active esta casilla si desea que la Protección IP compare el campo FROM del encabezado en adición al valor del campo SMTP MAIL. Esta opción se encuentra deshabilitada por omisión.

Utilizar esta opción puede originar problemas con ciertos tipos de mensajes, tales como aquellos enviados a listas de distribución. Por esto, deberá habilitarla solamente si está seguro de que la necesita.

4.2.2.2 Autenticación de SMTP



Autenticación SMTP (AUTH)

La autenticación se requiere siempre cuando el correo es de cuentas locales
Cuando esta opción se activa y un mensaje entrante dice ser de uno de los dominios de MDaemon, la cuenta debe ser primero autenticada o MDaemon rechazará la aceptación de mensajes para el envío. Esta opción se encuentra habilitada por omisión.

...a menos que el mensaje sea para una cuenta local
Si requiere autenticación cuando un mensaje es de un remitente local, pero desea saltarse la restricción de autenticación cuando el destinatario también es local, entonces haga clic en esta opción. Nota: ello puede ser necesario en algunas situaciones donde se requiera a algunos usuarios que usen diferentes servidores de correo para el correo electrónico entrante y saliente.

...a menos que Dominios Compartidos encuentre el remitente en otro servidor
Por omisión, cuando Dominios Compartidos 123 encuentra al remitente en otro servidor, ese remitente estará exento de la opción mencionada arriba *Autentificación se requiere siempre...*. Deshabilite esta casilla si desea requerir autentificación también para esos remitentes.

La autenticación se requiere siempre cuando el correo se envía desde IPs locales
Habilite esta opción si desea requerir autenticación cuando un mensaje entrante es enviado desde direcciones IP locales. Si no está autentificado el mensaje será rechazado. Las IPs Confiables 520 están exentas y esta opción se habilita por omisión para instalaciones nuevas.

Las credenciales deben coincidir con las del valor de la dirección return-path
Por omisión, las credenciales utilizadas durante la autentificación SMTP deben coincidir con aquellas de la dirección encontradas en el campo return-path del mensaje. Deshabilite esta opción si no desea requerir que return-path coincida. Para soportar almacenamiento y reenvío de puertas de enlace, existe una opción correspondiente localizada en la pantalla Ajustes Globales de Puertas de Enlace 259 que define por omisión "*Exentar el correo de puerta de enlace de requerimientos de coincidencia en las credenciales AUTH*".

Las credenciales utilizadas deben coincidir el valor de la dirección en el encabezado 'From:'
Por omisión, las credenciales utilizadas durante la autentificación SMTP deben coincidir con aquellas en la dirección en el campo del encabezado "From:". Deshabilite esta opción si no desea requerir que coincida el encabezado "From:". Para soportar almacenamiento y reenvío de puertas de enlace, existe una opción correspondiente localizada en la pantalla Ajustes Globales de Puerta de Enlace 259 en la que se configura por omisión "*Exentar el correo de puerta de enlace de requerimientos de coincidencia en las credenciales AUTH*".

Lista de Exentos
Utilice la opción Credenciales que coinciden con la Lista de Exentos para exentar una dirección de las opciones "*Las credenciales deben coincidir...*" mencionada arriba. Para exentar de la opción "*...deben coincidir con el valor de la dirección return-path*", la dirección en la lista de exentos debe coincidir con la dirección en el campo **Return-Path** del mensaje. Para exentar la opción "*...debe coincidir con el valor de la dirección en el encabezado 'From:'* , la dirección exenta debe coincidir con el valor de la dirección en el encabezado **From:** del mensaje.

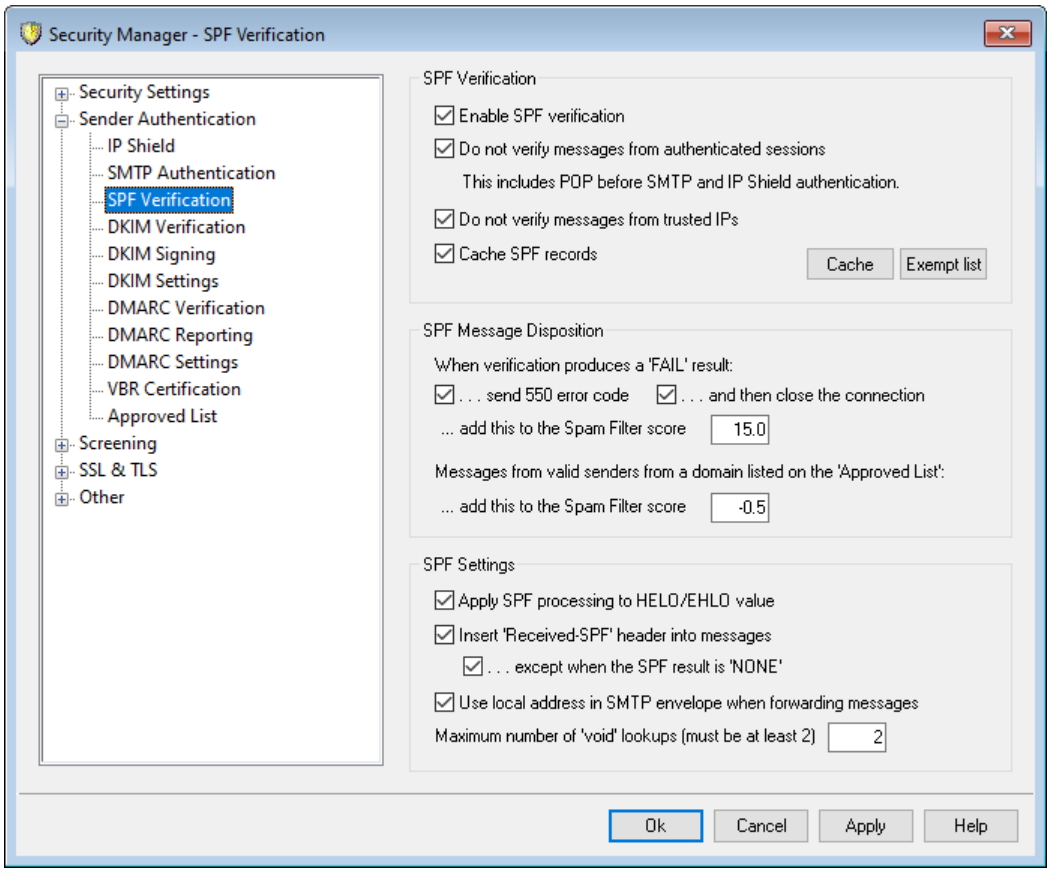
Correo de 'postmaster', 'abuse', 'webmaster' debe ser autentificado
Haga clic en esta casilla para requerir que los mensajes que digan ser de uno de los alias o cuentas "postmaster@...", "abuse@..." o "webmaster@..." , sean autentificados antes de que MDaemon los acepte. Los spammers y los hackers saben que dichas direcciones pueden existir y pueden por lo tanto intentar usar una de ellas para enviar correo a través de su sistema. Esta opción evitará que ellos y otros usuarios no autorizados puedan hacerlo. Esta opción está presente también en la Pantalla Ajustes 836 de los Alias. Si cambia esta configuración aquí, se cambiará también allá.

No aplicar POP antes de SMTP a las sesiones autenticadas
Si está utilizando la funcionalidad de seguridad POP antes de SMTP 518, puede hacer clic en esta opción para hacer que los usuarios autenticados estén exentos de esta restricción. Un usuario autenticado no necesitará comprobar su correo electrónico antes de enviar mensajes.

No permitir autentificación en el puerto SMTP
Esta opción deshabilita el soporte AUTH sobre el puerto SMTP. AUTH no se ofrecerá en la respuesta EHLO y será tratado como comando desconocido si lo proporciona el cliente SMTP. Este ajuste y la opción "*...agregar la dirección IP al Monitoreo Dinámico*" abajo son útiles en configuraciones donde todas las cuentas legítimas están utilizando el puerto MSA u otro puerto para enviar correo autentificado. En tales configuraciones el supuesto es que cualquier intento de autentificarse en el puerto SMTP debe provenir de un atacante.

...agregar la IP al Monitoreo Dinámico de todas formas si lo intentan
Al utilizar la opción *No permitir autentificación en el puerto SMTP* mencionada arriba, con este ajuste se agregará al Monitoreo Dinámico cualquier dirección IP de cualquier cliente que intente autentificarse en el puerto SMTP de todas formas. Así mismo la conexión se cerrará inmediatamente.

4.2.2.3 Verificación SPF



MDaemon soporta Sender Policy Framework (SPF) para ayudar a verificar los servidores de envío y proteger contra spoofing y phishing, que son dos tipos muy comunes de suplantación de correo en los que el remitente del mensaje intenta hacer que el mensaje parezca venir de alguien distinto.

Muchos dominios publican registros MX en los Servidores de Nombre de Dominio (DNS) para identificar las ubicaciones permitidas para recibir correo de ellos, pero eso no identifica a las ubicaciones permitidas para *enviar* correo de ellos. SPF es un método por el que los dominios pueden también publicar registros de remitente para

identificar dichas ubicaciones autorizadas a enviar mensajes. Realizando una búsqueda SPF en mensajes entrantes, MDaemon puede intentar determinar si el servidor remitente está autorizado o no a enviar correo para el supuesto dominio de envío y consecuentemente determinar si la dirección del remitente puede haber sido o no suplantada o burlada.

Use las opciones en esta pantalla para configurar las opciones SPF.

Para más información acerca de SPF, visite:

http://www.open-spf.org

Verificación SPF

Habilitar verificación SPF
Cuando esta opción está habilitada, MDaemon realizará consultas de datos SPF sobre el supuesto remitente de cada mensaje entrante, para asegurarse de que el servidor remitente tiene permitido enviar mensajes en su nombre. El host que MDaemon verificará se toma del valor `MAIL` que se obtiene durante el procesamiento SMTP. La verificación SPF se encuentra habilitada por omisión.

No verificar mensajes de sesiones autentificadas
Por omisión las conexiones autentificadas están exentas de consultas SPF. Las sesiones autentificadas incluyen aquellas verificadas vía Autentificación SMTP 523, POP antes de SMTP 518, o Protección de IP 521. Deshabilite esta opción si no desea exentar las sesiones autenticada de SPF.

No verificar mensajes de IPs de confianza
Active esta opción si quiere que las conexiones desde IPs de confianza 519 estén exentas de la verificación SPF.

Guardar en caché los resultados de la verificación
Por omisión, MDaemon guardará en caché temporalmente la política SPF de cada dominio obtenida durante la consulta a su DNS. Deshabilite la casilla si no desea guardar en caché las políticas SPF.

Caché
Este botón abre el caché SPF, que lista todos los registros SPF en caché en el momento.

Lista de Exentos
Haga clic en este botón para abrir la lista de excepciones de SPF en la que puede designar las direcciones IP, direcciones de correo y dominios que desea exentar de las búsquedas SPF. Las direcciones de correo se comparan contra el sobre SMTP, no contra el encabezado FROM del mensaje. Los Dominios se exentan colocando la palabra "spf" frente al nombre del dominio. MDaemon incluirá el registro SPF de ese dominio en todas las evaluaciones SPF utilizando una etiqueta "include:<domain>" especial de MDaemon. De esta forma puede hacer que su registro MX de respaldo sea tratado como una fuente SPF válida para todos los remitentes.

Manejo de mensajes SPF

Cuando la verificación produzca un resultado FAIL:

...Enviar código de error 550
Haga clic en esta casilla si quiere que se envíe un código de error 550 cuando el resultado de la consulta SPF es "Fail"

...y luego cerrar la conexión
Habilite esta opción si quiere que la conexión se cierre inmediatamente después de enviar el código de error 550.

...agregar al puntaje del Filtro de Spam
Especifique la cantidad que desea agregar al Puntaje de Spam del mensaje cuando falle la verificación SPF.

Mensajes de un remitente válido de un dominio en la 'Lista Aprobada'

...agregan la siguiente puntuación al Filtro de Spam
Especifique la cantidad que desea agregar a la puntuación de Spam de los mensajes cuando SPF confirme que se ha originado de un dominio encontrado en la Lista Aprobada 558.

Normalmente el valor especificado aquí debería ser un número negativo para que la puntuación de Spam se reduzca para los mensajes aprobados.

Ajustes SPF

Aplicar procesamiento SPF al valor HELO/EHLO
La opción aplica la verificación SPF al valor que pasa en el comando HELO o EHLO al inicio del proceso SMTP. Se encuentra habilitada por omisión.

Insertar encabezado 'Received-SPF' dentro de los mensajes
Haga clic en esta opción si quiere que un encabezado "Received-SPF" se inserte en cada mensaje.

...Excepto cuando el SPF resultante es 'NONE'
Habilite esta opción si no desea que el encabezado "Received-SPF" se inserte en el mensaje cuando el resultado de la consulta SPF sea "none".

Usar dirección local en el sobre SMTP cuando los mensajes sean reenviados
Habilite en esta opción si quiere que todo el correo reenviado por MDaemon utilice una dirección local en el sobre SMTP. Esto ayuda a reducir los problemas asociados con el reenvío. Normalmente los mensajes reenviados se envían usando una dirección de correo del remitente original y no la dirección de correo que hace realmente el reenvío. En algunas situaciones, utilizar una dirección de correo local puede ser necesario para prevenir al servidor de destino la identificación errónea del mensaje reenviado como una identidad "suplantada". Esta opción se encuentra habilitada por defecto.

Número máximo de consultas 'vacías' (debe ser por lo menos 2)
Este es el número máximo de consultas vacías permitido en una consulta SPF antes de que MDaemon genere un error permanente. Una consulta vacía es aquella que tiene por resultado 'el dominio no existe' o 'no hay respuestas'. Este valor debe ser por lo menos 2.

4.2.2.4 DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) es un sistema criptográfico de verificación de correo que puede ser utilizado para prevenir la suplantación (pretender ser la dirección de correo de otra persona para poder pasar por un remitente de mensaje distinto). Adicionalmente, dado que la mayoría de los mensajes de correo basura (Spam) contienen direcciones suplantadas, DKIM puede ayudar mucho en la reducción del Spam, aunque en las especificaciones originales no fuera diseñado como herramienta antispam. DKIM también puede usarse para asegurar la integridad de los mensajes entrantes o asegurar que el mensaje no ha sido manipulado entre la hora en la que dejó el servidor de correo firmante y la que llegó al suyo. En otras palabras, con la verificación criptográfica DKIM el servidor de destino puede saber con seguridad que el mensaje que llega proviene del servidor firmante y que nadie ha cambiado dicho mensaje en ningún modo.

Para poder asegurar la validez e integridad de los mensajes, DKIM utiliza un sistema de par de claves pública-privada. Una clave pública encriptada se publica en los registros de DNS del servidor de envío y luego cada mensaje saliente es firmado por el servidor usando la correspondiente clave privada. Para mensajes entrantes, cuando el servidor destino ve que el mensaje ha sido firmado, solicitará la clave pública de los registros DNS del servidor de envío y comparará dicha clave con la firma criptográfica del mensaje para determinar su validez. Si el mensaje entrante no puede ser verificado entonces el servidor destino sabe que contiene una dirección de correo suplantada y que ha sido manipulado o cambiado. Un mensaje fallido puede ser rechazado, o puede ser aceptado, pero se le puede ajustar la puntuación de Spam.

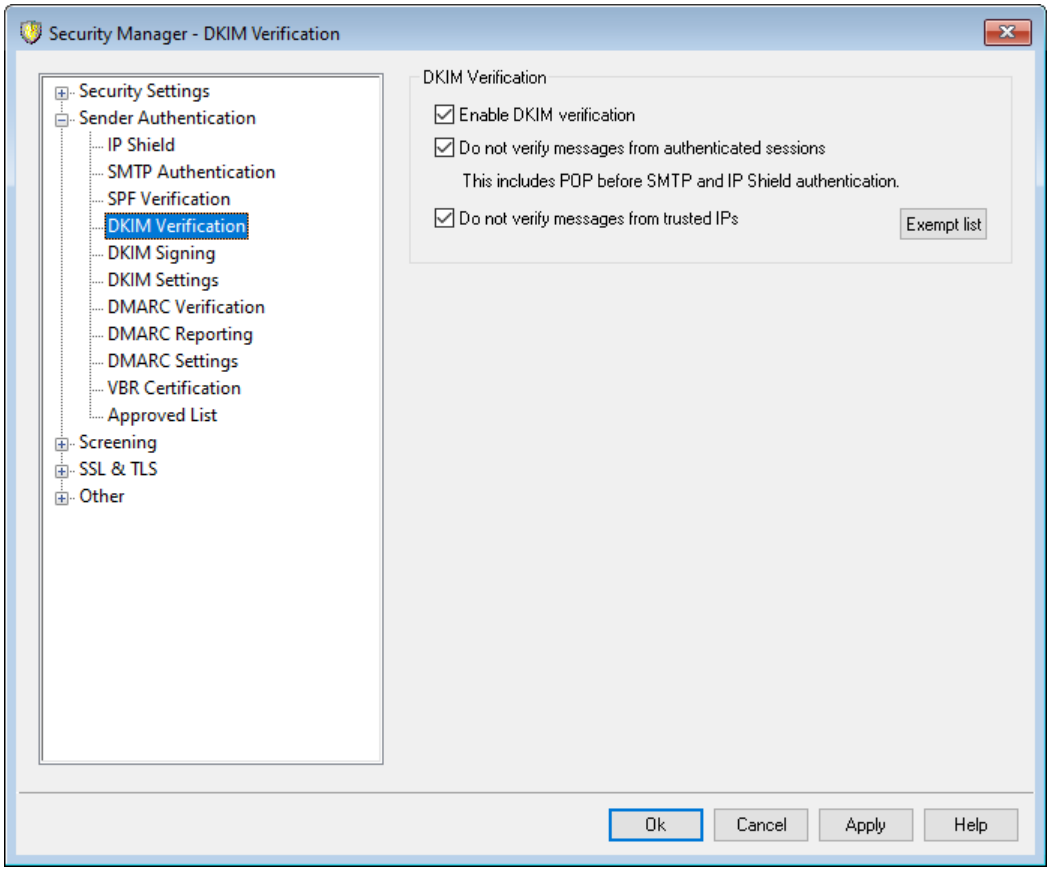
Para configurar MDaemon para que verifique los mensajes entrantes criptográficamente firmados, use las opciones que se indican en la pantalla de Verificación DKIM 530. Para configurar MDaemon para que firme los mensajes salientes, use las opciones que se dan en la pantalla Firma DKIM 532. Ambas están ubicadas bajo la sección Autenticación de Remitente del diálogo de Ajustes de Seguridad, en: Seguridad » Ajustes de Seguridad » Autenticación de Remitente. La interfaz principal 80 de MDaemon incluye una pestaña "DKIM" (ubicada bajo la pestaña Seguridad) que puede usarse para monitorear la actividad DK/DKIM en tiempo real, y puede registrar la actividad DKIM usando la opción en: Configurar » Configuración » Ajustes de Servidor » Logueo » Ajustes.

Ver:

Verificación DKIM 530
Firma DKIM 532
Ajustes DKIM 534

Para más acerca de DomainKeys Identified Mail, visite: http://www.dkim.org/.

4.2.2.4.1 Verificación DKIM



Use esta pantalla para configurar MDaemon para que verifique DomainKeys Identified Mail (DKIM) de los mensajes remotos entrantes. Cuando se habilita esta funcionalidad y un mensaje entrante ha sido criptográficamente firmado, MDaemon solicitará la clave pública del registro DNS del dominio de la firma y la usará para comprobar la firma DKIM y determinar su validez.

Si la firma pasa el test de verificación, el mensaje continuará al siguiente paso en el proceso normal de entrega. Adicionalmente, si el dominio extraído de la firma también aparece en la Lista Aprobada[558], la puntuación del Filtro de Spam recibirá un ajuste beneficioso.

Para más información sobre DKIM vea: http://www.dkim.org/

Verificación DKIM

Habilitar la verificación (DKIM)
Haga clic en esta opción para habilitar la verificación de DomainKeys Identified Mail para mensajes remotos entrantes.

No verificar mensajes de sesiones autentificadas
Haga clic en esta casilla si desea que las conexiones autenticadas estén exentas de las consultas SPF/Sender ID. Las sesiones autenticadas incluyen aquellas verificadas vía Autenticación SMTP[523], POP antes de SMTP[518], o la Protección IP[521].

No verificar mensajes de IPs confiables
Active esta opción si quiere que las conexiones desde IPs de confianza[519] estén exentas de la verificación criptográfica.

Lista de Exentos
Haga clic en este botón para abrir la lista de excepciones. Los mensajes que se originan de alguna dirección IP especificada en la lista no estarán sujetos a verificación criptográfica.

Encabezado Authentication-Results

Siempre que un mensaje se autentifica usando SMTP AUTH, SPF, DomainKeys Identified Mail o DMARC, MDaemon insertará la cabecera Authentication-Results en el mensaje, listando los resultados del proceso de autenticación. Si MDaemon está configurado para aceptar mensajes, aunque falle la autenticación, entonces el encabezado Authentication-Results contendrá un código que identificará la razón del fallo.

Se está realizando actualmente un trabajo vía la Internet Engineering Task Force (IETF) acerca de este encabezado y los protocolos de autenticación mencionados en esta sección. Puede encontrar más información en la página web de IETF, ubicada en: http://www.ietf.org/.

Encabezados DKIM en Mensajes de Lista de Distribución

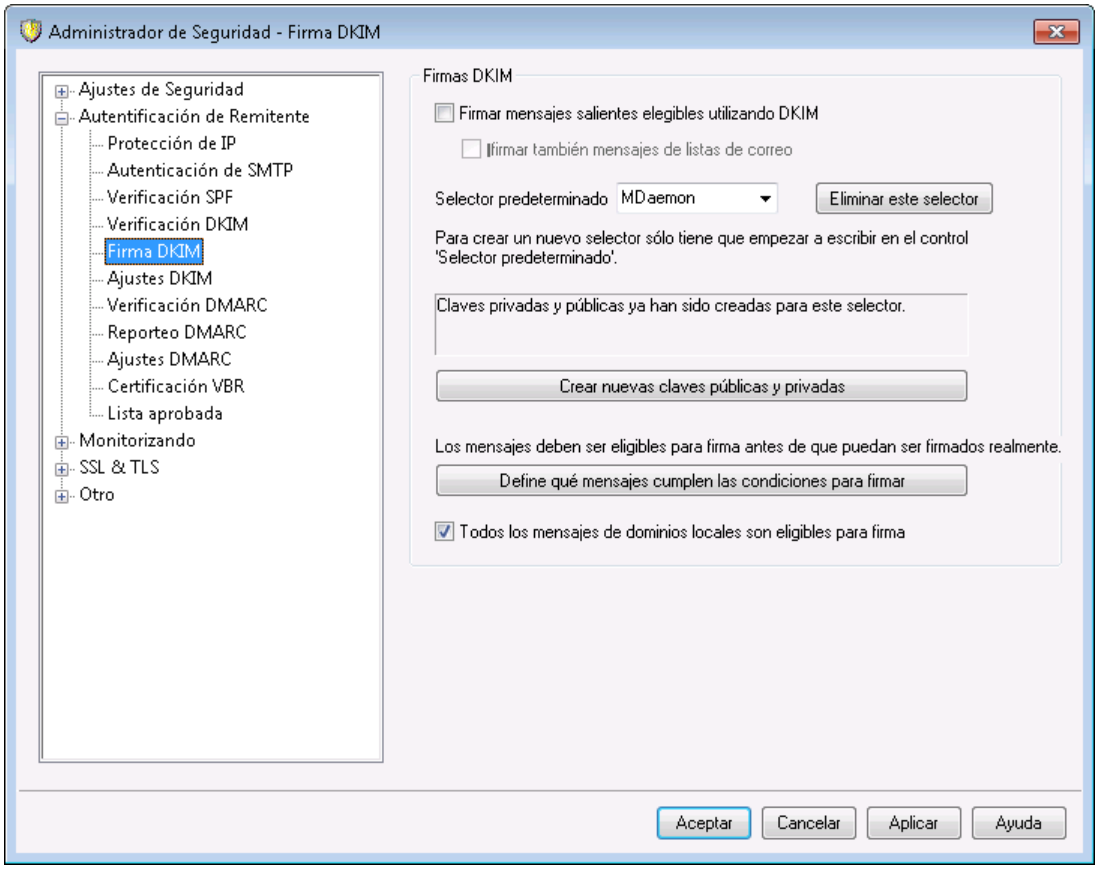
Por defecto, MDaemon segmenta las firmas DKIM de los mensajes entrantes de listas de distribución puesto que dichas firmas pueden ser rotas debido a los cambios que se les realiza a las cabeceras de mensaje durante el procesamiento de listas. Si desea que MDaemon deje las firmas en los mensajes de listas, puede configurarlo para que lo haga estableciendo manualmente la siguiente opción en el archivo `MDaemon.ini`:

```
[DomainKeys]
StripSigsFromListMail=No (por defecto es "Yes")
```

Ver:

DomainKeys Identified Mail[529]
Firma DKIM[532]
Ajustes DKIM[534]

4.2.2.4.2 Firma DKIM



Use las opciones contenidas en la pantalla Firma de DKIM para configurar MDaemon para que firme mensajes salientes elegibles utilizando DKIM y para definir los criterios que hacen esos mensajes elegibles. Puede usar también esta pantalla para designar selectores y generar las claves públicas y privadas correspondientes para usar con la especificación DKIM. Se crearán automáticamente al inicio un selector por defecto ("MDaemon") y una clave pública y privada por defecto. Todas las claves son únicas—nunca serán la misma de un sitio a otro, independientemente del selector aplicado. Por defecto, las claves se generan con un nivel de seguridad de 2048 bits.

Firma DKIM

Firmar los mensajes salientes elegibles utilizando DKIM
Haga clic en esta opción si desea que MDaemon utilice DomainKeys Identified Mail para firmar criptográficamente algunos de los mensajes salientes. Para que un mensaje sea firmado, debe cumplir los criterios designados bajo el botón de *Definir qué mensajes cumplen las condiciones para firma* y ser recibido por MDaemon para envío a través de una sesión autenticada. También existe la acción de Filtro de Contenido "*Sign with DKIM selector...*" que puede usar para hacer que los mensajes sean firmados.

...firmar mensajes de las listas de distribución
Haga clic en esta casilla si quiere firmar criptográficamente todos los mensajes salientes de las Listas de Distribución. Dado que MDaemon firmará todo el correo de todas las listas, no necesita usar la opción "*Definir qué mensajes cumplen las condiciones para firma*" para autorizarles la firma criptográfica.

Selector predeterminado
De la lista desplegable, escoja el selector cuya correspondiente pareja de claves pública/privada desee usar cuando firme los mensajes. Si desea crear un nuevo par de claves con un selector diferente, teclee el nombre de selector deseado y haga clic en "*Crear nuevas claves públicas y privadas*" siguiente. Si desea firmar los mensajes usando un selector alternativo, designe el selector específico bajo la opción "*Define qué mensajes cumplen las condiciones para firmar...*", o cree una regla de filtro de contenido utilizando la acción "*Sign with DKIM selector...*".

Eliminar este selector
Dé clic en este botón si desea eliminar un selector. Siga las instrucciones que aparecerán en la pantalla.

Crear nuevas claves públicas y privadas
Haga clic en este botón para generar una pareja de claves pública/privada para el selector arriba especificada. Se generará una pareja de claves pública/privada para el selector, y se generará y abrirá automáticamente el archivo `dns_readme.txt`. Este archivo contiene ejemplos de datos DKIM que necesitará para publicar sus registros DNS de dominio listando su política DKIM y la clave pública para el selector designado. El archivo lista ejemplos para los modos de prueba y normal, y para firmar todos los mensajes o sólo algunos que se originen en su dominio. Si está actualmente probando DKIM o este selector, necesitará usar la información contenida en las entradas de Testing para la Política o el selector, dependiendo de lo que esté probando. De otro modo necesitará usar las entradas de Not Testing.

Todas las claves se guardan en formato `PEM`, y todos los selectores y claves se almacenan bajo la carpeta `\MDaemon\Pem` de la siguiente manera

```
\MDaemon\Pem\<Selector>\rsa.public - clave pública para este
selector
\MDaemon\Pem\<Selector>\rsa.private - clave privada para este
selector
```

Los archivos contenidos en estas carpetas no están encriptados o escondidos, pero contienen claves de encriptación privada RSA que nunca deberían ser accedidas sin permiso. Deberá, por lo tanto, tomar medidas para asegurar estas carpetas y subcarpetas usando las herramientas de su sistema operativo.

Definir qué mensajes cumplen las condiciones para firma
Si ha elegido firmar los mensajes salientes elegibles, dé clic en este botón para editar el archivo `DKSign.dat`, que contiene la lista de dominios y direcciones que MDaemon usará para determinar si un mensaje debe o no ser firmado. Para cada dirección listada debe designar si el mensaje debe ser o no de la dirección en `To` o `From` para poder ser firmado, o puede designar algún otro encabezado tal como "`Reply-To`" o "`Sender`". Opcionalmente, puede designar un selector para cada entrada, que será usado cuando se firme un mensaje que coincida con dicha entrada. Finalmente, puede especificar un dominio de firma opcional que se use en la etiqueta "d=" dentro del encabezado de firma. Esto puede ser útil, por ejemplo, cuando tiene múltiples subdominios de firma. En dichos casos puede usar la etiqueta "d=" para indicarle a los servidores de destino que busquen las claves DKIM en un registro único de DNS y por lo tanto hacer posible que se

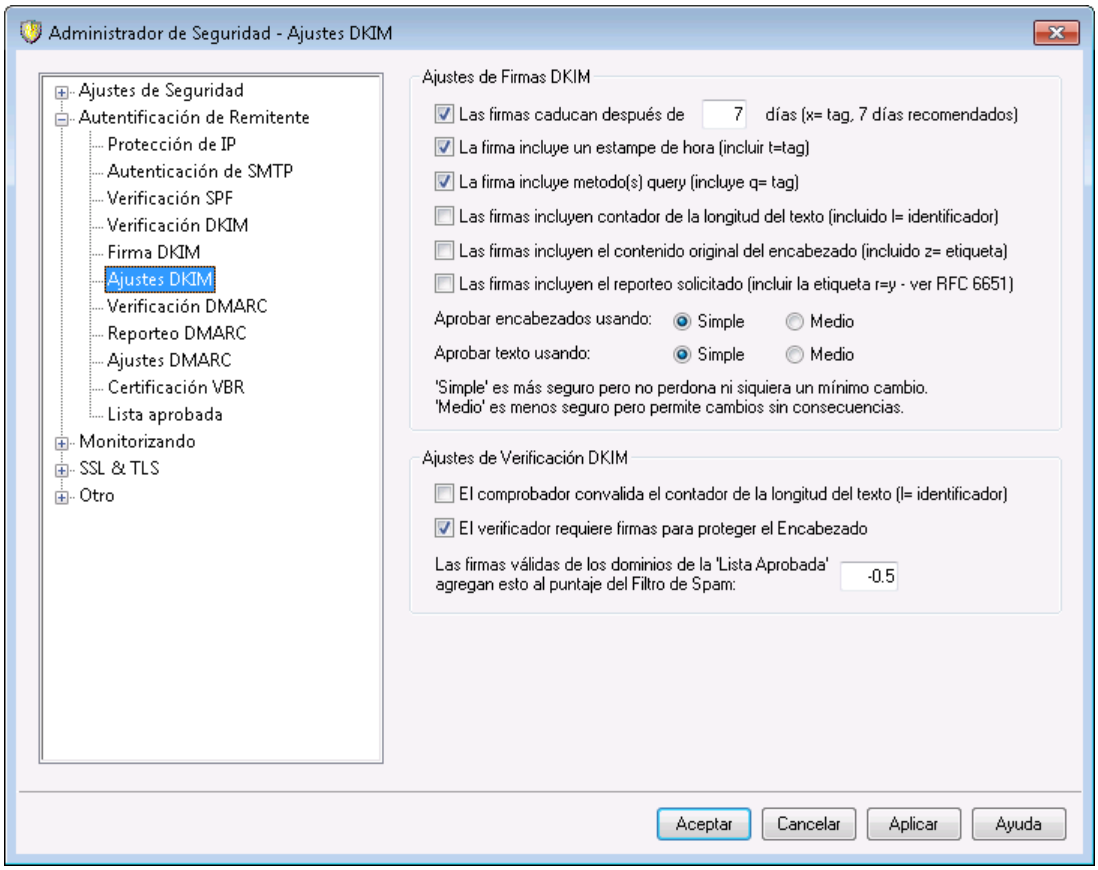
gestionen todas las claves en un registro en lugar de tener que gestionar registros separados para cada subdominio. Se permiten los comodines en los dominios y las direcciones.

Todos los mensajes de dominios locales son elegibles para firma
Use esta opción si desea hacer que todos los mensajes de los dominios locales sean elegibles para firma. Si usa esta opción entonces no necesita añadir ninguno de sus dominios locales a la lista de elegibilidad (el archivo `DKSign.dat`) a menos que quiera designar un selector específico o usar la etiqueta "d=" cuando se firmen correos específicos de un dominio. Esta opción está habilitada por defecto.

Ver:

DomainKeys Identified Mail 529
Ajustes DKIM 534
Verificación DKIM 530

4.2.2.4.3 Ajustes DKIM



Ajustes de firma DKIM

Las firmas caducan después de [XX] días (x= tag, 7 días recomendados)
Si desea limitar el número de días que una firma de DKIM puede considerarse válida, active esta opción para especificar el número de días deseado. Los mensajes con firmas expiradas siempre fallarán la verificación. Esta opción corresponde a la etiqueta "x=" de la firma. Esta opción está habilitada por defecto, con el valor establecido en 7 días.

La firma incluye una marca de hora de creación (incluir t=tag)
Cuando se habilita esta opción, el sello de hora de creación de la firma (etiqueta "t=") se incluirá en la firma. Está habilitado por defecto.

La firma incluye método(s) query (incluye q= tag)
Por defecto esta opción está habilitada. Hace que la firma incluya el método de consulta (p. ej. "q=dns").

Las firmas incluyen contador de la longitud del texto (incluido l= identificador)
Habilite esta opción si desea incluir una etiqueta contador de la longitud del mensaje en las firmas DKIM.

Las firmas incluyen el contenido original del encabezado (incluido z= etiqueta)
Haga clic en esta opción si desea incluir la etiqueta "z=" en la firma de DKIM. Esta etiqueta contendrá una copia de los encabezados originales del mensaje. Esto puede provocar unas firmas bastante grandes.

Las firmas incluyen los reportes solicitados (include r=y tag)
Habilite esta opción si desea incluir la etiqueta (tag) r=y en sus mensajes firmados. La presencia de esta etiqueta indica a los servidores destino que la soportan, que usted desea recibir reportes de falla AFRF cuando encuentren mensajes pretendiendo provenir de su dominio, pero que fallan la verificación DKIM. Sin embargo, para recibir esos reportes, también debe configurar el registro TXT de reporte DKIM en el DNS de su dominio. Ver RFC-6651: *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting*, para obtener información sobre la sintaxis e instrucciones sobre cómo hacerlo. Dado que esta opción requiere de cambios en el DNS, se encuentra deshabilitada por omisión.

Nombres Canónicos

El proceso de paso a nombres canónicos es en el que los encabezados y cuerpo del mensaje se convierten en nombres canónicos estándar y "normalizados" antes de crear la firma DKIM. Ello es necesario debido a que algunos servidores de correo y sistemas de retransmisión harán diversos cambios inconsecuentes al mensaje durante el proceso normal, los cuales podrían de otra forma romper la firma si no se usa una base canónica estándar para preparar cada mensaje antes de la firma. Actualmente existen dos procesos de transformación a canónico que son usados para la firma y verificación DKIM: el simple y el relajado. El simple es el método más estricto, que permite apenas ningún cambio en el mensaje. El relajado es más permisivo que el simple, y permite diversos cambios inconsecuentes.

Aprobar encabezados usando: Simple, Medio
Este es el método canónico usado para los encabezados del mensaje cuando se firma el mensaje. El método simple no permite cambios a los campos del encabezado en ninguna manera. El Relajado permite la conversión de nombres de

encabezado (no de sus valores) a letras minúsculas, conversión de uno o más espacios secuenciales en un sólo espacio, y otros cambios inocuos. La configuración por defecto es "Simple"

Aprobar texto usando: Simple, Medio
Este es el método canónico usado para el cuerpo del mensaje cuando se firma éste. El método simple ignora las líneas vacías al final del cuerpo del mensaje—no se permiten otros cambios al cuerpo. El Relajado permite líneas en blanco al final del mensaje, ignora los espacios al final de las líneas, reduce todas las secuencias de espacios en un único carácter de espacios, y otros cambios menores. La configuración por defecto es "Simple".

Ajustes de verificación DKIM

El verificador convalida el contador de la longitud del texto (l= identificador)
Cuando se habilite esta opción, MDaemon aprobará la etiqueta contador de longitud del cuerpo del mensaje cuando se encuentra en un mensaje entrante una firma de DKIM. Cuando la longitud real del cuerpo es mayor al valor contenido en esta etiqueta, MDaemon sólo verificará la cantidad especificada en la etiqueta — el resto del mensaje restará sin verificar. Esto indica que se le ha añadido algo al mensaje, y consecuentemente la porción no verificada podría ser considerada sospechosa. Cuando la longitud del cuerpo del mensaje es menor que el valor contenido en esta etiqueta, la firma no pasará la verificación (recibirá un resultado "`FAIL`"). Esto indica que alguna porción del mensaje fue eliminada, causando que la longitud del cuerpo sea menor que la cantidad especificada en esta etiqueta.

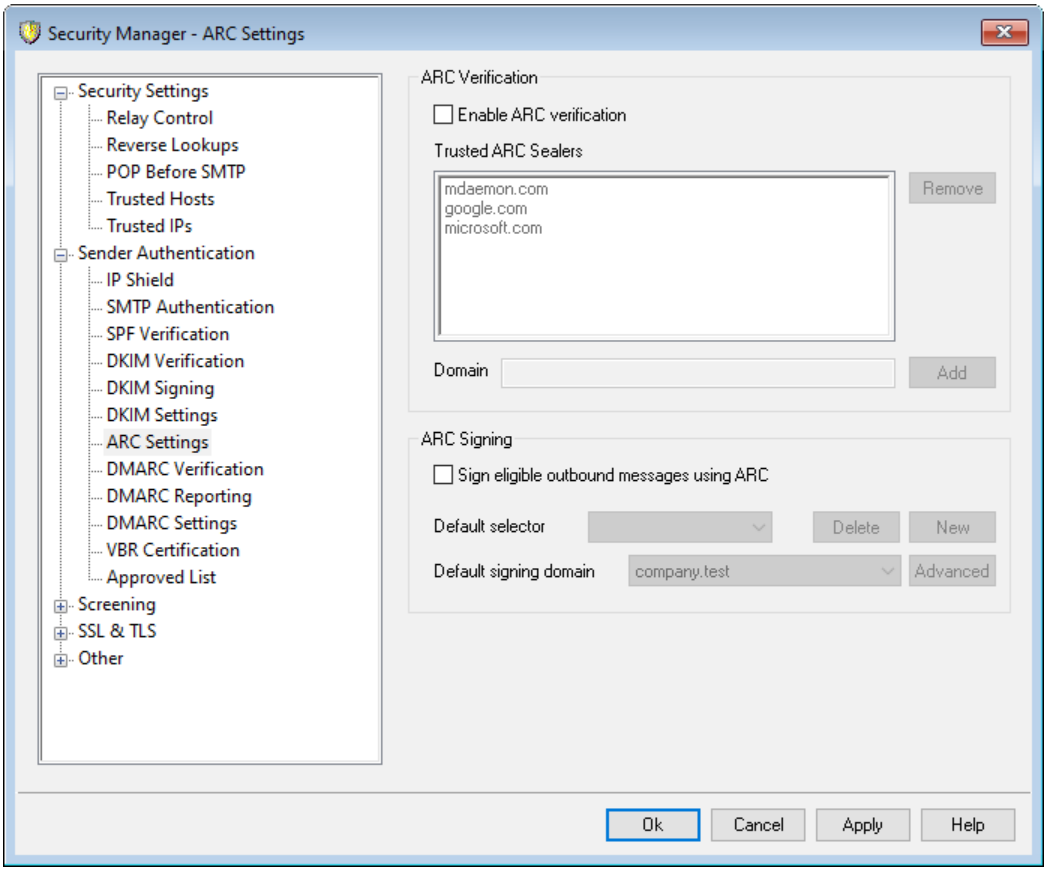
El verificador requiere firmas para proteger el Encabezado
Active esta opción si desea requerir que las firmas DKIM de los mensajes entrantes protejan el encabezado de Asunto.

Las firmas válidas de los dominios de la 'Lista Aprobada' agregan esta cantidad al puntaje del Filtro de Spam:
El valor especificado aquí se agregará al j del Filtro de Spam de cualquier mensaje DKIM firmado que reciba un resultado positivo cuando el dominio tomado de la firma aparece en la Lista Aprobada 558. Cuando la firma de un mensaje se verifica, pero el dominio no se encuentra en la Lista Aprobada, el puntaje del Filtro de Spam no se ajustará—la firma verificada no tendrá efecto en el puntaje. Sin embargo, el procesamiento normal y el puntaje del Filtro de Spam se aplicarán a ese mensaje.

Ver:

DomainKeys Identified Mail 529
Verificación DKIM 530
Firma DKIM 532

4.2.2.5 ARC Settings



Cadena Recibida Autenticada - Authenticated Received Chain (ARC) es un protocolo de autenticación de correo que permite a servidores de correo intermedios firmar los resultados de autenticación de un mensaje. Proporciona una "cadena de custodia" autenticada para un mensaje, permitiendo que cada servidor que maneja el mensaje vea qué servidores lo han procesado previamente y si se ha autenticado o no en cada paso. Cuando un servidor de correo ejecuta la Verificación DMARC 545 y encuentra que SPF 526 o DKIM 530 han fallado (debido por ejemplo a reenvíos o modificaciones de listas de distribución), puede consultar los resultados ARC de un servidor de confianza y utilizarlos para decidir si se acepta el mensaje.

Para más información sobre el protocolo ARC, vea : RFC 8617: The Authenticated Received Chain (ARC) Protocol.

Verificación ARC

Habilitar verificación ARC
Marque esta casilla para habilitar la verificación ARC.

Selladores ARC Confiables
Los Selladores ARC Confiables son los dominios en los que usted confía para consultar los resultados ARC. Los resultados ARC de dominios no confiables se ignoran al realizar la Verificación DMARC 545.

Firma ARC

Firmar mensajes salientes elegibles utilizando ARC
Los mensajes reenviados, mensajes de listas de distribución y de puertas de enlace con resultados de autenticación son elegibles para firmado ARC. La firma ARC requiere de un selector designado y el dominio firmante que se indica abajo.

Selector por omisión
Utilice esta opción para elegir el selector por omisión para utilizar en la firma ARC. Puede utilizar el mismo selector que utiliza para la Firma DKIM[532], o crear uno nuevo.

Dominio firmante por omisión
Elija el dominio por omisión para la firma ARC.

Avanzado
Si aloja múltiples dominios y desea utilizar un selector diferente o un dominio firmante distinto para cualquiera de ellos dé clic en **Avanzado** para hacer la configuración.

4.2.2.6 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) es una especificación diseñada para ayudar a reducir el abuso en el envío de mensajes de correo, tal como el Spam entrante y mensajes de phishing que simulan tener otros orígenes falsificando el encabezado `From:` del mensaje. DMARC hace posible a los propietarios de dominios utilizar el DNS (Domain Name System) para informar a los servidores receptores sobre su política DMARC, que consiste en la manera en que requieren que esos servidores manejen los mensajes que pretender ser enviados de sus dominios pero que no pueden ser autentificados como provenientes de ellos. Esta política, que se obtiene del servidor receptor vía consultas DNS al procesar el mensaje entrante, puede establecer que el servidor deberá poner en cuarentena o rechazar mensajes que no se cumplan con la política, o no ejecutar acción alguna (i.e. dejar que el mensaje proceda normalmente). Adicionalmente a la política, el registro DMARC en el DNS también puede contener peticiones al servidor para enviar reportes DMARC a algunos, describiendo el número de mensajes entrantes que pretendieron ser de su dominio y si pasaron o fallaron la autentificación, incluyendo detalles sobre los fallos. Las funcionalidades de reporteo de DMARC pueden ser útiles para determinar la efectividad de sus procedimientos de autentificación de correo y qué tan frecuentemente se utilizar su nombre de dominio para enviar mensajes falsificados.

Bajo la sección Autentificación de Remitente en el diálogo Ajustes de Seguridad, existen tres pantallas para configurar las funcionalidades DMARC de MDaemon, la verificación y reporteo: Verificación DMARC, Reporteo DMARC y Ajustes DMARC.

Verificación DMARC[545]

Como parte del proceso de verificación DMARC, MDaemon ejecuta una consulta DNS DMARC en el dominio encontrado en el encabezado `From:` de cada mensaje entrante. Esto se realiza para determinar si el dominio utiliza DMARC o no y si es así, para recuperar su registro DMARC DNS[540], que contiene su política y otra información relativa a DMARC. Adicionalmente, DMARC utiliza SPF[526] y DKIM[530] para validar cada mensaje y requiere que pase por lo menos esas pruebas a fin de pasar la verificación DMARC. Si el mensaje pasa entonces procederá normalmente por el resto de los procesos de entrega y filtrado de MDaemon. Sin embargo, si falla, el

destino del mensaje estará determinado por una combinación de la política DMARC del dominio y de la manera en que tenga configurado MDaemon para manejar esos mensajes.

Si el mensaje falla la verificación DMARC y el dominio DMARC tiene una política de "p=none" entonces no se ejecutará ninguna acción punitiva y continuará normalmente el procesamiento del mensaje. Alternativamente, cuando el dominio DMARC tiene una política restrictiva "p=quarantine" o "p=reject," MDaemon opcionalmente puede filtrar automáticamente el mensaje a la carpeta de Correo Basura del usuario destinatario. También puede decidir hacer que MDaemon rechace completamente el mensaje fallido cuando el dominio utiliza la política "p=reject". Adicionalmente, para mensajes fallidos con políticas restrictivas, MDaemon insertará un encabezado "X-MDDMARC-Fail-policy: quarantine" o "X-MDDMARC-Fail-policy: reject", dependiendo de la política. Esto le permite utilizar el Filtro de Contenido para ejecutar alguna acción basada en la presencia de esos encabezados, tal como enviar el mensaje a una carpeta específica para mayor escrutinio.

La Verificación DMARC se encuentra habilitada por omisión y es recomendada para la mayoría de las configuraciones de MDaemon.

Reporteo DMARC 548

Cuando MDaemon consulta un DNS buscando un registro DMARC, el registro puede contener etiquetas indicando que el propietario del dominio desea recibir reportes agregados o de falla respecto a los mensajes que pretenden provenir de su dominio. Las opciones en la pantalla Reporteo DMARC son para definir si usted está dispuesto o no a enviar los tipos de reporte requeridos y para especificar los metadatos que deben contener esos reportes. Los reportes agregados se envían diariamente a medianoche UTC y los reportes de falla se envían por mensaje, ya que cada incidente detona el reporte. Los reportes se envían siempre como archivos adjuntos de tipo XML y hay varias herramientas disponibles en línea para facilitar a los destinatarios la visualización de estos.

Por omisión, MDaemon no envía reportes agregados o de falla. Si está dispuesto a enviar cualquiera de los dos tipos de reporte, habilite la opción correspondiente en la pantalla Reporteo DMARC.

Ajustes DMARC 552

La pantalla Ajustes DMARC contiene varias opciones para incluir cierta información en los reportes DKIM, registros de bitácora DNS DMARC y para actualizar el archivo de Sufijo Público utilizado por MDaemon por DMARC.

Verificación DMARC y Listas de Distribución

Dado que el propósito de DMARC es asegurar que el dominio identificado en el encabezado From: de un mensaje, no haya sido falsificado, el servidor remitente debe tener permitido enviar mensajes en nombre de ese dominio. Esto puede convertirse en un problema único para listas de distribución, porque es común que las listas distribuyan mensajes en nombre de miembros de la lista provenientes de dominios externos dejando sin modificar el encabezado From:. Esto significa que cuando un servidor receptor intente utilizar la verificación DMARC en uno de esos mensajes, el mensaje habrá sido enviado por un servidor que no está afiliado oficialmente con el dominio del encabezado From:. Si sucede que el dominio DMARC está utilizando una política restrictiva, esto podría hacer que el mensaje entre en cuarentena o sea rechazado por el servidor receptor. En algunos casos esto podría

generar que el destinatario sea eliminado de la membresía de la lista. Para darle la vuelta a este problema, cuando MDaemon encuentra que están llegando mensajes para una lista provenientes de un dominio con una política DMARC restrictiva, MDaemon reemplazará el encabezado `From:` del mensaje con la dirección de la lista de correo. Alternativamente, usted puede configurar MDaemon para rechazar la aceptación de cualquier mensaje para una lista cuando provenga de un dominio con una política restrictiva. Esta última opción podría hacer imposible para un usuario de un dominio con una política restrictiva que envíe mensajes a la lista. La opción para reemplazar el encabezado `From:` se localiza en la pantalla Encabezados 286 del editor de listas de distribución. La opción para rechazar mensajes se localiza en la pantalla Ajustes 283.

Utilizando DMARC para sus dominios MDaemon

Si desea utilizar DMARC para uno de sus propios dominios, lo que significa que desea que lo servidores receptores de correo que soportan DMARC puedan utilizar DMARC para verificar los mensajes que pretender provenir de usted, entonces primero debe asegurarse de que ha creado registros SPF y DKIM en su DNS, correctamente formateados para ese dominio; debe tener por lo menos una de esas opciones funcionando correctamente para utilizar DMARC. Si utiliza DKIM, también debe configurar las opciones Firmas DKIM 532 en MDaemon para firmar los mensajes del dominio. Adicionalmente, debe crear un registro DNS DMARC para el dominio. Al consultar el DNS buscando este registro TXT especialmente formateado, el servidor receptor puede determinar su política DMARC y varios parámetros opcionales tales como: el modo de autentificación que usted utiliza, si desea o no recibir reportes agregados, la dirección de correo la que se deben enviar los reportes y otros.

Una vez que ha configurado correctamente DMARC y ha empezado a recibir reportes XML DMARC, existe una variedad de herramientas en línea disponibles para leer esos reportes y diagnosticar cualquier problema potencial. Para su conveniencia, también se tiene una herramienta de Reporteo DMARC colocada para usted en la carpeta \MDaemon\App\. Vea el archivo DMARCReporterReadMe.txt para instrucciones sobre su uso.

Definir un registro de recursos DMARC TXT

A continuación, se presenta una descripción general de los componentes más básicos utilizados comúnmente para construir un registro DMARC. Para información más detallada o para información sobre configuraciones más avanzadas, vea: www.dmarc.org.

Campo Propietario (Owner)

El campo Propietario (Owner) (también llamado "Name" o "left-hand") siempre debe ser **`_dmarc`**, o puede tomar la forma **`_dmarc.domain.name`** si desea especificar el dominio o subdominio al que aplica el registro.

Ejemplo:

Registro DMARC para el dominio **example.com**

```
_dmarc IN TXT "v=DMARC1;p=none"
```

Este registro aplicaría a mensajes provenientes de user@example.com o cualquier subdominio de example.com, como user@support.example.com, user@mail.support.example.com, y demás.

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```
Este registro solo aplicaría a mensajes provenientes de user@support.example.com, no a mensajes provenientes, por ejemplo, de user@example.com.

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
Este registro aplicaría a mensajes provenientes de: user@support.example.com, user@a.support.example.com, user@a.b.support.example.com y demás.

Etiquetas y Valores del Registro DMARC

Etiquetas Requeridas

Etiqueta (Tag)	Valor	Notas
v=	**DMARC1**	Esta es la etiqueta Version, que debe ser la primera etiqueta en la porción especifica de texto del registro DMARC. Aunque otros valores de etiquetas DMARC no son sensibles a mayúsculas, el valor de la etiqueta **v=** debe contener en mayúsculas el valor: **DMARC1**. Ejemplo: `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	Esta es la etiqueta Política, que debe ser la segunda etiqueta en el registro DMARC, después de la etiqueta **v=**. **p=none** significa que el servidor receptor no deberá ejecutar ninguna acción basado en los resultados de la consulta DMARC. Los mensajes que fallen esta verificación DMARC no deberán entrar en cuarentena o ser rechazados basados en esa falla. Pueden ser puestos en cuarentena o rechazados por otras razones, como por fallar las pruebas del filtro de Spam u otras verificaciones de seguridad no relacionadas con DMARC. Utilizar **p=none** en ocasiones se denomina "monitorear" o "modo monitoreo" porque puede utilizarlo con la etiqueta **rua=** para recibir reportes agregados de dominios receptores sobre sus mensajes, pero esos mensajes no serán penalizados por los dominios por no pasar la verificación DMARC. Esta es la política que debe utilizar hasta que haya probado a fondo su implementación DMARC y esté seguro de que está listo para avanzar hacia la política más restrictiva **p=quarantine**. **p=quarantine** es la política a utilizar cuando desea que otros servidores de correo traten un mensaje como sospechoso cuando su encabezado **From:** dice que proviene de usted, pero el mensaje falla la verificación DMARC. Dependiendo de la política local del servidor, esto podría significar que se sujete el mensaje a escrutinio adicional, colocándole en la carpeta de correo basura del destinatario, enrutándolo a un servidor diferente o ejecutando alguna otra acción.

		p=reject indica que desea que el servidor receptor rechace cualquier mensaje que falle la verificación DMARC. Algunos servidores, sin embargo, pueden aceptar estos mensajes pero ponerlos en cuarentena o sujetarlos a escrutinio adicional. Esta es la política más restrictiva y en general no debe ser utilizada a menos que esté completamente seguro de sus políticas de correo y los tipos de mensajes o servicios que desea permitir que utilicen sus cuentas. Por ejemplo, si desea permitir a sus usuarios unirse a listas de distribución de terceros, utilizar servicios de reenvío, utilizar funcionalidades "share this" en sitios web o similares, entonces al utilizar **p=reject** con certeza hará que se rechacen algunos mensajes legítimos. Esto podría causar también que algunos usuarios sean bloqueados o eliminados automáticamente de ciertas listas de correo. Ejemplo: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

Etiquetas Opcionales
Todas las etiquetas listadas abajo son opcionales. Cuando no se utiliza ninguna de ellas en un registro, se asumen los valores por omisión.

Etiqueta (Tag)	Valor	Notas
sp=	**none** **quarantine** **reject** — **Default:** Si no se utiliza **sp=** , la etiqueta **p=** aplica al dominio y subdominios.	Esta etiqueta es para especificar que se utilice una política para subdominios del domino al que aplica el registro DMARC. Por ejemplo, si esta etiqueta se utiliza en un registro que tiene alcance sobre example.com, entonces la política definida en la etiqueta **p=** aplicará a los mensajes provenientes de example.com y la política definida en la etiqueta **sp=** aplicará a los mensajes provenientes de subdominios de example.com, tales como mail.example.com. Si se omite del registro esta etiqueta, aplicará la etiqueta **p=** al dominio y subdominios. Ejemplo: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

rua=	Listas separadas por coma de direcciones de correo a las que se deben enviar reportes DMARC agregados. Las direcciones deben registrarse como URIs con la forma: **mailto:user@example.com**
	Default: none
	Si no se utiliza esta etiqueta, no se enviarán reportes agregados.
		Esta etiqueta indica que desea recibir reportes agregados DMARC de los servidores que reciben mensajes que pretenden provenir en su encabezado **From:** de un remitente de su dominio. Especifique una o más direcciones de correo tipo URIs de la forma: **mailto:user@example.com**, separando múltiples URIs con comas.
		Ejemplo:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`
		Ordinariamente estas direcciones se encontrarán en el dominio cubierto por este registro. Si desea enviar reportes a una dirección en algún otro dominio, entonces la zona DNS de ese dominio debe contener también un registro DMARC especial indicando que aceptará reportes DMARC del dominio.
		Registro ejemplo en example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		Registro requerido en example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

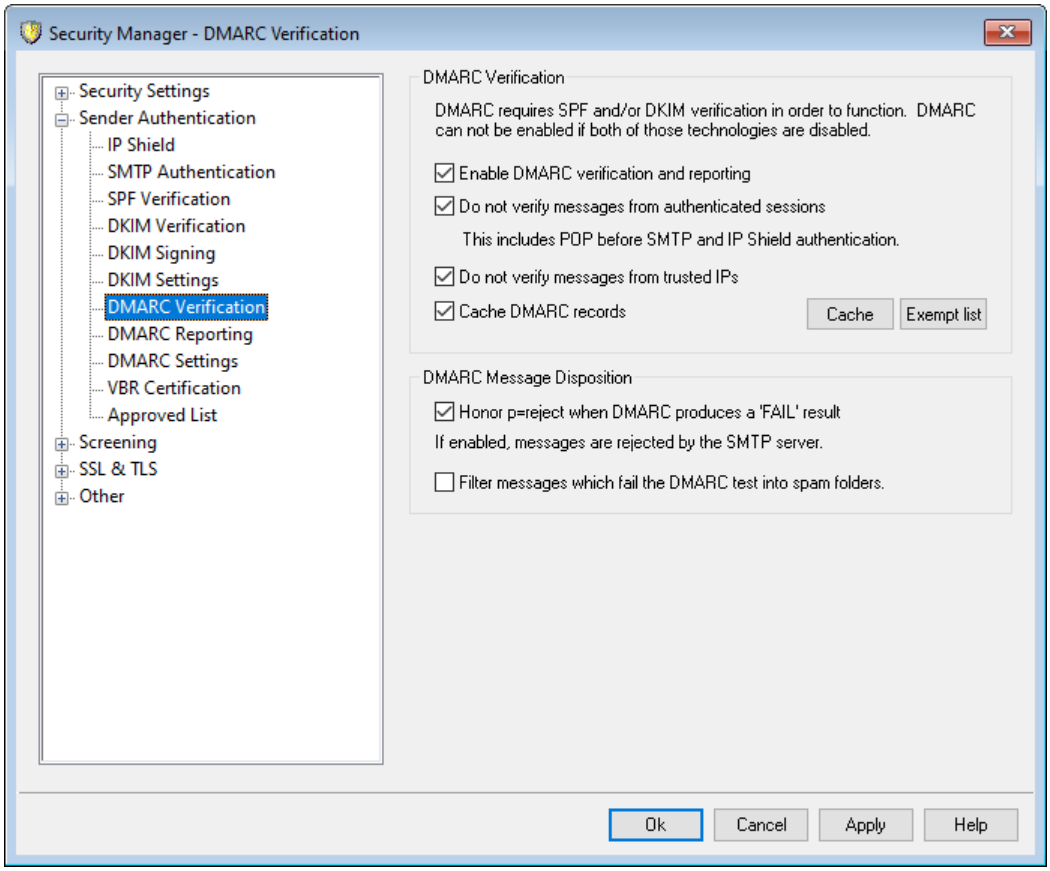
ruf=	Listas separadas por comas de direcciones de correo a las que se deben enviar los reportes de falla DMARC. Las direcciones deben ser registradas como URIs en la forma: **mailto:user@example.com** — **Default: none** Si no se utiliza esta etiqueta, no se enviarán reportes de falla.	Esta etiqueta indica que desea recibir reportes de falla de servidores que reciben mensajes que pretenden provenir de un remitente de su dominio de acuerdo con lo indicado en el encabezado **From:**, cuando las condiciones especificadas en la etiqueta **fo=** se han cumplido. Por omisión, cuando no se especifica etiqueta **fo=**, los reportes de falla se envían cando el mensaje falla todas las verificaciones DMARC, (i.e. falla tanto SPF como DKIM). Especifique una o más direcciones de correo como URIs de la forma: **mailto:user@example.com**, separando múltiples URIs con comas.
		
		Ejemplo:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		
		Ordinariamente estas direcciones se encontrarán en un dominio cubierto por este registro. Si desea enviar reportes a una dirección en algún otro dominio, entonces el archivo de zona DNS de ese dominio también debe contener un registro DMARC especial indicando que aceptará reportes DMARC para el dominio.
		
		Registro ejemplo en example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		
		Registro requerido en example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Para información más detallada sobre la especificación DMARC, ver: www.dmarc.org.

Ver:

Verificación DMARC 545
Reporteo DMARC 548
Ajustes DMARC 552
Listas de Distribución » Ajustes 283
Listas de Distribución » Encabezados 286

4.2.2.6.1 Verificación DMARC



.

Verificación DMARC

Habilitar la verificación y reporteo DMARC
Cuando se habilita esta opción, MDaemon ejecutará consultas DNS DMARC sobre el dominio encontrado en el encabezado `From:` de los mensajes entrantes y enviará reportes agregados y de falla si lo ha configurado para hacerlo en la pantalla Reporteo DMARC 548. DMARC utiliza SPF 526 y DKIM 530 para validar mensajes, por lo que al menos una de esas funcionalidades debe estar habilitada antes de que se utilice DMARC. La verificación y reporteo DMARC se encuentran habilitadas por omisión y deberán utilizarse en la mayoría de las configuraciones de MDaemon.

Al deshabilitar el soporte a DMARC, puede ser que permita un incremento en el ingreso de Spam, phishing y otros mensajes falsificados. También podría originar que algunos de los mensajes de sus listas de distribución sean rechazados por otros servidores y aun hacer que los miembros de la lista sean eliminados de ellas. No debe deshabilitar DMARC a menos que esté absolutamente seguro de que no lo necesita.

No verificar mensajes de sesiones autentificadas
Por omisión, MDaemon no ejecutará consultas DMARC en mensajes que son recibidos desde sesiones autentificadas. Estas sesiones incluyen aquellas verificadas por Autentificación SMTP 523, POP antes de SMTP 518, o Protección de IP 521.

No verificar mensajes enviados desde IPs de confianza
Por omisión, MDaemon no ejecutará consultas DMARC en mensajes que provienen de direcciones IP de confianza 520.

Guardar en Caché registros DMARC
Por omisión MDaemon no conservará un caché de los datos de los registros DMARC encontrados en la consulta del DNS. Al conservar temporalmente un caché, puede incrementar la eficiencia del sistema al procesar mensajes similares que lleguen en el futuro cercano desde el mismo dominio.

Cache
Este botón abre el caché DMARC, que enlista todos los registros DMARC en caché en ese momento.

Lista de Exentos
Dé clic en este botón para abrir la lista de exentos DMARC. Los mensajes provenientes de cualquier dirección IP especificada en esta lista no estarán sujetos a verificación DMARC.

La verificación DMARC también soporta la Certificación VBR 555 y la Lista Aprobada 558, que puede exentar con base en identificadores DKIM verificados y rutas SPF de fuentes confiables. Así que, por ejemplo, si un mensaje entrante falla la verificación DMARC, pero tiene una firma DKIM válida de un dominio en la Lista Aprobada, el mensaje no estará sujeto a la política punitiva DMARC (i.e. el mensaje es tratado como si la política fuera "p=none"). Lo mismo ocurre si la verificación de ruta SPF se encuentra un dominio de la Lista Aprobada.

Disposición de Mensajes DMARC

Respetar p=reject cuando DMARC produce un resultado 'FAIL'

Por omisión, esta opción está habilitada, lo que significa que MDaemon respetará la política DMARC `p=reject` cuando el encabezado `From:` de un dominio ha publicado esa política en su registro DMARC y los mensajes fallan la verificación DMARC. Los mensajes que fallen la verificación DMARC serán rechazados durante la sesión SMTP.

Cuando esta opción se encuentra deshabilitada y un mensaje falla la verificación DMARC, MDaemon insertará el encabezado "`X-MDDMARC-Fail-policy: reject`" en el mensaje en lugar de rechazarlo. En ese caso puede utilizar el Filtro de Contenido para ejecutar alguna acción basada en la presencia de ese encabezado, tal como enviar el mensaje a una carpeta específica para mayor escrutinio. Más aun, puede utilizar la opción *"Filtrar mensajes que fallen la prueba DMARC a la carpeta de correo basura",* opción que se describe abajo,

para hacer que el mensaje se coloque en la carpeta de correo basura del destinatario.

Aun si deja esta opción deshabilitada, el mensaje podría ser rechazado por alguna otra razón no relacionada con DMARC, tal como tener un Puntaje del Filtro de Spam 676 superior al umbral permitido.

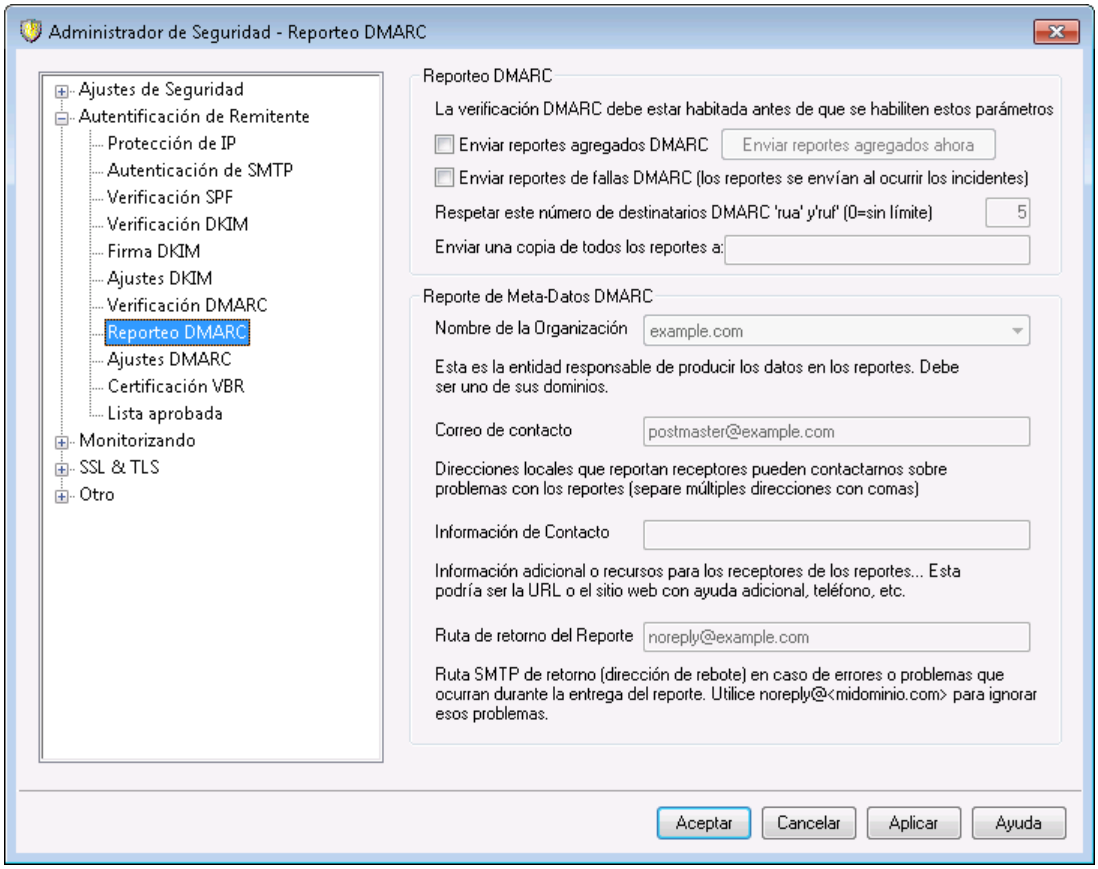
Filtrar los mensajes que fallen la prueba DMARC a la carpeta de correo basura
Habilite esta opción si desea filtrar automáticamente los mensajes hacia la carpeta de correo basura del destinatario, siempre que fallen la verificación DMARC. Si esta carpeta no existe aún para el usuario, MDaemon la creará cuando sea necesario.

Al habilitarse, esta opción solo se aplica al dominio en el From: que haya publicado una política DMARC restrictiva (i.e. p=quarantine o p=reject). Cuando el dominio publica una política p=none, indica que el dominio solo está monitoreando DMARC y no deberán tomarse medidas punitivas.

Ver:

DMARC 538
Reporteo DMARC 548
Ajustes DMARC 552
Listas de Distribución » Ajustes 283
Listas de Distribución » Encabezados 286
Lista Aprobada 558

4.2.2.6.2 Reporteo DMARC



Cuando MDaemon consulta los DNS respecto a un registro DMARC, el registro puede contener varias etiquetas indicando que el propietario del dominio desea recibir reportes DMARC referentes a mensajes que pretenden provenir de ese dominio. Las opciones en la pantalla Reporteo DMARC son para definir si usted desea o no enviar reportes DMARC agregados o de falla a aquellos dominios cuyos registros DMARC los soliciten y para especificar los metadatos que contendrán esos reportes. Las opciones en esta pantalla solo están disponibles cuando se habilita la opción "*Habilitar verificación y reporteo DMARC*" en la pantalla Verificación DMARC 545. Más aun, la especificación DMARC requiere el uso de STARTTLS 577 siempre que se ofrezca por los receptores de reportes. Por esto, deberá habilitar STARTTLS si esto es posible.

Reporteo DMARC

Enviar reportes agregados DMARC
Habilitar esta opción si está dispuesto a enviar reportes agregados DMARC a los dominios que lo soliciten. Cuando la consulta DMARC al DNS sobre el dominio en el encabezado `From:` de un mensaje entrante, indica que existe un registro DMARC que contiene la etiqueta "`rua=`" (ej. `rua=mailto:dmarc-reports@example.com`), significa que el propietario del dominio desea recibir reportes agregados DMARC. Entonces MDaemon almacenará la información relativa a DMARC sobre el dominio y los mensajes entrantes que pretenden provenir de él. Registrará las direcciones de correo a las que se deben enviar los reportes agregados, los métodos de verificación utilizados para cada mensaje (SPF, DKIM o ambos) y si el mensaje pasó o falló, el servidor remitente, su dirección IP, la política DMARC aplicada, etc. Entonces, cada día a medianoche UTC, MDaemon utilizará los datos almacenados para generar el reporte de cada dominio y enviarlo a las direcciones

determinadas. Una vez que se envían los reportes, los datos DMARC almacenados se depuran y MDaemon reiniciará el proceso de nuevo.

MDaemon no soporta la etiqueta de intervalo de reportes DMARC (i.e. "ri=") para reportes agregados. MDaemon enviará reportes agregados cada día a medianoche UTC a cualquier dominio para el que haya compilado datos DMARC desde la última ocasión en que se generaron y enviaron reportes DMARC.

Enviar reportes agregados ahora
Dé clic en este botón si desea generar y enviar un conjunto de reportes agregados de los datos DMARC almacenados en ese momento, en lugar de esperar a que MDaemon lo haga automáticamente en el siguiente evento a la medianoche UTC. Así se envían los reportes inmediatamente y se limpian los datos DMARC almacenados, exactamente como lo que sucede diariamente a medianoche UTC. MDaemon empezará a almacenar datos DMARC nuevamente hasta el siguiente evento de medianoche UTC o hasta que se dé clic de nuevo en el botón, lo que suceda primero.

Dado que MDaemon debe estar corriendo a medianoche UTC para enviar reportes agregados y limpiar automáticamente los datos almacenados DMARC, si MDaemon está detenido a esa hora, no se generarán reportes y los datos DMARC no se eliminarán. La recolección de datos DMARC continuará cuando MDaemon se vuelva a ejecutar, pero los reportes no se generarán y los datos no se depurarán hasta el siguiente evento de medianoche UTC o si se le das clic en el botón "*Enviar reportes agregados ahora*".

Enviar reportes de falla DMARC (los reportes se envían conforme ocurren los incidentes)
Habilite esta opción si está dispuesto a enviar reportes de falla DMARC a dominios que lo soliciten. Cuando la consulta DNS DMARC sobre el dominio del encabezado `From:` de un mensaje entrante indica que su registro DMARC contiene la etiqueta "`ruf=`" (vgr. `ruf=mailto:dmarc-failure@example.com`), significa que el dominio desea recibir reportes de falla DMARC. A diferencia de los reportes agregados, estos reportes se generan en tiempo real conforme ocurren los incidentes que los detonan y contienen datos detallados referentes a cada incidente y los errores que originaron la falla. Estos reportes se pueden utilizar para análisis forense por el administrador del dominio para corregir problemas con la configuración de su sistema de correo o para identificar otros problemas tales como ataques de phishing.

El tipo de falla que detonará un reporte de falla depende del valor de la etiqueta "`fo=`" tag en el registro DMARC del dominio. Por omisión un reporte de falla solo se generará si todas las verificaciones DMARC subyacentes fallan (i.e. que fallen tanto SPF como DKIM), pero los dominios pueden utilizar varios valores de etiqueta "`fo=`" para indicar que desean recibir reportes solo de fallas SPF, solo de fallas DKIM, falla de ambos o alguna otra combinación. Consecuentemente, es posible que se generen múltiples reportes de falla de un único mensaje dependiendo del número de destinatarios en la etiqueta "`ruf=`" del registro

DMARC y del número de fallas de autentificación independientes que se encuentren en un mensaje durante el procesamiento. Si desea limitar el número de destinatarios a los que MDaemon enviará cualquier reporte dado, utilice la opción "*Respetar hasta este número de destinatarios DMARC 'rua' y 'ruf'* " descrita abajo.

Para el formato de reporte, MDaemon respetará la etiqueta `rf=afrf` (Authentication Failure Reporting Using the Abuse Reporting Format), que es el valor por omisión DMARC. Todos los reportes se envían con este formato, aun si el registro DMARC de un dominio contiene la etiqueta `rf=iodef` tag.

A fin de soportar el reporte de fallas DMARC, MDaemon soporta completamente: RFC 5965: An Extensible Format for Email Feedback Reports, RFC 6591: Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6652: Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format, RFC 6651: Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting, y RFC 6692: Source Ports in Abuse Reporting Format (ARF) Reports.

Cuando la etiqueta DMARC "`fo=`" solicita reportes de fallas relativas a SPF, MDaemon envía reportes de fallas SPF de acuerdo con la RFC 6522. Por esto, las extensiones de esa especificación deben estar presentes en el registro SPF del dominio. Los reportes de falla SPF no se envían independientemente del procesamiento DMARC o en la ausencia de las extensiones de la RFC 6522.

Cuando una etiqueta DMARC "`fo=`" solicita reportes de fallas DKIM, MDaemon envía reportes de fallas DKIM de acuerdo con la RFC 6651. Por esto, las extensiones de esa especificación deben estar presentes en el campo DKIM-Signature del encabezado y el dominio debe publicar un registro TXT de reporte DKIM en su DNS. Los reportes de falla DKIM no se envían independientemente del procesamiento DMARC o en la ausencia de las extensiones de la RFC 6651.

Respetar hasta este número de destinatarios DMARC 'rua' y 'ruf' (0 = sin límite)
Si desea limitar el número de destinatarios a los que MDaemon enviará cualquier reporte agregado DMARC o reporte de falla DMARC, especifique el número máximo aquí. Si la etiqueta "`rua=`" o "`ruf=`" de un registro DMARC contiene más direcciones de su límite definido, entonces MDaemon enviará el reporte dado a las direcciones enlistadas, en orden, hasta que se alcance el número máximo de direcciones. Por omisión no se establece límite.

Enviar por correo una copia de todos los reportes a:
Registre aquí una o más direcciones de correo separadas por coma para enviarles una copia de todos los reportes DMARC agregados o de fallas (fo=0 o fo=1 solamente).

MetaDatos de los Reportes DMARC

Utilice estas opciones para especificar los metadatos de su empresa u organización, que serán incluidos en los reportes DMARC que envíe.

Nombre de la Organización
Esta es la entidad responsable de producir los reportes DMARC. Debe ser uno de sus dominios de MDaemon. Seleccione el dominio de la lista desplegable.

Correo de Contacto
Utilice esta opción para especificar las direcciones de correo locales que los destinatarios de reportes pueden contactar sobre problemas con los mismos. Separe múltiples direcciones con coma.

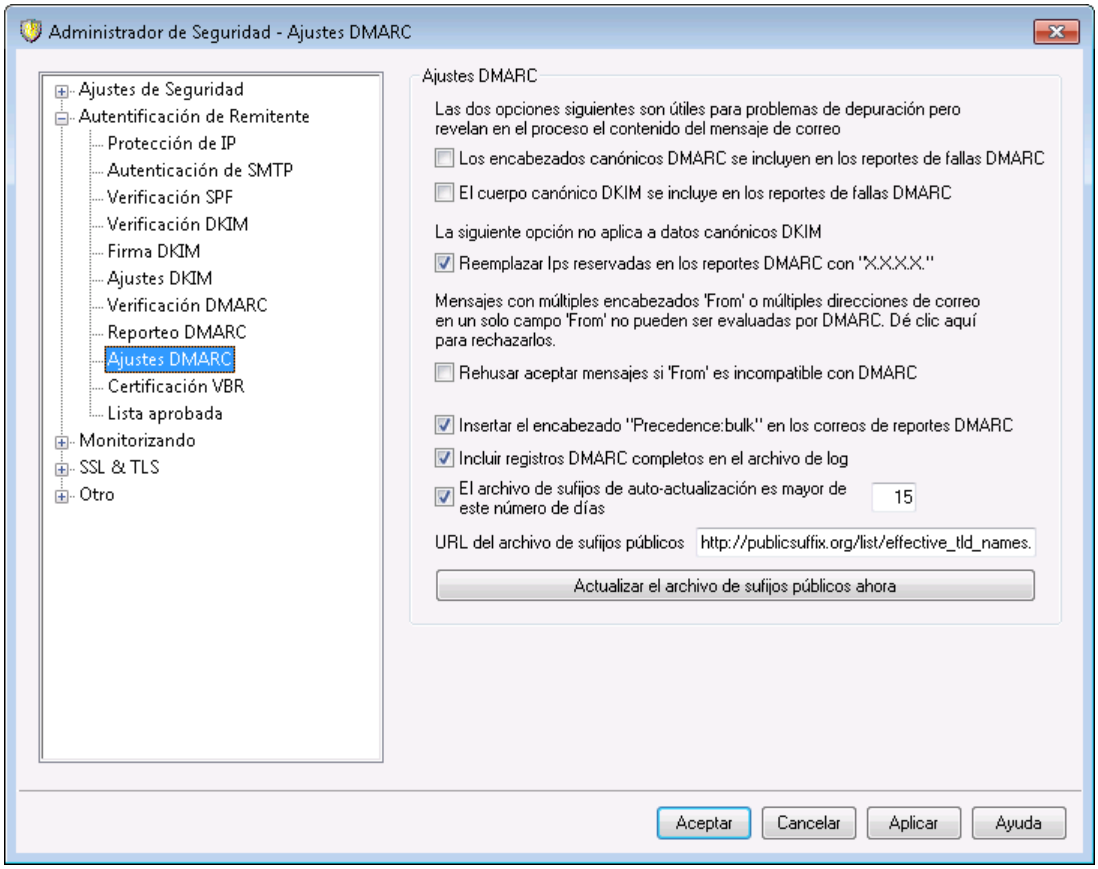
Información de Contacto
Utilice esta opción para incluir cualquier información adicional de contacto para los destinatarios de los reportes, tal como el sitio web, número de teléfono, etc.

Ruta de retorno del Reporte
Esta es la ruta de retorno SMTP (bounce address) utilizada por los mensajes de reportes que envía MDaemon, en caso de que existan problemas de envío. Utilice `noreply@<mydomain.com>` para ignorar esos problemas.

Ver:

DMARC 538
Verificación DMARC 545
Ajustes DMARC 552

4.2.2.6.3 Opciones DMARC



Ajustes DMARC

Incluir encabezados canónicos DKIM en los reportes de falla DMARC
Habilite esta opción si desea incluir encabezados canónicos 534 en los reportes de falla 548 DMARC. Esta opción está deshabilitada por omisión.

Incluir el cuerpo canónico DKIM en los reportes de falla DMARC
Habilite esta opción si desea incluir el cuerpo canónico 534 DKIM en los reportes de falla 548 DMARC. Esta opción está deshabilitada por omisión.

Reemplazar IPs reservadas con "X.X.X.X" en los reportes DMARC
Por omisión, MDaemon reemplaza sus direcciones IP reservadas en los reportes DMARC con "X.X.X.X". Deshabilite esta opción si desea hacer visibles sus IPs reservadas en los reportes DMARC. Esta opción no aplica a los datos canónicos DKIM.

Rechazar la aceptación de mensajes si 'From' es incompatible con DMARC
Habilite esta opción si desea rechazar mensajes que sean incompatibles con los requerimientos DMARC en referencia a la construcción del encabezado 'From'. Estos son mensajes con múltiples encabezados 'From' o múltiples direcciones de correo en un solo encabezado 'From'. Tales mensajes en este momento están exentos del procesamiento DMARC. Este ajuste se encuentra deshabilitado por omisión por qué tener múltiples direcciones en un solo encabezado 'From' no es técnicamente una violación de protocolo, pero habilitar este ajuste le ayudará a maximizar la protección DMARC. Este ajuste solo se aplica cuando se encuentra habilitada la Verificación DMARC 545.

Insertar el encabezado "Precedence: bulk" en los mensajes de reporte DMARC
Por omisión MDaemon insertará un encabezado "bulk" en los mensajes de reportes DMARC. Deshabilite esta casilla si no desea que se inserte ese encabezado.

Incluir los registros DMARC completos en el archivo de registro
Por omisión, MDaemon graba los registros completos que obtiene durante las consultas DNS DMARC. Deshabilite esta opción si no desea incluir el registro DMARC completo en el archivo de registro.

Actualizar automáticamente el archivo público de sufijos si es mayor que este número de días
DMARC requiere un archivo público de sufijos para determinar confiablemente los dominios correctos a consultar para los registros DNS DMARC. Por omisión MDaemon actualizará en automático su archivo almacenado de sufijos públicos siempre que exceda de 15 días. Modifique el valor de esta opción si desea actualizar el archivo de sufijos públicos con mayor o menor frecuencia. Deshabilite esta opción si no desea actualizarlo automáticamente.

URL del archivo Público de Sufijos
Esta es la URL del archivo público de sufijos que MDaemon descargará para uso con DMARC. Por omisión MDaemon utiliza el archivo localizado en: http://publicsuffix.org/list/effective_tld_names.dat.

Actualizar el archivo público de sufijos ahora
De clic en este botón para actualizar manualmente el archivo público de sufijos desde la *URL del archivo Público de Sufijos* especificada arriba.

Ver:

DMARC 538
Verificación DMARC 545
Reportes DMARC 548
Ajustes DKIM 534

4.2.2.7 Certificación de Mensajes

La certificación de mensajes es un proceso por el cual una entidad emite un cupón o "certifica" la buena conducta de correo de otra entidad. Consecuentemente, cuando esta entidad certificadora es una en la que los servidores de correo confían, los mensajes enviados de un dominio certificado por dicha entidad podrán ser visualizados con menos sospecha. Así pues, el servidor de recepción puede estar razonablemente seguro de que el dominio de envío se adhiere a un conjunto de buenas prácticas de correo y no envía Spam u otros mensajes problemáticos. La certificación es beneficiosa porque ayuda a asegurar que los mensajes no serán errónea o innecesariamente etiquetados por el análisis de Spam que no ofrece garantías. También ayuda a disminuir los recursos requeridos para procesar cada mensaje.

MDaemon soporta la Certificación de Mensajes a través del protocolo de correo "Vouch-By-Reference" o Aval por Referencia (VBR), que MDaemon Technologies ayudó a crear a través de su participación en el Domain Assurance Council (DAC). VBR proporciona un mecanismo a través del cual los Proveedores de Servicios de Certificación (CSP) o "certificadores" avalan las buenas prácticas de correo de dominios específicos.

Certificar Mensajes Entrantes

Es fácil configurar la funcionalidad de Certificación de Mensajes de MDaemon para comprobar los mensajes entrantes. Todo lo que tiene que hacer es hacer clic en la opción *Habilitar la certificación para mensajes entrantes* en el diálogo Certificación VBR (Seguridad » Ajustes de Seguridad » Autenticación de Remitente » Certificación VBR) e incluir uno o más proveedores de certificación en los que confía para certificar los mensajes entrantes (e.g. `vbr.example.com`). También puede escoger hacer exentos del filtro de Spam a los mensajes certificados o dar a sus puntuaciones de Filtro de Spam un ajuste beneficioso.

Certificar Mensajes Salientes

Antes de que pueda configurar MDaemon para insertar datos de certificación en los mensajes salientes, primero necesitará establecer uno o más CSPs que certifiquen su correo.

Para configurar su servidor MDaemon para que use la Certificación de Mensajes con su correo saliente, después de haberse registrado con un CSP:

1. Abra el diálogo de Certificación VBR: haga clic en Seguridad » Ajustes de Seguridad » Autenticación de Remitente » Certificación VBR.
2. Haga clic en "*Insertar datos de certificación en los mensajes salientes*."
3. Haga clic en "*Configurar un dominio para la certificación de mensajes*." Esto abre el diálogo de configuración de Certificación.
4. Escriba el *nombre de dominio* cuyos mensajes salientes vayan a contener los datos de certificación.
5. Use la lista desplegable *Tipo de Correo* para escoger el tipo de correo para el que su CSP está de acuerdo con certificar para este dominio, o introduzca un nuevo tipo si el tipo deseado no está en la lista.
6. Introduzca uno o más CSPs que certificarán el correo saliente del dominio. Si tiene más de un CSP use espacios para separarlos entre ellos.
7. Haga clic en "*Aceptar*."
8. Configure su servidor para firmar los mensajes salientes de dominio con DKIM 529, o asegúrese de que están siendo enviados desde un servidor aprobado por SPF 526. Ello es necesario para garantizar que el mensaje se origina desde usted. Un mensaje no puede estar certificado a menos que el servidor de recepción pueda determinar primero si el mensaje es auténtico.

VBR no requiere que los mensajes certificados sean transmitidos por o a su CSP. El CSP no firma o valida mensajes específicos—certifica las buenas prácticas de correo del dominio.

Especificación VBR - RFC 5518:

http://tools.ietf.org/html/rfc5518

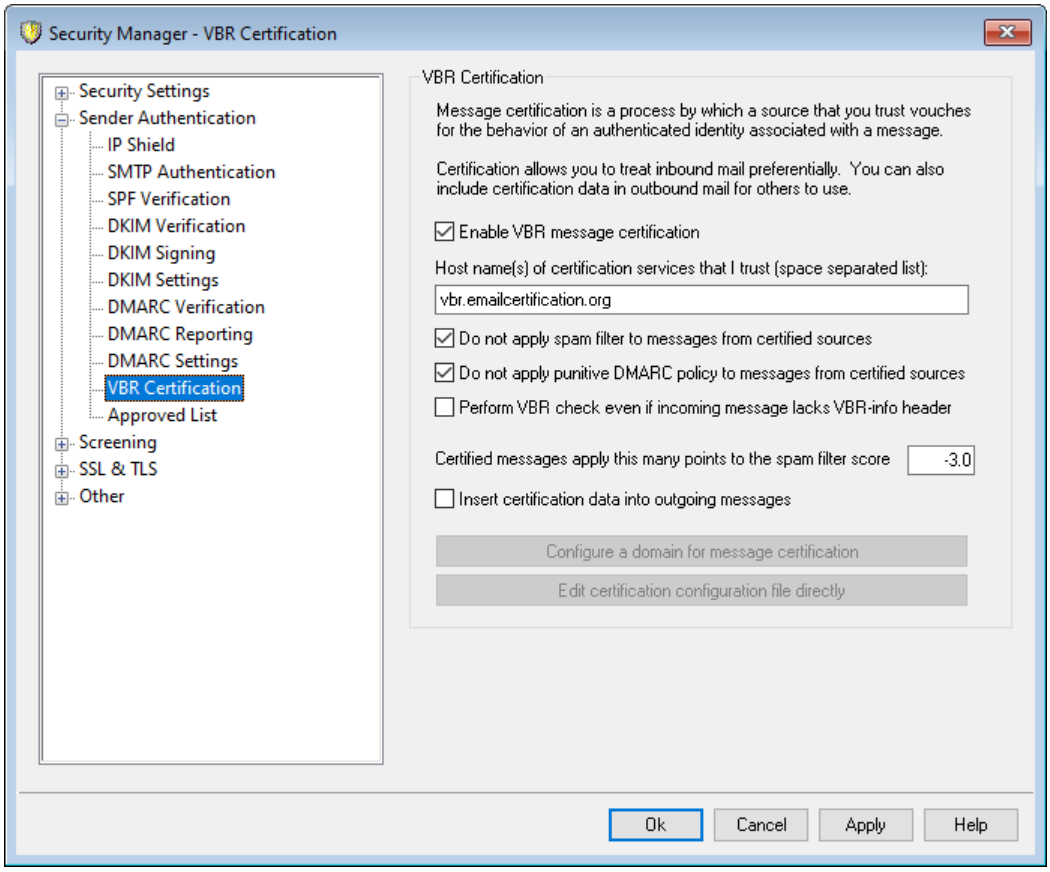
Para más información acerca de DKIM visite:

http://www.dkim.org/

Ver:

Certificación VBR 555

4.2.2.7.1 Certificación VBR



El diálogo de Certificación VBR está ubicado en: Seguridad » Ajustes de Seguridad » Autenticación de Remitente » Certificación VBR.

Certificación VBR

Habilitar Certificación VBR de mensajes
Haga clic en esta casilla para habilitar la certificación de los mensajes entrantes. Cuando MDaemon recibe un mensaje entrante que necesita certificación, consultará al proveedor confiable de servicios de certificación (Certification Service Provider - CSP) para confirmar si el mensaje debe ser o no considerado "certificado". Si es así, entonces el mensaje o bien estará exento del filtrado de Spam o bien tendrá ajustada la puntuación del Filtro de Spam 675, dependiendo de la opción que haya seleccionado a continuación.

Nombre de Host(s) de servicios de certificación en los que confío (lista separada mediante espacios):
Use este cuadro para introducir los nombres de host de los servicios de certificación en los que confía. Si confía en múltiples servicios, entonces separe cada uno con un espacio.

No aplicar filtro de Spam a los mensajes de fuentes certificadas
Escoja esta opción si desea que los mensajes de fuentes certificadas estén exentos de Filtro de Spam.

No aplicar políticas DMARC punitivas a los mensajes de fuentes certificadas
Esta opción asegura que los mensajes verificados de fuentes certificadas no serán penalizados si el dominio remitente publica una política DMARC 545 (ej. p=quarantine o p=reject) y el mensaje falla la verificación DMARC. Esta opción se encuentra habilitada por omisión.

Ejecutar una verificación VBR aun si el mensaje entrante carece de encabezado con información VBR
Habilite esta opción si dese ejecutar verificaciones VBR aun cuando los mensajes entrantes carezcan del encabezado con información VBR. Normalmente este encabezado es necesario, pero VBR puede funcionar sin él. Cuando falte el encabezado MDaemon consultará sus CSP confiables utilizando el tipo de correo "all". Esta opción se encuentra deshabilitada por omisión.

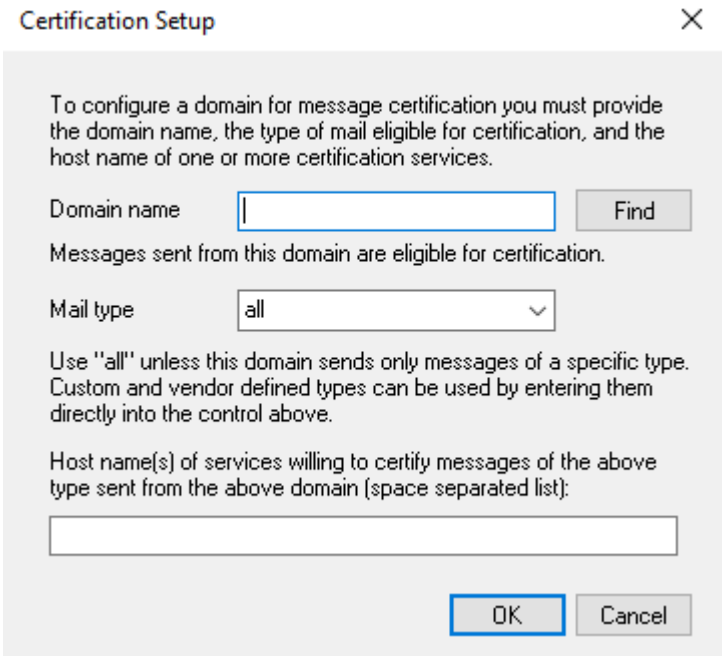
Los mensajes certificados aplican esta cantidad de puntos a la puntuación para el filtro de Spam
Si no desea hacer exentos a los mensajes certificados del filtro de Spam, use esta opción para designar la cantidad que desea ajusta la puntuación del Filtro de Spam del mensaje. Normalmente esto será un número negativo para que los mensajes reciban un ajuste benéfico. La configuración por defecto es "-3.0".

Insertar datos de certificación en los mensajes salientes
Haga clic en esta casilla para insertar los datos de certificación en los mensajes salientes. Entonces, haga clic en el botón *Configurar un dominio para certificación de mensajes* para abrir el diálogo de Configuración de Certificación para designar los dominios específicos a ser certificados y los CSPs asociados a éstos.

Configurar un dominio para la certificación de mensajes
Después de habilitar la opción anterior de *Insertar datos de certificación en los mensajes salientes*, haga clic en este botón para abrir el diálogo de Configuración de Certificación. En este diálogo se designa el dominio cuyos mensajes salientes serán certificados, el tipo de correo que se certificará, y los CSPs asociados al dominio.

Editar el archivo de configuración directamente
Después de habilitar la opción anterior de *Insertar datos de certificación en mensajes salientes*, haga clic en este botón para abrir el archivo de configuración de Vouch-by-Reference (VBR). Cualquier dominio que haya configurado vía el diálogo de Configuración de Certificación para que use VBR será listado en este archivo, junto con los datos VBR asociados. Puede usar este archivo para editar dichas entradas o para crear entradas nuevas manualmente.

Configuración de Certificación



Después de habilitar la opción *Insertar datos de certificación en los mensajes salientes* del diálogo de Certificación, haga clic en el botón *Configurar un dominio para la certificación de mensajes* para abrir el diálogo de Configuración de Certificación. Este diálogo se usa para designar el dominio cuyos mensajes salientes serán certificados, el tipo de correo que se certificará, y los CSPs asociados con el dominio.

Configuración de Certificación

Nombre del dominio
Use esta opción para introducir el nombre del dominio cuyos mensajes salientes serán certificados.

Encontrar
Si ha establecido anteriormente la Configuración de Certificación de Mensajes para un dominio en particular, escribe el *Nombre del dominio* y luego haga clic en este botón y las configuraciones de dicho dominio se listarán en las opciones del diálogo de Configuración de Certificación.

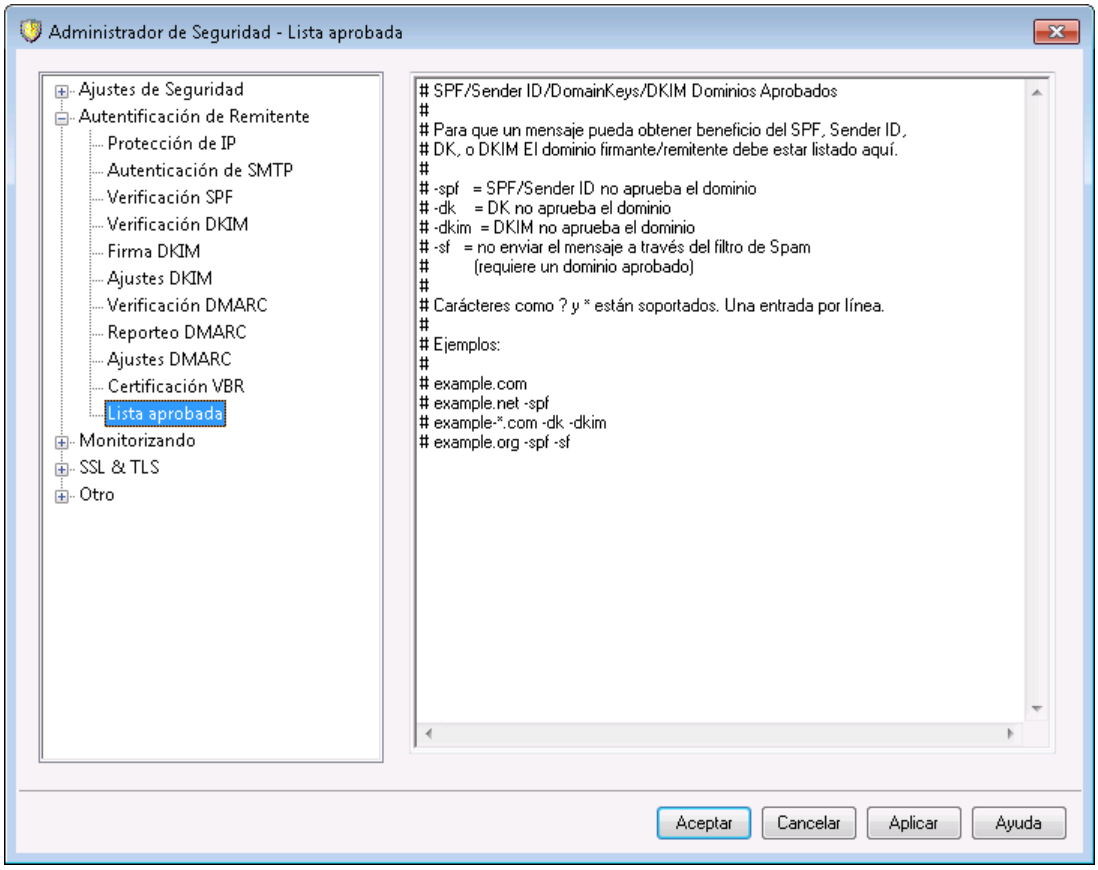
Tipo de correo
Use esta lista desplegable para escoger el tipo de correo que el CSP asociado ha accedido a certificar para este dominio. Si el tipo no está listado puede introducirlo manualmente.

Nombres de Host(s) de servicios...
Introduzca los nombres de host de los CSPs que han accedido a certificar los mensajes salientes del dominio (por ejemplo, `vbr.emailcertification.org`). Si introduce más de un CSP, entonces separe cada uno con un espacio.

Ver:

Certificación de Mensajes 553

4.2.2.8 Lista aprobada



Dado que algunos spammers y remitentes de correo masivo han empezado a usar SPF o a firmar mensajes con firmas válidas DKIM, el hecho de que un mensaje esté firmado y verificado no es garantía de que usted no lo vaya a considerar Spam, aun cuando asegure que el mensaje haya sido originado de una fuente válida. Por esta razón, la puntuación de Spam del mensaje no bajará como resultado de la verificación SPF o DKIM a menos que el dominio que se extraiga de la lista esté en la Lista de Aprobados. Esto es esencialmente una lista de permitidos que puede usar para designar dominios a los que se les permita reducir su puntuación de Spam cuando los mensajes entrantes estén verificados.

Cuando un mensaje firmado por uno de estos dominios es verificado por SPF o DKIM, su puntuación de Spam se reducirá de acuerdo con las configuraciones encontradas en las pantallas SPF 526 y Verificación DKIM 530. Puede, sin embargo, añadir cualquier combinación de marcas listadas a continuación si desea prevenir cualquiera de esos métodos de verificación de que reduzcan la puntuación. También existe una marca que puede usar para prevenir que los mensajes verificados pasen a través del Filtro de Spam.

-spf No reduzca la puntuación de Spam para los mensajes verificados por SPF enviados desde este dominio.

-dkim No reduzca la puntuación de Spam para los mensajes DKIM verificados para este dominio.

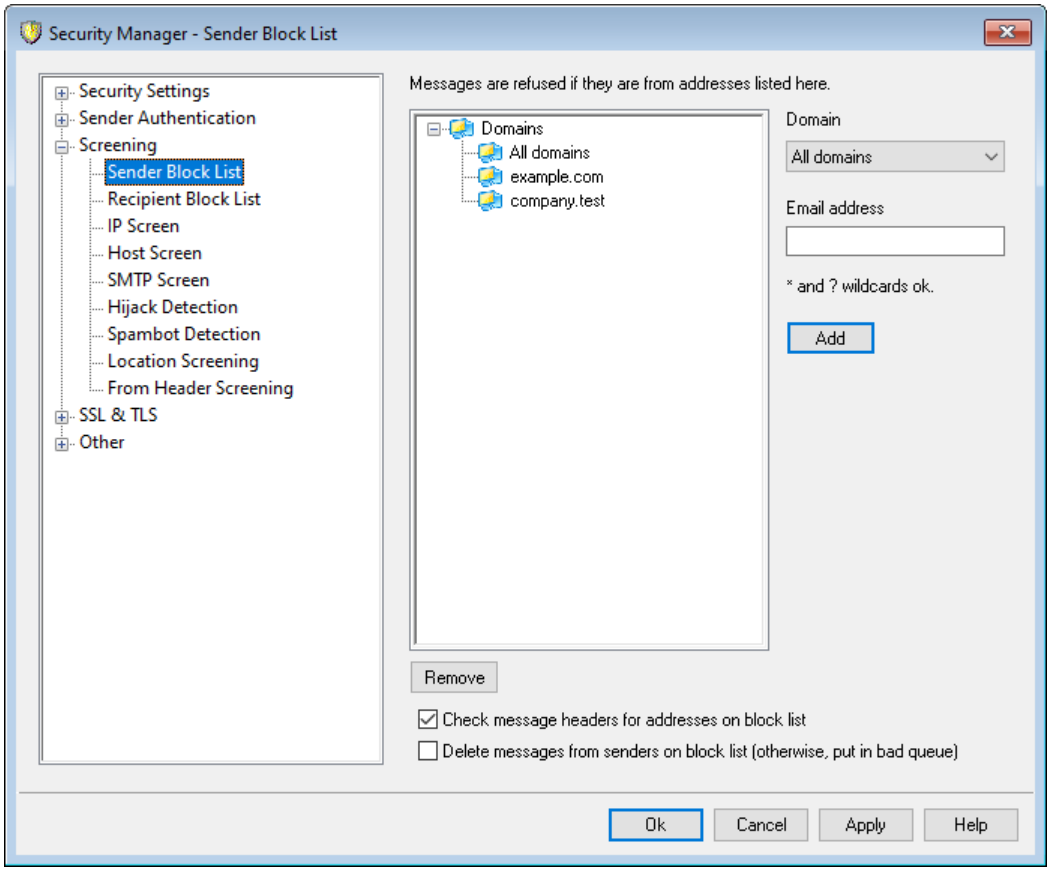
-sf No procesar a través del Filtro de Spam los mensajes verificados para este dominio.

DMARC y la Lista Aprobada

La verificación DMARC[545] también utiliza la Lista Aprobada, que exentar con base en identificadores DKIM verificados y rutas SPF de fuentes confiables para usted. Así que, por ejemplo, si llega un mensaje que falle la verificación DMARC, pero tiene una firma DKIM válida de un dominio en la Lista Aprobada, el mensaje no será sujeto a política DMARC punitiva (i.e. el mensaje es tratado como si la política fuera "`p=none`"). Lo mismo ocurre si la ruta de verificación SPF coincide para un dominio en la Lista Aprobada.

4.2.3 Monitoreo

4.2.3.1 Lista de Remitentes Bloqueados



La Lista Remitentes Bloqueados se localiza en: `Seguridad » Ajustes de Seguridad » Monitoreo`. Esta lista contiene las direcciones a las que no se les permite enviar tráfico de correo a través del servidor. Si llega un mensaje proveniente de una dirección en esta lista, se rehusará su aceptación durante la sesión SMTP. Esto es útil para controlar usuarios problema. Las direcciones se pueden poner bloquear en base a dominios o globalmente (aplicable a todos los dominios de MDaemon).

Los mensajes se rechazan si provienen de las direcciones enlistadas aquí
Esta ventana despliega todas las direcciones bloqueadas, indicando el dominio que las está incluyendo está bloqueando.

Dominio
Seleccione el dominio con el que se asociará esta lista de direcciones bloqueadas. En otras palabras, ¿cuál es el dominio del que quiere impedir la recepción de correo de la dirección especificada? Seleccione "Todos los Dominios" de esta lista para poner la dirección en lista de bloqueadas, globalmente.

Dirección de correo electrónico
Registre la dirección que desea poner en lista de bloqueados. Se aceptan comodines, por esto "*@ejemplo.net" suprimirá cualquier mensaje proveniente de cualquier usuario del dominio "ejemplo.net" y "usuario1@*" suprimirá cualquier mensaje de cualquier dirección que inicie con "usuario1@*", sin importar el dominio del que provenga el mensaje.

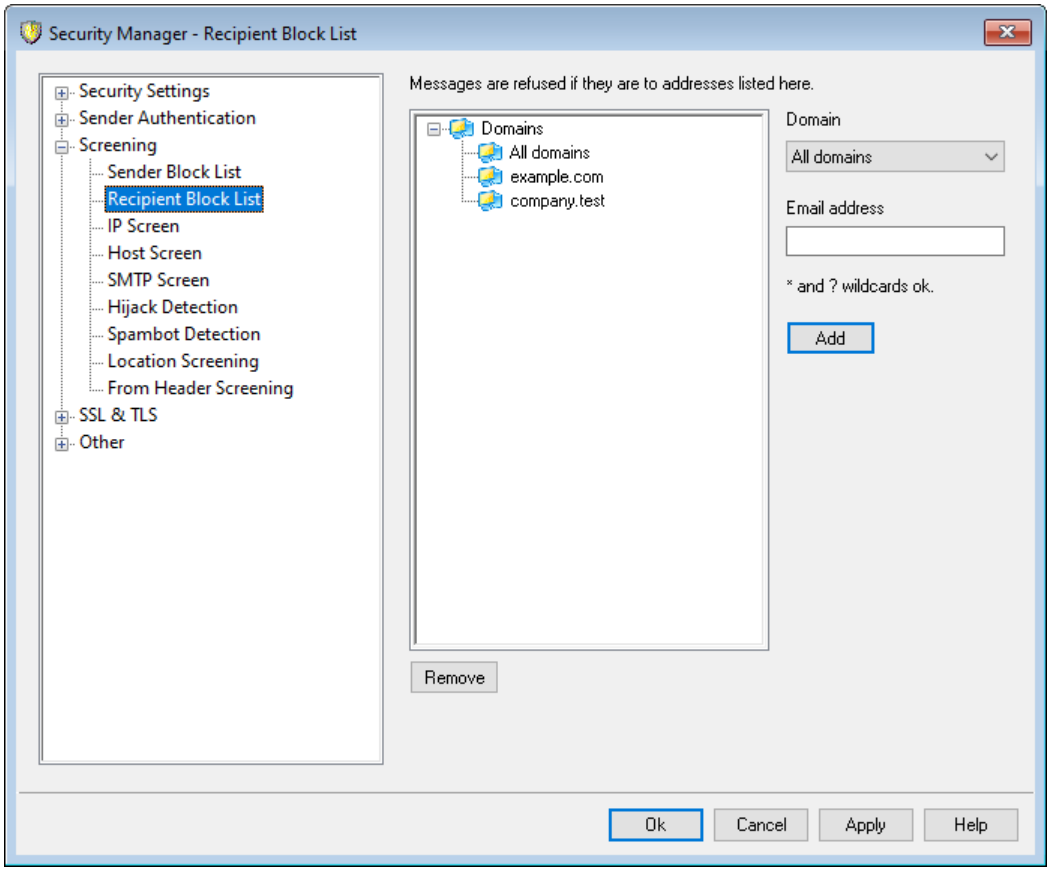
Agregar
Dé clic en este botón para agregar la dirección registrada a la lista de bloqueados.

Eliminar
Dé clic en este botón para eliminar el registro que ha seleccionado en la lista.

Buscar remitentes en lista de bloqueados, en los encabezados de los mensajes
Por omisión, MDaemon aplica la lista negra a los valores encontrados en los encabezados From/Sender durante la sesión SMTP. Esto impide que el mensaje se intercepte posteriormente y sea movido a la cola de erróneos por el proceso MTA.

Eliminar mensajes enviados desde remitentes bloqueados (de otra forma colocarlos en la cola de erróneos)
Habilite esta opción si desea que MDaemon elimine mensajes entrantes provenientes de remitentes que se encuentren en la Lista de Bloqueados. Además del correo normal, esta opción también se aplica a los mensajes que llegan vía MultiPOP y DomainPOP. Cuando la opción está deshabilitada, el mensaje será colocado en la Cola de Mensajes Erróneos en lugar de ser eliminado. Esta opción está deshabilitada por omisión.

4.2.3.2 Lista de Destinatarios Bloqueados



La Lista de Destinatarios Bloqueados se localiza en: `Seguridad » Ajustes de Seguridad » Monitorización`. Esta lista contiene direcciones de correo a las que no se les permite recibir correo a través de su servidor. Si llega un mensaje dirigido a una dirección en la lista, será rechazado. Las direcciones serán bloqueadas por dominio específico o globalmente (en todos los dominios de MDaemon). La Lista de Destinatarios Bloqueados opera sobre únicamente sobre los datos RCPT del sobre SMTP (no sobre los encabezados de mensajes).

Se rechazan los mensajes si se dirigen a las direcciones enlistadas aquí
Esta ventana despliega todas las direcciones bloqueadas actualmente, relacionadas por el dominio que las está bloqueando.

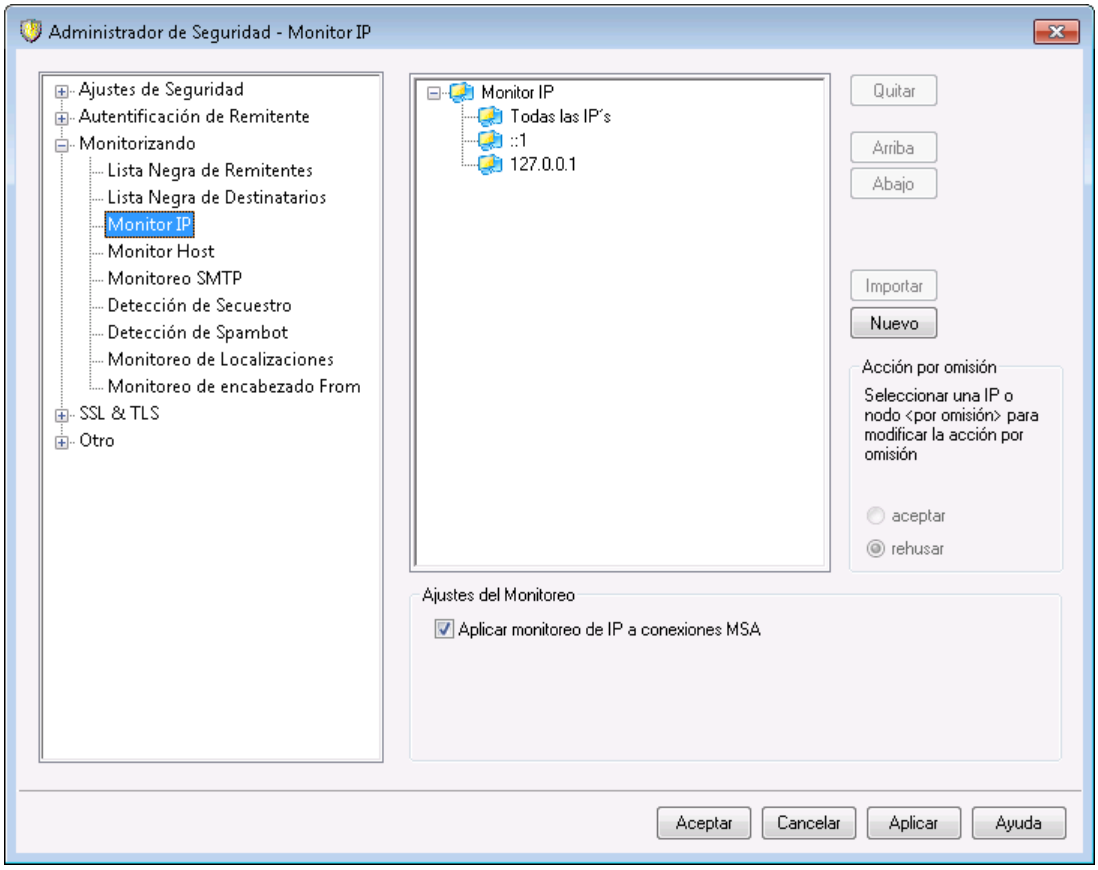
Dominio
Seleccione el dominio al que se asociará esta dirección bloqueada. En otras palabras, ¿en qué dominio desea prevenir la recepción de correo para la dirección especificada?. Seleccione "Todos los Dominios" de esta lista para poner la dirección en lista de bloqueados globalmente.

Direcciones de Correo Electrónico
Registre la dirección que desea incluir en lista de bloqueados. Se aceptan comodines, por lo que "*@ejemplo.net" suprimirá cualquier mensaje para cualquier usuario en el dominio "ejemplo.net", y "usuario1@*" suprimirá cualquier mensaje dirigido a cualquier dirección que inicie con "usuario1@", sin importar el dominio al que va dirigido.

Agregar
Dé clic en este botón para agregar la dirección designada a la lista de bloqueados.

Eliminar
Dé clic en este botón para eliminar el registro seleccionado en la lista.

4.2.3.3 Monitor IP



La pantalla Monitor IP se localiza bajo: Seguridad » Ajustes de Seguridad » Monitoreo. Se utiliza para definir direcciones IP remotas específicas a las que se les permitirá o no conectarse a sus direcciones IP locales. Las direcciones IP remotas que usted coloque en el monitor IP se pueden asociar ya sea con todas sus direcciones IP locales o con IPs individuales. Se permite notación CIDR y los comodines *, #, y ?.

Por ejemplo:

..*.*	Coincide con cualquier dirección IP
#.#.#.#	Coincide con cualquier dirección IP
192.*.*.*	Coincide con cualquier dirección IP que inicia con 192
192.168.*.239	Coincide con direcciones IP desde la 192.168.0.239 a la 192.168.255.239
192.168.0.1??	Coincide con direcciones IP desde la 192.168.0.100 a la 192.168.0.199

Nuevo elemento de Monitor IP

Para crear un nuevo registro en el Monitor IP, dé clic en **Nuevo**. Se abrirá la pantalla Nuevo elemento de Monitor IP para crear el registro.

IP Local
En la lista desplegable seleccione ya sea "Todas las IPs" o la IP específica a la que aplicará este elemento.

IP Remota (se permite CIDR y los comodines * ? y #)
Introduzca la dirección IP remota que desea agregara la lista, asociada con la IP Local designada arriba.

Aceptar conexiones
Seleccionar esta opción significa que las direcciones IP remotas especificadas podrán conectarse a la dirección IP local asociada.

Rechazar conexiones
Seleccionar esta opción significa que las direcciones IP remotas especificadas NO PODRÁN conectarse a la dirección IP local asociada. La conexión será rechazada o cerrada.

Agregar
Cuando haya terminado de introducir la información en las opciones anteriores, dé clic en este botón para agregar el registro a la lista.

Importar

Seleccione una dirección IP y dé clic en este botón si desea importar datos de direcciones IP de archivos APF O .htaccess. MDaemon soporta estos archivos de manera limitada como sigue:

- Se soportan "deny from" y "allow from"
- Solo se importan valores IP (no nombres de dominio)
- Se permite notación CIDR pero no se permite direcciones IP parciales
- Cada línea puede contener cualquier número de direcciones IP separadas por espacios o comas. Por ejemplo: "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5" y similares.
- Se ignoran las líneas que inician con #.

Eliminar

Para eliminar una entrada, selecciónela en la lista y dé clic en **Eliminar**.

Acción por Omisión

Para especificar la acción por omisión para las conexiones desde direcciones IP remotas que no se estén definidas, seleccione una dirección IP de la lista y dé clic en **aceptar** o **rechazar**. Una vez que se ha especificado la acción por omisión, puede modificarla seleccionando el nodo "<por omisión>" bajo la dirección IP y seleccionando el nuevo ajuste por omisión.

aceptar
Cuando se selecciona esta opción, las conexiones desde cualquier dirección IP no definidas específicamente en el Monitor IP, serán aceptadas.

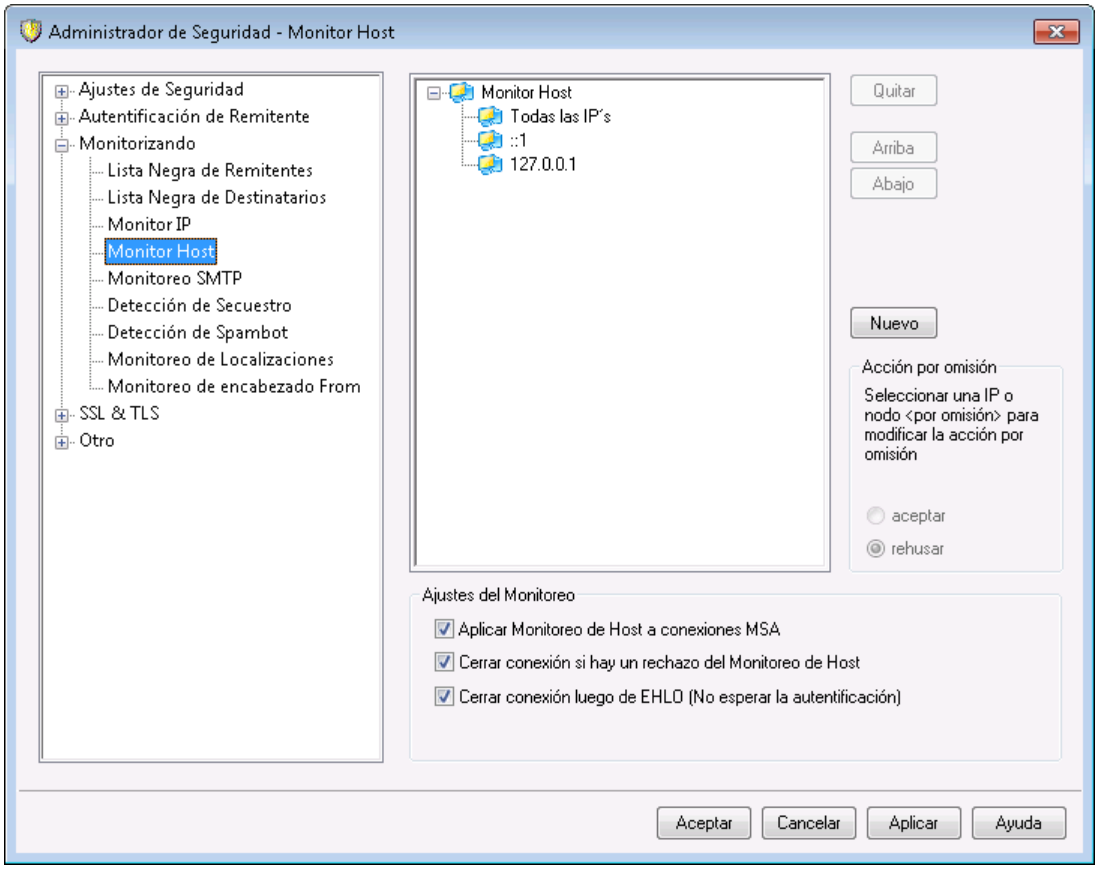
rechazar
Cuando se selecciona esta opción, las conexiones desde cualesquiera direcciones IP no definidas específicamente en la pantalla monitor IP, serán cerradas o rechazadas.

El Monitor IP nunca bloqueará IPs confiables[519] o IPs locales.

Ajustes de Monitoreo

Aplicar Monitor IP a conexiones MSA
Utilice esta opción para aplicar el Monitor IP a las conexiones hechas al puerto MSA[115] del servidor. Normalmente esto no es necesario. Este ajuste se encuentra habilitado por omisión.

4.2.3.4 Monitor Host



El Monitor Host está ubicado en: Seguridad » Ajustes de Seguridad » Monitoreo. El monitor Host se usa para definir que hosts remotos estarán autorizados a conectar a sus direcciones IP locales. Puede especificar una lista de hosts y configurar el servidor para permitir sólo conexiones de dichos hosts, o puede configurarlo para

rechazar conexiones de los hosts listados. El monitor host compara los valores EHLO y PTR determinados durante la sesión SMTP con los valores aquí especificados.

Nuevo Elemento de Monitor Host

Para crear una nueva entrada en el Monitor de Host, dé clic en **Nuevo**. Se abrirá el diálogo Nuevo Elemento de Monitor de Host para crear el registro.

IP Local
Utilice esta lista desplegable para seleccionar las direcciones IP locales a las que aplicará este registro del Monitor de Host. Seleccione "Todas las IPs" si desea aplicarlo a todas sus direcciones IP locales.

Host Remoto (se aceptan los comodines * y #)
Introduzca el host remoto que desea agregar a la lista, asociado con la IP local determinada arriba.

Aceptar conexiones
Seleccionar esta opción significa que al host remoto especificado se le permitirá conectarse a la dirección IP local asociada.

Rechazar conexiones
Seleccionar esta opción significa que al host remoto especificado NO se le permitirá conectarse a la dirección IP local asociada. La conexión será rechazada o cerrada.

Eliminar

Para eliminar una entrada, selecciónela en la lista y dé clic en **Eliminar**.

Acción por Omisión

Para especificar la acción por omisión para conexiones desde host remotos que no han sido definidos, seleccione una dirección IP de la lista y dé clic en **aceptar** o **rechazar**. Una vez que se ha especificado la acción por omisión, la puede modificar seleccionando el nodo "<omisión>" bajo la dirección IP y luego seleccionando el nuevo ajuste por omisión.

aceptar
Cuando se selecciona esta opción, las conexiones desde cualquier host no definido específicamente en el Monitor de Host, serán aceptadas.

rechazar
Cuando se selecciona esta opción, las conexiones desde cualquier host no definido específicamente en el Monitor de Host, serán rechazadas.

El Monitor de Host nunca bloqueará las IP confiables 519 o los hosts locales.

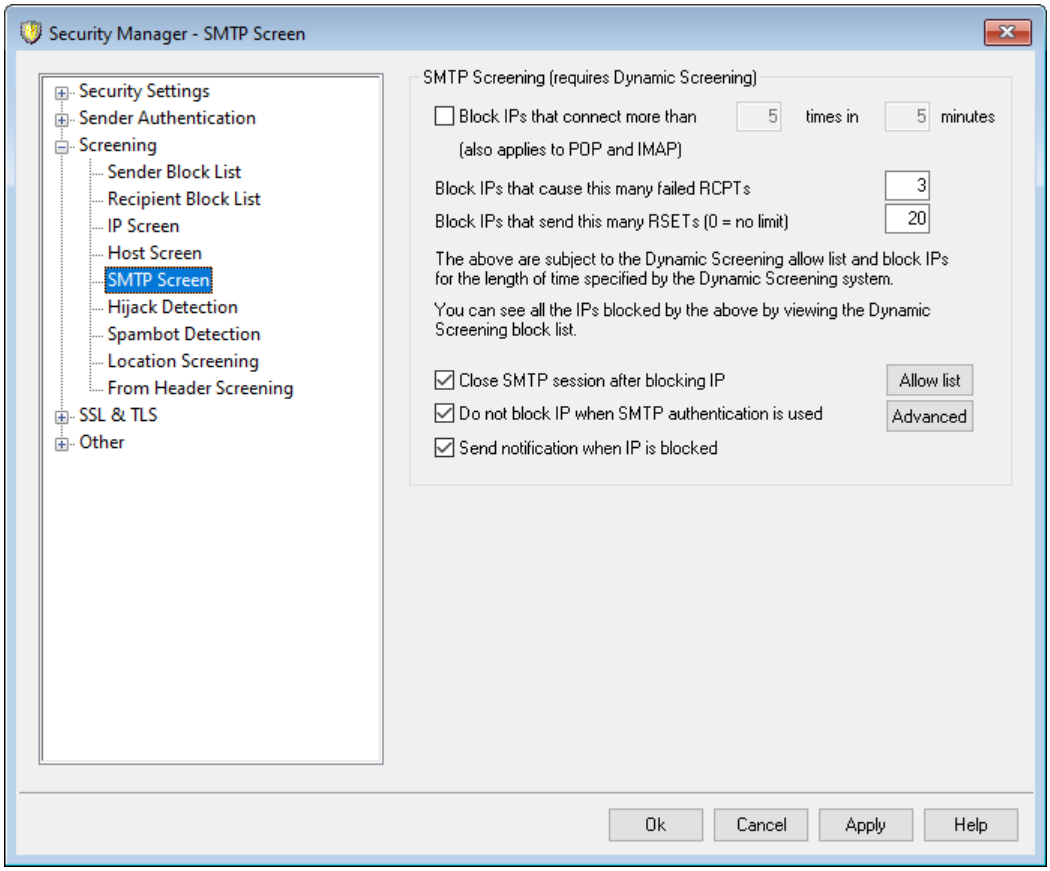
Ajustes de Monitor

Aplicar Monitor de Host a las conexiones MSA
Utilice esta opción para aplicar el Monitor de Host a las conexiones hechas al puerto MSA 115 del servidor. Este ajuste se encuentra habilitado por omisión.

Cerrar las conexiones si hay rechazo en el Monitor de Host
Cuando se habilita esta opción, la conexión se cerrará inmediatamente cuando haya rechazo por el Monitor de Host.

Cerrar las conexiones luego de EHLO (No esperar a la autenticación)
Habilite esta opción si desea cerrar las conexiones prohibidas inmediatamente después del EHLO/HELO. Normalmente se esperaría a la autenticación. Este ajuste está habilitado por omisión.

4.2.3.5 Pantalla SMTP



Utilizando la pantalla SMTP, puede bloquear direcciones IP que se conectan a MDaemon demasiadas veces dentro de un número determinado de minutos. También puede bloquear aquellas que causan demasiados RCPTs fallidos y aquellas que envían demasiados comandos RSET. La pantalla SMTP requiere del Monitoreo Dinámico y utiliza la Lista Dinámica de Bloqueados 625 y la Lista Dinámica de Permitidos 624.

Bloquear IPs que se conectan más de [X] veces en [X] minutos
Dé clic en esta casilla si desea bloquear temporalmente direcciones Ip que se conectan a su servidor un número excesivo de veces en un periodo de tiempo limitado. Especifique el número de minutos y el número de conexiones permitidas en ese periodo. Las direcciones se bloquean durante la cantidad de tiempo especificada en la pantalla Rastreo de Fallos de Autentificación 615. Esta opción solo aplica para conexiones POP e IMAP.

Bloquear IPs que generan esta cantidad de RCPTs fallidos
Cuando una dirección IP genera este número de errores "Destinatario desconocido" durante una sesión de correo, será bloqueada automáticamente durante la cantidad de tiempo especificada en la pantalla Rastreo de Fallos de Autentificación 615. Si ocurren con frecuencia errores "Destinatario desconocido" es una indicación de que el remitente es un spammer, dado que ellos comúnmente intentan enviar mensajes a direcciones obsoletas o incorrectas.

Bloquear IPs que envían esta cantidad de RSETs (0 = sin límite)
Utilice esta opción si desea bloquear cualquier dirección IP que emite un número determinado de comandos RSET durante una sola sesión de correo. Utilice "0" si no desea establecer un límite. Existe una opción similar en la pantalla Servidores 100 bajo Ajustes de Servidor, que puede ser utilizada para establecer un límite al número permitido de comandos RSET. La dirección IP será bloqueada durante la cantidad definida de tiempo en la pantalla Rastreo de Fallos de Autentificación 615.

Cerrar sesión SMTP luego de bloquear la IP
Si habilita esta opción, MDaemon cerrará la sesión SMTP luego de que la dirección IP sea bloqueada. Se encuentra habilitada por omisión.

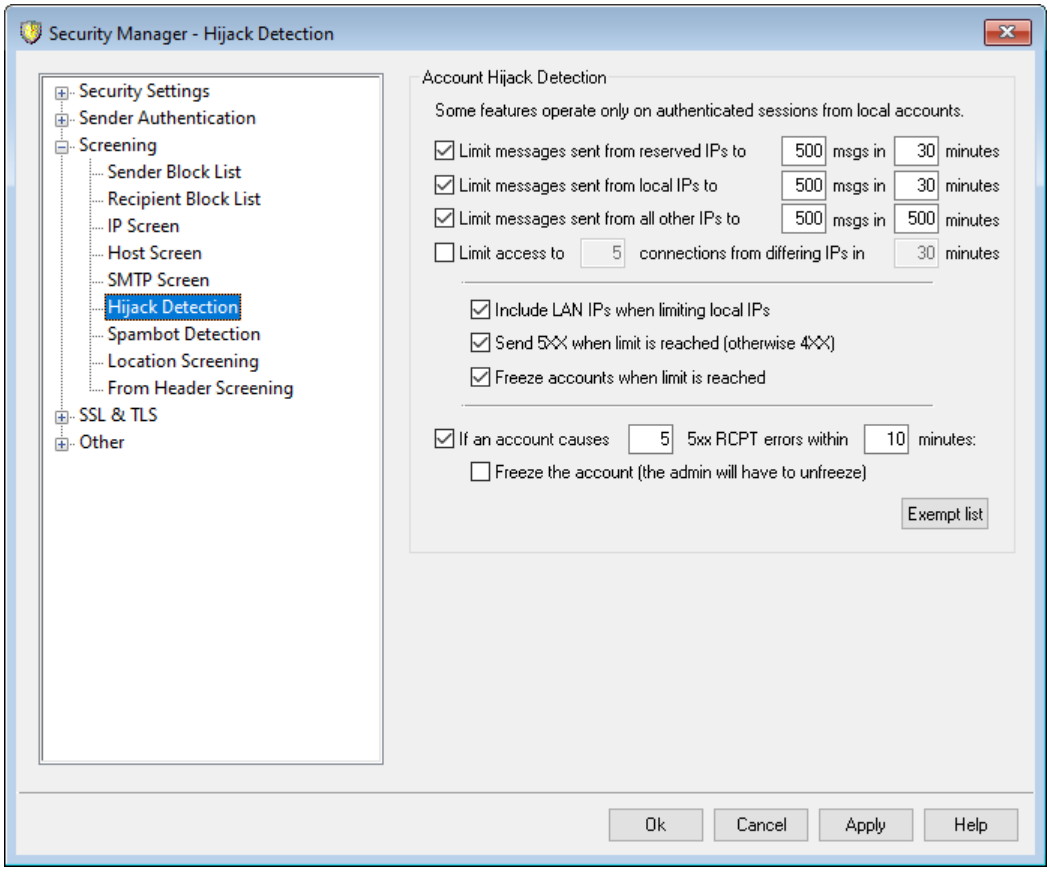
No bloquear IPs cuando se utiliza la autentificación SMTP
Dé clic en esta caja si desea que los remitentes que autentifican sus sesiones de correo antes de enviar mensajes, estén exentos del Monitoreo Dinámico. Se encuentra habilitada por omisión.

Enviar notificación cuando se bloquea una IP
Por omisión, cuando alguna dirección IP es bloqueada en automático por el sistema de Monitoreo Dinámico, las opciones *Reporte de Bloqueo de Direcciones IP* 619 del Monitoreo Dinámico, se utilizarán para notificarle dicha acción. Deshabilite esta casilla si no desea ser notificado cuando una dirección IP sea bloqueada debido a la funcionalidad de Monitoreo SMTP.

Lista de Permitidos
Dé clic en este botón para abrir la Lista Dinámica de Permitidos 624. Las direcciones IP listadas aquí están exentas del Monitoreo SMTP.

Avanzado
Este botón abre el diálogo del Monitoreo Dinámico 610.

4.2.3.6 Detección de Cuentas Secuestradas



Detección de Cuentas Secuestradas

Las opciones en esta pantalla se pueden utilizar para detectar cuando una cuenta de MDaemon posiblemente haya sido secuestrada, e impedir automáticamente que envíe mensajes a través de su servidor. Por ejemplo, si un spammer de alguna manera obtiene la contraseña de una cuenta, esta funcionalidad le impedirá utilizarla para enviar correo basura masivo a través de su sistema. Puede definir un número máximo de mensajes que se pueden enviar desde una cuenta en un número dado de minutos, con base en la dirección IP de la que se esté conectando. También puede elegir deshabilitar las cuentas que alcancen el límite. Existe también una *Lista de Exentos* que se puede utilizar para exentar ciertas direcciones de esta restricción. La Detección de Cuentas Secuestradas está habilitada por omisión.

La Detección de Cuentas Secuestradas solo aplica a cuentas locales sobre sesione autentificadas, la cuenta del Postmaster está exenta en automático.

Limitar mensajes enviados desde IPs reservadas a [xx] mensajes en [xx] minutos
Utilice esta opción para impedir que las cuentas de MDaemon conectadas desde IPs reservadas envíen más del número especificado de mensajes en el número de minutos determinados. Las direcciones IP reservadas son principalmente las definidas por los RFCs (por ejemplo, 127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10 y FE80::/64).

Limitar mensajes enviados desde IPs locales a [xx] mensajes en [xx] minutos
Utilice esta opción para impedir que las cuentas de MDaemon conectadas desde cualquier IP local envíen más del número especificado de mensajes en el número determinado de minutos. Las IPs locales son todas las direcciones IP configuradas para cualquiera de sus dominios de MDaemon.

Limitar mensajes enviados desde todas las otras IPs a [xx] mensajes en [xx] minutos
Utilice esta opción para impedir que las cuentas de MDaemon conectadas desde cualquiera otra IP envíen más del número especificado de mensajes en el número determinado de minutos.

Limitar el acceso a [xx] conexiones de distintas IPs en [xx] minutos
Utilice esta opción para limitar el número permitido de conexiones desde direcciones IP distintas, dentro de un número especificado de minutos. Por ejemplo, en circunstancias normales si su cuenta se accesa desde diez direcciones IP diferentes dentro de un rango pequeño de minutos, lo más probable es que la cuenta haya sido secuestrada. Esta opción se encuentra deshabilitada por omisión.

Incluir IPs de la LAN al limitar IPs locales
Por omisión las IPs de la LAN[608] se incluyen al utilizar la opción arriba "*Limitar mensajes enviados desde IPs locales...*". Deshabilite esta casilla si no desea incluir las IPs de la LAN al limitar IPs locales.

Enviar 5XX cuando se alcanza el límite (4XX en otro caso)
Por omisión cuando se alcanza alguno de los límites, MDaemon enviará un código de respuesta 5XX a la cuenta secuestrada. Deshabilite esta opción si en lugar de esto, desea enviar un código 4XX.

Congelar cuentas cuando se alcance el límite
Marque esta caja si desea congelar las cuentas que intenten enviar más del número permitido de mensajes. Cuando esto ocurra, el servidor envía un mensaje 552, la conexión se cierra y la cuenta es congelada de inmediato. La cuenta congelada ya no podrá enviar o descargar su correo, pero MDaemon seguirá aceptando correo entrante dirigido a esa cuenta. Finalmente, cuando la cuenta sea congelada, se enviará un mensaje al Postmaster informándole de esto. Si el Postmaster desea rehabilitar la cuenta simplemente tendrá que dar respuesta al mensaje.

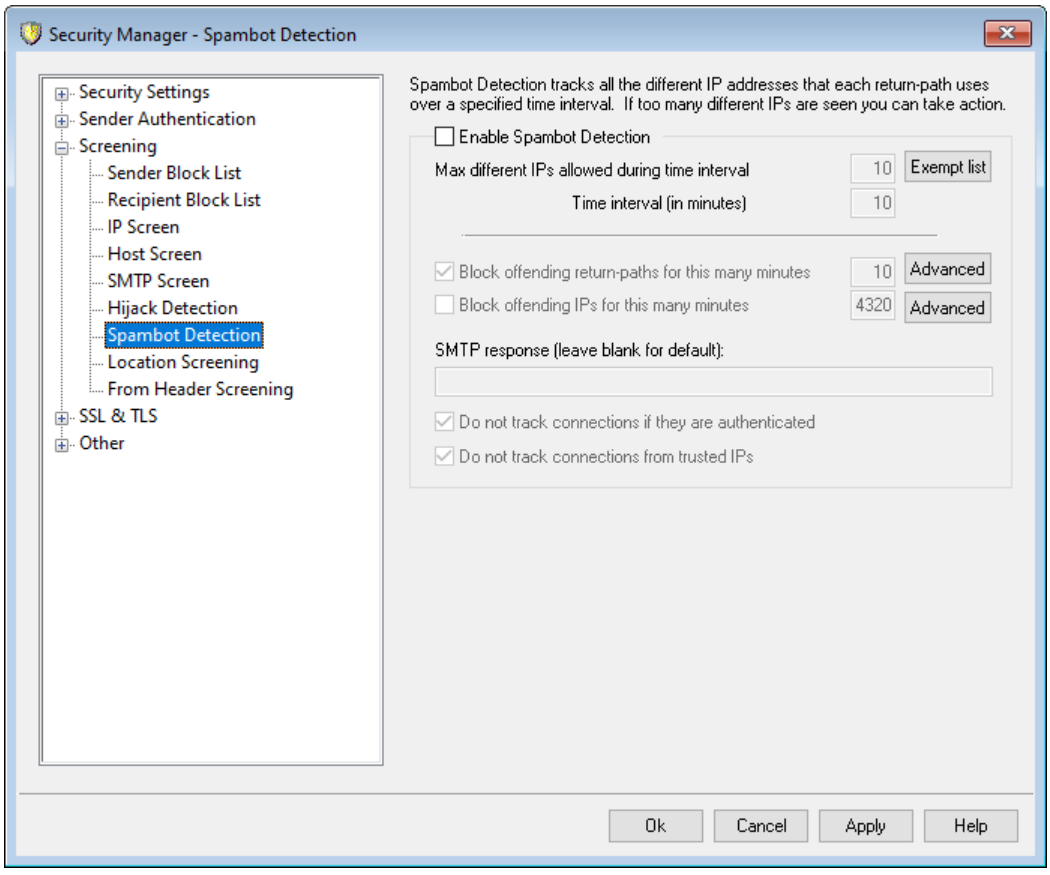
Si una cuenta genera [xx] 5xx RCPT errores dentro de [xx] minutos
Esta opción monitorea cuantas veces una cuenta intenta enviar mensajes a un destinatario inválido durante un rango de tiempo determinado, Una característica común del correo basura es que los mensajes con frecuencia se envían a un gran número de destinatarios inválidos, debido a que el spammer intenta enviar a direcciones viejas o adivinar nuevas. Por esto, si una cuenta de MDaemon empieza a enviar mensajes a un número notorio de destinatarios inválidos en un rango de tiempo corto, es un buen indicador de que la cuenta ha sido secuestrada y está siendo utilizada para enviar spam. Al utilizar esta opción junto con la opción siguiente "*Congelar la cuenta...*" puede ayudar a detener una cuenta secuestrada antes de que haga mucho daño. Nota: Para esta opción, un

destinatario inválido se define como un código de error 5xx en respuesta a un comando RCPT al intentar enviar el correo de la cuenta.

Congelar la cuenta (el administrador tendrá que descongelar)
Utilice esta opción si desea congelar una cuenta cuando se alcance el umbral determinado arriba "*Si una cuenta genera [xx] 5xx RCPT errores...*". Cuando esto ocurre el administrador será notificado por correo para que pueda investigar el problema y descongelar la cuenta.

Lista de Exentos
Use la *Lista de Exentos* para definir las direcciones que desee estén exentas de la Detección de Cuentas Secuestradas. Se permiten comodines. Por ejemplo, "`boletines@ejemplo.com`" exentará a la cuenta "boletines", en tanto que "*@`boletines.ejemplo.com`" exentará todas las cuentas de MDaemon pertenecientes al dominio boletines.ejemplo.com. La cuenta de Postmaster está exenta en automático de la Detección de Cuentas Secuestradas.

4.2.3.7 Detección de Spambot



La detección de Spambot rastrea las direcciones IP de todos los valores que utilizan las conexiones `SMTP MAIL` (return-path) en un periodo dado de tiempo. Si un número desordenado de diferentes direcciones IP utiliza el mismo valor return-path en un periodo corto de tiempo, esto puede indicar una red de spambot. Cuando se detecta un spambot, la conexión actual se cierra inmediatamente y el valor return-path se coloca opcionalmente en lista de bloqueados durante el periodo de tiempo

que usted especifique. Opcionalmente también puede incluir en lista de bloqueados todas las direcciones IP de spambot por un periodo de tiempo determinado.

Habilitar Detección de Spambot
Dé clic en esta caja para habilitar la Detección de Spambot. Se encuentra deshabilitada por omisión.

Max IPs diferentes permitidas durante un intervalo de tiempo
Este es el número de direcciones IP diferentes para las que un return-path dado se puede conectar durante el intervalo específico de tiempo.

Intervalo de Tiempo (en minutos)
Especifique el intervalo de tiempo (en minutos) a utilizar al intentar detectar redes de spambot.

Lista de Exentos
Dé clic en este botón para abrir la lista de Exentos de la Detección de Spambot. Aquí puede especificar las direcciones IP, remitentes y destinatarios que están exentos de la detección de Spambot.

Poner en lista de bloqueados los valores return-path ofensivos durante estos minutos
Utilice esta opción si desea colocar en lista negra los valores return-path de spambots detectados. MDaemon no aceptará mensajes con un return-path en lista negra durante el número determinado de minutos. Esta opción se encuentra habilitada por omisión.

Avanzado
Dé clic en este botón para abrir el Archivo de Remitentes de Spambot. Despliega los valores return-path en lista de bloqueados y el número de minutos faltantes antes de que sean eliminados de la lista de bloqueados.

Colocar en Lista negra las IPs ofensivas durante estos minutos
Utilice esta opción si desea colocar en lista negra las direcciones IP de spambot detectadas. MDaemon no aceptará mensajes de direcciones IP en Lista Negra durante el número de minutos determinado. Esta opción se encuentra deshabilitada por omisión.

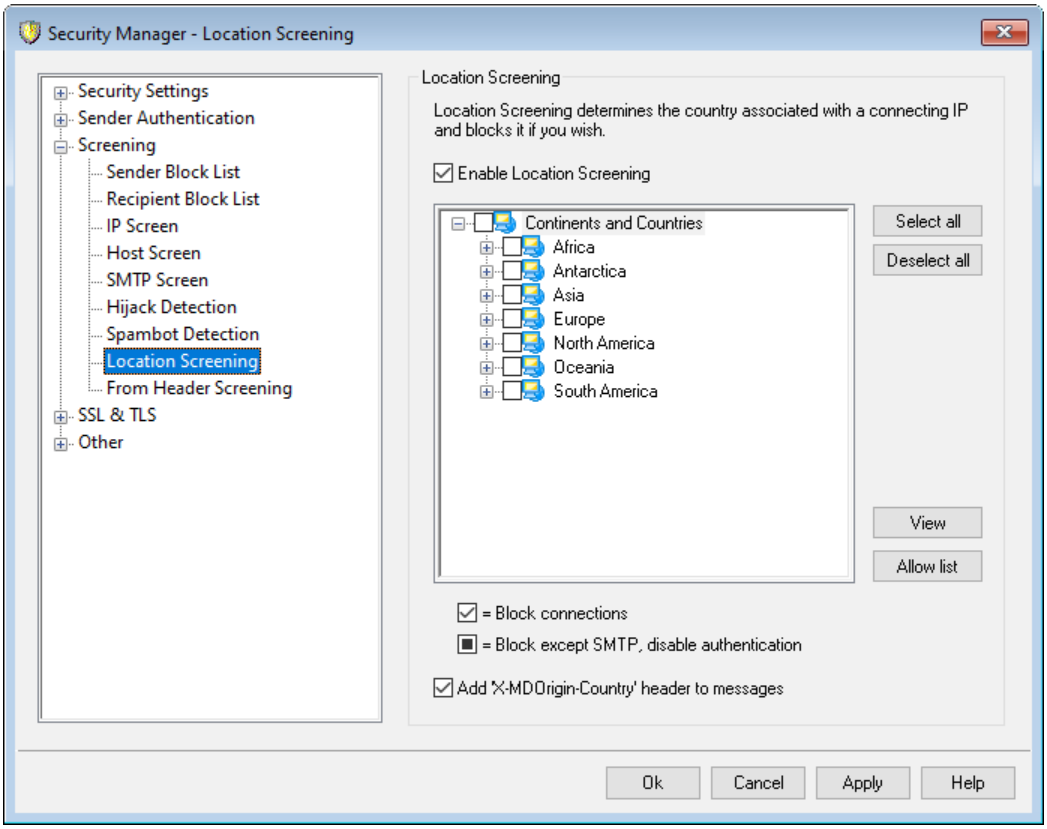
Avanzado
Dé clic en este botón para abrir el archivo de IP´s de Spambot Despliega las direcciones IP en lista negra y el número de minutos faltantes antes de que cada IP sea removida de la lista negra.

Respuesta SMTP (dejar en blanco por omisión)
Utilice esta opción si desea personalizar la respuesta SMTP a los spambots intentando enviar mensajes desde valores return-path o IP´s en lista de bloqueados. MDaemon devolverá la respuesta SMTP "`551 5.5.1 <texto personalizado>`", en lugar de la respuesta por omisión. Dejé el valor el blanco para utilizar la respuesta por omisión de MDaemon.

No rastrear conexiones si están autentificadas
Por omisión, MDaemon no rastreará sesiones autentificadas[523] para la Detección de Spambot. Deshabilite esta casilla si no desea exentar las conexiones autentificadas.

No rastrear conexiones desde IPs confiables
Por omisión la Detección de Spambot no rastreará conexiones desde Direcciones IP confiables[520]. Deshabilite esta casilla si no desea exentar IPs confiables.

4.2.3.8 Monitoreo de Localizaciones



Monitoreo de Localizaciones

El Monitoreo de Localizaciones es un sistema de bloqueo geográfico que puede utilizar para bloquear conexiones entrantes SMTP, POP o IMAP, Webmail, ActiveSync, AutoDiscovery[85], AutoDiscovery, XML API, Administración Remota, CalDAV/CardDAV, XMPP y Minger provenientes de regiones del mundo no autorizadas. MDaemon determina el país asociado con la dirección IP que se conecta, bloquea la conexión si proviene de una localización restringida y agrega una línea al registro del Monitoreo. Para SMTP, el Monitoreo de Localizaciones puede bloquear opcionalmente solo las conexiones que utilizan AUTH. Esto es útil, por ejemplo, si no cuenta con usuarios en país específico, pero desea habilitar la recepción de correo desde ahí. De esa forma puede bloquear solo a aquellos que intentan iniciar sesión en su servidor.

La carpeta `\MDaemon\Geo\` contiene archivos de base de datos que sirven como base de datos maestra de IPs de países. Los archivos fueron proporcionados por MaxMind (www.maxmind.com) y es posible descargar actualizaciones de ahí, si lo desea.

Habilitar Monitoreo de Localizaciones
El Monitoreo de Localizaciones está habilitado por omisión, pero no se bloquean regiones o países; MDaemon solo registra el país o región que se conecta. Para bloquear una ubicación, dé clic en la caja hasta que aparezca una marca de verificación al lado de la región o país que se desea bloquear. Si desea bloquear solo conexiones AUTH, lo que significa que las conexiones SMTP se permitirán, entonces dé clic de nuevo en la casilla para que esté completamente llena. Cuando está habilitado el Monitoreo de Localizaciones, sin importar si hay ubicaciones bloqueadas o no, MDaemon insertará el encabezado "`X-MDOrigin-Country`" en los mensajes, para fines del filtro de contenido. Este encabezado contiene el código de dos dígitos ISO 3166 de países y continentes.

Marcar/Desmarcar todos
Utilice este botón para Marcar o Desmarcar todas las localizaciones de la lista.

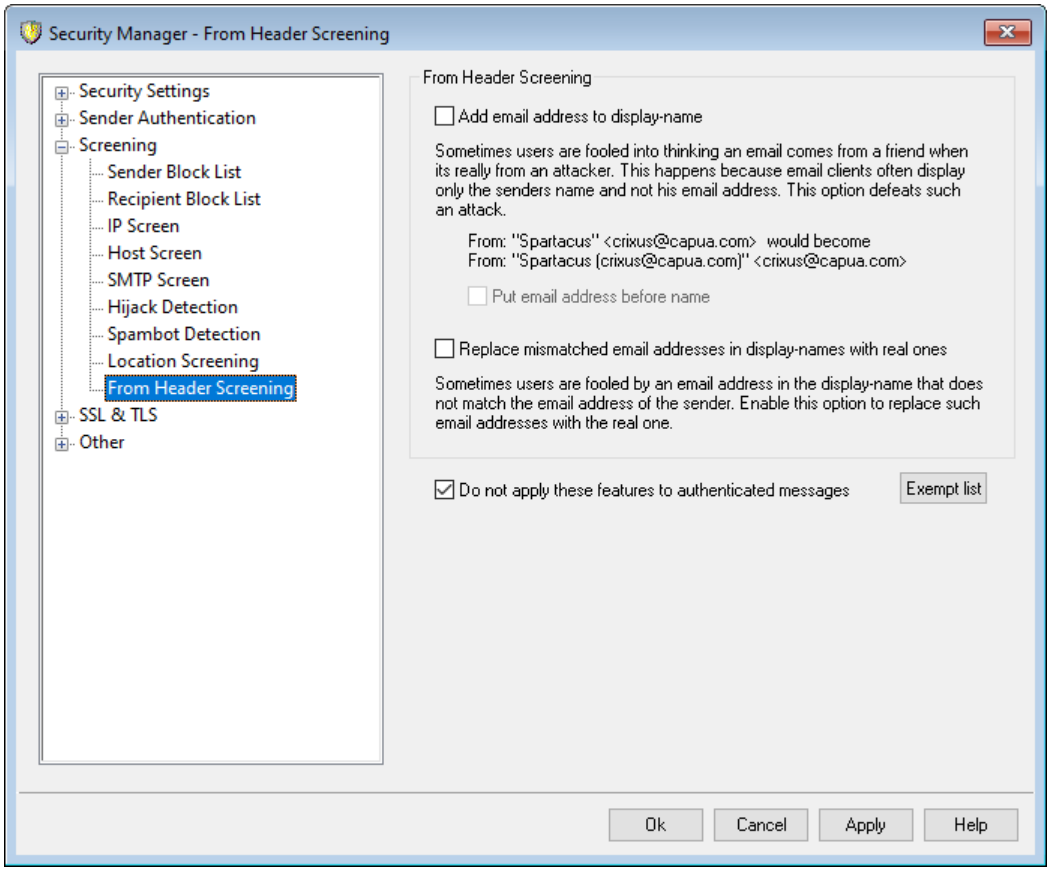
Ver
Dé clic en este botón para visualizar el archivo de texto con la lista de todas las localizaciones que se encuentran bloqueadas actualmente por el Monitoreo de Localizaciones. Si habilita/deshabilita cualquier caja en la lista de localizaciones entonces el botón *Ver* no estará disponible hasta después de que dé clic en **Aplicar**.

Lista de Permitidos
Este botón abre la Lista de Permitidos del Monitoreo Dinámico 624, que también se utiliza para el Monitoreo de Localizaciones. Si desea exentar una dirección IP del Monitoreo de Localizaciones, dé clic en este botón y especifique la dirección IP, así como cuando desea que esa entrada expire.

Las conexiones SMTP se aceptan, pero la autentificación se bloquea
Marque esta caja si, para conexiones SMTP, desea bloquear solo las conexiones que intentan utilizar autentificación.

Agregar el encabezado 'X-MDOrigin-Country' a los mensajes
Por omisión, cuando el Monitoreo de Localizaciones está habilitado, MDaemon insertará el encabezado "`X-MDOrigin-Country`" en los mensajes, para el filtro de contenido y otros propósitos. Este encabezado contiene los códigos ISO 3166 de dos caracteres para país y continente en lugar de nombres completos.
Deshabilite esta casilla si no desea insertar el encabezado en los mensajes.

4.2.3.9 Monitoreo del Encabezado From



Monitoreo del Encabezado From

Esta función de seguridad modifica el encabezado "From:" de los mensajes entrantes para hacer que la porción del nombre del encabezado contenga tanto el nombre como la dirección de correo. Esto se hace para combatir una táctica común utilizada en spam y ataques donde se hace parecer que el mensaje proviene de alguien más. Al desplegar una lista de mensajes, los clientes de correo comúnmente despliegan solo el nombre del remitente en lugar del nombre y la dirección de correo. Para ver la dirección de correo, el destinatario debe primero abrir el mensaje o realizar alguna otra acción, tal como dar clic derecho en el campo, pasar el puntero sobre el nombre o similar. Por esta razón los atacantes comúnmente construyen correos de manera que aparece una persona o empresa legítima en la porción visible del encabezado "From:" en tanto que la dirección de correo ilegítima está oculta. Por ejemplo, el verdadero encabezado "From:" de un mensaje podría ser `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, pero su cliente podría desplegar solo `"Honest Bank and Trust"` como remitente. Esta funcionalidad modifica la porción visible del encabezado para mostrar las dos partes. En el ejemplo de arriba el remitente ahora aparecería como `"Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>`, dándole una clara indicación de que el mensaje es fraudulento.

Agregar la dirección de correo al nombre de despliegue
Habilite esta opción si desea modificar la porción visible al cliente del encabezado "From:" en los mensajes entrantes para incluir tanto el nombre como la dirección de correo del remitente. La construcción del nuevo encabezado se modificará de `"Nombre del Remitente" <mailbox@example.com>` a `"Nombre del Remitente(mailbox@example.com)" <mailbox@example.com>`. Esto solo aplica

a mensajes hacia usuarios locales y esta opción está deshabilitada por omisión. Considere cuidadosamente antes de habilitar esta opción ya que muchos usuarios pueden no esperar o desear que se modifique el encabezado From:, aun cuando les pudiera ayudar a identificar mensajes fraudulentos.

Colocar la dirección de correo antes del nombre
Al utilizar la opción anterior *Agregar la dirección de correo al nombre de despliegue*, habilite esta opción si desea intercambiar el nombre y dirección de correo en el encabezado "From:" modificado, colocando la dirección de correo primero. Utilizando el ejemplo anterior, `"Nombre del Remitente" <mailbox@example.com>` ahora se modificaría a: `"mailbox@example.com (Nombre del Remitente)" <mailbox@example.com>`.

Reemplazar direcciones inconsistente en nombres de despliegue con los valores reales
Otra táctica utilizada en el spam es colocar un nombre y dirección en apariencia legítimos en la porción del nombre de despliegue en el encabezado "From:" aunque no sea la direccione remitente real. Utilice esta opción si desea reemplazar la dirección de correo visible en mensajes como este con la dirección real de correo del remitente.

No aplicar estas funcionalidades a mensajes autentificados
Marque esta casilla si no desea aplicar las opciones del Monitoreo del Encabezado From a los mensajes entrantes que han sido autentificados por MDaemon.

Lista de Exentos
Utilice esta opción para agregar direcciones a la lista de exentos del Monitoreo del Encabezado From. No se modificarán los encabezados "From:" de los mensajes destinados a las direcciones enlistadas aquí.

4.2.4 SSL & TLS

MDaemon soporta el Protocolo Transport Layer Security (TLS)/Secure Sockets Layer (SSL) para SMTP, POP e IMAP 577, MDaemon Administración Remota 584 y el servidor web de Webmail 580. El protocolo SSL, desarrollado por la Netscape Communications Corporation, es el método estándar para proteger las comunicaciones Internet de cliente/servidor. Provee autenticación de servidor, encriptación de datos, y autenticación opcional de cliente para las conexiones TCP/IP. Además, dado que SSL está integrado en la mayoría de los navegadores, simplemente instalando un certificado digital válido en su servidor activará las capacidades de conectividad SSL del navegador cuando conecte a MDRA o Webmail.

Si está conectando a los puertos estándar de correo a través de un cliente de correo en lugar de usar Webmail, MDaemon soporta la extensión STARTTLS sobre TLS para SMTP e IMAP y la extensión STLS para POP3. Aun así, primero debe tener su cliente configurado para usar SSL, y debe soportar dichas extensiones—no todos los clientes de correo las soportan. Utilice las páginas Lista No STARTTLS 588 y Lista

STARTTLS[589] para definir hosts y direcciones específicos que deben o no, respectivamente, utilizar STARTTLS.

El diálogo SSL & TLS también contiene una página para habilitar DNSSEC[593] (DNS Security Extensions), la página Extensiones SMTP[590] para habilitar RequireTLS, MTA-STA, y Reporteo TLS y la página Let's Encrypt[594] para el caso en que se utilizan los servicios de Let's Encrypt Certificate Authority (CA).

Las opciones para activar y configurar SSL están ubicadas bajo la sección SSL & TLS del diálogo de Ajustes de Seguridad en: `Seguridad » Administrador de Seguridad » SSL & TLS`. Las configuraciones SSL de puerto para SMTP, POP3, e IMAP están ubicadas en la pantalla Puertos[115] en: Configuración » `Ajustes del Servidor`.

Para información acerca de la creación y uso de Certificados SSL, vea:

Crear y Usar Certificados SSL[912]

—

El protocolo TLS/SSL se describe en RFC-4346: The Transport Layer Security (TLS) Protocol Version 1.1

La extensión STARTTLS para SMTP se describe en RFC-3207: SMTP Service Extension for Secure SMTP over Transport Layer Security

El uso de TLS con los protocolos IMAP y POP3 se describe en RFC-2595: Using TLS with IMAP, POP3 and ACAP

DNSSEC (DNS Security Extensions) se define en: RFC-4033: DNS Security Introduction and Requirements y RFC-4035: Protocol Modifications for the DNS Security Extensions

Para una descripción completa de RequireTLS, vea: RFC 8689: SMTP Require TLS Option.

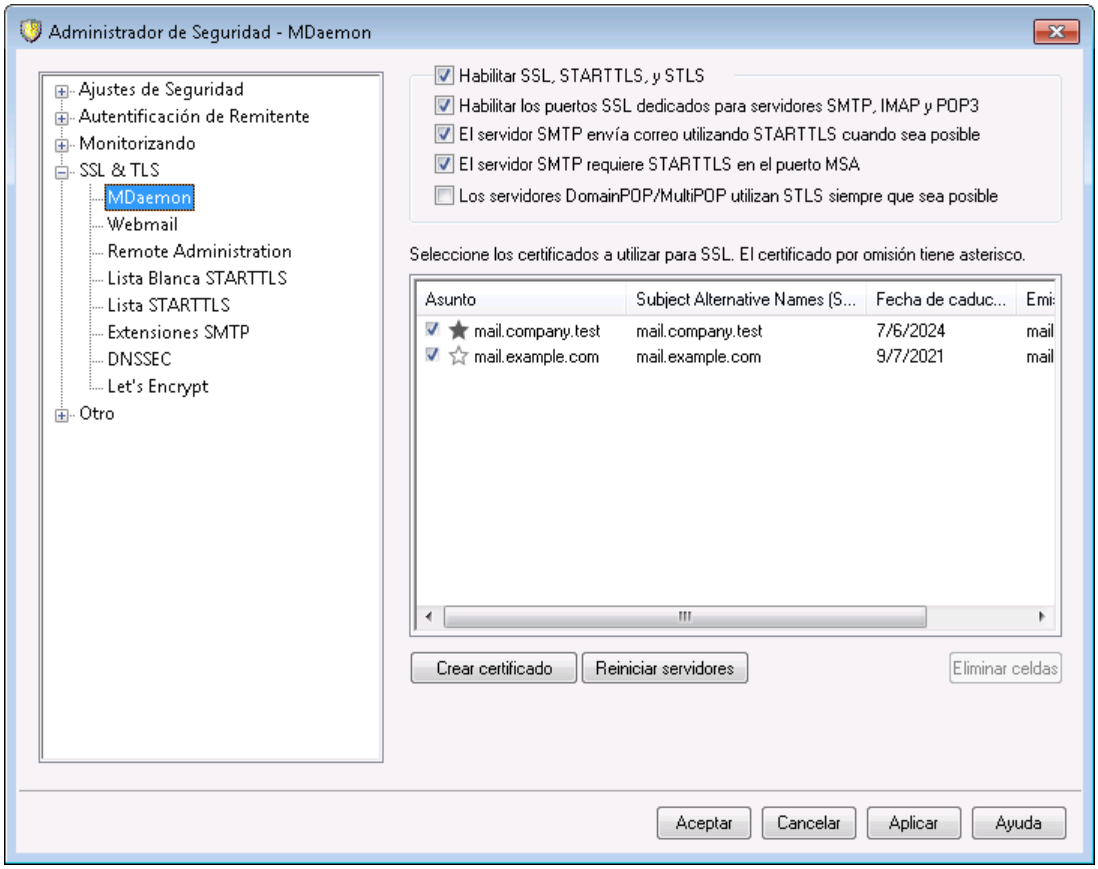
El soporte a MTA-STS se describe en RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

El reporteo TLS se discute en RFC 8460: SMTP TLS Reporting.

Ver:

SSL & TLS » MDaemon[577]
SSL & TLS » Webmail[580]
SSL & TLS » Administración Remota[584]

4.2.4.1 MDaemon



Habilitar SSL, STARTTLS, y STLS
Haga clic en esta casilla para activar soporte para el protocolo SSL/TLS y las extensiones STARTTLS y STLS. Luego, escoja el certificado que quiera usar de la lista siguiente.

Habilitar los puertos SSL dedicados para los servidores SMTP, IMAP y POP3
Habilite esta opción si quiere hacer disponible los puertos SSL dedicados especificados en Puertos 115 bajo Dominios y Servidores por Defecto. Esto no afectará a los clientes que usen STARTTLS y STLS en los puertos de correo por defecto — simplemente provee de un nivel adicional de soporte para SSL.

El servidor SMTP envía correo utilizando STARTTLS siempre que sea posible
Haga clic en esta opción si quiere que MDaemon intente usar la extensión STARTTLS para cada mensaje SMTP que envíe. Si un servidor al cual MDaemon esté conectando no soporta STARTTLS entonces el mensaje se enviará normalmente sin usar SSL. Use la Lista No STARTTLS 588 si desea prevenir el uso de STARTTLS para ciertos dominios.

El servidor SMTP requiere STARTTLS en el puerto MSA
Habilite esta opción si desea requerir SSL para conexiones al servidor hechas en el Puerto MSA 115.

Los servidores DomainPOP/MultiPOP utilizan STLS siempre que sea posible
Verifique esta casilla si desea que los servidores DomainPOP y MultiPOP utilicen la extensión STLS siempre que esto sea posible.

Seleccionar el certificado a utilizar para SSL

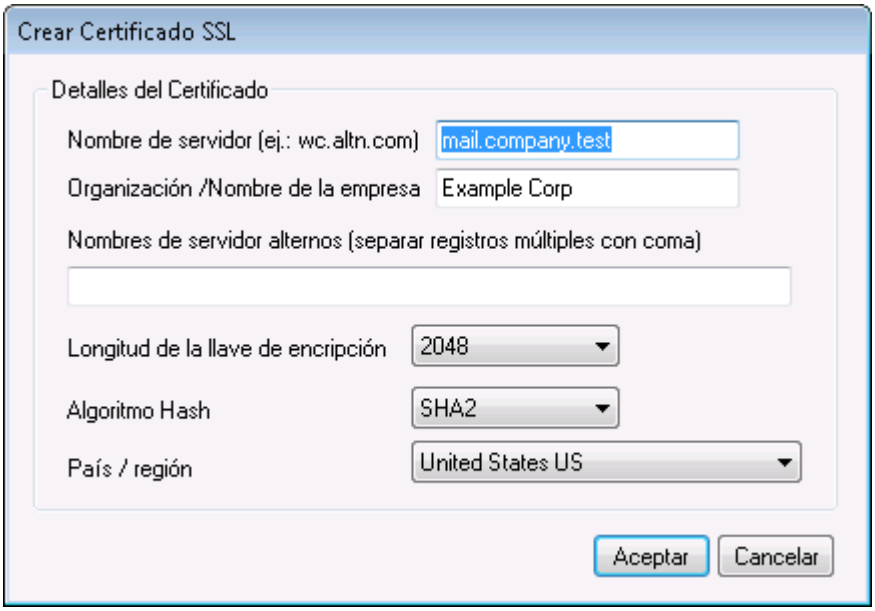
Esta caja despliega sus certificados SSL. Marque la casilla al lado de cualquiera de los certificados que desea estén activos. Dé clic en la estrella al lado del certificado que desea definir como el certificado por omisión. MDaemon soporta la extensión Server Name Indication (SNI) para el protocolo TLS, que permite que se utilice un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará en todos los certificados activos y elegirá aquel que tenga el nombre de host solicitado en su campo Subject Alternative Names (puede especificar los nombres alternos al crear el certificado). Si el cliente no solicita un nombre de host, o si no se encuentra un certificado coincidente, entonces se utilizará el certificado por omisión. Dé doble clic en cualquier certificado para abrir el diálogo de Certificados de Windows para revisar (solo disponible en la interface de aplicaciones no en la administración remota basada en navegador).

Eliminar

Seleccione un certificado en la lista y haga clic en este botón para eliminarlo. Aparecerá un cuadro de confirmación y le preguntará si está seguro de que desea eliminar el certificado.

Crear Certificado

Dé clic en este botón para abrir el diálogo Crear Certificado SSL.



Detalles del Certificado

Nombre de host

Al crear un certificado, introduzca el nombre de host al que quiere que conecten sus usuarios (por ejemplo, "mail.ejemplo.com").

Nombre de empresa/organización

Introduzca aquí el nombre de la organización o empresa que es "propietaria" del certificado.

Nombres de host alternativos (separar entradas múltiples con coma)

Si existen nombres de host alternativos a los que sus usuarios se pueden conectar y desea que este certificado se aplique a esos nombres, regístrelos aquí

separados por coma. Se permiten comodines, de manera que "*.example.com" aplica a todos los subdominios de example.com (por ejemplo, "wc.example.com", " mail.example.com"y demás).

MDaemon soporta la extensión Server Name Indication (SNI) al protocolo TLS, que permite que se utilice un certificado diferente para cada uno de los nombres de host de su servidor. MDaemon buscará en los certificados activos y elegirá aquel que contenga el nombre de host solicitado en el campo Subject Alternative Names. Si el cliente no solicita un nombre de host o si no se encuentra un certificado coincidente, se utilizará el certificado por omisión.

Longitud de clave de encriptación
Seleccione la longitud de bit deseada para la llave de encriptación para este certificado. Mientras más larga sea la llave de encriptación, más seguros serán los datos transferidos. Note, sin embargo, que no todas las aplicaciones soportan llaves mayores de 512.

País/Región
Escoja el País o la región en la que reside su servidor.

Algoritmo Hash
Seleccione el algoritmo hash que desea utilizar: SHA1 o SHA2. El valor por omisión es SHA2.

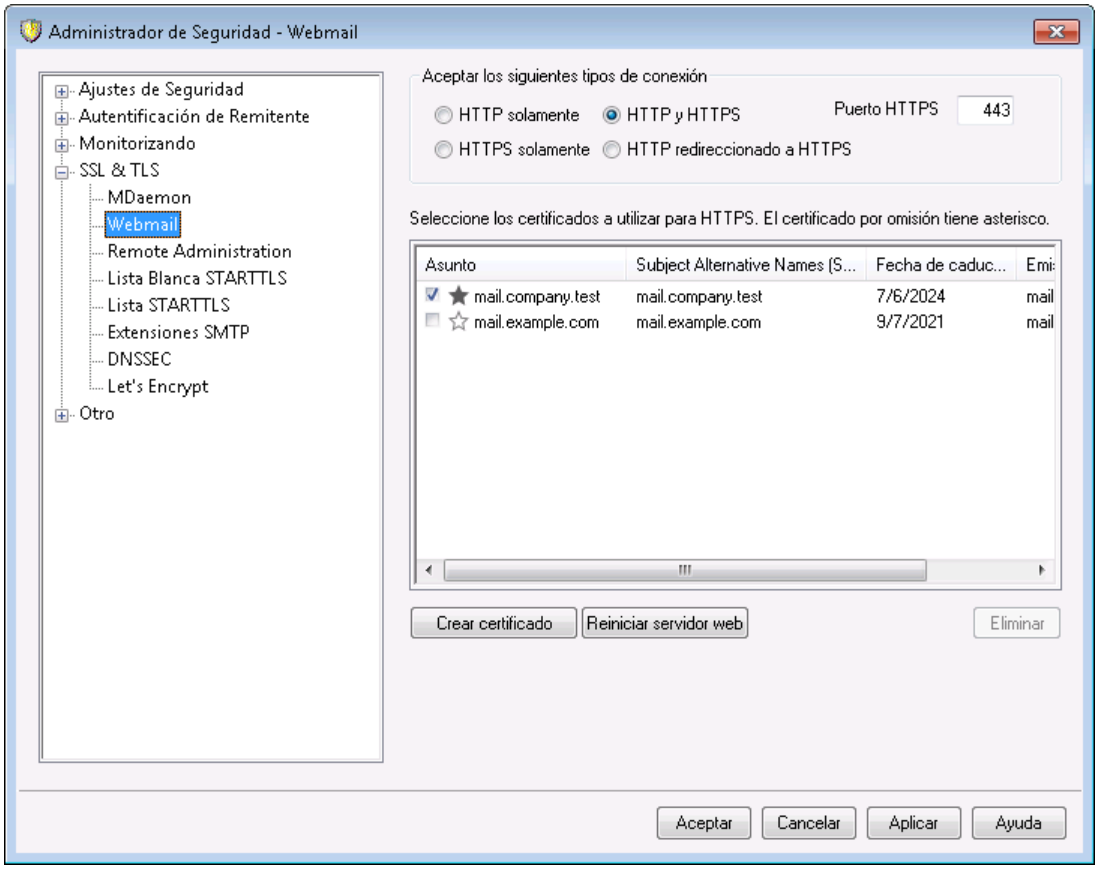
Reiniciar servidores

Haga clic para reiniciar los servidores SMTP/IMAP/POP. Los servidores deben ser reiniciados cuando cambie un certificado.

Ver:

SSL & TLS 575
Crear y Usar Certificados SSL 912

4.2.4.2 Webmail



El servidor web integrado de MDaemon soporta el protocolo Secure Sockets Layer (SSL). SSL es el método estándar para asegurar comunicaciones web cliente/servidor. Proporciona autentificación del servidor, encripción de datos y autentificación opcional del cliente para conexiones TCP/IP. Más aun, dado que el soporte de HTTPS (i.e. HTTP sobre SSL) está integrado en la mayoría de los navegadores, al instalar simplemente un certificado digital válido se activará la conexión del cliente utilizando capacidades SSL.

Las opciones para habilitar y configurar Webmail para utilizar HTTPS se localizan en la pantalla SSL & HTTPS bajo Configuración » Servicios Web & IM » Webmail". Para su conveniencia, sin embargo, estas opciones también se encuentran bajo "Seguridad » Administrador de Seguridad » SSL & TLS » Webmail".

Para más información acerca del protocolo SSL y los Certificados, vea: **SSL y Certificados** 575

Esta pantalla sólo aplica a Webmail cuando se utilice el servidor web integrado. Si configura Webmail para que use algún otro servidor como IIS, estas opciones no se usarán — el soporte SSL/HTTPS tendrá que ser configurado usando las herramientas del otro servidor web.

Aceptar los siguientes tipos de conexiones

Sólo HTTP
Escoja esta opción si no desea permitir ninguna conexión HTTPS a Webmail. Sólo se aceptarán conexiones HTTP.

HTTP y HTTPS
Escoja esta opción si desea activar el soporte SSL dentro de Webmail, pero no desea forzar a los usuarios de Webmail a que utilicen HTTPS. Webmail escuchará conexiones en el puerto HTTPS designado aquí, pero seguirá respondiendo a las conexiones http normales en el puerto TCP de Webmail designado en la pantalla Servidor Web 326 de Webmail.

Sólo HTTPS
Escoja esta opción si desea requerir HTTPS cuando conecte con Webmail. Webmail responderá sólo a conexiones HTTPS cuando se active esta opción — no responderá a solicitudes HTTP.

HTTP es redireccionado a HTTPS
Escoja esta opción si desea redireccionar todas las conexiones HTTP a HTTPS en el puerto HTTPS.

Puerto HTTPS
Utilice este puerto TCP para que Webmail escuche a conexiones SSL. El puerto por defecto para SSL es 443. Si se usa el puerto por defecto, no tendrá que escribir el número de puerto en la URL de WorldClient cuando se conecte vía HTTPS (p. ej. "https://ejemplo.com" es equivalente a "https://ejemplo.com:443").

Esto no es lo mismo que el puerto de Webmail designado en la pantalla Servidor Web 326 de Webmail. Si sigue permitiendo conexiones HTTP a Webmail entonces dichas conexiones deben usar ese otro puerto para conectarse correctamente. Las conexiones HTTPS deberán usar el puerto HTTPS.

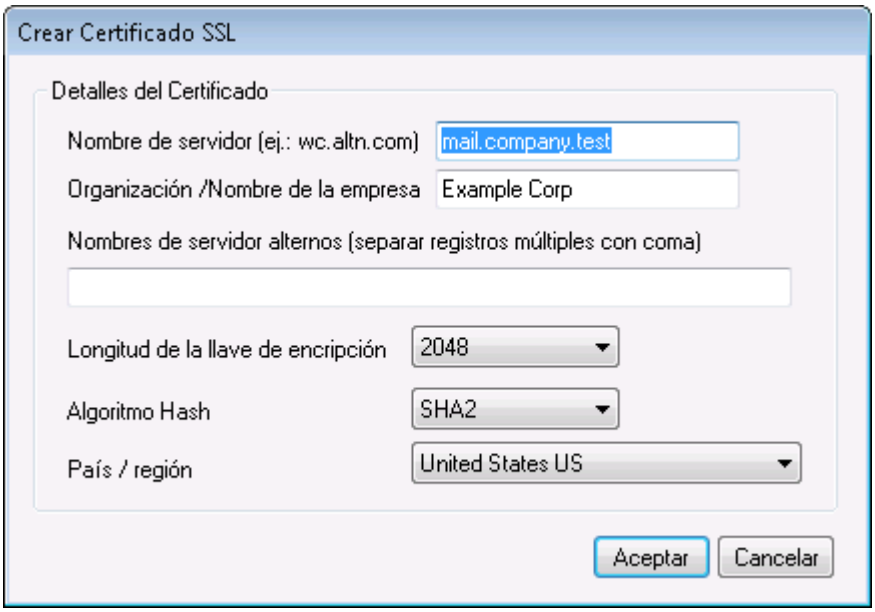
Seleccionar el certificado a utilizar para HTTPS/SSL

Esta caja muestra sus certificados SSL. Marque la caja al lado de cualquier certificado que desee se encuentre activo. Dé clic en la estrella al lado del certificado que desee configurar como el certificado por omisión. MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite utilizar un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará en los certificados activos y elegirá aquel que contenga el nombre de host solicitado en el campo Subject Alternative Names (puede especificar los nombres alternativos al crear el certificado). Si un cliente no solicita un nombre de host o si no se encuentra un certificado coincidente, se utilizará el certificado por omisión. Dé doble clic en cualquier certificado para abrir el diálogo de Certificados de Windows para revisarlo (solo disponible en la interface de escritorio, no en la administración remota vía web).

Eliminar
Seleccione el certificado de la lista y haga clic en este botón para eliminarlo. Un mensaje de confirmación se abrirá y le preguntará si está seguro de que quiere borrar el certificado.

Crear Certificado

Dé clic en este botón para abrir el diálogo Crear Certificado.



Detalles del Certificado

Nombre de Servidor
Al crear un certificado, registre el nombre del servidor al que se conectarán sus usuarios (por ejemplo, "wc.example.com").

Nombre de Organización/empresa
Registre aquí la organización o empresa "propietaria" del certificado

Nombres de servidor alternos (separe múltiples registros con una coma)
Si existen nombres de host alternos a los que se puedan conectar los usuarios y desea que este certificado se aplique también a esos nombres, registre aquí esos nombres de dominio separados por comas. Se permiten comodines, de manera que "`*.example.com`" aplica para todos los subdominios de `example.com` (por ejemplo, "`wc.example.com`", "`mail.example.com`", etc.).

MDaemon soporta la extensión del protocolo TLS denominada Server Name Indication (SNI), que permite que se utilice un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará en los certificados activos y seleccionará aquel que contenga el nombre de host solicitado en el campo Subject Alternative Names. Si el cliente no solicita un nombre de host o no se encuentra un certificado coincidente, se utiliza el certificado por omisión.

Longitud de la llave de Encripción
Seleccione la longitud de bit deseada para la llave de encripción de este certificado. Mientras más larga sea la llave más segura será la transferencia de datos. Note, sin embargo, que no todas las aplicaciones soportan longitudes de llave superiores a 512.

País/región
Elija el país o región en que reside su servidor.

Algoritmo Hash
Elija el algoritmo hash que desea utilizar: SHA1 o SHA2. El valor por omisión es SHA2.

Reiniciar servidor web

Dé clic en este botón para reiniciar el servidor web. Este debe reiniciarse ante de que se utilice un nuevo certificado.

Utilizar Let's Encrypt para Administrar su Certificado

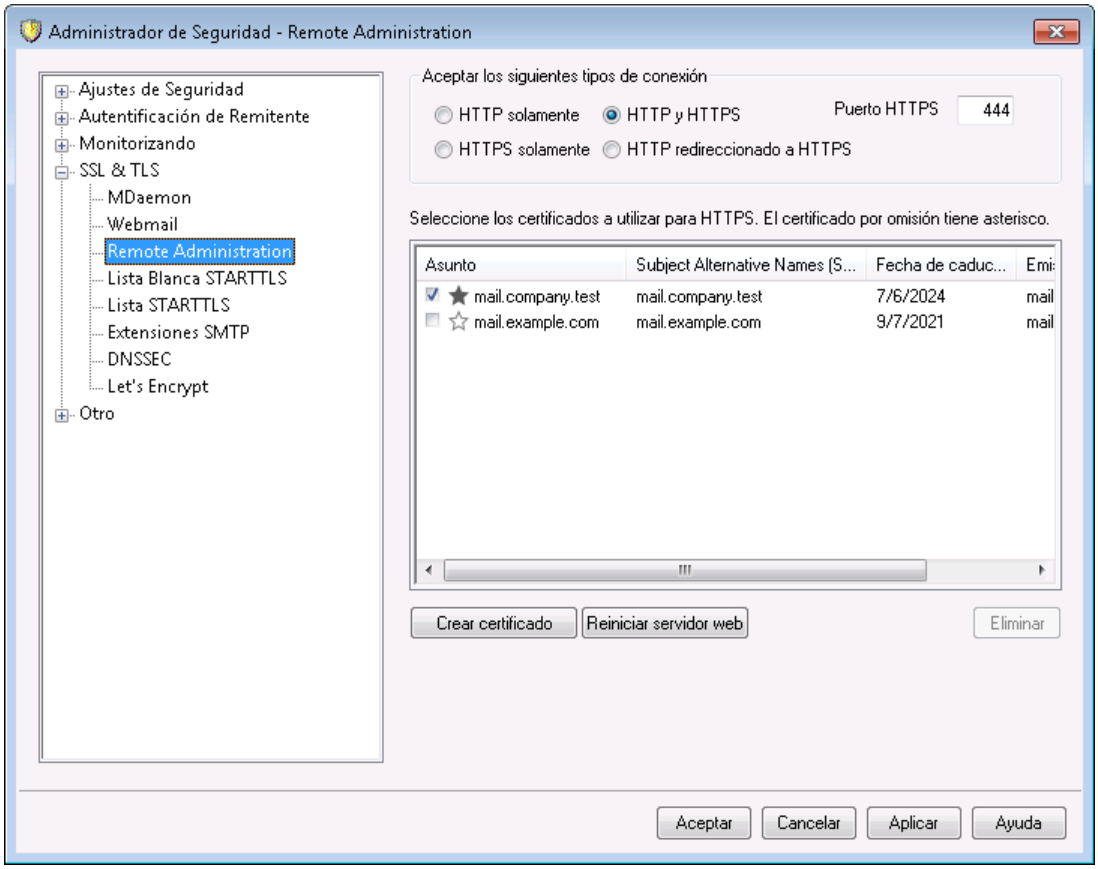
Let's Encrypt es una autoridad de Certificación (Certificate Authority - CA) que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los procesos completos de creación, validación, firma y renovación manuales de certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se cuenta con la pantalla Let's Encrypt 594 para ayudarle a configurar y ejecutar fácilmente el script de PowerShell incluido en la carpeta "`MDaemon\LetsEncrypt`". Al ejecutar el script se configurará todo lo necesario para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta HTTP de Webmail para completar la validación http-01. Utiliza el Nombre de host SMTP 192 del dominio por omisión 190 como dominio para el certificado, incluye cualesquiera *Nombres de host Alternos* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para utilizar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" , denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora del inicio de ejecución del script. También, se envían mensajes de notificación de la ocurrencia de errores, si se especifica una *Cuenta de correo de Admin para notificaciones*. Vea el tema Let's Encrypt 594 para más información.

Ver:

SSL & Certificados 575
Crear y Utilizar Certificados SSL 912

4.2.4.3 Administración Remota



El servidor web integrado en MDaemon soporta el protocolo Secure Sockets Layer (SSL). SSL es el método estándar de asegurar las comunicaciones web servidor/cliente. Proporciona autentificación de servidor, encripción de datos y autentificación opcional de cliente para conexiones TCP/IP. Más aun, dado que el soporte HTTPS (i.e. HTTP sobre SSL) está integrado en todos los principales navegadores, al instalar simplemente un certificado digital en su servidor, se activarán las capacidades de conexión SSL de los clientes.

Las opciones para habilitar y configurar la Administración Remota para utilizar HTTPS se localizan en la pantalla SSL & HTTPS bajo Configuración » Web & Servicios IM » Administración Remota". Para su conveniencia, sin embargo, estas opciones también se encuentran bajo "Seguridad » Ajustes de Seguridad » SSL & TLS » Administración Remota".

Para más información sobre el protocolo SSL y Certificados ver: **SSL & Certificados** 575

Esta pantalla solamente aplica para la Administración Remota al utilizar el servidor web integrado de MDaemon. Si configura la Administración Remota para utilizar algún otro servidor web tal como IIS, estas opciones no se utilizarán — el soporte a SSL/HTTPS tendrá que ser configurado utilizando las herramientas del otro servidor web.

Aceptar los siguientes tipos de conexión

Solo HTTP
Seleccione esta opción si no desea permitir conexiones HTTPS para la Administración Remota. Solo se aceptarán conexiones HTTP.

HTTP y HTTPS
Seleccione esta opción si desea habilitar soporte SSL para la Administración Remota, pero no desea forzar a los usuarios de la Administración Remota a utilizar HTTPS. Administración Remota escuchará conexiones en el puerto HTTPS definido abajo, pero de todas maneras responderá a conexiones HTTP normales en el puerto TCP asignado para la Administración Remota en la pantalla Servidor Web 356.

Solo HTTPS
Seleccione esta opción si desea requerir HTTPS al conectarse a la Administración Remota. Esta responderá solo a conexiones HTTPS cuando esta opción esté habilitada — no responderá a peticiones HTTP.

HTTP redirigido a HTTPS
Seleccione esta opción si desea redirigir todas las conexiones HTTP a HTTPS en el puerto HTTPS.

Puerto HTTPS
Este es el puerto TCP en el que la Administración Remota escuchará las conexiones SSL. El puerto SSL por omisión es el 443. Si se utiliza este puerto, no tendrá que incluir el número de puerto en la URL de la Administración Remota al conectarse vía HTTPS (ej. "https://example.com" es equivalente a "https://example.com:443").

Este no es el mismo puerto para Administración Remota que se define en la pantalla Servidor Web 356. Si está permitiendo conexiones HTTP para la Administración Remota entonces esas conexiones deben utilizar ese otro puerto para conectarse exitosamente. Las conexiones HTTPS deben utilizar el puerto HTTPS.

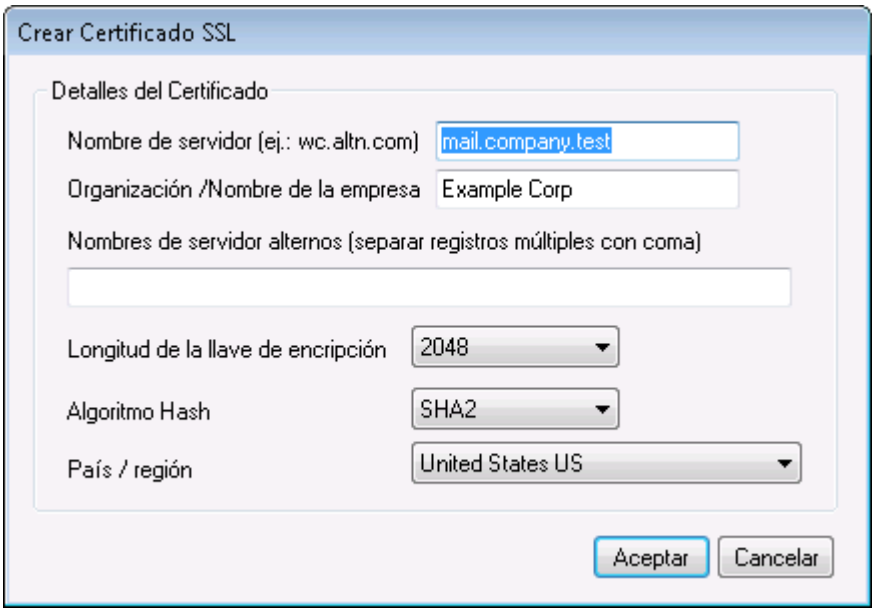
Seleccionar certificado a utilizar para HTTPS/SSL

Esta caja muestra sus certificados SSL. Marque la casilla al lado de cualquier certificado que desee activar. Dé clic en la estrella al lado del que desea que se considere el certificado por omisión. MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite que se utilice un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon buscará los certificados activos y elegirá el que contenga el nombre de host solicitado en el campo Subject Alternative Names (puede especificar los nombres alternos al crear el certificado). Si el cliente no solicita un nombre de host o si no se encuentra un certificado coincidente, se utilizará el certificado por omisión. Dé doble clic en cualquier certificado para abrirlo en el diálogo de Certificados de Windows, para revisarlo (solo disponible en la interface de escritorio, no en la administración remota vía web).

Eliminar
Seleccione un certificado en la lista y dé clic en este botón para eliminarlo. Se abrirá una caja de conformación que le preguntará si está seguro de que desea eliminar ese certificado.

Crear Certificado

Dé clic en este botón para abrir el diálogo Crear Certificado .



Detalles del Certificado

Nombre de Servidor
Al crear un certificado, registre qué usuarios se conectarán (por ejemplo "wc.example.com").

Organización/nombre de empresa
Registre aquí la organización o empresa "propietaria" del certificado.

Nombres de servidor alternativos (separe múltiples registros con una coma)
Si se tienen nombres de host alternativos a los que se puedan conectar los usuarios y desea que este certificado aplique también para esos nombres, entonces registre aquí los nombres de dominio separados por comas. Se permiten comodines, de manera que "`*.example.com`" aplicará para todos los subdominios de `example.com` (por ejemplo, "`wc.example.com`", "`mail.example.com`"y demás).

MDaemon soporta la extensión Server Name Indication (SNI) del protocolo TLS, que permite utilizar un certificado distinto para cada uno de los nombres de host de su servidor. MDaemon revisará los certificados activos y elegirá el que contenga el nombre de host solicitado en el campo Subject Alternative Names. Si el cliente no solicita un nombre de host o no se encuentra un certificado correspondiente, se utilizará el certificado por omisión.

Longitud de la llave de Encripción
Seleccione la longitud de bit deseada para la llave de encripción de este certificado. Mientras más larga sea más segura será la transferencia de datos. Note, sin embargo, que no todas las aplicaciones soportan longitudes de llave mayores de 512.

País/región
Elija el país o región en que reside su servidor.

Algoritmo Hash
Elija el algoritmo hash que desea utilizar: SHA1 o SHA2. El ajuste por omisión es SHA2.

Reiniciar el servidor web

Dé clic en este botón para reiniciar el servidor web. Este se debe reiniciar antes de utilizar el nuevo certificado.

Utilizar Let's Encrypt para Administrar su Certificado

Let's Encrypt es una autoridad de Certificación (Certificate Authority - CA) que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los procesos completos de creación, validación, firma y renovación manuales de certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se cuenta con la pantalla Let's Encrypt[594] para ayudarle a configurar y ejecutar fácilmente el script de PowerShell incluido en la carpeta "`MDaemon\LetsEncrypt`". Al ejecutar el script se configurará todo lo necesario para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta HTTP de Webmail para completar la validación http-01. Utiliza el Nombre de host SMTP[192] del dominio por omisión[190] como dominio para el certificado, incluye cualesquiera *Nombres de host Alternos* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para utilizar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" , denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora del inicio de ejecución del script. También, se envían mensajes de notificación de la ocurrencia de errores, si se especifica una *Cuenta de correo de Admin para notificaciones*. Vea el tema Let's Encrypt[594] para más información.

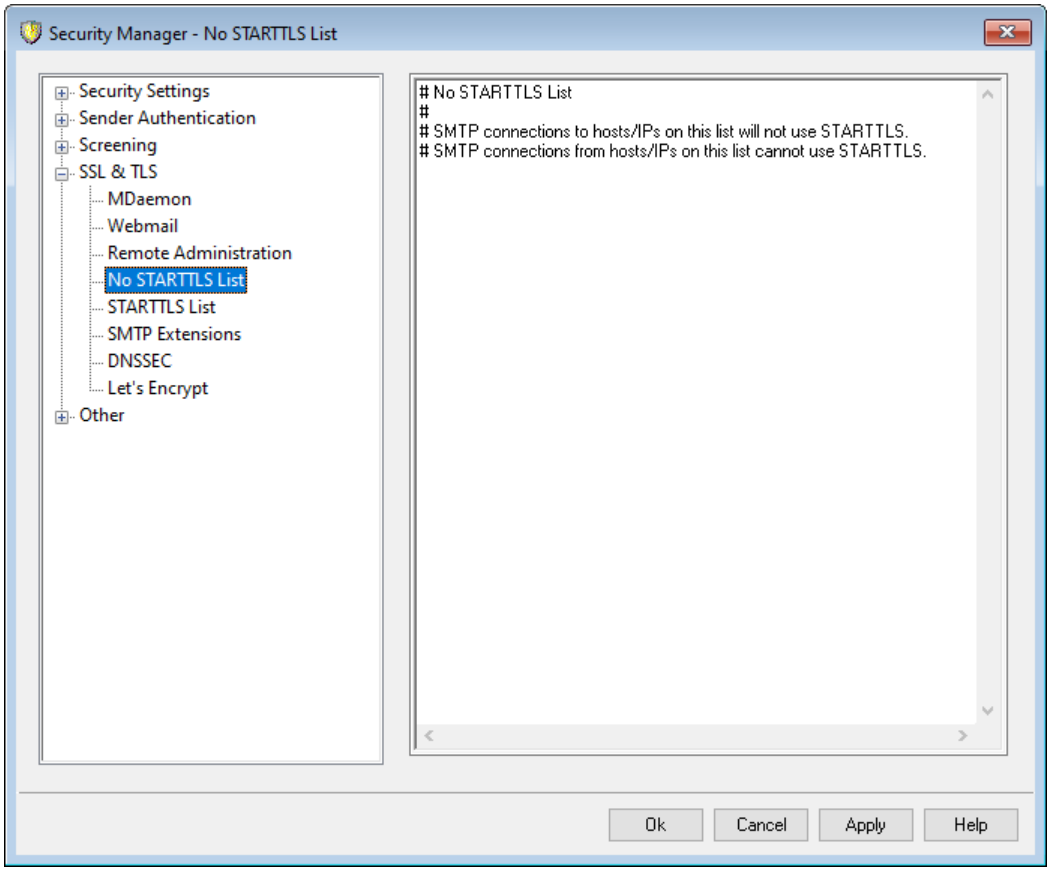
Para más información sobre SSL y Certificados ver:

SSL y Certificados 575
Crear y Utilizar Certificados SSL 912

Para más información sobre Administración Remota ver:

Configuración Remota 354
Administración Remota » Servidor Web 356
Valores por Omisión de Acceso Web 798
Editor de Cuentas » Web 720
Artículo de la Base de Conocimientos: How to setup Webmail, Remote Administration, ActiveSync, CalDav, CardDav, AutoDiscover, MDDP, Webmail API, and XML API services in IIS

4.2.4.4 Lista No STARTTLS



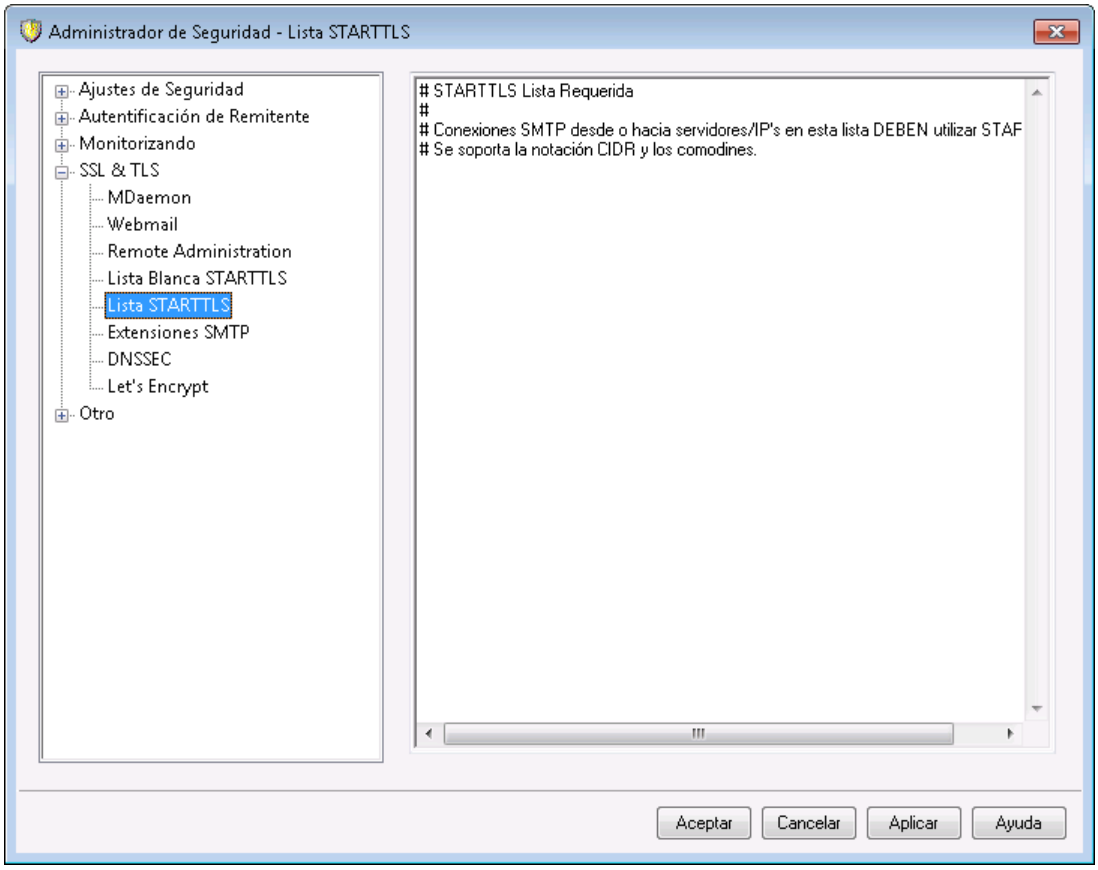
Use esta lista para prevenir el uso de STARTTLS cuando envíe o reciba correo de ciertos servidores o direcciones IP

La Lista No STARTTLS tiene precedencia sobre la Lista de STARTTLS Requerido 589 y la opción *El Servidor SMTP requiere STARTTLS en el puerto MSA* 577.

La extensión STARTTLS para SMTP se define en RFC-3207, que se puede consultar en:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.2.4.5 Lista STARTTLS

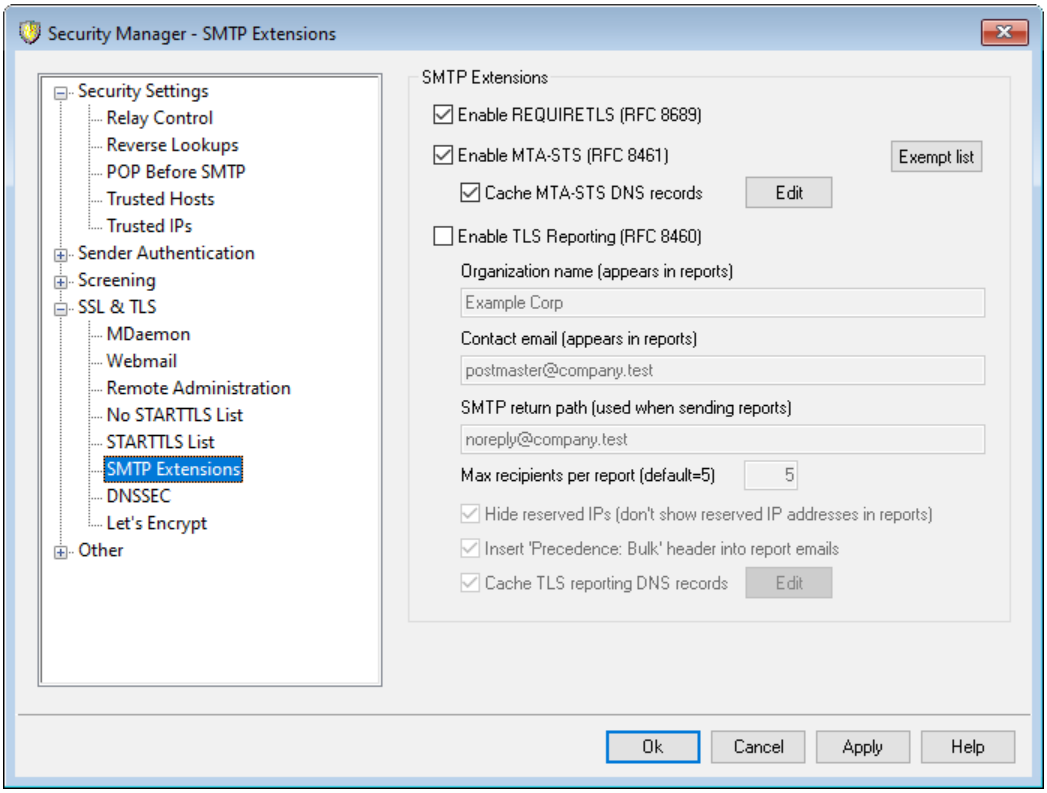


Utilice esta pantalla para especificar los servidores, direcciones IP y direcciones MAIL FROM que requieren el uso de la extensión STARTTLS a fin de recibir o enviar correo desde o hacia su servidor.

La extensión STARTTLS para SMTP se define en RFC-3207, que se puede visualizar en:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.2.4.6 Extensiones SMTP



Extensiones SMTP

Habilitar REQUIRETLS (RFC 8689)

RequireTLS le permite marcar mensajes que **deben** ser enviados utilizando TLS. Si no es posible TLS (o si los parámetros del intercambio de certificado TLS son inaceptables) los mensajes serán rechazados en lugar de ser entregados inseguramente. Para una descripción completa de RequireTLS, vea: RFC 8689: SMTP Require TLS Option.

RequireTLS se encuentra habilitado por omisión pero los únicos mensajes que estarán sujetos al proceso RequireTLS son los mensajes específicamente marcados por una regla del Filtro de contenido utilizando la nueva acción del Filtro de Contenido 648, "*Marcar mensajes para REQUIRETLS...*", o mensajes enviados a `<local-part>+requiretls@domain.tld` (por ejemplo, `arvel+requiretls@mdaemon.com`). Todos los demás mensajes serán tratados como si el servicio estuviera deshabilitado. Se deben cumplir varios requerimientos a fin de que un mensaje se envíe utilizando RequireTLS. Si cualquiera de ellos falla, el mensaje será rechazado en lugar de ser enviado si validación. Los requerimientos son:

- RequireTLS debe estar habilitado.
- El mensaje debe estar marcado como que requiere el tratamiento RequireTLS, vía la acción del Filtro de contenido o la dirección "`<localpart>+requiretls@...`".
- Las consultas DNS para hosts MX destino deben utilizar DNSSEC 593 (ver abajo) o el MX debe ser validado vía MTA-STS.
- La conexión al host destino debe utilizar SSL (STARTTLS).
- El certificado SSL del host destino debe coincidir con el nombre del host MX y la cadena de una entidad certificadora confiable.

- El servidor destino debe soportar REQUIRETLS y manifestarlo en la respuesta EHLO.

RequireTLS requiere de consultas DNSSEC de registros MX de hosts, o el MX debe ser validado vía MTA-STS. Puede configurar DNSSEC[593] especificando los criterios con los que las consultas solicitarán el servicio DNSSEC. La funcionalidad Caché de IP[121] cuenta con una opción para aceptar declaraciones DNSSEC y existen instrucciones relativas a DNSSEC en el encabezado del archivo de Hosts MX Hosts[113]. Finalmente, DNSSEC requiere de servidores de DNS configurados adecuadamente, lo cual va más allá del alcance de este archivo de ayuda.

Habilitar MTA-STS (RFC 8461)
El soporte a MTA-STS se encuentra habilitado por omisión y se describe en RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP MTA Strict Transport Security (MTA-STS) es un mecanismo que habilita a los proveedores de correo (SPs) a declarar su capacidad de recibir conexiones SMTP seguras utilizando TLS (Transport Layer Security) y a especificar si los servidores SMTP remitentes deberán rehusar la entrega a hosts MX que no ofrezcan TLS con un certificado de servidor confiable. Para configurar MTA-STS para su propio dominio, necesitará un archivo de política MTA-STS que se puede descargar vía HTTPS de la URL https://mta-sts.domain.tld/.well-known/mta-sts.txt, donde "domain.tld" es su nombre de dominio. El archivo de política debe contener líneas con el formato siguiente:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

Mode puede ser "none", "testing", o "enforce". Debe haber una línea "mx" para cada uno de sus nombres de host MX. Se puede utilizar comodines para subdominios, tal como "*.domain.tld". Max age es en segundos. Los valores comunes son 86400 (1 día) y 604800 (1 semana).

También se necesita un registro DNS TXT en _mta-sts.domain.tld, donde "domain.tld" es su nombre de dominio. Debe tener un valor con el formato:

```
v=STSv1; id=20200206T010101;
```

El valor para "id" se debe modificar cada vez que el archivo de política se modifique. Es común utilizar la fecha/hora (timestamp) para el id.

Lista de Exentos
Utilice esta lista para exentar dominios específicos de MTA-STA .

Cache de registros MTA-STS DNS
MDaemon por omisión guarda en caché registros MTA-STS DNS. Dé clic en **Editar** para visualizar o editar el archivo de caché actual.

Habilitar reporteo TLS (RFC 8460)
El reporteo TLS se encuentra deshabilitado por omisión y se discute en RFC 8460: SMTP TLS Reporting.

El reporteo TLS permite a los dominios que utilizan MTA-STS ser notificados sobre cualquier fallo para recuperar la política MTA-STS o negociar un canal seguro utilizando STARTTLS. Al habilitarse, MDaemon enviará un reporte diario a

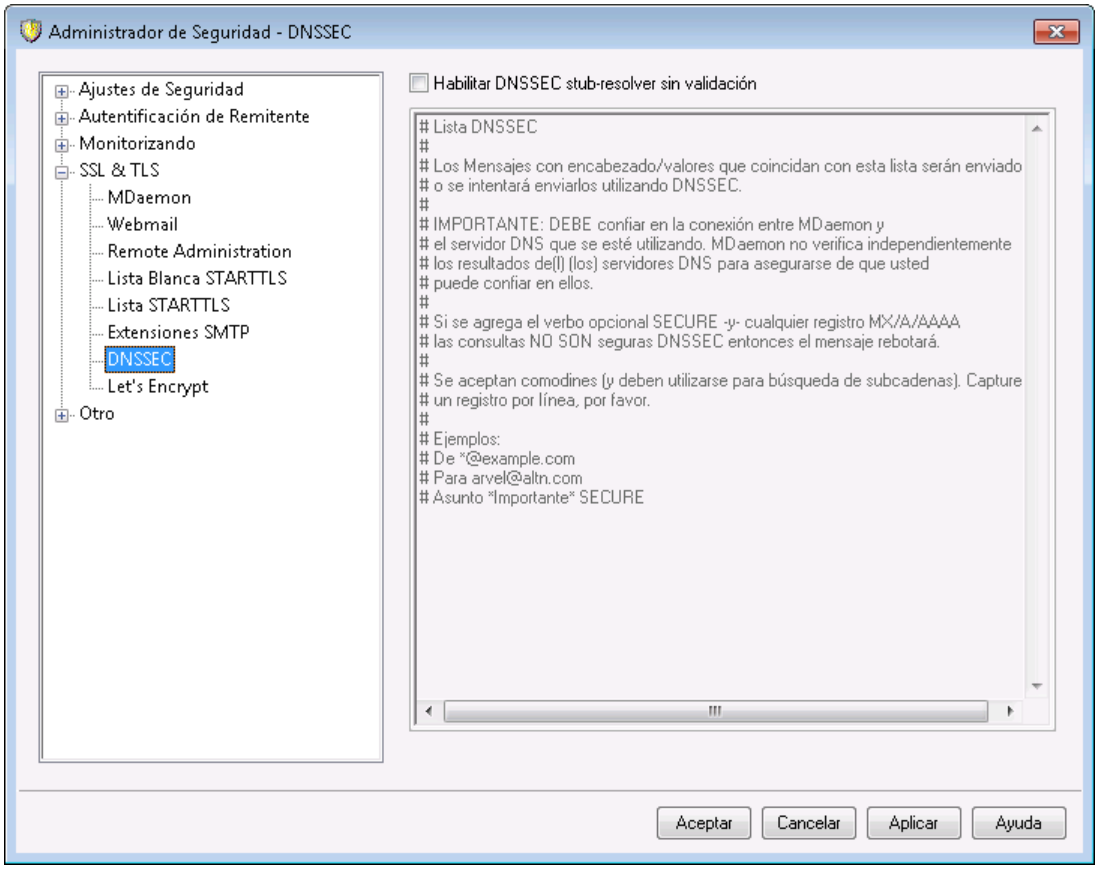
cada dominio habilitado para STS al que ha enviado (o intentado enviar) correo ese día. Existen varias opciones proporcionadas para configurar la información que contendrán sus reportes.

Para configurar el Reporteo TLS para su dominio, habilite Firma DKIM 532 y cree un registro DNS TXT en `_smtp._tls.domain.tld`, donde "domain.tld" es su nombre de dominio, con un valor con el formato:

```
v=TLSRPTv1; rua=mailto:mailbox@domain.tld
```

Donde mailbox@domain.tld es la dirección de correo donde quiere que se envíen los reportes de su dominio.

4.2.4.7 DNSSEC



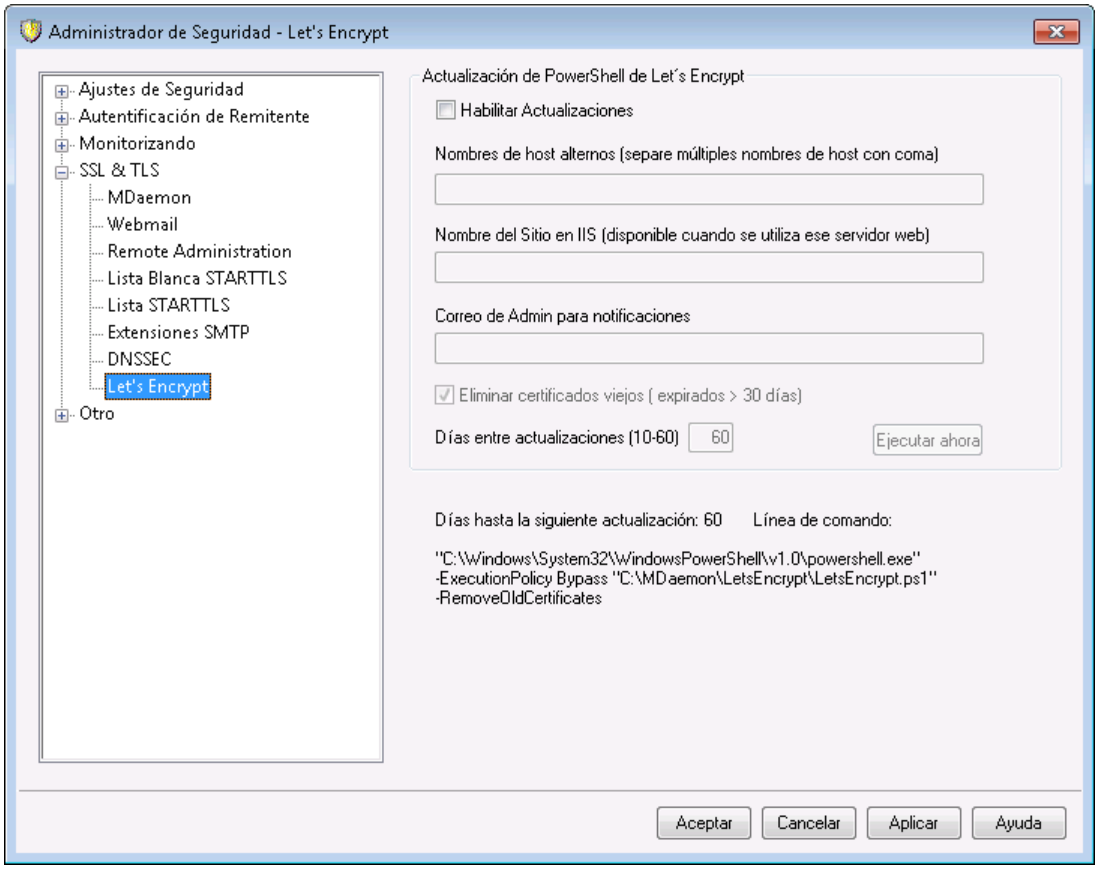
La opción DNSSEC (DNS Security Extensions) permite a MDaemon actuar como un "Stub Resolver" No Validador, de Seguridad, que se define en los RFCs 4033 y 4035 como "una entidad que envía consultas DNS, recibe respuestas DNS y es capaz de establecer un canal seguro apropiado hacia un servidor de nombres seguro recursivo que proporcionará esos servicios por parte de un stub resolver seguro". Esto significa que durante las consultas DNS de MDaemon, puede solicitar el servicio DNSSEC de sus servidores DNS, estableciendo el bit AD (Authentic Data) en las consultas y verificándolas en las respuestas. Esto puede proporcionar un nivel adicional de seguridad durante el procesamiento DNS para algunos mensajes, aunque no todos, dado que DNSSEC aún no está soportado por todos los servidores DNS o por todos los dominios de nivel superior.

Cuando se habilita, el servicio DNSSEC solo se aplica a mensajes que cumplen sus criterios de selección; se puede solicitar o requerir tan amplia o estrictamente como usted decida. Simplemente defina cualquier combinación de "`Header Value`" a su elección en esta pantalla y MDaemon solicitará el servicio DNSSEC para los mensajes que coincidan con estos criterios siempre que ejecute una consulta de DNS. Cuando los resultados de DNS no incluyan datos autentificados, entonces no habrá consecuencias negativas; MDaemon simplemente regresará a su comportamiento de DNS normal. Sin embargo, si usted desea *requerir* DNSSEC para ciertos mensajes, agregue "SECURE" a la combinación header/value (ej. `To *@example.net SECURE`). Para esos mensajes, cuando los resultados DNS fallan porque no incluyen datos autentificados, el mensaje será regresado al remitente. **Nota**: Dado que las consultas DNSSEC consumen más tiempo y recursos y porque DNSSEC aún no está soportado por todos los servidores, MDaemon no está configurado para aplicar DNSSEC por omisión para la entrega de todos los mensajes. Sin embargo, si usted desea utilizar DNSSEC para todos los mensajes, lo puede hacer incluyendo "`To *`" en sus criterios.

Los registros de las sesiones de correo incluirán una línea en el encabezado si el servicio DNSSEC fue utilizado y "DNSSEC" aparecerá al lado de los datos seguros, en los registros.

Dado que MDaemon es un "Stub Resolver" no validador, solicitará datos autentificados de su servidor DNS pero no tiene manera de verificar independientemente que los datos que obtiene del servidor son seguros. Por esta razón, para utilizar exitosamente la opción DNSSEC, debe asegurarse de que confía en la conexión a su servidor de DNS. Por ejemplo, si se ejecuta en localhost o en una LAN o ubicación segura.

4.2.4.8 Let's Encrypt



Utilizar Let's Encrypt para administrar su Certificado

Para soportar SSL/TLS y HTTPS 575 para MDaemon 577, Webmail 580 y Administración Remota 584, necesita contar con un Certificado SSL/TLS. Los Certificados son pequeños archivos emitidos por una Autoridad de Certificación (Certificate Authority o CA) que se utilizan para verificar a un cliente o navegador que se ha conectado al servidor que pretendía y habilita SSL/TLS/HTTPS para asegurar la conexión a ese servidor. Let's Encrypt es un CA que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar la complejidad del proceso manual actual de crear, validar, firmar, instalar y renovar los certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se proporciona esta pantalla para apoyarle a configurar y ejecutar el script de PowerShell incluido en la carpeta "`MDaemon\LetsEncrypt`". Al ejecutar el script se configurará todo para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta Webmail HTTP para completar la validación http.01. Utiliza el nombre de host SMTP 192 del dominio por omisión 190 como dominio para el certificado, incluye cualquier *Nombres Alternos de host* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para usar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora de inicio del script. También se enviarán correos de notificación cuando ocurran errores, si lo especifica en *Correo del Admin para notificaciones*.

Let's Encrypt requiere PowerShell 5.1 y .Net Framework 4.7.2, lo que significa que no funcionará en Windows 2003. Así mismo, Webmail 326 debe estar escuchando en el puerto 80 y el script no funcionará si usted tiene configurado un nombre de host SMTP 192 (i.e. FQDN) para su dominio por omisión, que no apunte a su servidor MDaemon.

Actualizaciones de PowerShell de Let's Encrypt

Habilitar actualizaciones
Dé clic en esta casilla si desea crear y actualizar automáticamente una certificación SSL/TLS vía el script de Let's Encrypt. El certificado se actualizará cada 10-60 días de acuerdo con el ajuste indicado abajo *Días entre actualizaciones*.

Nombres Alternos de host (separe múltiples nombres de host con coma)
Si desea configurar hombres de host alternos en el certificado, específíquelos aquí, separados por comas. No necesita incluir el nombre de host SMTP para su dominio por omisión en esta lista. Por ejemplo, si su dominio por omisión fuera "`example.com`," configurado con un nombre de host SMTP "`mail.example.com`" y desea utilizar el nombre de host alterno "`imap.example.com`," entonces solo debe incluir "`imap.example.com`" como nombre de host alterno. Si no desea utilizar ningún nombre de host alterno, deje esta opción en blanco. **Nota:** si incluye nombres de host alternos, la validación HTTP para Let's Encrypt debe completarse para cada uno de ellos para validar el control de su servidor sobre ese nombre de host. Si la validación no se completa el proceso fallará.

Nombre de sitio IIS (disponible cuando se utiliza un servidor web externo)
Si está ejecutando Webmail vía IIS, ingrese el nombre del sitio IIS aquí. Debe tener instaladas las herramientas de Web Scripting de Microsoft a fin de que el certificado se configure automáticamente en IIS.

Correo del Admin para notificaciones
Especifique aquí la dirección de correo de un administrador si desea ser notificado cuando ocurra un error durante la actualización de Let's Encrypt.

Eliminar certificados antiguos (expirados > 30 días)
Por omisión, MDaemon eliminará cualquier certificado antiguo que haya expirado hace más de 30 días. Deshabilite esta casilla si no desea que se eliminen automáticamente.

Días entre actualizaciones (10-60)
Utilice esta opción para especificar la frecuencia con que deberá actualizarse su certificado, de 10 a 60 días. El ajuste por omisión es 60 días.

Ejecutar Ahora
Dé clic en este botón para ejecutar el script de inmediato.

4.2.5 Otros

4.2.5.1 Protección de Backscatter - Descripción

Backscatter

"Backscatter" se refiere a los mensajes de respuesta que sus usuarios reciben de correos que nunca han enviado. Esto ocurre cuando los mensajes de spam o mensajes enviados con virus contienen una dirección de "Return-Path" falsificada. Consecuentemente, cuando uno de estos mensajes es rechazado por el servidor de destino, o si el servidor tiene una autorespuesta de "fuera de la oficina/vacaciones" asociada con su cuenta, el mensaje de respuesta se dirigirá a la dirección falsificada. Esto puede provocar a gran número de Notificaciones de Estado de Entrega (DSNs) falsos o mensajes de autorespuesta que acaban en los buzones de sus usuarios. Además, los spammers y los autores de virus frecuentemente toman ventaja de este fenómeno y algunas veces lo usan para lanzar ataques de Denegación de Servicio (DoS) contra los servidores de correo, provocando que llegue una avalancha de correos no válidos de servidores ubicados en todo el mundo.

La Solución de MDaemon

Para combatir al backscatter, MDaemon contiene una funcionalidad llamada Protección de Backscatter (BP). BP puede ayudarle a asegurar que sólo lleguen Mensajes de Estado de Entrega y autorespuestas válidos a sus cuentas, usando un hash de clave privada, método que genera e inserta un código sensible a la hora en la dirección de "Return-Path" de los mensajes salientes de sus usuarios. Entonces, cuando uno de estos mensajes se encuentra un problema de entrega y es devuelto, o cuando se recibe una autorespuesta con una ruta de entrega "`mailer-daemon@...`" o `NULL`, MDaemon verá el código especial y sabrá que es un correo genuinamente automatizado en respuesta a un mensaje enviada por una de sus cuentas. Si la dirección no contiene el código especial, o si el código tiene más de siete días de antigüedad, será registrado por MDaemon y podrá ser rechazado.

La Protección de Backscatter[598] está ubicada bajo el menú Seguridad de MDaemon en: Seguridad » Ajustes de Seguridad » Otro » Protección de Backscatter.

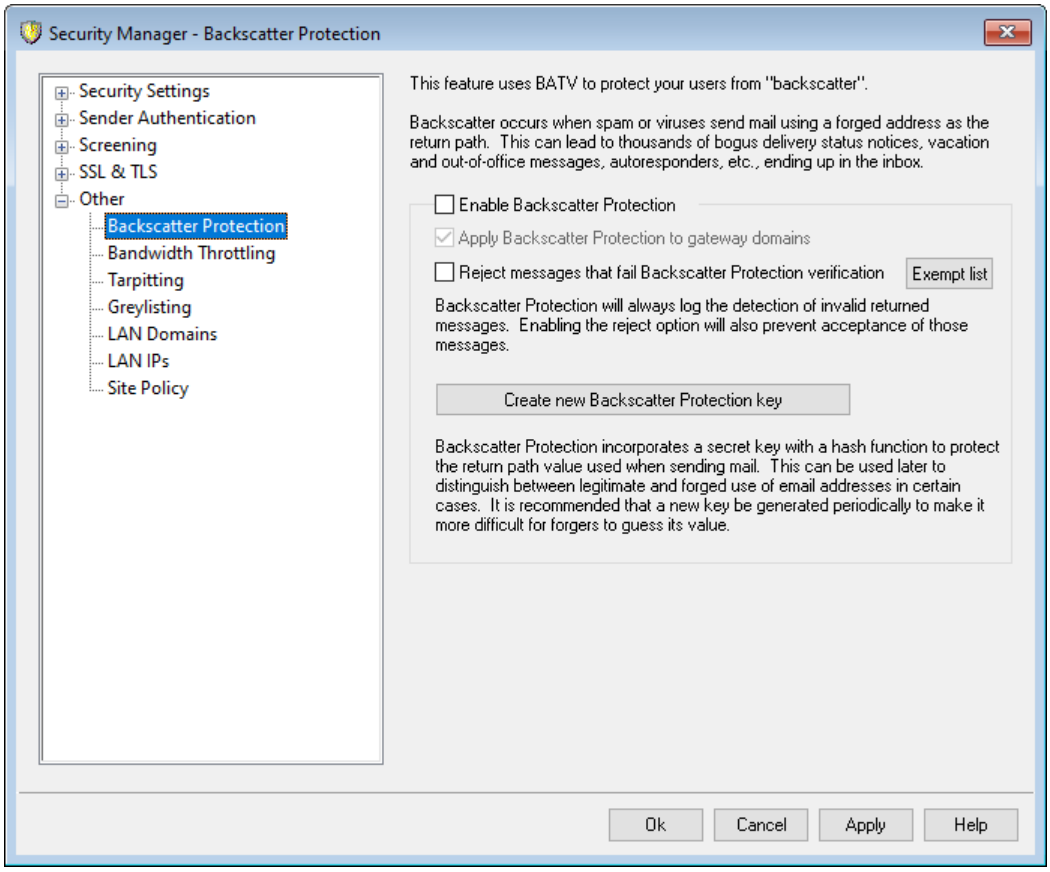
La protección de Backscatter es una implementación de Bounce Address Tag Validation (BATV). Para más acerca de BATV, visite:

`http://www.mipassoc.org/batv/`

Ver:

Protección de Backscatter[598]

4.2.5.1.1 Protección Backscatter



Protección de Backscatter

Habilitar Protección Backscatter
Haga clic en esta casilla si desea insertar un código de Protección especial de Backscatter en cada una de las direcciones de "Return-Path" de los mensajes. MDaemon generará este código especial usando la clave privada encontrada en el archivo `rsa.private` ubicado en la carpeta de MDaemon `PEM\_batv\`, y el código será válido durante 7 días. Cualquier DSN o mensaje de autorespuesta entrantes (con una dirección de retorno de "`mailer-daemon@...`" o `NULL`) debe tener un código BP válido y no expirado o fallarán la verificación de BP.

Si deshabilita esta opción, MDaemon no insertará el código especial de protección de Backscatter en los mensajes salientes. Sin embargo, continuará comprobando los DSNs y autorespuestas entrantes para asegurarse que ningún mensaje entrante con un código válido sea rechazado por error.

Aplicar la Protección de Backscatter a los dominios de puerta de enlace
Cuando se habilita la protección de Backscatter, haga clic en esta opción si también desea aplicarla a los dominios para los que MDaemon actúa como puerta de enlace o servidor de respaldo (vea Administrador de Puertas de Enlace 255).

Rechazar mensajes que fallen en la verificación de Backscatter
Haga clic en esta casilla si desea rechazar DSNs y otros mensajes de autorespuesta que fallen la verificación BP. Los mensajes con una dirección de respuesta de "mailer-daemon@..." o NULL darán error si no contienen el código especial o si los siete días del ciclo de vida del código han expirado. Dada la solidez de la Protección de Backscatter, no hay falsos positivos o "áreas grises" — un mensaje es válido o no lo es. Por esta razón es seguro configurar MDaemon para que rechace los mensajes inválidos, mientras se asegure que todos los mensajes salientes de sus cuentas contengan el código especial de BP. En todos los casos, sin embargo, el resultado de la verificación BP será registrado en el archivo log SMTP-in, aun y cuando escoja no rechazar los mensajes que fallen la verificación. Los mensajes entrantes para puertas de enlace no serán rechazados a menos que aplique la opción anterior de *...aplicar la Protección de Backscatter a los dominios de puerta de enlace.*

Cuando habilita la Protección de Backscatter, deberá esperar alrededor de una semana antes de configurarlo para que rechace mensajes de autorespuesta inválidos. Esto es porque durante ese tiempo puede seguir recibiendo DSNs o autorespuestas a mensajes que fueron enviados antes de que se activara BP. Si BP se configura para rechazar mensajes inválidos durante ese periodo entonces esos mensajes de respuesta legítimos serán rechazados por error. Después de una semana debería ser seguro empezar a rechazar mensajes inválidos. Este mismo aviso aplica cuando crea una nueva clave BP y escoge eliminar la clave antigua inmediatamente en lugar de permitir que continúe funcionando otros siete días. (Vea la opción siguiente *Crear una nueva llave de protección Backscatter*).

Lista de Exentos
Haga clic en este botón para abrir la lista de Exentos de Protección Backscatter. Use esta lista para designar cualquier dirección IP o dominios que desee estén exentos de la Protección Backscatter.

Crear una nueva llave de protección Backscatter
Haga clic en este botón para generar una nueva clave de Protección Backscatter. Esta clave es usada por MDaemon para crear y luego verificar los códigos especiales BP que se insertan en los mensajes. La clave está ubicada en un archivo llamado rsa.private en la carpeta de MDaemon PEM_batv\. Cuando se genera la nueva clave, se abrirá un cuadro para informarle que la clave antigua continuará funcionando durante siete días más a menos que desee borrarla inmediatamente. Si escoge borrar la clave inmediatamente ello podría causar que algunos mensajes entrantes fallen la verificación BP, puesto que serían respuestas a mensajes que contienen el código especial generado por la clave antigua.

Si tiene su tráfico de correo dividido entre múltiples servidores, puede que necesite compartir la clave con todos los otros servidores o Mail Transfer Agents (MTAs).

Ver:

Protección Backscatter - Descripción 597

4.2.5.2 Regular el tráfico del ancho de banda - Descripción

La funcionalidad de Regulación del Tráfico del Ancho de Banda hace posible que controle el consumo de ancho de banda usado por MDaemon. Puede controlar la velocidad a la que las sesiones o servicios progresan — puede establecer diferentes velocidades para cada servicio primario de MDaemon en base a dominio, incluyendo los dominios y las puertas de enlace. También puede establecer límites en conexiones locales seleccionando "Tráfico Local" del cuadro desplegable. Esto le permite crear configuraciones especiales de ancho de banda que tendrán efecto si la conexión se realiza desde o hacia una IP local o nombre de dominio.

La Regulación de ancho de banda puede aplicarse en base a sesión o en base a servicio. Cuando se usa en modo por sesión, cada sesión será regulada independientemente a la velocidad asociada. Así pues, múltiples sesiones del mismo tipo de servicio que ocurran de manera simultánea podrían exceder el valor configurado de un servicio. Cuando se configura una regulación de ancho de banda en base a servicio, MDaemon monitoreará el uso combinado de todas las sesiones del mismo tipo de servicio y distribuirá fracciones iguales del total de ancho de banda a cada uno. Entonces múltiples sesiones compartirán el máximo configurado de ancho de banda por igual. Esto permite establecer un límite a un servicio por completo.

Cuando se extiende la regulación de ancho de banda a una puerta de enlace de dominio, debe manejarse de manera un tanto diferente que un dominio normal puesto que las puertas de enlace de dominio no tienen dirección IP específica asociada a ellos. MDaemon debe usar el valor pasado en el comando RCPT para determinar si una sesión entrante de SMTP está destinada o no a una puerta de enlace. Si lo está, la regulación de ancho de banda para SMTP entrante será aplicada. Debido a las limitaciones de SMTP, incluso si un destinatario de un mensaje de múltiples destinatarios está dirigido a una puerta de enlace entonces la sesión entera será regulada.

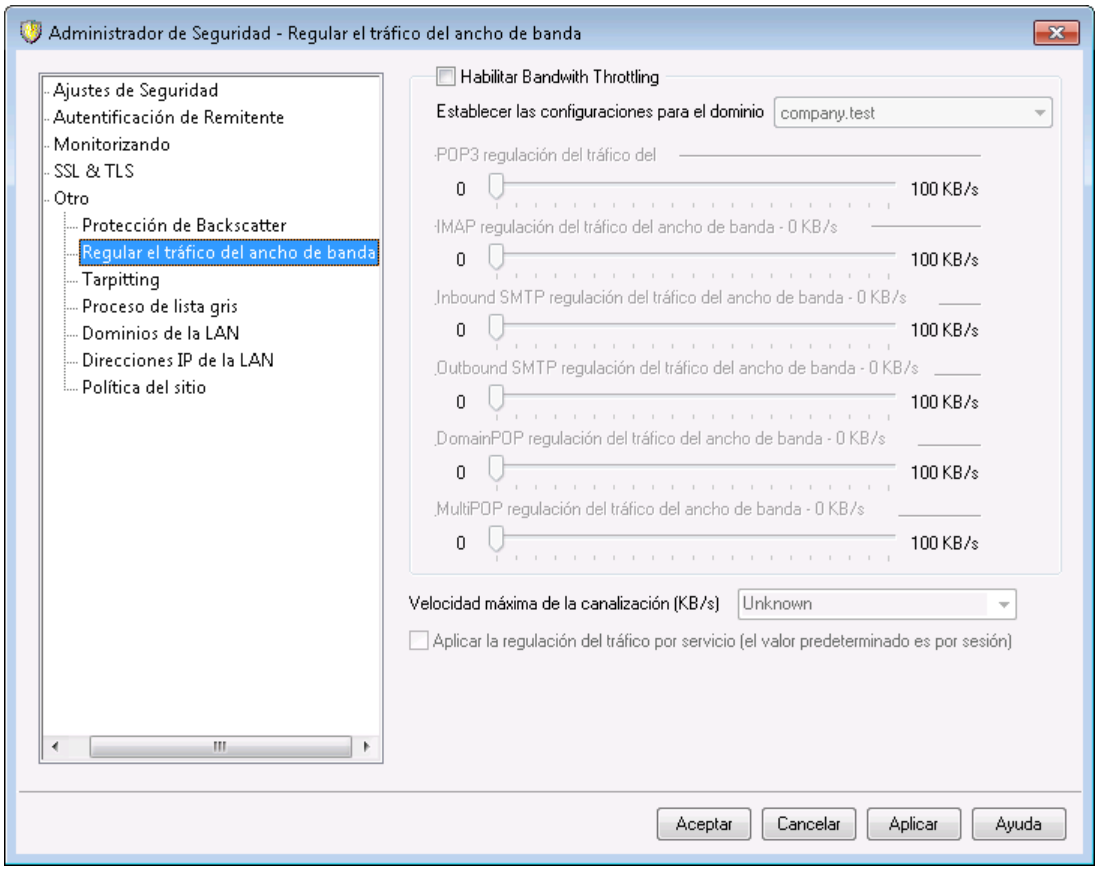
El sistema de regulación de ancho de banda está calibrado en kilobytes por segundo (KB/s). Un valor de "0" significa que no se aplicará límite a la velocidad a la que una sesión (o servicio) progresa, así pues, usará el máximo disponible de ancho de banda. Un valor de "10", por ejemplo, forzar a MDaemon a regular hacia abajo deliberadamente la velocidad de transmisión para que permanezca justo por encima de los 10 KB/s.

Los picos de actividad al inicio de una sesión pueden y van a exceder los límites fijados. La regulación se aplica y se hace más definida a medida que la sesión progresa.

Ver:

Regular el Tráfico del ancho de banda 601
Direcciones IP de la LAN 608

4.2.5.2.1 Regular el tráfico del ancho de banda



Habilitar regulación del ancho de banda

Verifique esta casilla si desea activar la regulación del ancho de banda.

Establecer las configuraciones para el dominio
Escoja el dominio de la lista desplegable y luego ajuste las opciones correspondientes a los varios servicios para configurar la regulación de ancho de banda para el dominio seleccionado. Una configuración de "0" en un control particular cualquiera significa que no se ha establecido límite de ancho de banda para dicho tipo de servicio. En la lista desplegable, la última entrada listada es *Tráfico Local*. Establecer la regulación de ancho de banda para esta opción determinará los límites para el tráfico local (p. ej. sesiones y servicios que ocurran en su red LAN en lugar de externamente). La pantalla de Direcciones IP de la LAN 608 puede usarse para listar las direcciones IP que deberían ser tratadas como locales.

Servicios

[Tipo de servicio] regulación del tráfico – XX KB/s
Después de seleccionar un dominio de la lista desplegable, ajuste estos controles para establecer las limitaciones de ancho de banda para el dominio seleccionado. Una configuración de "0" significa que no se aplica límite de ancho de banda a ese tipo particular de servicio. Si establece el deslizador en cualquier número que no sea "0" se limitará el máximo de ancho de banda a eses número de kilobytes por segundo para el servicio designado.

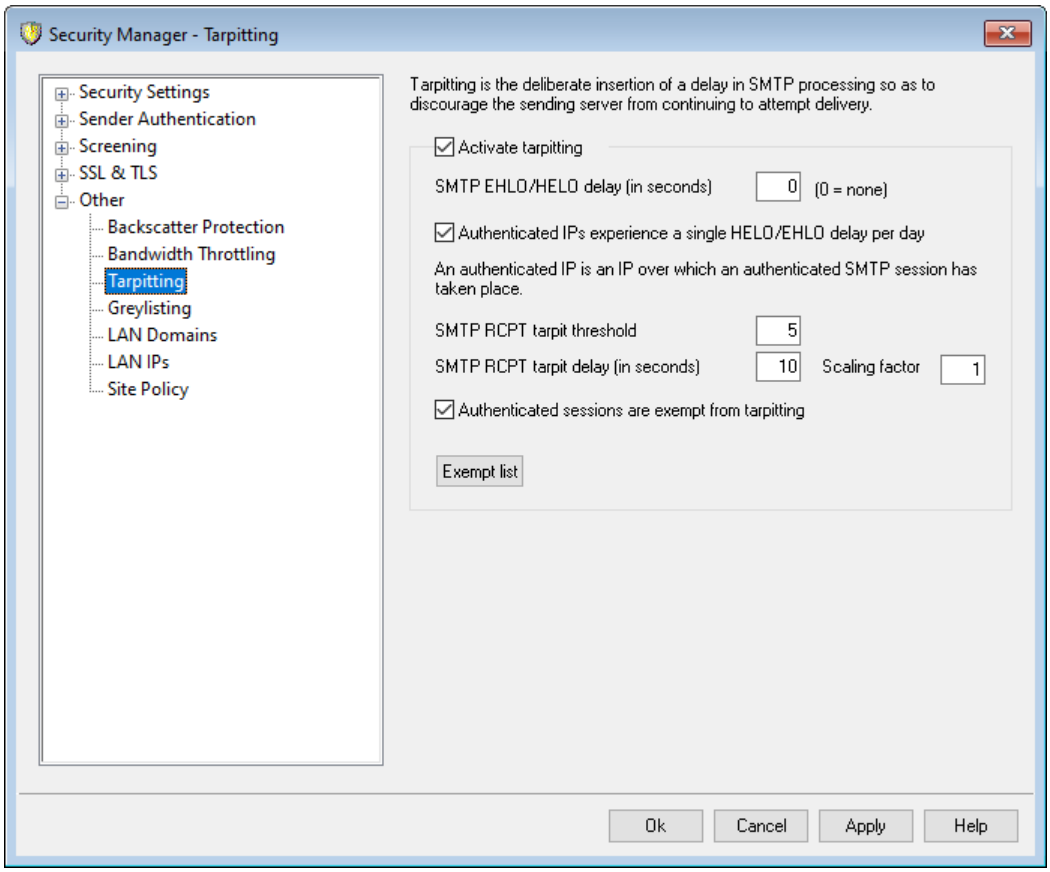
Máxima velocidad por conexión (KB/s)
De la lista desplegable, seleccione la velocidad máxima de su conexión en Kilobytes por segundo.

Aplicar regulación por servicio (por omisión se regula por sesión)
Dé clic en esta casilla si desea regular el uso del ancho de banda en case a servicios en lugar de utilizar el criterio por omisión que es en base a sesiones. Cuando se regula en base a servicios, el ancho designado a cada servicio se dividirá de manera equitativa entre todas las sesiones activas de un tipo dado de servicio. Así, el total de ancho de banda utilizado, por ejemplo, por múltiples clientes IMAP conectándose al mismo tiempo, nunca podrá exceder de la cantidad definida para el servicio sin importar cuantos clientes se conecten. Si la regulación se hace en base a sesiones, entonces ninguna de las sesiones IMAP por sí misma excederá el límite establecido, pero el total de sesiones simultáneas múltiples si lo pudieran hacer.

Ver:

Regular el tráfico del ancho de banda - Descripción 600

4.2.5.3 Tarpitting



El Tarpitting se ubica bajo el menú seguridad en: Seguridad » Ajustes de Seguridad » Otro » Tarpitting.

Tarpitting hace posible que se haga lenta deliberadamente una conexión una vez se haya encontrado un número de comandos RCPT del remitente de un mensaje. Ello es para descorazonar a los spammers de intentar usar su servidor para intentar enviar correo masivo no solicitado ("Spam"). Puede especificar el número de comandos RCPT permitidos antes de que tarpitting empiece y el número de segundos de retraso de la conexión cada vez que un comando subsecuente se recibe de dicho host durante la conexión. La asunción detrás de esta técnica es que, si a los spammers les lleva un periodo de tiempo extremadamente largo enviar cada mensaje, ello les desmotivará de intentar usar su servidor para hacerlo nuevamente en el futuro.

Activar el tarpitting
Haga clic en esta casilla para activar las funcionalidades de tarpitting de MDaemon.

Retardo SMTP EHLO/HELO (en segundos)
Use esta opción para retrasar la respuesta del servidor a los comandos SMTP EHLO/HELO. Retrasando las respuestas incluso por tan sólo diez segundos puede potencialmente salvar una cantidad significante de tiempo de proceso reduciendo la cantidad de Spam recibido. Frecuentemente los spammers dependen del envío rápido de sus mensajes y por lo tanto no esperan mucho tiempo para las respuestas a los comandos EHLO/HELO. Incluso con un pequeño retraso, las herramientas de Spam a veces se rendirán y continuarán su camino en lugar de esperar una respuesta. Las conexiones en el puerto MSA (designado en la pantalla Puertos 115 bajo Ajustes del Servidor) siempre están exentas de este retraso. La configuración por defecto para esta opción es "0", lo cual significa que EHLO/HELO no será retrasado.

Las IP autenticadas tienen una sola transmisión HELO/EHLO por día
Haga clic en esta casilla si desea limitar el retraso EHLO/HELO a una vez por día para las conexiones autenticadas de una dirección IP dada. El primer mensaje de dicha dirección IP será retrasado, pero cualquier mensaje subsecuente enviado desde la misma dirección IP no lo será.

Umbral del tarpit RCPT de SMTP
Especifique el número de comandos SMTP RCPT que desea permitir para un host dado durante una sesión de correo antes de que MDaemon empiece a usar tarpitting en ese host. Por ejemplo, si el número se estableció en 10 y un host de envío intenta enviar un mensaje a 20 direcciones (20 comandos RCPT), entonces MDaemon permitiría las 10 primeras normalmente y luego pausaría después de cada comando subsecuente durante el número de segundos especificado en el control inferior *Demora de tarpit de RCPT de SMTP.*

Demora de tarpit de RCPT de SMTP (en segundos)
Una vez se alcanza el *Umbral de tarpit de RCPT de SMTP* para un host, este es el número de segundos que MDaemon se pausará después de cada comando RCPT subsecuente recibido de dicho host durante la sesión de correo.

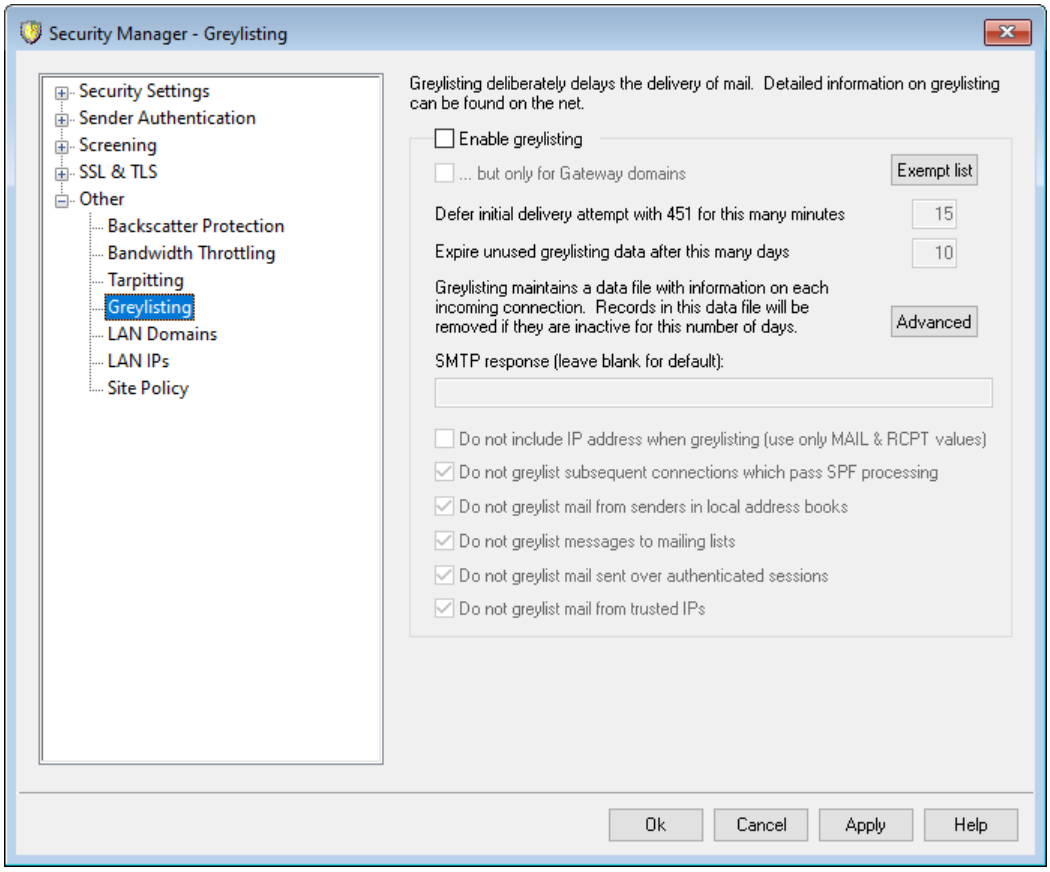
Factor de escala
Este valor es el multiplicador por el que el retraso base de tarpit se incrementará con el tiempo. Cuando el umbral de tarpit se alcanza y se aplica el retraso de tarpit a una sesión, cada retraso se multiplicará por este valor para determinar la duración del siguiente retraso en la sesión. Por ejemplo, si el retraso de tarpit se establece en 10 y el factor de escala en 1.5 entonces el primer retraso será de 10 segundos, el segundo de 15 segundos, el tercero 22,5, y así (10x1,5=15,

15x1,5=22,5, etc.). El factor de escala por defecto es 1, lo cual significa que el retraso no será incrementado.

Las sesiones autentificadas están excluidas del análisis del tarpit
Haga clic en esta casilla si quiere que los remitentes que autentifiquen sus sesiones de correo estén exentos del Tarpitting.

Lista de Exentos
Haga clic en este botón para abrir la Lista Dinámica de Permitidos[624], que también se utiliza para el Tarpitting. En ella puede definir direcciones IP que desea que estén exentas de tarpitting.

4.2.5.4 Lista Gris



El proceso de lista gris está ubicado bajo el diálogo de Seguridad en: `Seguridad » Ajustes de Seguridad » Otro » Proceso de lista gris`. La lista gris es una técnica para combatir el Spam que explota el hecho de que los servidores SMTP reintentan la entrega de cualquier mensaje que reciba un código de error temporal ("try again later"). Usando esta técnica, cuando un mensaje llega de un remitente que no está en lista de permitidos y desconocido previamente, su remitente, destinatario y la IP del servidor de envío se registrarán y el mensaje será rechazado por la Lista Gris durante la sesión SMTP con un código de error temporal. Además, durante el período de tiempo designado (pongamos, 15 minutos) cualquier intento de envío futuro también será temporalmente rechazado. Dado que los "spammers" no suelen realizar posteriores intentos de entrega cuando un mensaje es rechazado, la lista

gris puede ayudar a reducir significativamente la cantidad de Spam que sus usuarios reciben. Pero, aun y cuando los spammers intentarán nuevamente la entrega en un momento posterior, es posible que para entonces los spammers puedan ser identificados por otras opciones para combatir el Spam (como las Listas de Bloqueo de DNS[701]) que los bloquearán con éxito. Es importante hacer notar, sin embargo, que esta técnica puede retrasar deliberadamente correo "bueno" juntamente con el "malo". Pero, los mensajes legítimos deberían seguir siendo enviados en algún momento posterior después de que el periodo de lista gris haya expirado. También es importante hacer notar que no tiene manera de saber cuánto tiempo los servidores de envío esperarán antes de realizar otros intentos de entrega. Es posible que rechazar a propósito un mensaje con un error temporal pudiera causar que éste sea retrasado tampoco como unos minutos o tanto como un día entero.

Existen diversos problemas tradicionales y efectos laterales negativos asociados con el proceso de lista gris, y la pantalla de Lista Gris contiene un número de opciones diseñadas para lidiar con ellos.

Primero, algunos dominios de envío utilizan un grupo de servidores de correo para enviar correo saliente. Dado que un servidor diferente puede ser usado para cada intento de envío, cada intento sería tratado como una nueva conexión por el motor de lista gris. Esto podría multiplicar la cantidad de tiempo que llevaría pasar a través de la lista gris, dado que cada uno de dichos intentos se registraría en lista gris como mensajes separados en lugar de intentos de un mensaje previo.

Utilizando una opción de búsqueda SPF, este problema puede resolverse para los dominios que publiquen sus datos SPF. Además, existe una opción de ignorar la IP del servidor de correo de envío completamente. Si usa esta opción reducirá la eficiencia de la lista gris, pero resuelve completamente el problema del grupo de servidores.

Segundo, la lista gris tradicionalmente crea una base de datos muy grande dado que cada conexión entrante debe ser registrada. MDaemon minimiza la necesidad de rastrear conexiones colocándolas en la funcionalidad de lista gris casi al final del proceso de secuencia SMTP. Esto permite que las otras opciones de MDaemon rechacen un mensaje antes de llegar a la fase de lista gris. Como resultado, el tamaño del archivo de datos se reduce notablemente, y puesto que es residente en memoria apenas ejerce impacto a nivel práctico.

Finalmente, muchas opciones están disponibles para minimizar el impacto de la lista gris en los mensajes "buenos". Primero, los mensajes enviados a las listas de distribución pueden ser excluidos. Después, la lista gris tiene su propia lista de exentos en la que puede designar direcciones IP, remitentes y destinatarios que se desee estén exentos del proceso. Finalmente, la lista gris contiene una opción para usar la libreta privada de direcciones de cada cuenta como base de datos de lista de exentos. Así, el correo de o a un usuario en la libreta de direcciones de éste puede excluirse de la lista gris.

Para más información acerca de la lista gris en general, visite el sitio de Even Harris en:

http://projects.puremagic.com/greylisting/

Proceso de Lista Gris

Habilitar el proceso de la lista gris
Haga clic en esta opción para habilitar la funcionalidad de Lista Gris en MDaemon.

...pero sólo para dominios de la puerta de enlace
Haga clic en esta casilla si sólo quiera aplicar la lista gris a los mensajes dirigidos a los dominios de puerta de enlace.

Lista de Exentos
Este botón abre la lista blanca del proceso de lista gris donde puede designar remitentes, destinatarios, y direcciones IP que estarán exentas del proceso de lista gris.

Aplazar el intento de entrega inicial con 451 tantos minutos
Designe el número de minutos que se pondrá en lista gris un intento de envío después del intento inicial. Durante dicho periodo de tiempo, cualquier intento de envío subsecuente por la misma combinación de servidor/remitente/destinatario (triplet de lista gris) generará otro código de error temporal. Después de que haya pasado el periodo de lista gris, no se implementarán más retrasos en dicho triplet a menos que el registro de la base de datos de lista gris expire.

Los registros de la base de datos de la lista gris no utilizados caducan tras tantos días
Después de que el periodo inicial de lista gris haya pasado para un triplet de lista gris dado, no habrá más mensajes que coincidan con dicho triplet que sean retrasados por la lista gris. Aun así, si no hay mensajes que coincidan con dicho triplet durante el número de días designado en esta opción, su registro de base de datos de lista gris expirará. Un intento subsiguiente de dicho triplet hará que se cree un nuevo registro de lista gris y tendrá que pasar por el periodo inicial de nuevo.

Avanzado
Haga clic en este botón para abrir la base de datos de lista gris, que puede usar para revisar o editar los triplets guardados.

Respuesta SMTP (dejar en blanco por omisión)
Si proporciona una cadena personalizada en este espacio, entonces MDaemon emitirá una respuesta "`451 <su texto personalizado>`" en lugar del valor por omisión que es "`451 Listas Grises habilitado. Intente de nuevo en X minutos.`" Esto es útil, por ejemplo, si desea definir una cadena que contenga una URL hacia la descripción del proceso de Listas Grises.

No incluir la dirección IP al realizar el proceso de poner en la lista gris (usar sólo valores de MAIL RCPT)
Haga clic en esta casilla si no desea usar la dirección IP del servidor remitente como uno de los parámetros de lista gris. Esto solucionará el potencial problema inicial que puede ser causado por los grupos de servidores, pero reducirá la eficiencia de la Lista Gris.

No poner en la lista gris conexiones que pasen el procesamiento SPF
Cuando use esta opción, si un mensaje entrante coincide con un triplet de remitente y de destinatario, pero no de servidor de envío, pero el proceso de SPF determina que el servidor de envío es una alternativa válida al que está listado en el triplet, el mensaje será tratado como un envío subsiguiente que coincide con dicho triplet en lugar de una nueva conexión que requiera un registro de lista gris.

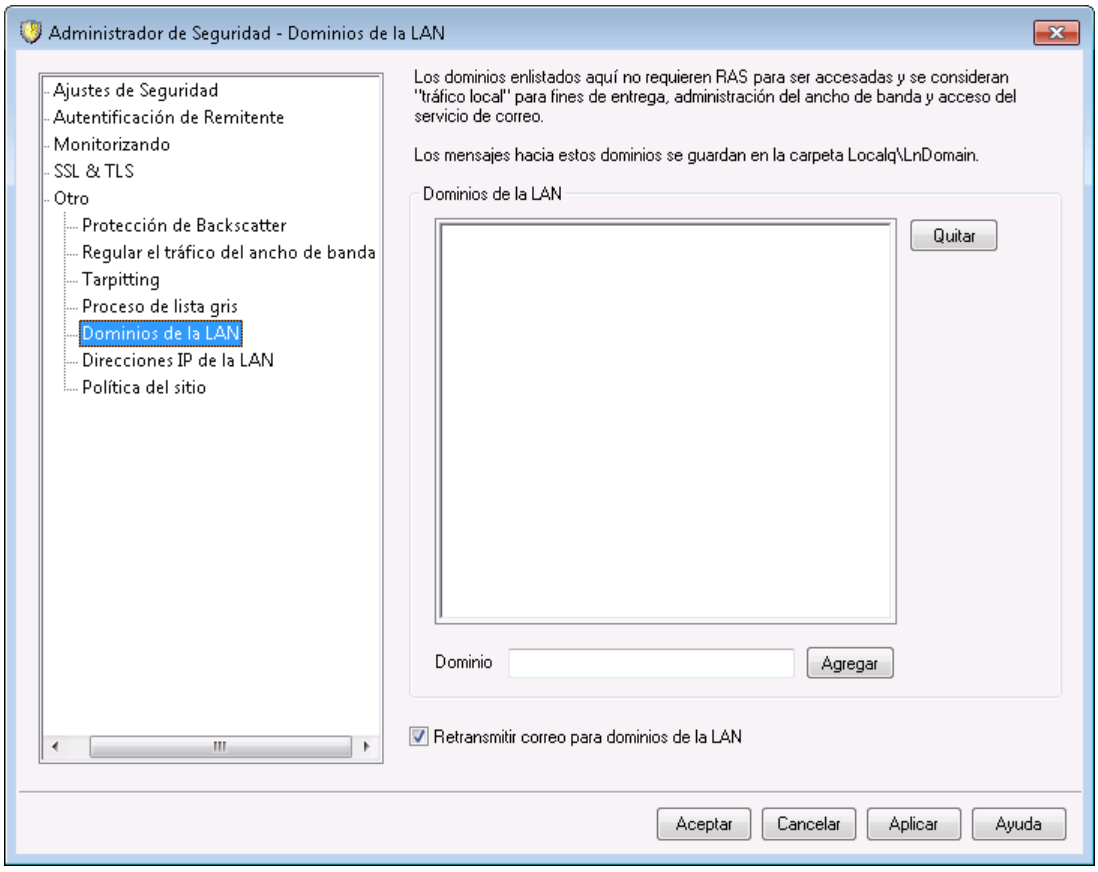
No poner en la lista gris los remitentes que están en la libreta de direcciones local
Haga clic en esta opción si desea hacer exento el mensaje de la lista gris cuando su remitente esté listado en la libreta de direcciones del destinatario.

No considerar de la lista gris los mensajes para las listas de distribución
Haga clic en esta casilla si quiere hacer exentos a los mensajes de lista de correo de la lista gris.

No poner en lista gris el correo enviado mediante sesiones autentificadas
Use esta opción si quiere que todos los mensajes que vengan de una sesión autentificada estén exentos de la lista gris.

No considerar de la lista gris el corre de las IPs de confianza
Use esta opción si desea que todos los mensajes que vengan de IPs de confianza estén exentos de la lista gris.

4.2.5.5 Dominios de la LAN



Dominios de la LAN

Los dominios enlistados aquí son considerados por MDaemon como parte de su LAN local (local area network). Por esto, no se requiere enlace por marcación o una conexión de Internet a fin de entregar el mensaje en alguno de ellos.

Dominio
Ingrese aquí un nombre de dominio y dé clic en *Agregar* para incluirlo a la lista.

Agregar
Luego de especificar un dominio en la opción *Dominio*, dé clic en este botón para agregarlo a la lista.

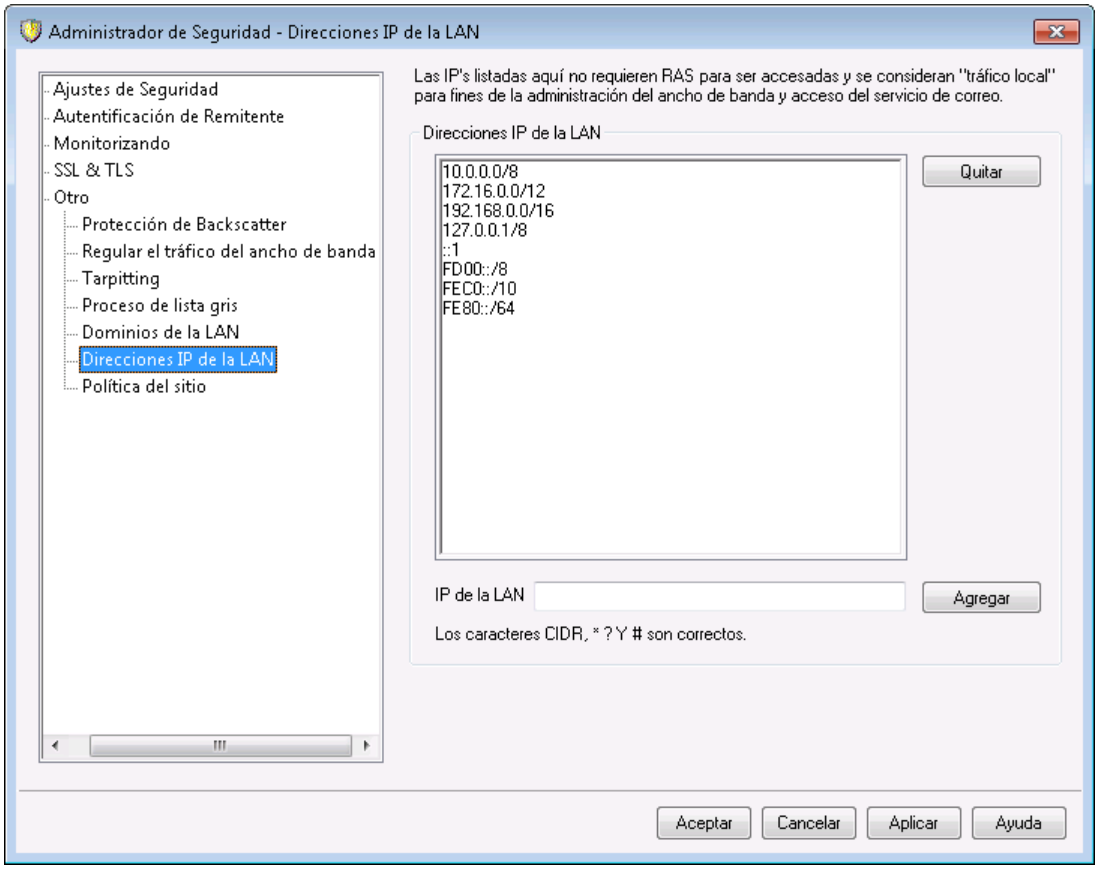
Eliminar
Seleccione un dominio en la lista y dé clic en este botón para eliminarlo.

Retransmitir correo para dominios de la LAN
Si esta casilla está habilitada, MDaemon retransmitirá correo para estos dominios. Esto da una medida de control sobre el tráfico enviado de y hacia estos dominios.

Ver:

IPs de la LAN 608

4.2.5.6 Direcciones IP de la LAN



IPs de la LAN

Similar a Dominios de la LAN, esta pantalla se utiliza para enlistar las direcciones IP que residen en su LAN (red de área local). Estas direcciones IP, por lo tanto, no requieren RAS o una conexión de Internet para conectarse a ellas y se les trata

como tráfico local para propósitos de regulación del ancho de banda. Más aun, hay algunas otras restricciones de seguridad y prevención de Spam de las que pueden estar exentas por ser direcciones locales.

Eliminar
Seleccione una dirección IP de la lista y luego haga clic en este botón para quitarla.

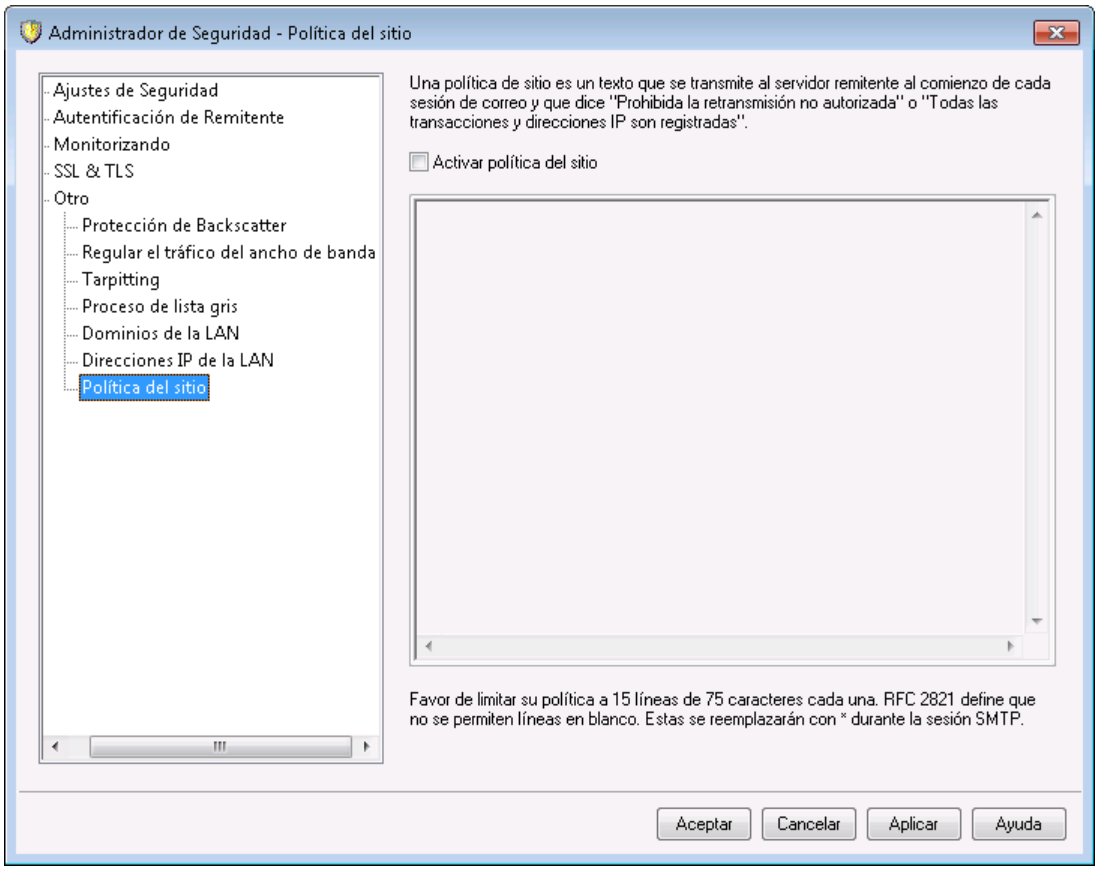
IP de la LAN
Introduzca una dirección IP para agregarla a la lista de IPs de la LAN y dé clic en *Agregar*. Los comodines tales como 127.0.*.* están permitidos.

Agregar
Después de introducir una dirección IP en la opción *IP de la LAN*, haga clic en este botón para agregarla a la lista.

Ver:

Dominios de la LAN 607

4.2.5.7 Política del Sitio



Crear una declaración de Política de Sitio SMTP
Use este diálogo para especificar una declaración de Política de Sitio para su servidor. El texto se guarda en el archivo `policy.dat` ubicado en la subcarpeta de MDaemon `\app\` y se transmite a los servidores de envío al principio de cada sesión SMTP. Un ejemplo de una política de sitio común es "`Este servidor no permite retransmisión`" o "`Se prohíbe el uso no autorizado.`" No necesita añadir a cada línea "`220`" o "`220-`". MDaemon gestiona cada línea acorde, con o sin los códigos añadidos.

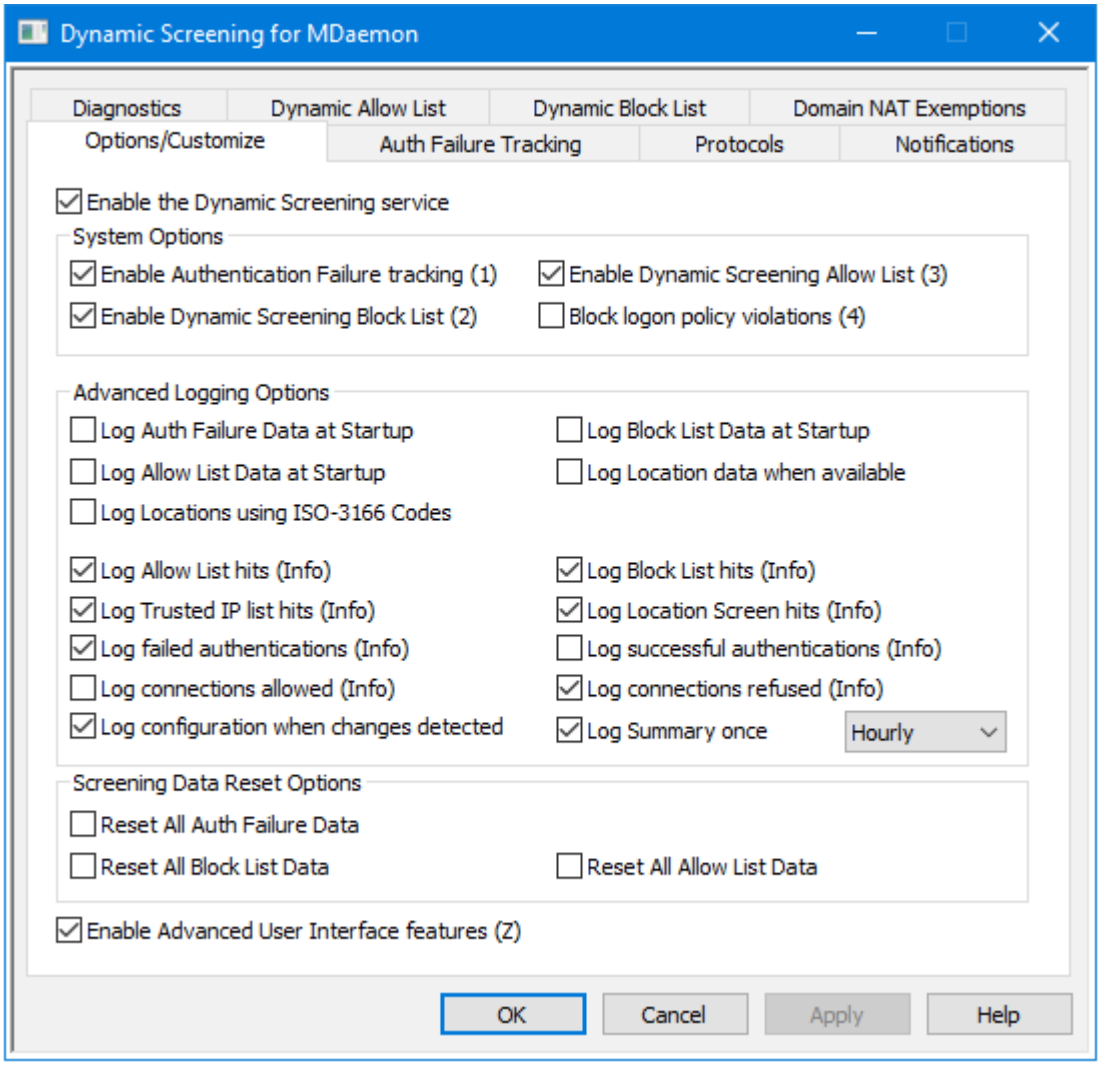
Una política de uso del sitio con una declaración respecto a la retransmisión de correo se vería de esta manera durante una transacción SMTP:

```
220-MDaemon Technologies ESMTP MDaemon
220-Este sitio no retransmite correo no autorizado.
220-Si no es un usuario autorizado del servidor
220-no debe retransmitir correo a través de él.
220
HELO ejemplo.com...
```

El archivo `POLICY.DAT` debe componerse sólo de texto ASCII imprimible y no debe tener más de 512 caracteres por línea; aun así, es altamente recomendado que no use más de 75 caracteres por línea. El tamaño máximo de este archivo es 5000 bytes. MDaemon no mostrará archivos mayores a 5000 bytes.

4.3 Monitoreo Dinámico

4.3.1 Opciones/Personalizar



Utilizando el Monitoreo Dinámico, MDaemon puede rastrear el comportamiento de conexiones entrantes para identificar actividad sospechosa y responder en concordancia. Puede bloquear una dirección IP[615] (o rango de direcciones) impidiendo que se conecte cuando falla la autentificación un número determinado de veces dentro de un rango de tiempo específico. También puede congelar las cuentas[615] que intentan autentificarse cuando fallas demasiadas veces demasiado rápido. Así mismo, cuando se bloquea una dirección IP o se congela una cuenta, no es permanente. La dirección IP que se conecta será bloqueada durante el número de minutos, horas o días que usted especifique y las cuentas congeladas se pueden "descongelar" automáticamente después de un tiempo determinado o manualmente por el administrador.

Habilitar el servicio de Monitoreo Dinámico
Marque esta casilla para habilitar el servicio de Monitoreo Dinámico. También lo puede habilitar/habilitar en la sección Servidores en el panel de navegación de la interface de usuario de MDaemon.

Opciones del Sistema

Habilitar el Monitoreo de Fallos de Autentificación
Cuando se habilita esta opción, el servicio de Monitoreo Dinámico rastreará los fallos de autentificación para los protocolos definidos en la pestaña Protocolos[617]

y ejecutará las acciones determinadas en las opciones determinadas en la pestaña Monitoreo de Fallos de Autentificación[615]. Esta opción se encuentra habilitada por omisión.

Habilitar la Lista de Bloqueados del Monitoreo Dinámico
Esta opción habilita la habilidad del servicio de Monitoreo Dinámico para bloquear direcciones y rangos de IP´s. Puede administrar la lista de bloqueados desde la pestaña Lista Dinámica de Bloqueados[625]. La opción de Lista de Bloqueados se encuentra habilitada por omisión.

Habilitar la Lista de Permitidos del Monitoreo Dinámico
Esta opción habilita la funcionalidad de Lista Dinámica de Permitidos[624] del servicio de Monitoreo Dinámico, que puede utilizar para exentar direcciones y rangos de IP, para excluirlos del Monitoreo Dinámico. La Lista de Permitidos se encuentra habilitada por omisión.

Bloquear violaciones a la Política de Inicio de sesión
Por omisión, MDaemon requiere que las cuentas utilicen la dirección completa de correo al iniciar sesión en lugar el segmento del buzón de la dirección (ej. deben utilizar "`user1@example.com`" en lugar de solamente "`user1`"). Esto se controla por la opción "*Los servidores requieren la dirección de correo completa para autentificación*" en la página Sistemas[494]. Cuando esta opción está habilitada, también puede habilitar la opción *Bloquear violaciones a la Política de inicio de sesión* si desea bloquear las direcciones IP que intenten iniciar sesión sin utilizar la dirección de correo completa. Esta opción está deshabilitada por omisión.

Opciones Avanzadas de Registro

Registrar datos de fallos de Autentificación al iniciar el servicio
Esta opción habilita la escritura de todos los datos de fallos de autentificación[615] almacenados en ese momento por el Monitoreo Dinámico en el archivo de registro al iniciar el servicio. Esta opción se encuentra deshabilitada por omisión.

Registrar datos de la Lista de Bloqueados al iniciar el servicio
Habilita la escritura en el archivo de registro de todos los datos de Lista Dinámica de Bloqueados[625] que se encuentren almacenados en el momento del inicio del servicio. Esta opción se encuentra deshabilitada por omisión.

Registrar datos de la Lista de Permitidos al iniciar el servicio
Habilita la escritura en el archivo de registro de todos los datos de Lista Dinámica de Permitidos[624] que se encuentren almacenados en el momento del inicio de servicio. Esta opción se encuentra deshabilitada por omisión.

Registrar datos de Localización cuando estén disponibles
Marque esta casilla si desea registrar los datos de localización de cada conexión, cuando estén disponibles.

Registrar datos de Localización utilizando códigos ISO-3166
Marque esta casilla si desea utilizar los códigos de país de dos letras ISO-3166 al registrar localizaciones, en lugar de utilizar nombres.

Registrar todas las coincidencias de lista de permitidos
Esta opción agrega una entrada al archivo de registro del Monitoreo Dinámico cada vez que una conexión entrante proviene de una dirección que se encuentre en la Lista Dinámica de Permitidos[624].

Registrar todas las coincidencias de lista de bloqueados
Esta opción agrega una entrada al archivo de registro del Monitoreo Dinámico cada vez que una conexión entrante proviene de una dirección que se encuentre en la Lista Dinámica de Bloqueados 625.

Registrar todas las coincidencias de IP´s confiables
Esta opción agrega una entrada en el registro del Monitoreo Dinámico cada vez que una conexión entrante proviene de una dirección IP Confiable 520.

Registrar todas las coincidencias del Monitoreo de Localizaciones
Esta opción agrega una entrada en el registro del Monitoreo Dinámico cada vez que una conexión entrante es rechazada debido al Monitoreo de Localizaciones 572.

Registrar todas las autentificaciones fallidas
Esta opción agrega una entrada en el registro del Monitoreo Dinámico cada vez que una conexión entrante falla la autentificación.

Registrar todas las autentificaciones exitosas
Habilite esta opción si desea registrar todos los intentos entrantes de autentificación exitosos. Esta opción se encuentra deshabilitada por omisión.

Registrar todas las conexiones permitidas
Habilite esta opción si desea crear una entrada en el registro por cada conexión que pasa el Monitoreo Dinámico y se le permite proceder. Esta opción se encuentra deshabilitada por omisión.

Registrar todas las conexiones rechazadas
Esta opción agrega una entrada para registrar todas las ocasiones en que una conexión entrante es rechazada por el Monitoreo Dinámico.

Registrar la configuración cuando se detectan cambios
Esta opción agrega una entrada en el registro para todas las configuraciones del Monitoreo Dinámico cuando se detectan cambios provenientes de fuentes externa (tal como una edición manual del archivo INI). Los cambios normales se registran a nivel Info.

Registrar el resumen una vez [Diario | Cada hora | Por minuto]
Agrega al registro del Monitoreo Dinámico un resumen de las estadísticas del servicio una vez cada día, hora o minuto. Por omisión el resumen se registra cada hora.

Opciones de Restablecimiento de los Datos de Monitoreo

Restablecer todos los datos de Falla Auth
Dé clic en esta casilla si desea eliminar todos los datos de autentificación del Monitoreo Dinámico. Debe dar clic en **Aplicar** o en **OK** para que se ejecute el restablecimiento.

Restablecer todos los datos de Lista de Bloqueados
Dé clic en esta casilla si desea eliminar todos los datos de la Lista de Bloqueados del Monitoreo Dinámico. Debe dar clic en **Aplicar** o en **OK** para que se ejecute el restablecimiento.

Restablecer todos los datos de la Lista de Permitidos
Dé clic en esta casilla si desea eliminar todos los datos de la Lista de Permitidos del Monitoreo Dinámico. Debe dar clic en **Aplicar** o en **OK** para que se ejecute el restablecimiento.

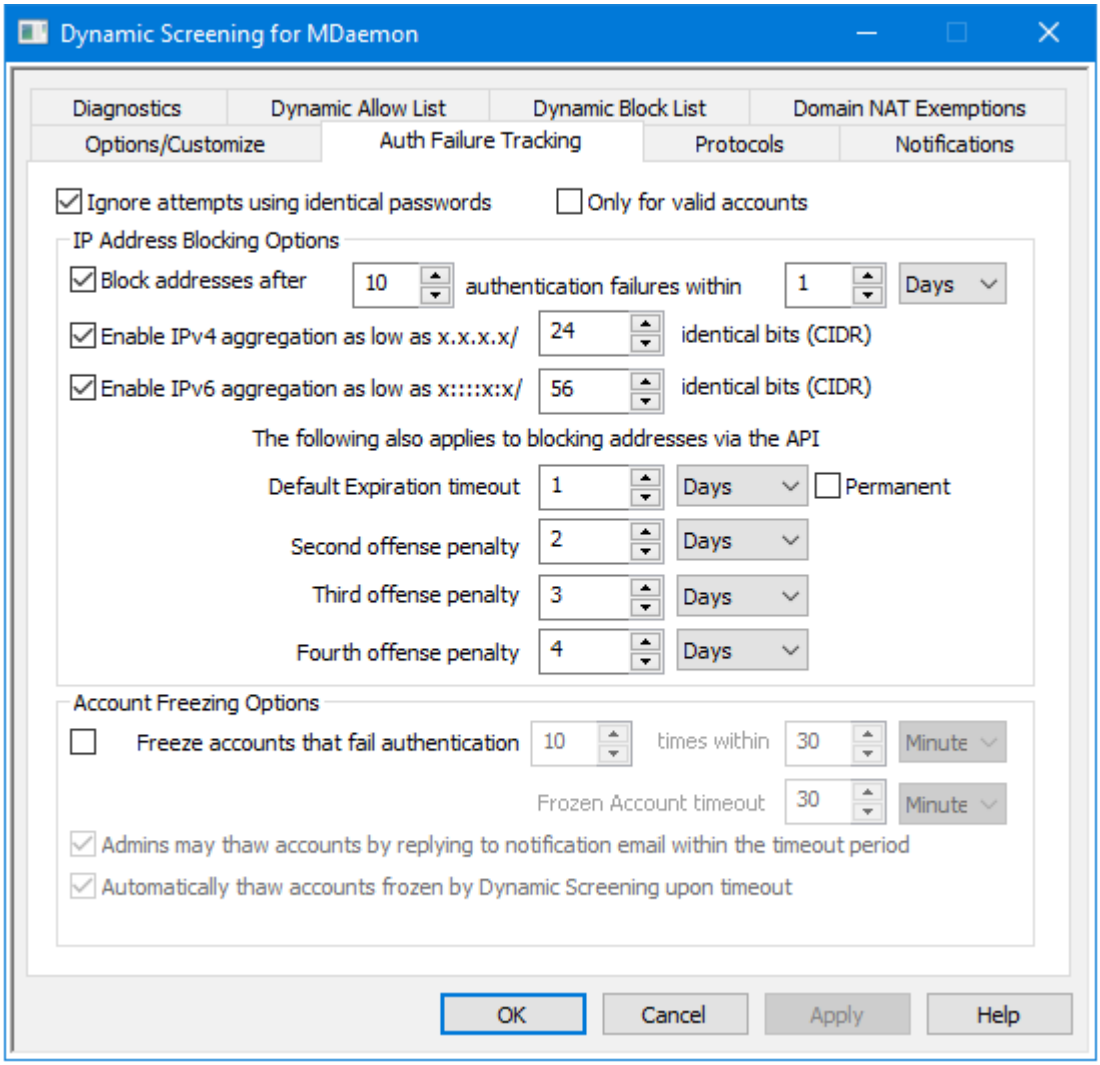
Habilitar las Opciones Avanzadas de Interface de Usuario

Marque esta casilla y luego abra/reabra la sesión de configuración de MDaemon para que se muestren varias funcionalidades avanzadas del Monitoreo Dinámico. Se agregó la pantalla Exención NAT de Dominio 628 al diálogo de Monitoreo Dinámico, donde puede definir las combinaciones de direcciones IP/dominios para exentar del bloqueo del Monitoreo Dinámico cuando usuarios válidos en esa dirección IP fallan la autentificación de contraseña. También se agregaron varios accesos rápidos de Monitoreo Dinámico a la barra de herramientas y se agregó una opción al menú de Monitoreo Dinámico bajo la sección Servidores de la interface principal, que le permiten pausar en lugar de deshabilitar el servicio de Monitoreo Dinámico, impidiendo que los clientes tengan acceso al servicio mientras usted administra los ajustes.

Ver:

Rastreo de Fallos de Autentificación 615
Lista Dinámica de Permitidos 624
Lista Dinámica de Bloqueados 625
Exenciones NAT de Dominio 628
Protocolos 617
Monitoreo de Localizaciones 572
Pantalla SMTP 566

4.3.2 Monitoreo de Fallos de Autentificación



Ignorar intentos de autentificación utilizando contraseñas idénticas

Esta opción aplica a las Opciones de Bloqueo de Direcciones IP y a las opciones de Congelamiento de Cuentas descritas abajo. Por omisión, cuando falla un intento de autentificación, los intentos subsecuentes serán ignorados si se utiliza la misma contraseña. No contarán contra el número de fallos permitidos antes de bloquear una dirección IP o congelar la cuenta. Múltiples intentos utilizando la misma contraseña incorrecta ocurren típicamente cuando, por ejemplo, la contraseña de correo del usuario ha sido modificada o expirado y el cliente está intentando automáticamente iniciar sesión utilizando la contraseña anterior.

Solo para cuentas válidas

Active esta opción si solo desea ignorar los intentos de autentificación con contraseñas idénticas cuando intentan iniciar sesión para una cuenta válida. Esto significa que, por ejemplo, un usuario actualizó su contraseña en un cliente pero otro cliente aún tiene configurada la contraseña anterior. Esos intentos de iniciar sesión del cliente que no está actualizado serán ignorados. Un bot que intente nombres de inicio de sesión aleatorios con contraseñas similares no tendrá el mismo beneficio y será bloqueado tan pronto como sobrepase el umbral de fallos de autentificación.

Opciones de Bloqueo de Direcciones IP

Bloquear direcciones luego de [xx] fallos de autentificación dentro de [xx] [Minutos | Horas | Días]
Dé clic en esta casilla si desea bloquear temporalmente una dirección IP cuando falla la autentificación hacia su servidor un número excesivo de veces en un periodo de tiempo limitado. Especifique el número de minutos, horas o días y el número de fallos permitidos en ese periodo.

Habilitar agregación IPv4 tan baja como x.x.x.x/ [xx] bits idénticos (CIDR)
Esta opción bloqueará un rango de direcciones IPv4 cuando los fallos de autentificación provengan de direcciones IP cercanas entre ellas en lugar de provenir de una sola dirección.

Habilitar agregación IPv6 tan baja como x::::x:x/ [xx] bits idénticos (CIDR)
Esta opción bloqueará un rango de direcciones IPv6 cuando los fallos de autentificación provengan de direcciones IP cercanas entre ellas en lugar de provenir de una sola dirección.

Penalización por Múltiples Ofensas

Esta es la cantidad de tiempo que una dirección o rango de IP´s serán bloqueadas por el sistema de Monitoreo Dinámico cuando falla el número determinado de intentos de autentificación. Por omisión la cantidad de tiempo que se bloquea una dirección IP se incrementa con cada falta subsecuente. Esto es, por omisión si una dirección IP viola el límite de fallos de autentificación, será bloqueada durante un día. Si esa misma dirección IP subsecuentemente viola el límite de nuevo, se agregará la *Penalización por Segunda Ofensa* al *Tiempo de expiración por omisión*, después se agregará la *Penalización por Tercera Ofensa* y así sucesivamente. La duración de la penalización llega a un máximo al agregar la *Cuarta penalización*.

Límite de tiempo de expiración
Esta es la cantidad de tiempo que una dirección IP o un rango de direcciones, será bloqueada impidiendo conectarse a MDaemon si viola el límite de fallos de autentificación especificado arriba. Por omisión es un día.

Penalización de la segunda falta
Esta es la cantidad de tiempo que se agregará al *Tiempo de expiración por omisión* cuando una dirección IP o rango de IP´s sea bloqueado por segunda vez por el Monitoreo Dinámico.

Penalización de la tercera falta
Esta es la cantidad de tiempo que se agregará al *Tiempo de expiración por omisión* cuando una dirección IP o rango de IP´s sea bloqueado por tercera vez por el Monitoreo Dinámico.

Penalización de la cuarta falta

Esta es la cantidad de tiempo que se agregará al *Tiempo de expiración por omisión* cuando una dirección IP o rango de IP´s sea bloqueado por cuarta vez u ocasiones subsecuentes, por el Monitoreo Dinámico.

Permanente
Dé clic en esta caja si desea bloquear permanentemente una dirección IP que viole el límite de fallos de autentificación, en lugar de bloquearla temporalmente utilizando las penalizaciones por ofensas descritas arriba.

Opciones de Congelación de Cuentas

Congelar cuentas que fallas la autentificación [xx] veces dentro de [xx] [Minutos | Horas | Días]
Marque esta casilla si desea modificar el Estatus de la Cuenta 715 a CONGELADA cuando falla el número especificado de intentos de autentificación en el periodo de tiempo designado. De todas formas, MDaemon aceptará mensajes entrantes para la cuenta congelada, pero nadie puede iniciar sesión a la cuenta o enviar o recibir mensajes hasta que se "descongele" (i.e. el Estatus de la Cuenta se modifica a HABILITADA). Esta opción se encuentra habilitada por omisión.

Tiempo de Espera de Congelamiento
Esta es la cantidad de tiempo que una cuenta permanece congelada, si tiene habilitada la opción de abajo *Automáticamente descongelar cuentas congeladas al vencer el tiempo de espera del Monitoreo Dinámico.*

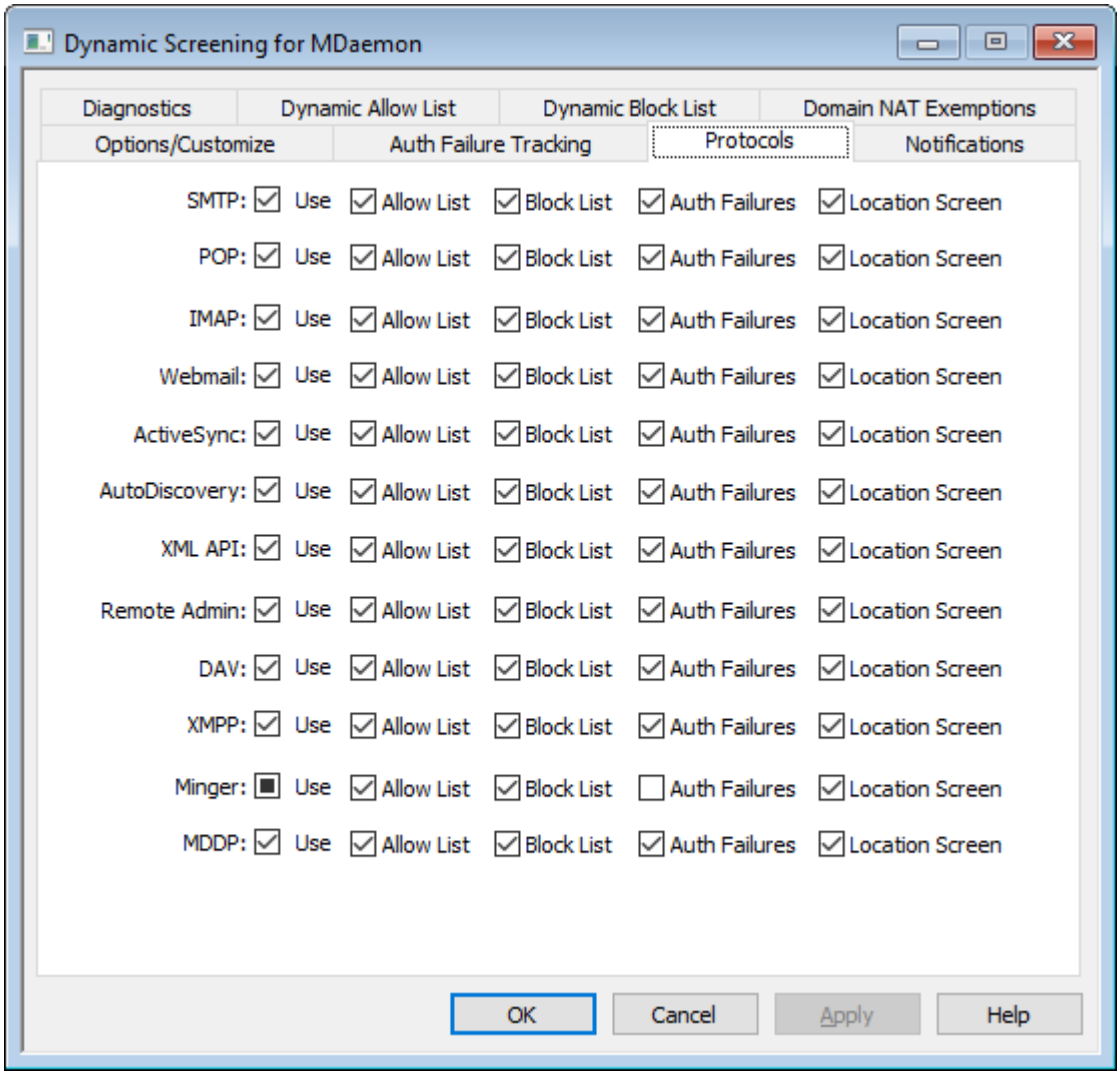
Los Administradores pueden descongelar cuentas replicando al correo de notificación dentro del límite de tiempo
Cuando el Monitoreo Dinámico congela una cuenta, por omisión un administrador recibirá un mensaje de notificación al respecto. El administrador puede entonces "descongelar" la cuenta (i.e. modificar su estatus a "Habilitada") simplemente respondiendo al correo, si esta opción se encuentra habilitada. La opción se encuentra habilitada por omisión y requiere que las opciones Reportes de Cuentas Congeladas en la pestaña Notificaciones 619 se encuentren habilitadas.

Automáticamente descongelar cuentas congeladas por el Monitoreo Dinámico al terminar el límite de tiempo
Marque esta casilla si desea descongelar automáticamente cuentas congeladas cuando haya transcurrido el periodo *Tiempo de Espera de Cuentas Congeladas*. Esta opción se encuentra deshabilitada por omisión.

Ver:

Opciones/Personalizar 610
Lista Dinámica de Permitidos 624
Lista Dinámica de Bloqueados 625
Notificaciones 619

4.3.3 Protocolos



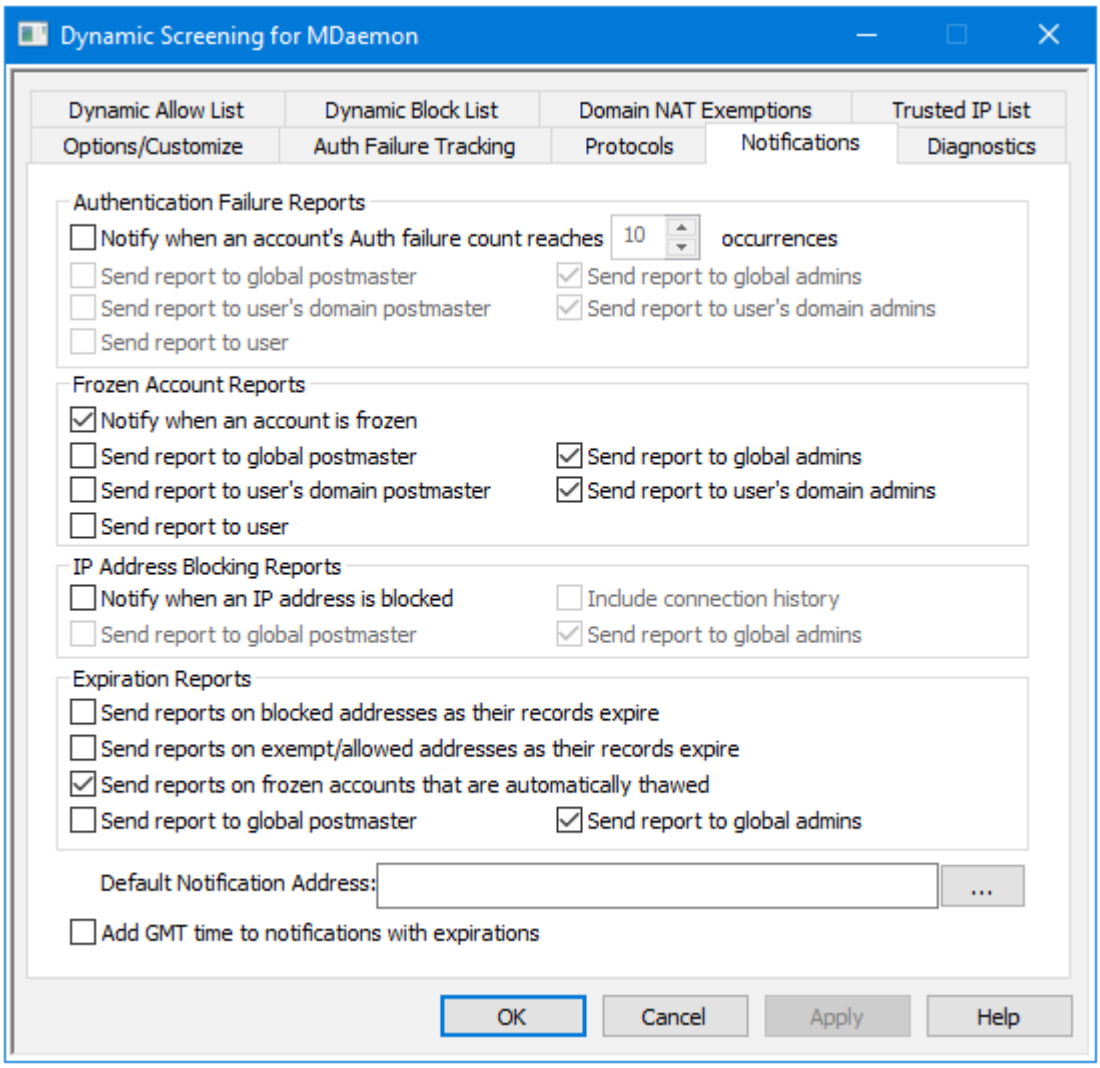
Por omisión el servicio de Monitoreo Dinámico se aplica a los protocolos siguientes: SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 85. la API de Administración, MDaemon Administración Remota, WebDAV, CalDAV, XMPP y Minger. Utilice las opciones en la pestaña Protocolos para determinar para cuáles protocolos se verificarán las sesiones entrantes contra la Lista Dinámica de Permitidos 624 y la Lista Dinámica de Bloqueados 625 y para cuales se realizará el monitoreo de fallos de autentificación 615 y para las que aplicará el Monitoreo de Localizaciones 572. Por omisión, todas las opciones en este diálogo están habilitadas excepto los fallos de autentificación Minger.

Ver:

Monitoreo de Fallos de Autentificación 615
Lista Dinámica de Permitidos 624
Lista Dinámica de Bloqueados 625

4.3.4 Notificaciones

=



Reportes de Fallos de Autentificación

Notificar cuando el conteo de fallos de Autentificación de una cuenta llega a [xx] ocurrencias
Esta opción hace que MDaemon envíe un mensaje de notificación al postmaster o a otro destinatario predeterminado cuando una cuenta falla la autentificación un número especificado de veces seguidas. Si ninguna de las direcciones de correo seleccionada se puede resolver, MDaemon enviará el mensaje a la *Dirección de Notificación por Omisión* designada abajo. Si no se especifica una dirección, el mensaje no se enviará. La opción se encuentra habilitada por omisión y está configurada a 10 ocurrencias.

Enviar reporte al postmaster global
Marque esta casilla si desea enviar los reportes al postmaster global[834]. Se encuentra habilitada por omisión.

Enviar reporte a los administradores globales
Marque esta casilla si desea enviar los reportes a los administradores globales[757].

Enviar reporte al postmaster del dominio del usuario
Marque esta casilla si desea enviar los reportes al postmaster del dominio[834] para la cuenta que falló los intentos de autentificación. Esta opción solo está disponible para MDaemon Private Cloud.

Enviar reporte a los administradores del dominio del usuario
Marque esta casilla si desea enviar los reportes a los administradores del dominio[757] para la cuenta que falló los intentos de autentificación.

Enviar reporte al usuario
Esta opción solo se encuentra disponible en MDaemon Private Cloud.

Reporte de Cuentas Congeladas

Notificar cuando se congela una cuenta
Esta opción hace que MDaemon envíe un mensaje de notificación al postmaster u otro destinatario seleccionado, cuando una cuenta se congela por demasiados fallos de autentificación[615]. Si no se puede resolver ninguna de las direcciones seleccionadas, MDaemon enviará el mensaje a la Dirección de Notificaciones por omisión determinada abajo. Si no se ha especificado una cuenta, el mensaje no se enviará. Esta opción se encuentra habilitada por omisión.

Enviar reporte al postmaster global
Marque esta casilla si desea enviar los reportes al postmaster global[834]. La opción se encuentra habilitada por omisión.

Enviar reporte a los administradores globales
Marque esta casilla si desea enviar los reportes a los administradores globales[757].

Enviar reporte al postmaster del dominio del usuario
Marque esta casilla si desea enviar los reportes al postmaster del dominio[834] al que pertenece la cuenta que está congelada. Esta opción solo está disponible en MDaemon Private Cloud.

Enviar reporte a los administradores del dominio del usuario
Marque esta casilla si desea enviar los reportes a los administradores del dominio[757] para la cuenta que está congelada.

Enviar reporte al usuario
Esta opción solo está disponible en MDaemon Private Cloud.

Reportes de bloqueos de Direcciones IP

Notificar cuando una dirección IP es bloqueada
Esta opción hace que MDaemon envíe un mensaje de notificación al postmaster u otro destinatario seleccionado cada vez que una dirección IP es bloqueada por el sistema de Monitoreo Dinámico. Si ninguna de las direcciones de correo seleccionada se puede resolver, MDaemon enviará el mensaje a la Dirección de Notificaciones por omisión, determinada abajo. Si no se ha especificado dirección, el mensaje no se enviará. Esta opción se encuentra deshabilitada por omisión.

Incluir historial de conexión
Marque esta casilla si desea que el reporte incluya el historial registrado de conexiones de la dirección IP bloqueada.

Enviar reporte al postmaster global
Marque esta casilla si desea enviar los reportes al postmaster global[834].

Enviar reporte a los administradores globales
Marque esta casilla si desea enviar los reportes a los administradores globales[757].

Reportes de Expiración

Enviar reportes de direcciones bloqueadas cuando expiran los registros
Esta opción envía un reporte a las direcciones designadas cuando una dirección IP bloqueada expira en la Lista Dinámica de Bloqueados[625]. Se encuentra habilitada por omisión.

Enviar reportes sobre direcciones exentas/permitidas cuando sus registros expiran
Esta opción envía un reporte a las direcciones designadas siempre que una dirección en lista blanca expira y se elimina de la Lista Dinámica de Permitidos[624]. Se encuentra habilitada por omisión.

Enviar reportes sobre cuentas congeladas que se descongelan automáticamente
Esta opción envía un reporte a las direcciones designadas siempre que una cuenta congelada se descongela automáticamente[615] luego de que ha transcurrido el periodo de *Tiempo de Espera de Cuentas Congeladas*. Se encuentra habilitada por omisión.

Enviar reporte al postmaster global
Marque esta casilla si desea enviar los reportes al postmaster global[834]. Esta opción se encuentra habilitada por omisión.

Enviar reporte a los administradores globales
Marque esta casilla si desea enviar los reportes a los administradores globales[757].

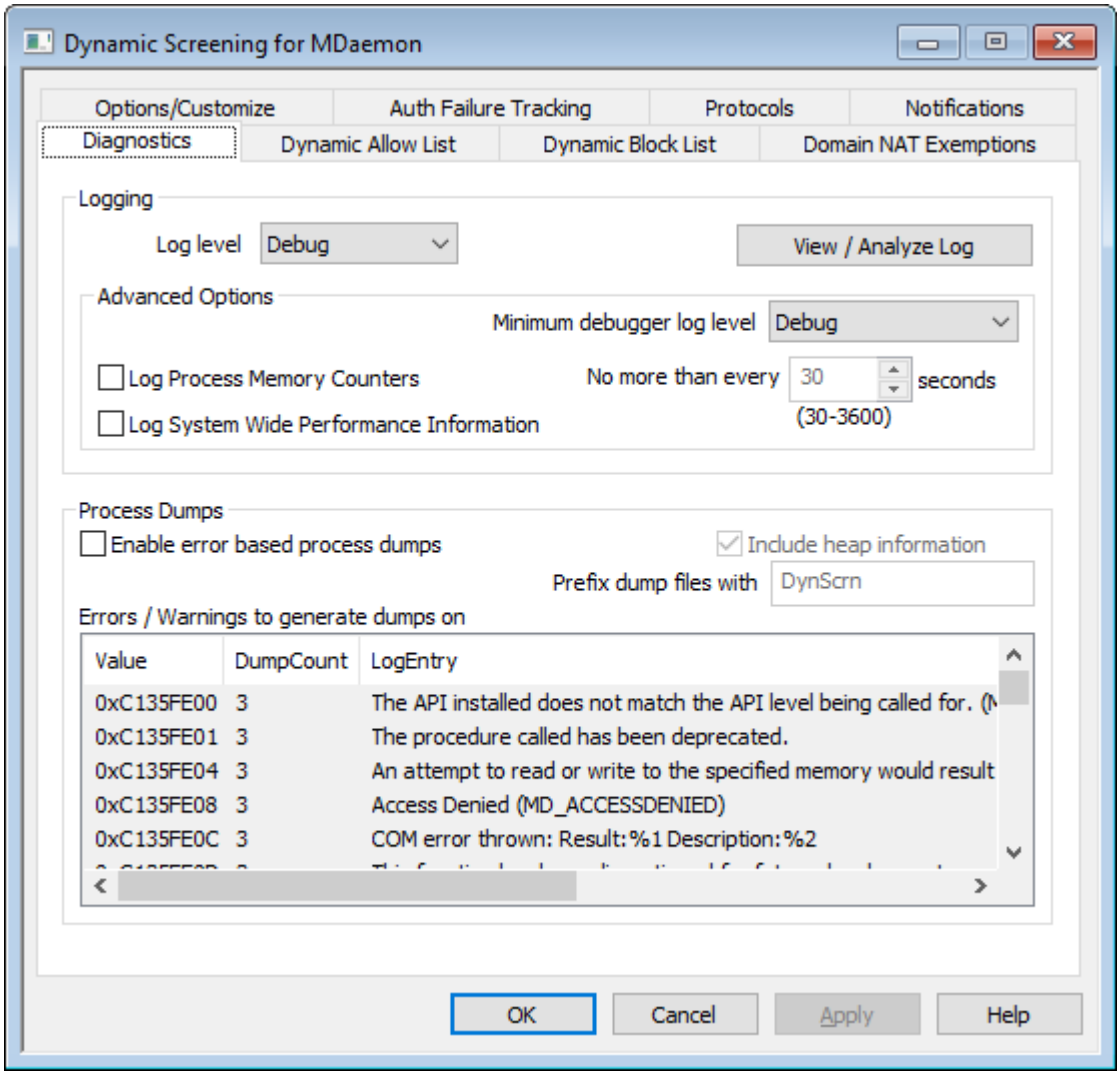
Dirección de Notificaciones por Omisión
Esta es la dirección a la que se enviarán los reportes de notificaciones cuando no exista otra dirección o no se pueda resolver ninguna de las direcciones determinadas. Si no se puede resolver ninguna dirección y no se designa una *Dirección de Notificaciones por Omisión*, el reporte no se enviará.

Agregar la hora GMT a las notificaciones con expiraciones
Por omisión, cuando los reportes de notificación se envían e incluyen la hora de expiración, este dato se lista en la hora del servidor local. Habilite esta opción si también desea incluir la hora GMT. Esto es útil cuando sus administradores globales se encuentran localizados en otras zonas horarias.

Ver:

Opciones/Personalizar[610]
Monitoreo de Fallos de Autentificación[615]

4.3.5 Diagnósticos



Esta pantalla contiene opciones avanzadas que en la mayoría de los casos no necesitarán ser utilizadas a menos que intente diagnosticar un problema con el Monitoreo Dinámico o sea indicación de soporte técnico.

Registro

Nivel de Registro
Se soportan seis niveles de registro dependiendo de la más alta a más baja cantidad de datos registrados:

Depurar Es el nivel de registro más detallado. Incluye todas las entradas disponibles y típicamente solo se utiliza al diagnosticar un problema o cuando el administrador requiere información detallada.

Info Registro Moderado. Incluye operaciones generales sin detalle. Es el nivel de registro por omisión.

Advertencia Incluye advertencias, errores, errores críticos y eventos de inicio/cierre de la aplicación.

Error Se registran errores, errores críticos y eventos de inicio/cierre de la aplicación.

Críticos Se incluyen errores críticos y eventos de inicio/cierre de la aplicación.

Ninguno Solo se registran eventos de inicio/cierre de la aplicación.

Ver/Analizar el Registro
Dé clic en este botón para abrir el Sistema de Visor Avanzado de Registros de MDaemon. Por omisión, los registros se almacenan en: "..\MDaemon\Logs\"

Opciones Avanzadas

Nivel mínimo de registros para el depurador
Este es el nivel mínimo de registros a emitir al depurador. Los niveles disponibles de registro son los mismos descritos previamente.

Registrar contadores de procesamiento de memoria
Marque esta casilla para incluir en el archivo de registro información específica de procesos de Memoria, Identificadores e Hilos. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos. Las entradas al registro solo se emiten si los datos se han modificado desde la última vez que se registraron.

Registrar información del desempeño general del sistema
Marque esta casilla si desea incluir en el registro información del desempeño general del sistema. Esto es útil para encontrar pistas potenciales y problemas de asignación de recursos.

No más de cada [xx] segundos
Utilice esta opción para establecer el límite de la frecuencia con que se registrará la información de procesos y desempeño.

Volcados de Proceso

Habilitar volcados de procesos con base en errores
Habilite esta opción si desea generar volcados de proceso siempre que ocurran advertencias o errores específicos que usted determine abajo.

Incluir información de la pila en los volcados
Por omisión, se incluye información de la pila en los volcados de procesos. Deshabilite esta casilla si no desea que se incluya esta información.

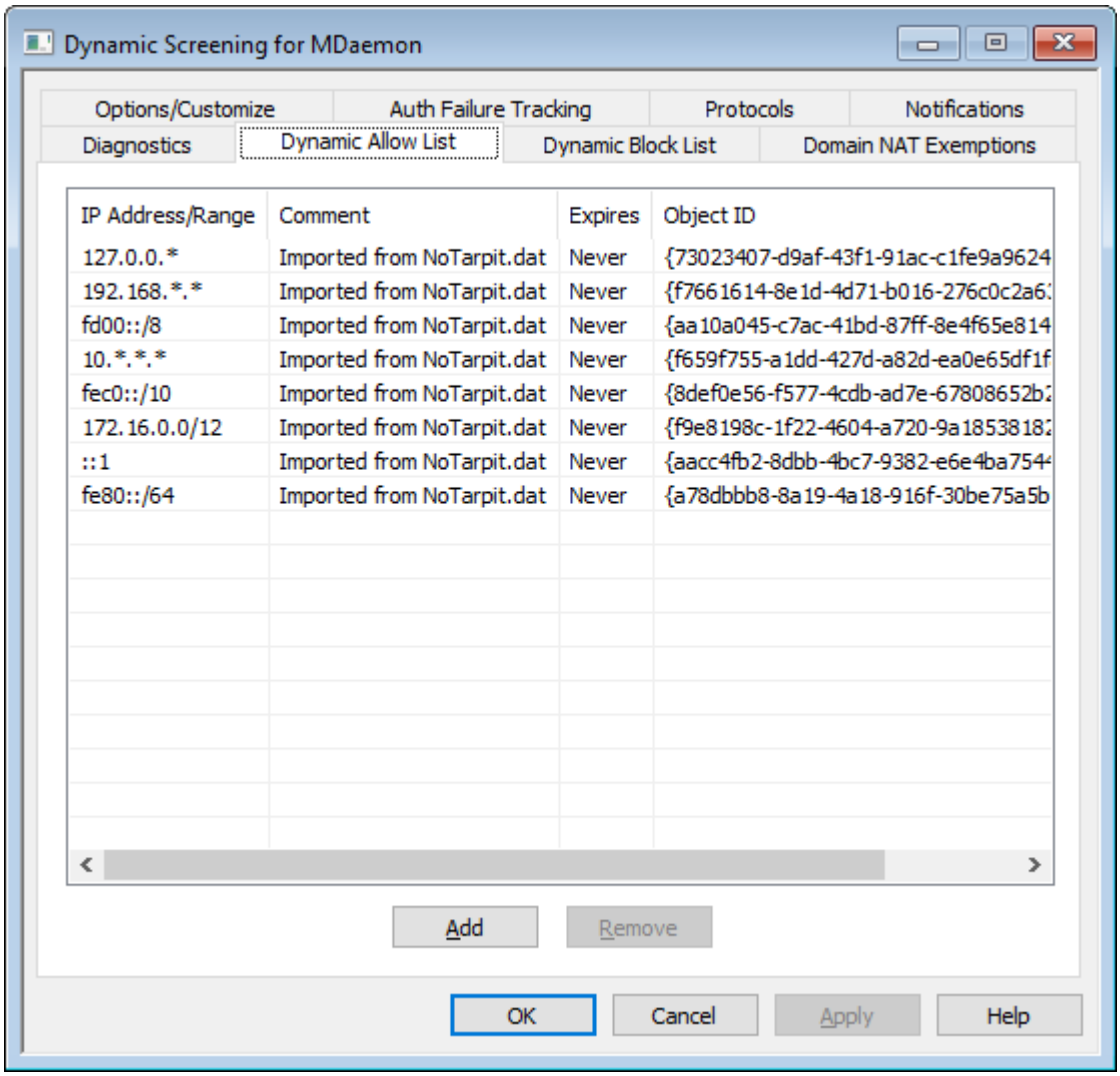
Prefijo para los archivos de volcado
Los nombres de archivos de volados de procesos inician con este texto.

Errores/Advertencias para genera volcados
Dé clic derecho en esta área y utilice las opciones *Agregar/Editar/Eliminar Registro...* para administrar la lista de errores o advertencias que detonarán volcados de procesos. Por cada entrada puede definir el número de volcados de proceso permitidos antes de que se desactive.

Ver:

Monitoreo Dinámico » Opciones/Personalizar 610

4.3.6 Lista Dinámica de Permitidos

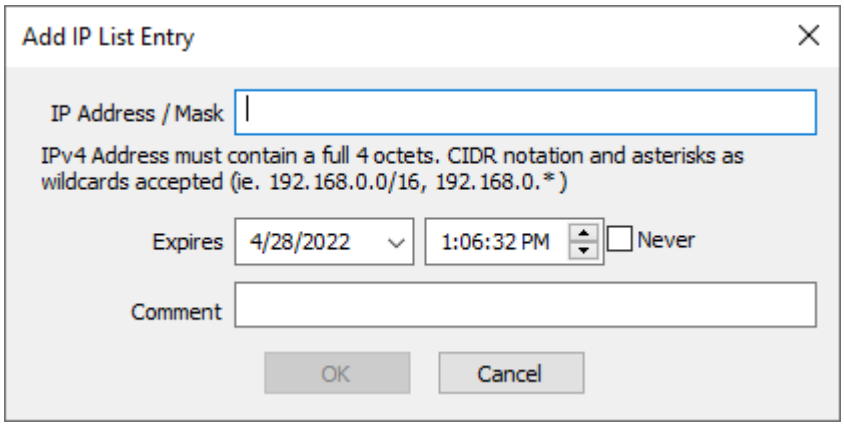


La Lista Dinámica de Permitidos contiene la lista de direcciones IP o rangos de direcciones que estarán exentos de bloqueo por el servicio de Monitoreo Dinámico, cuando intenten conectarse a MDaemon. Las direcciones se pueden agregar a la Lista Blanca Dinámica dando clic en el botón **Agregar**. Cada entrada contiene la dirección o rango de IP´s, la fecha y hora en que expirará la entrada (o "Nunca", si no expirará", cualquier comentario que desee hacer sobre la entrada y un Object ID. La Lista Blanca Dinámica también es utilizada por el Monitoreo SMTP 566, Monitoreo de Localizaciones 572 y el Tarpitting 602.

Agregar una dirección o rango de IP´s a la Lista Dinámica de Permitidos

Para agregar una entrada a la lista:

1. Dé clic en **Agregar**. Con esto se abre el diálogo Agregar Entrada a la Lista de IP´s



2. Capturar la dirección o rango de IP´s.
3. Seleccione la fecha y hora en que desea que expire o dé clic en **Nunca**.
4. Ingrese un comentario para la entrada (opcional).
5. Dé clic en **OK**.

Eliminar una Entrada de la Lista

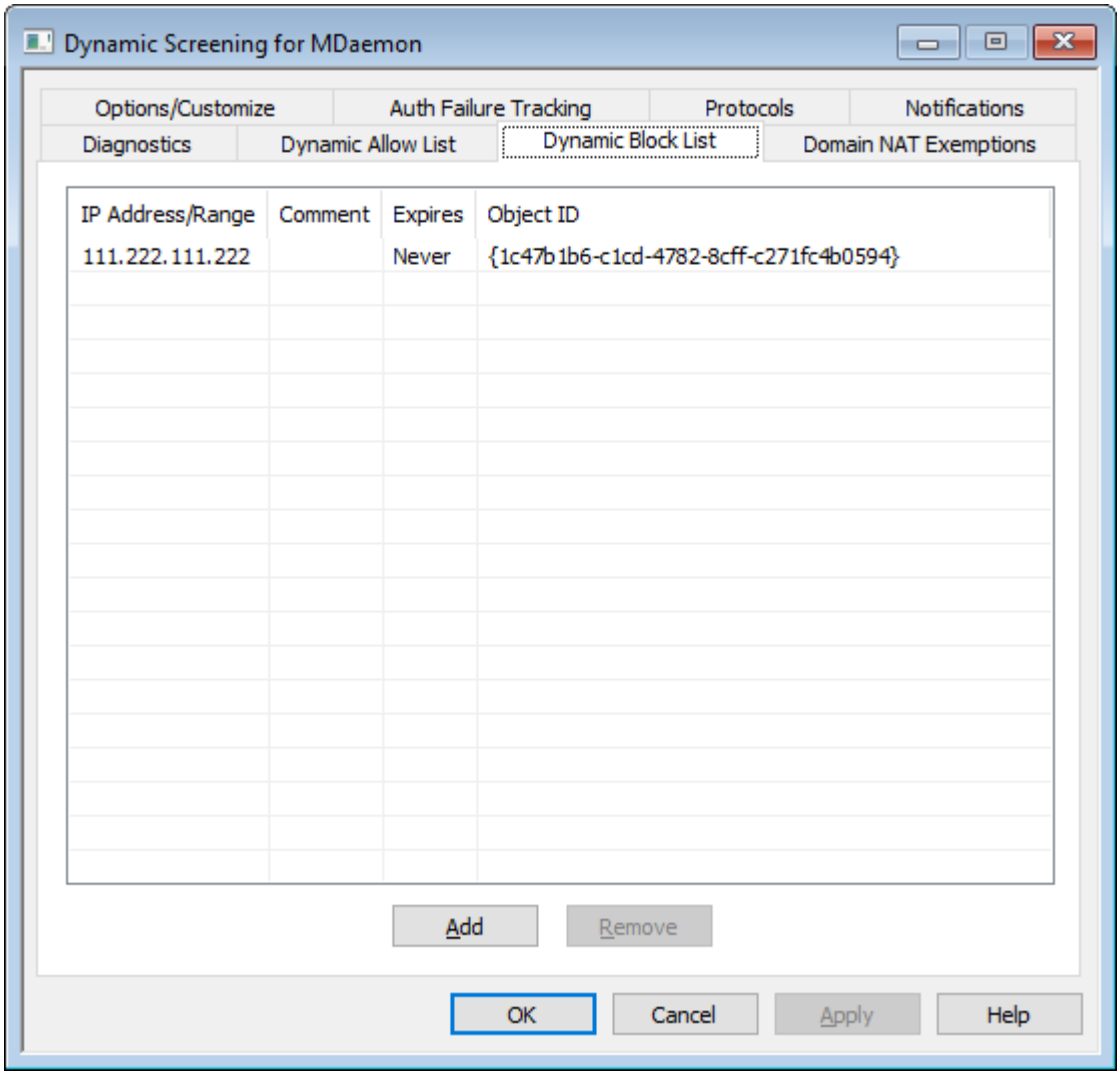
Para eliminar una o más entradas de la lista:

1. Seleccione la entrada o entradas que desea eliminar de la lista (Ctrl+clic para seleccionar múltiples entradas).
2. Dé clic en **Eliminar**.

Ver:

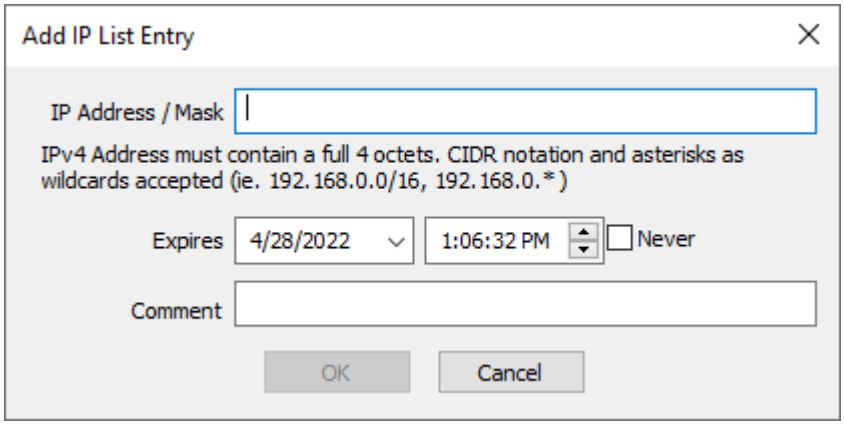
Opciones/Personalizar 610
Monitoreo de Fallos de Autentificación 615
Lista Dinámica de Bloqueados 625
Protocolos 617

4.3.7 Lista Dinámica de Bloqueados



La Lista Dinámica de Bloqueados contiene la lista de direcciones IP o rangos de direcciones, que serán bloqueados por el servicio de Monitoreo Dinámico cuando intentan conectarse a MDaemon. Las direcciones se pueden agregar automáticamente desde el Monitoreo de Fallos de Autentificación 615 y el Monitoreo SMTP 566 y agregarse manualmente dando clic en el botón **Agregar**. Cada entrada contiene la dirección o rango de IP´s, la fecha y hora en que esa entrada expirará (o "Nunca" si no expirarán), cualquier comentario que desee hacer sobre la entrada y un Object ID.

1. Dé clic en **Agregar**. Esto abre el diálogo Agregar entrada a la Lista de IPs.



2. Registre la dirección o rango de direcciones IP.
3. Seleccione la fecha y hora en que desea que expire o dé clic en **Nunca**.
4. Capture un comentario respecto a esa entrada (opcional).
5. Dé clic en **OK**.

Eliminar una entrada de la Lista

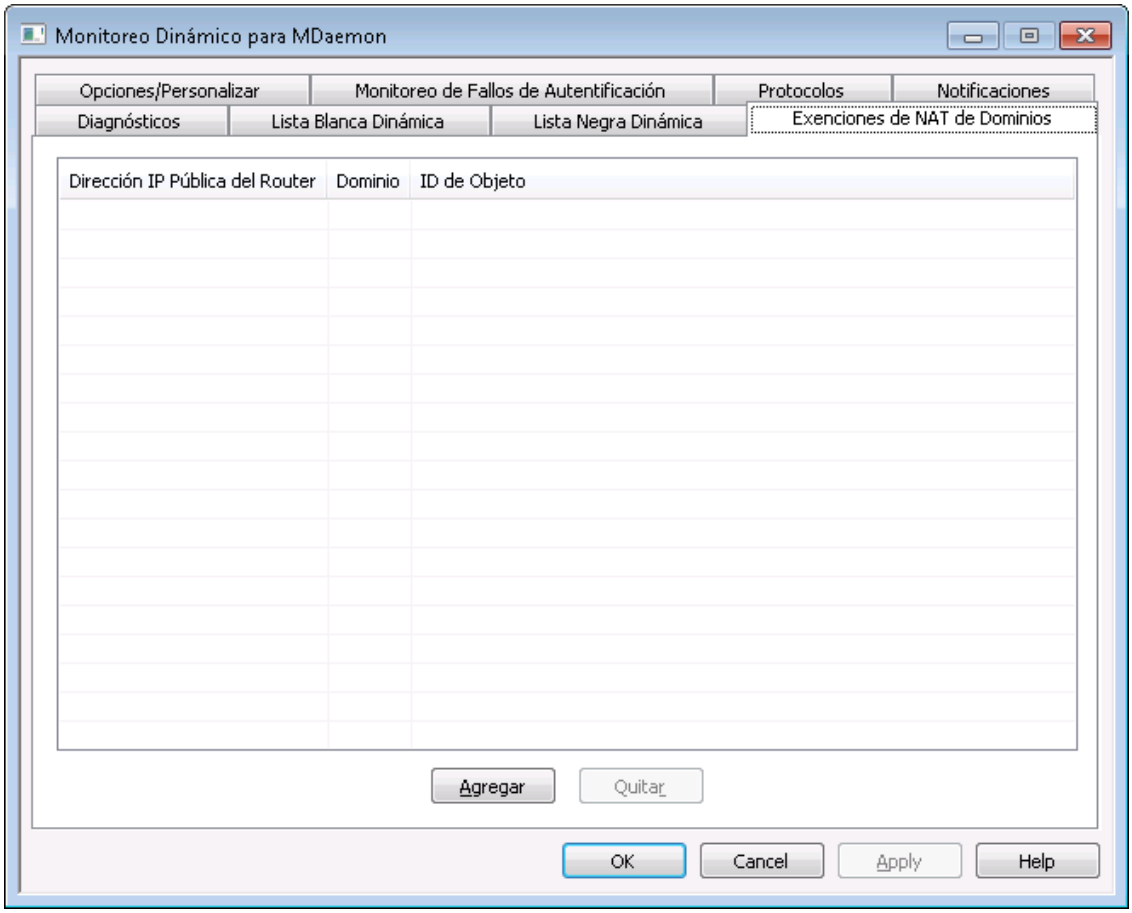
Para eliminar una o más entradas de la lista:

1. Seleccione la entrada y entradas que desea eliminar de la lista (Ctrl+clic para seleccionar múltiples entradas).
2. De clic en **Eliminar**.

Ver:

Opciones/Personalizar 610
Monitoreo de Fallos de Autentificación 615
Lista Dinámica de Permitidos 624
Protocolos 617

4.3.8 Exención Nat de Dominio



Esta pantalla está disponible si ha activado la opción *Habilitar las funciones avanzadas en la Interface de Usuario* en la pantalla Opciones/Personalizar 610 del Monitoreo Dinámico.

Utilice esta funcionalidad para dar servicio a un grupo de usuarios de MDaemon que residen en la misma red de área local externa (LAN), que utilizan NAT (network address translation) para proporcionar una única dirección IP pública compartida para todos ellos. Al agregar la dirección IP Pública de su LAN y el dominio de MDaemon al que pertenecen las cuentas, puede impedir que las direcciones IP sean bloqueadas por el Monitoreo Dinámico cuando uno o más usuarios fallen la autentificación debido a una contraseña incorrecta. Sin esta funcionalidad, un usuario válido con un cliente de correo mal configurado puede hacer que la dirección IP pública de la LAN sea bloqueada e impedirá que todos los usuarios puedan tener acceso a su correo. Esto puede suceder, por ejemplo, cuando se modifica la contraseña de un usuario, pero se olvida de actualizar su cliente de correo con el nuevo valor.

Las direcciones IP listadas aquí de todas maneras pueden ser bloqueadas por otras razones, tal como bots que intenten iniciar sesión a cuentas no válidas, clientes mal configurados intentando abrir sesión en un dominio de MDaemon distinto del asociado a la dirección IP, etc. Si desea excluir completamente una dirección IP del Monitoreo Dinámico, utilice la Lista Dinámica de Permitidos 624.

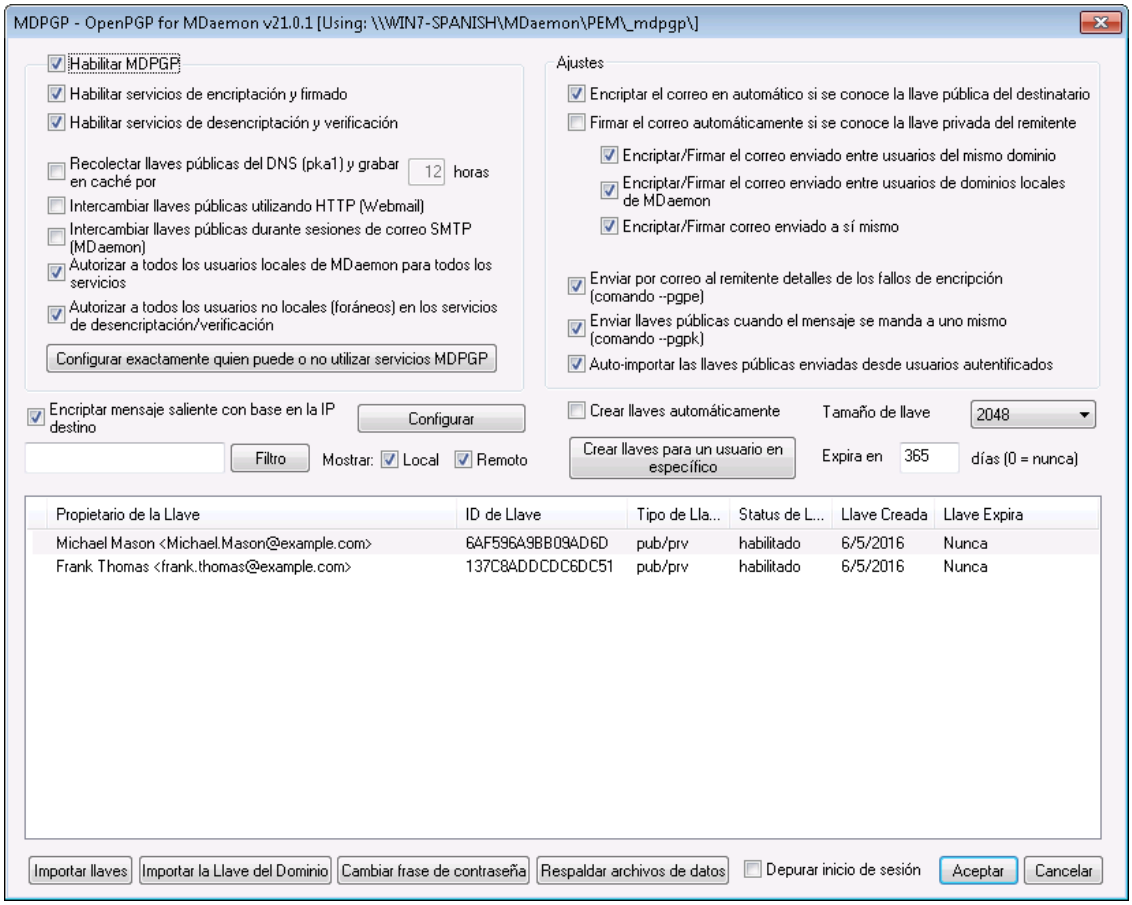
Agregar Exención NAT de Dominio

Dé clic en **Agregar**, registre la *Dirección IP Pública del Ruteador* de la LAN externa y seleccione el *Dominio* de MDaemon cuyos usuarios iniciarán sesión desde esa dirección IP. Luego, dé clic en **OK**.

Ver:

Opciones/Personalizar 610

4.4 MDPGP



OpenPGP es un protocolo estándar de la industria para intercambiar datos encriptados; existe una variedad de complementos OpenPGP para clientes de correo que permiten a los usuarios enviar y recibir mensajes encriptados. MDPGP es el componente OpenPGP de MDaemon que puede proporcionar encripción, desencripción y servicios básicos de manejo de llaves para sus usuarios sin requerir que utilicen un complemento con el cliente de correo.

MDPGP encripta y desencripta correos utilizando un sistema de llaves pública/privada. Para hacer esto, cuando desee utilizar MDPGP para enviar un mensaje privado y seguro a alguien, MDPGP encriptará ese mensaje utilizando una

"llave" que usted habrá obtenido previamente de esa persona (i.e. su "llave pública") y la habrá importado a MDPGP. Alternativamente, si el remitente desea enviarle un mensaje privado, entonces él debe encriptar el mensaje utilizando su llave pública, que habrá obtenido de usted. Es absolutamente necesario dar la llave pública al remitente porque si ella él no podrá enviarle un mensaje encriptado de tipo OpenPGP. Su llave pública única debe ser utilizada para encriptar el mensaje porque su llave privada única es lo que utilizará MDPGP para desencriptar el mensaje cuando llegue.

A fin de que MDPGP firme, encripte y desencripte mensajes, mantiene dos almacenes de llaves (i.e. llaveros) —uno de llaves públicas y uno de llaves privadas. MDPGP puede generar las llaves de sus usuarios automáticamente si se requiere o usted puede crearlas manualmente para usuarios en específico. También puede importar llaves que fueron creadas en otra instancia. Más aun, MDaemon puede buscar las llaves públicas adjuntas a mensajes autentificados de usuarios locales y luego importar esas llaves automáticamente. De esa manera el usuario puede solicitarle a alguien su llave pública y luego enviar esa llave a sí mismo de manera que MDPGP la detecte e importe a su llavero público. MDPGP nunca almacena múltiples copias de la misma llave, pero puede haber múltiples llaves diferentes para una misma dirección. Finalmente, siempre que llegue un mensaje proveniente de una dirección que cuenta con una llave en un llavero, MDPGP lo firmará, encriptará o desencriptará como sea necesario, de acuerdo con sus ajustes. Si una dirección cuenta con múltiples llaves, MDPGP utilizará la que se haya designado como llave preferida para encriptar el mensaje. Si no se ha definido una llave preferida, entonces MDPGP utilizará la primera. Al desencriptar un mensaje, MDaemon intentará con cada una.

Puede configurar los servicios de firma y encripción de MDPGP para operar ya sea en automático o manualmente. Cuando se configura para operar automáticamente, MDPGP firmará y encriptará los mensajes en automático siempre que sea posible. Cuando se configura para operar manualmente, MDPGP solo firmará o encriptará los mensajes cuando el usuario remitente inserte un comando especial en el Asunto de esos mensajes. En cualquier caso, los mensajes solo se firmarán o encriptarán (o desencriptarán) cuando la cuenta tenga permiso de utilizar esos servicios.

La especificación OpenPGP se describe en los RFCs 4880 y 3156.

Habilitar MDPGP

Habilitar MDPGP
MDPGP está habilitado por omisión, pero no firmará, encriptará o desencriptará ningún mensaje hasta que usted genere o importe llaves al llavero o hasta que utilice la opción siguiente para que MDPGP *Genere llaves automáticamente.*

Habilitar servicios de encripción & firmado
Por omisión los mensajes se pueden firmar y encriptar cuando las llaves requeridas se encuentran en el llavero. Deshabilite esta opción si no desea permitir que MDPGP firme o encripte mensajes.

Los mensajes se pueden firmar sin estar encriptados, pero cualquier mensaje encriptado por MDPGP siempre será firmado también.

Habilitar servicios de desencripción & verificación
Por omisión los mensajes encriptados entrantes serán desencriptados si se conoce la llave privada del destinatario. Así mismo, MDPGP también verificará las firmas integradas en los mensajes no encriptados. Note, sin embargo, que tanto el destinatario como el remitente deben estar autorizados para utilizar los servicios de desencripción&verificación, ya sea a través de la opción "*Autorizar a todos...*" o "*Configurar exactamente quien...*" (todos están autorizados por omisión). Deshabilite esta opción si no desea verificar firmas incrustadas o permitir que MDPGP desencripte cualquier mensaje, por ejemplo, si desea que todos los usuarios manejen su propia desencripción vía un cliente complementario. Al deshabilitar esta opción, cualquier mensaje entrante encriptado se manejará como mensaje normal y se colocará en el buzón del destinatario.

Recolectar llaves públicas del DNS (pka1) y guardar en caché por [xx] horas
Habilite esta opción si desea que MDPGP consulte las llaves públicas del destinatario en el DNS utilizando PKA1. Esto es útil porque automatiza el proceso de obtener las llaves públicas de algunos destinatarios, previniendo que usted o sus usuarios tengan que obtenerlas e importarlas manualmente a fin de enviar mensajes encriptados. Cuando se realizan consultas PKA1, cualquier llave URI encontrada se recolecta inmediatamente, se valida y agrega al llavero. Las llaves recolectadas e importadas exitosamente al llavero utilizando este método, se rastrean en un archivo llamado `fetchedkeys.txt` y estas llaves expiran en automático luego de un número de horas especificado en esta opción o de acuerdo con el valor TTL del registro PKA1 que las refirió, cualquiera que sea el valor mayor. Por esto, el valor especificado aquí es la duración mínima que esa llave permanecerá en caché. El valor por omisión es 12 horas y el valor permitido menor es 1 hora.

Si desea publicar sus propias llaves públicas en su DNS entonces debe crear registros TXT especiales. Por ejemplo, para el usuario `frank@example.com` con el key-id: `0A2B3C4D5E6F7G8H`, en el DNS del dominio "`example.com`" usted debe generar un registro TXT en "`frank._pka.example.com`" (reemplazando la @ en la dirección de correo con la cadena "`._pka.`"). Los datos del registro TXT se verían así: "`v=pka1; fpr=<key's full fingerprint>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H`" donde `<key's full fingerprint>` es la huella completa de la llave (40 caracteres que representan el valor completo de 20 bytes) Puede ver el valor completo de la huella de la llave dando doble clic en la llave en la IU de MDPGP.

Intercambiar llaves públicas utilizando HTTP (Webmail)
Habilite esta opción si desea utilizar WorldClient como servidor básico de llaves públicas: WorldClient respetará las peticiones de llaves públicas de sus usuarios. El formato de la URL para hacer la petición se ve así: "`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`". Donde `<WorldClient-URL>` es la ruta de su servidor WorldClient (por ejemplo, "`http://wc.example.com`") y `<Key-ID>` es el id de llave de 16 caracteres de la llave que usted desea (por

ejemplo, "0A1B3C4D5E6F7G8H"). El id de llave se construye con los últimos 8 bytes de la huella de la llave - 16 caracteres en total.

Intercambiar llaves públicas durante sesiones de correo SMTP (MDaemon)
Marque esta casilla si desea habilitar la transmisión automática de llaves públicas como parte del proceso SMTP de entrega de mensajes. Para hacerlo, el servidor SMTP de MDaemon respetará el comando SMTP denominado RKEY. Al enviar un mensaje de correo a un servidor que soporta RKEY, MDaemon ofrecerá transmitir la llave pública preferida actual del remitente hacia el otro host. Este responderá indicando ya sea que ya cuenta con esa llave ("250 2.7.0 Key already known") o que la necesita, en cuyo caso la llave se transfiere inmediatamente en formato armadura-ASCII ("354 Enter key, end with CRLF.CRLF") como cualquier otro mensaje de correo. Las llaves que han expirado o han sido revocadas nunca se transmiten. Si MDaemon cuenta con múltiples llaves para el remitente siempre enviará la llave marcada en ese momento como preferida. Si no existe una llave preferida entonces se enviará la primera que se encuentre. Si no ha llaves válidas entonces no se hace nada. Solo se ofrecen llaves públicas que pertenecen a usuarios locales.

Las transferencias de llaves públicas ocurren como parte de la sesión SMTP de correo que entrega el mensaje proveniente del usuario. A fin de que las llaves públicas se transmitan de manera que sean aceptadas, la llave pública debe enviarse junto con un mensaje que lleve Firma DKIM[532] del dominio del propietario de la llave con el valor i= definido como la dirección del propietario de la llave, que también debe coincidir exactamente con la dirección del encabezado From:, del cual solo debe existir uno. El "propietario de la llave" se toma de la llave misma. Así mismo, el mensaje debe llegar proveniente de un host en la ruta SPF[526] del remitente. Finalmente, el propietario de la llave (o su dominio completo, vía el uso de comodines) debe ser autorizado por RKEY agregando un registro apropiado en el archivo de reglas MDPGP (existen instrucciones para esto en el archivo de reglas9 indicando que el dominio es confiable para intercambiar llaves. Toda esta verificación se realiza automáticamente, sin embargo, usted debe tener habilitados DKIM[529] y Verificación SPF[526] o no se podrá hacer nada.

El registro de transacciones MDPGP muestra el resultado y detalles de todas las llaves importadas o eliminadas y el registro de sesiones SMTP también rastrea esta actividad. Este proceso rastrea la eliminación de llaves existentes y la selección de nuevas llaves preferidas y actualiza a todos los servidores participantes a los que envía correo, cuando se modifican valores.

Autorizar a todos los usuarios locales de MDaemon a utilizar todos los servicios

Por omisión las cuentas locales de MDaemon están autorizadas para utilizar cualquiera de los servicios MDPGP que tenga habilitados: firma, encripción, desencripción y verificación. Si hay usuarios específicos a los que no desea permitir utilizar uno o más de estos servicios, puede utilizarla opción "*Configurar exactamente quien puede o no utilizar servicios MDPGP*" para excluirlos. Deshabilite esta opción si solo desea autorizar a usuarios locales específicos. En ese caso utilice la opción "*Configurar exactamente quien puede o no utilizar servicios MDPGP*" para dar acceso a quién usted disponga.

Autorizar a todos los usuarios no locales (externos) en los servicios de desencripción/verificación
Por omisión cualquier mensaje entrante encriptado para un destinatario local, proveniente de un remitente no-local puede ser desencriptado si MDPGP conoce la llave privada del destinatario local. De manera similar, MDPGP verificará las

firmas incrustadas en los mensajes entrantes de usuarios no-locales. Si existen ciertos remitentes no-locales cuyos mensajes no desea desencriptar o verificar puede utilizar la opción siguiente: "*Configurar exactamente quién puede o no utilizar servicios MDPGP*" para restringir a esos remitentes en esos servicios. Deshabilite esta opción si no desea desencriptar mensajes o verificar firmas incrustadas cuando el remitente sea una dirección no-local. En ese caso puede utilizar la opción "*Configurar exactamente quién puede o no utilizar servicios MDPGP*" para especificar excepciones a esa restricción.

Configurar exactamente quién puede o no utilizar servicios MDPGP
Dé clic en este botón para abrir el archivo `rules.txt` para configurar los permisos de usuario para MDPGP. Utilizando este archivo puede especificar quién tiene permiso de firmar mensajes, encriptar mensajes y recibir mensajes desencriptados. También puede restringir específicamente a algunos usuarios de estas opciones. Por ejemplo, puede utilizar la regla "`+*@example.com`" para permitir a todos los usuarios de `example.com` encriptar mensajes y luego agregar "`-frank@example.com`" para impedir específicamente que `frank@example.com` lo pueda hacer. Vea el texto al inicio del archivo `rules.txt` para ejemplos e instrucciones.

Rules.txt Notas y Sintaxis

- Solo el correo SMTP autentificado de usuarios de este servidor MDaemon es elegible para el servicio de encripción. Sin embargo, puede especificar las direcciones no locales que desea restringir del servicio de encripción, significando que MDPGP **no** encriptará mensajes hacia ellos, aun cuando se conozca la llave pública.
- Si existe un conflicto entre los ajustes en el archivo `rules.txt` y la opción global "*Autorizar a todos los usuarios locales de MDaemon para todos los servicios MDPGP*", se utiliza el ajuste en `rules.txt`.
- Si existe un conflicto entre los ajustes en `rules.txt` y la opción global "*Autorizar a todos los usuarios no locales en los servicios de desencripción/verificación*", se utilizará el ajuste en el archivo `rules.txt`.
- El texto después de # en una línea e ignora.
- Separe múltiples direcciones de correo en la misma línea con un espacio.
- Se permiten comodines (* y ?) en las direcciones de correo.
- Aun cuando los mensajes encriptados MDPGP siempre van firmados, el otorgar permisos de encripción a un usuario no le otorga permisos de firmar mensajes desencriptados. A fin de firmar mensajes desencriptados, la cuenta debe contar con permisos de firma.
- Cada dirección de correo debe tener un prefijo con alguna de las siguientes etiquetas:

  + (más) - la dirección puede utilizar el servicio de encripción MDPGP.

  - (menos) - las direcciones **no pueden** utilizar el servicio de encripción MDPGP.

  ! (exclamación) - la dirección **puede** utilizar el servicio de desencripción MDPGP.

  ~ (tilde) - la dirección **no puede** utilizar el servicio de desencripción MDPGP.

^ (caret) - la dirección **puede** utilizar el servicio de firmado MDPGP.

= (igual) - la dirección **no puede** utilizar el servicio de firmado MDPGP.

$ (dólar) - la dirección puede utilizar el servicio de verificación MDPGP.

& (ampersand) - la dirección **no** puede utilizar el servicio de verificación MDPGP.

Ejemplos:

`+*@*` — todos los usuarios de todos los dominios pueden encriptar.

`!*@*` — todos los usuarios de todos los dominios pueden desencriptar.

`^*@*` — todos los usuarios de todos los dominios pueden firmar.

`^*@example.com` — todos los usuarios de example.com pueden firmar.

`+frank@example.com ~frank@example.com` — el usuario puede encriptar, pero no desencriptar.

`+GROUP:EncryptingUsers` — Miembros del grupo `EncryptingUsers` de MDaemon pueden encriptar.

`^GROUP:Signers` — Miembros del grupo `Signers` de MDaemon pueden firmar.

Modos de Encripción/Firma

Modo Automático

Utilice la opción Ajustes para configurar MDPGP para firmar y encriptar mensajes automáticamente para cuentas que tengan permiso para hacerlo. Cuando una cuenta envía un mensaje autentificado y MDPGP conoce la llave requerida, el mensaje será firmado o encriptado de acuerdo con los ajustes siguientes.

El código especial en el Asunto, descrito en la sección Modo Manual siempre tiene precedencia sobre las opciones del Modo Automático. Por esto si una de estas opciones está deshabilitada, una cuenta que tenga permisos de firmar o encriptar mensajes puede hacer manualmente que el mensaje sea firmado o encriptado utilizando uno de los códigos.

Ajustes

Encriptar el correo automáticamente si se conoce la llave privada del destinatario
Por omisión, si una cuenta tiene permiso de encriptar mensajes, MDPGP los encriptará en automático si conoce la llave privada de la cuenta del destinatario. Deshabilite esta opción si no desea que se encripten en automático; los mensajes se pueden encriptar manualmente utilizando los códigos especiales descritos en la sección Modo Manual descrita abajo.

Firmar el correo automáticamente si se conoce la llave pública del remitente
Dé clic en esta opción si desea que MDPGP firme en automático los mensajes cuando se conoce la llave privada de la cuenta remitente, si la cuenta tiene permitido firmar mensajes. Aun cuando esta opción está deshabilitada, los

mensajes se pueden firmar manualmente utilizando los códigos especiales descritos en la sección Modo Manual descrita abajo.

Encriptar/Firmar correo entre usuarios del mismo dominio
Cuando MDPGP se configura para encriptar o firmar mensajes en automático, esta opción hace que MDPGP lo haga aun cuando los mensajes se envíen entre usuarios del mismo dominio, suponiendo que se conocen las llaves requeridas. Esta opción se encuentra habilitada por omisión.

Encriptar/Firmar correo entre usuarios de dominios locales de MDaemon
Cuando MDPGP se configura para encriptar o firmar mensajes en automático, esta opción hace que MDPGP lo haga aun cuando los mensajes se envíen entre usuarios de dominios locales de MDaemon, suponiendo que se conocen las llaves requeridas Por ejemplo si sus dominios de MDaemon incluyen "example.com" y "example.net," entonces los mensajes enviados entre los usuarios de esos dominios se encriptarán o firmarán automáticamente Esta opción está habilitada por omisión.

Encriptar/firmar correo enviado a uno mismo
Cuando MDPGP se configura para encriptar o firmar mensajes automáticamente, esto se hará aun cuando el usuario de MDaemon esté enviando un mensaje a sí mismo (ej. frank@example.com envía a frank@example.com). Por esto, si la cuenta tiene permiso de utilizar tanto encripción como desencripción (los ajustes por omisión) MDPGP aceptará el mensaje del usuario, lo encriptará e inmediatamente lo desencriptará y colocará en el buzón del mismo usuario. Si, sin embargo, la cuenta no está configurada para desencripción, esto hará que el mensaje se encripte y luego se coloque en el buzón del mismo usuario aun encriptado. Esta opción está deshabilitada por omisión.

Modo Manual

Cuando ha deshabilitado las opciones *Firmar correo automáticamente...* y *Encriptar correo automáticamente...* descritas arriba, estará utilizando MDPGP en Modo Manual. MDPGP no firmará o encriptará ningún mensaje excepto aquellos que sean autentificados y contengan alguno de los siguientes códigos en el encabezado Asunto del mensaje:

--pgps Firmar el mensaje si es posible. El código se puede colocar al inicio o final del Asunto.

--pgpe Encriptar el mensaje si es posible. El código se puede colocar al inicio o final del Asunto.

--pgpx El mensaje **DEBE** ser encriptado. Si no se puede encriptar (ej. porque la llave del destinatario no se conoce) entonces no se entregará; el mensaje será rebotado/devuelto a su remitente. El código se puede colocar al inicio o final del Asunto.

--pgpk Enviarme mi llave pública. El usuario coloca este código al inicio del Asunto y se envía el mensaje a sí mismo. MDPGP le enviará por correo su llave pública.

--pgpk<Email> Enviarme la llave pública de esta dirección. El usuario coloca este código al inicio del Asunto y envía el mensaje a sí mismo. MDPGP le enviará por correo la llave pública de esa dirección.

Ejemplo:

```
Asunto: --pgpk<frank@example.com>
```

Administración de Llaves

Las llaves Públicas y Privadas se administran utilizando las opciones la mitad inferior del diálogo MDPGP. Existe una entrada para cada llave y puede dar clic derecho a cualquier registro y exportar la llave, eliminarla o habilitar/deshabilitarla, configurarla como Llave Preferida (vea "*Intercambiar llaves públicas durante las sesiones SMTP*, arriba) o configurarla como llave del Dominio (ver abajo). Cuando dé clic en **Exportar llave**, esta se grabará en la carpeta `\MDaemon\Pem\_mdpgp\exports\` y opcionalmente usted puede enviar la llave pública a una dirección de correo. Las opciones "Mostrar Local/Remota" y "Filtrar" se proporcionan para ayudarle a localizar ciertas direcciones o grupos.

Utilizar una Llave de Dominio

Opcionalmente puede utilizar una sola llave para encriptar todos los mensajes dirigidos a un dominio específico, sin importar quién sea el remitente. Esto es útil si, por ejemplo, uno de sus dominios y un dominio hospedado en otra ubicación desean encriptar todos los correos que se envían entre ellos, pero no desean configurar y administrar llaves de encripción individuales para cada cuenta de usuario en ambos dominios. Existen múltiples maneras de lograr esto:

- Si ya cuenta con una llave pública para otro dominio y desea utilizarla para encriptar todos los mensajes salientes que se dirigen a él, dé clic en la llave y dé clic en **Configurar como llave del Dominio**. Luego registre el nombre de dominio y dé clic en **OK**. Esto creará una regla en el Filtro de Contenido que hará que todos los mensajes dirigidos a ese dominio sean encriptados utilizando la llave definida.
- Si le han proporcionado la llave pública del dominio pero no se encuentra aún en la lista, dé clic en **Importar la Llave de Dominio**, registre el nombre de dominio y dé clic en OK, luego navegue al archivo del dominio `public.asc` y dé clic en **Abrir**. Esto también creará una regla en el Filtro de Contenido para encriptar mensajes a ese dominio.
- Personalice sus reglas del Filtro de Contenido como lo requiera para modificar exactamente qué mensajes se deben encriptar antes de enviar a los dominios.
- Para crear una llave nueva para uno de sus dominios, para entregarla a otro dominio para encriptar los mensajes que le envíen, siga las instrucciones en "*Crear llaves para un usuario específico*" descrita abajo, seleccionando "`_Domain Key (domain.tld)_ <anybody@domain.tld>`" en la lista.

No utilice una llave para encriptar mensajes salientes para los que también tiene la llave privada correspondiente. Si lo hace, MDPGP encriptará los mensajes e inmediatamente

verá que la llave de desencripción es conocida e inmediatamente desencriptará el mensaje.

Enviar por correo detalles de los fallos de encripción al remitente (comando --pgpe)
Cuando alguien utiliza el comando --pgpe para enviar correo encriptado y la encripción falla (por ejemplo, porque no se encontró llave de encripción), entonces esta opción generará el envío de un correo de notificación al remitente informándole del fallo. Esta opción se encuentra deshabilitada por omisión, lo que significa que no se enviarán mensajes de notificación de fallos.

Enviar por correo llaves públicas cuando se envía correo a uno mismo (comando --pgpk)
Cuando un usuario envía un correo a sí mismo con el asunto "--pgpk<email address>" (ej. --pgpk<frank@example.com>). Si existe una llave pública para <email address> se le enviará por correo a quién la solicitó.

Autoimportar llaves públicas enviadas de usuarios autentificados
Por omisión, cuando un usuario autentificado envía un mensaje de correo con una llave pública como adjunto en formato ASCII, MDPGP importará esa llave pública al llavero. Esta es una manera sencilla para que el usuario incorpore las llaves públicas de sus contactos en el llavero de MDPGP, enviando por correo la llave pública a sí mismo como archivo adjunto. Deshabilite esta opción si no desea autoimportar llaves.

Crear llaves automáticamente
Habilite esta opción si desea que MDPGP cree pares de llaves pública/privada para cada usuario de MDaemon. En lugar de generar todas al mismo tiempo, sin embargo, MDPGP las creará a lo largo del tiempo, creando el par para cada usuario en la siguiente ocasión en que se procese un mensaje para ese usuario. Esta opción está deshabilitada por omisión para conservar recursos y evitar generación innecesaria de llaves para cuentas que puede ser nunca utilicen MDPGP.

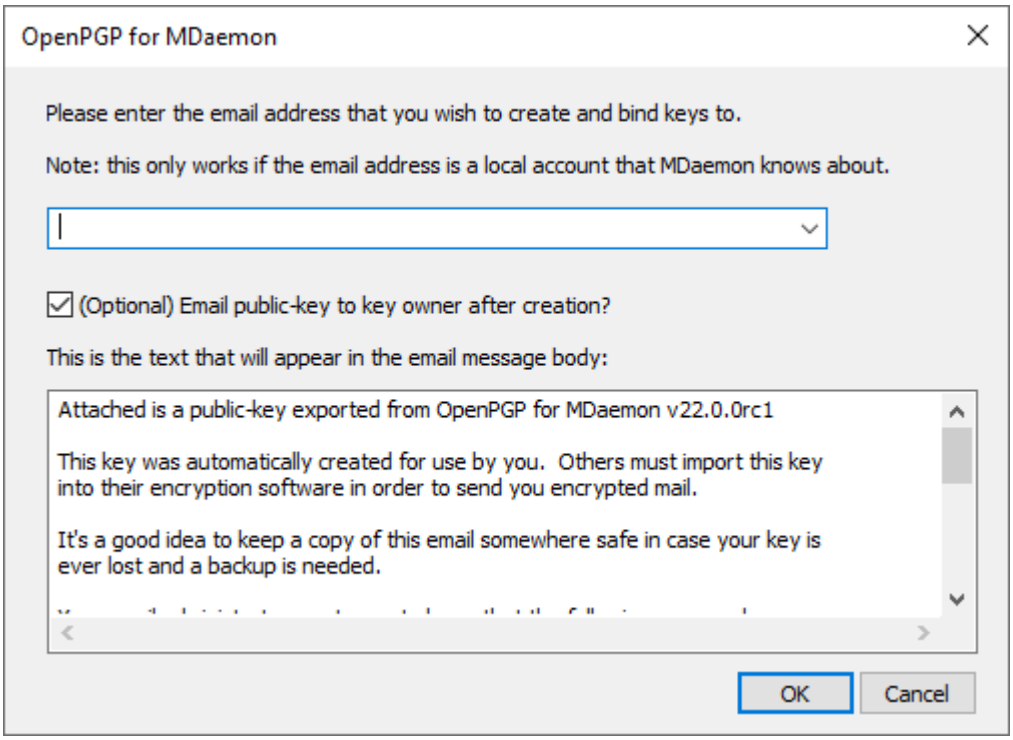
Tamaño de la Llave
Utilice esta opción para especificar el tamaño de la llave para las llaves que genera MDPGP. Puede configurar el tamaño de la llave a 1024, 2048, o 4096. El valor por omisión es de llaves de 2048 bits.

Expira en [xx] días (0=nunca)
Utilice esta opción para especificar el número de días que será válida una llave generada por MDPGP desde su fecha de creación hasta que expire. Configure esta opción en "0" si no desea que las llaves expiren. El valor por omisión es 0.

Crear llaves para un usuario específico
Para generar manualmente un par de llaves para una cuenta:

1. Dé clic en **Crear llaves para un usuario en específico**.
2. Seleccione la cuenta de la lista desplegable. Si desea crear una única llave para aplicar a todas las cuentas del dominio, elija la opción "_Domain Key (domain.tld)_ <anybody@domain.tld>" de la lista.

3. **Opcional:** Marque la caja **Enviar la llave pública al propietario de la llave...** si desea enviar la llave al usuario con adjunto en un correo.
4. Dé clic en **OK**.



Encriptar mensajes salientes con base en la IP destino
Si desea utilizar una llave de encripción específica para encriptar todos los mensajes destinados a cierta dirección IP, habilite esta opción y dé clic en Configurar para abrir el archivo de Encripción de Transporte de Mensajes de MDaemon, en el que puede enlistar las direcciones IP y llaves ID asociadas. Cualquier sesión SMTP saliente para entregar un mensaje a una de las IPs enlistadas encriptará el mensaje utilizando la llave asociada, justo antes de la transmisión. Si el mensaje ya fue encriptado por alguna otra llave, este paso se omitirá.

Importar llaves
Si desea importar manualmente una llave hacia MDPGP, dé clic en este botón, localice el archivo de la llave y dé clic en **Abrir**. Al importar el archivo de una llave privada, no necesita importar la llave pública correspondiente ya que está incluida en la llave privada. Si está importando una llave privada protegida con contraseña entonces MDPGP le solicitará capturar la contraseña. Sin ésta, no podrá importar la llave privada. Luego de importar la llave privada, MDaemon modificará la contraseña de esa llave a cualquiera contraseña que MDPGP esté utilizando.

Importar llave de Dominio
Si le han proporcionado una llave de encripción para encriptar todos los mensajes que se envían a cierto dominio, dé clic en este botón, registre el nombre de dominio, dé clic en **OK** y luego navegue al archivo del dominio `public.asc` y dé clic en **Abrir**. Esto agregará la llave pública del Dominio a la lista y creará una regla en el Filtro de Contenido para encriptar todos los mensajes salientes para ese dominio, sin importar el remitente.

Modificar contraseña
Las llaves privadas se encuentran protegidas en todo momento por una contraseña. Al intentar importar una llave privada, de registrar su contraseña. Al exportar una llave privada, esa llave exportada estará protegida con la contraseña y no podrá ser utilizada o importada en ningún otro lugar, sin ella. La contraseña por omisión de MDPGP es **MDaemon**. Por razones de seguridad deberá modificarla cuando empiece a utilizar MDPGP, porque hasta que lo haga, cada llave creada o importada exitosamente por MDPGP tendrá configurada o modificará su contraseña a **MDaemon**. Puede modificar la contraseña en cualquier momento dando clic en **Modificar contraseña** en la pantalla MDPGP. Cuando modifique la contraseña, cada llave privada en el llavero se actualizará a esta nueva contraseña.

Respaldar archivos de datos
Dé clic en este botón para respaldar sus llaveros actuales `Keyring.private` y `Keyring.public`. Por omisión los archivos de respaldo se copiarán a: "`\MDaemon\Pem\_mdpgp\backups`" y contendrán la fecha y la extensión `.bak` incorporada en los nombres de archivo.

- Los mensajes reenviados no se encriptan.
- Los mensajes de Autorespuestas no se encriptan.
- No se soportan servidores de Llave o revocación de Llaves, excepto como se describen las opciones descritas arriba "*Recolectar llaves públicas de DNS (pka1) y poner en caché durante [xx] horas*" y "*Enviar llaves públicas sobre HTTP (Webmail)*"
- La acción de encriptar en el Filtro de Contenido no funciona sobre mensajes previamente encriptados y las acciones encriptar y desencriptar están sujetas a todos los requerimientos de la configuración MDPGP.
- Las listas desplegables que despliegan las cuentas de MDaemon muestran las primeras 500 cuentas por omisión. Puede configurar `MaxUsersShown=0` en `plugins.dat` para visualizar todas las cuentas. Esto puede tardar más en cargar cuando sean muchas cuentas.
- `MDPGPUtil.exe` es una herramienta que puede encriptar y desencriptar vía opciones de línea de comando. Corra MDPGPUtil sin argumentos desde la línea de comando para obtener ayuda.

4.5 Outbreak Protection

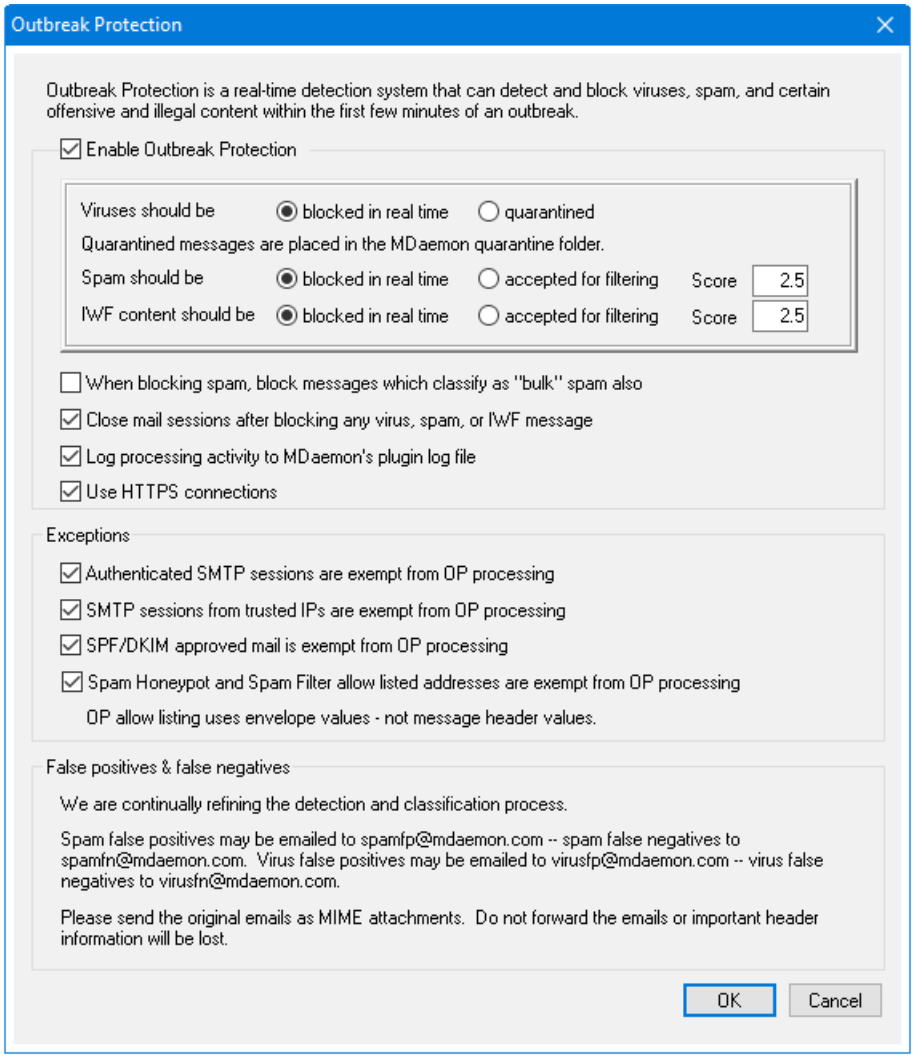
Outbreak Protection es parte de la funcionalidad opcional MDaemon AntiVirus[668]. Al habilitar MDaemon AntiVirus por primera vez, se habilitará un periodo de prueba de 30 días. Si desea adquirir esta funcionalidad, contacte a su distribuidor autorizado de MDaemon o visite: www.mdaemon.com.

Outbreak Protection (OP) es accesible desde el menú Seguridad de MDaemon (Seguridad » Outbreak Protection..., o Ctrl+Shift+1). Es una tecnología revolucionaria antispam, antivirus y antiphishing, capaz de proteger proactivamente la infraestructura de correo de MDaemon, en automático y en minutos después de la dispersión.

Outbreak Protection es completamente agnóstico a contenido, lo cual significa que no se basa en análisis estrictamente léxico del contenido del mensaje. Así pues, no requiere reglas heurísticas, filtro de contenido o actualizaciones de firma. Además, eso significa que no puede ser engañado por textos semilla, cambios inteligentes de deletreo, tácticas de ingeniería social, barreras de lenguaje, o diferencias en las técnicas de codificación. En lugar de esto, OP se basa en las tecnologías de Detección de Patrones Recurrentes y de Zero-hour. Se basa en análisis matemático de la estructura del mensaje y distribución de éste a través de SMTP—analiza "patrones" asociados con una transmisión de correo y los compara a patrones similares recopilados de millones de correo alrededor del mundo, que se usan como muestra y comparación en tiempo real. **Nota:** OP nunca transmite el contenido de los mensajes ni puede derivar el contenido del mensaje con base en los patrones extraídos.

Dado que los mensajes se analizan a nivel mundial en tiempo real, la protección se provee en minutos—incluso segundo—de un nuevo brote. Para virus, el nivel de protección es crítico ya que normalmente pasan diversas horas después de un brote antes de que los proveedores tradicionales de antivirus puedan verificar y enviar una actualización de firma de virus, y puede pasar todavía más tiempo antes de que dicha actualización se ponga en producción. Durante dicho intervalo, los servidores sin Outbreak Protection son vulnerables a ese brote en particular. De manera similar, los mensajes de Spam normalmente requieren tiempo y esfuerzo para ser analizados y crear un filtro seguro antes de que puedan ser reconocidos por los sistemas tradicionales de heurística y sistemas basados en contenido.

Es importante mencionar, sin embargo, que la funcionalidad Outbreak Protection no es un reemplazo de antivirus, antispam y técnicas antiphishing tradicionales. De hecho, OP provee otra capa especializada de protección por encima de las ya existentes de heurística, firmas, y herramientas basadas en contenido que se encuentran en MDaemon. Específicamente, OP está diseñado para lidiar con brotes a gran escala y no para mensajes antiguos, únicos u orientados específicamente que pueden ser captados más fácilmente por las herramientas tradicionales.



Outbreak Protection

Habilitar Outbreak Protection

Haga clic en esta casilla para habilitar la protección Outbreak Protection en su servidor. Los mensajes entrantes se analizarán para ver si forman parte de un brote actual de virus, Spam o phishing. El resto de las opciones de este diálogo se usan para determinar qué se hará con los mensajes que se determinen como parte de un brote y para designar a los remitentes que estarán exentos del procesamiento OP.

Los virus deberían ser...

bloqueados en tiempo real

Seleccione esta opción si desea bloquear los mensajes durante el proceso SMTP cuando se determinan como una parte de un brote de virus. Estos mensajes no se pondrán en cuarentena ni serán enviados a sus destinatarios—serán rechazados por el servidor.

cuarentena

Seleccione esta opción si desea aceptar mensajes que OP determine como parte de un brote de virus. Aunque estos mensajes no serán rechazados por el servidor, serán puestos en cuarentena en lugar de ser enviados a sus

destinatarios. Los mensajes en cuarentena se colocan en la carpeta cuarentena.

El Spam deberá ser...

bloqueado en tiempo real
Seleccione esta opción si desea bloquear mensajes durante el proceso SMTP cuando OP confirme que son parte de un brote de Spam. Estos mensajes no serán marcados como Spam y enviados a sus destinatarios—serán rechazados por el servidor. Los mensajes clasificados por OP como correo "bulk" (masivo) puede que no sean bloqueado por esta opción a menos que active la siguiente opción de *Al bloquear el Spam, los mensajes bloqueados se clasifican como Spam "bloque" también.* Los mensajes clasificados como "bulk" por OP podrían ser simplemente parte de algunas listas de distribución muy grandes o de contenido distribuido de maneras similares, así que puede considerar o no dichos mensajes como Spam. Por dicha razón, este tipo de mensajes generalmente no se deberían puntuar negativamente o ser bloqueados por OP.

aceptado por el filtrado
Seleccione esta opción si desea aceptar mensajes que OP confirme como parte de un brote de Spam, para que puedan estar sujetos al filtrado de Spam y al procesamiento del filtro de contenido. Estos mensajes no serán bloqueados por OP, pero tendrán sus puntuaciones de Filtro de Spam ajustadas de acuerdo con la opción *Puntuación* siguiente.

Cuando use la opción *aceptado por el filtrado,* OP no hará que un correo confirmado como mensaje de Spam sea bloqueado, pero el correo podrá seguir siendo bloqueado por MDaemon durante el proceso SMTP si ha configurado el Filtro de Spam para usar la opción *SMTP rechaza mensajes con puntuación mayor o igual a [xx]*, ubicada en la pantalla del Filtro de Spam 676.

Por ejemplo, si la siguiente opción de puntuación hiciera que la puntuación del Filtro de Spam fuera 15.0, entonces el mensaje se seguiría rechazando como Spam si también tiene la opción del filtro de Spam *"SMTP rechaza..."* para rechazar mensajes que tengan una puntuación de 15.0 o superior.

Puntuación
Cuando use la opción anterior de *aceptados por el filtrado*, esta será la cantidad que se añadirá a la puntuación del Filtro de Spam cuando OP confirme que el mensaje es parte de un brote de Spam.

Contenido IWF

La siguiente opción aplica a contenido identificado por la Internet Watch Foundation (IWF) como referentes de sitios con abusos a menores (p. ej. sitios de pornografía infantil). Habilita en OP el uso de una lista de URL integradas provista por la IWF para detectar y marcar mensajes que refieran a dicho contenido. La IWF opera un "soporte" independiente de Internet para reportar contenido en línea potencialmente ilegal, incluyendo contenido de abuso a menores ubicado en cualquier parte del mundo. Trabajan en conjunto con la policía, gobiernos, la mayor parte de la industria en línea, y el público para

combatir la disponibilidad de contenido ilegal en línea. La lista URL de la Fundación se actualiza diariamente con nuevos sitios que contienen imágenes de abuso a menores.

Muchas organizaciones tienen reglas internas que gobiernan el contenido del correo enviado o recibido por sus empleados, especialmente con respecto a material obsceno o ilegal. Adicionalmente, muchos países han considerado ilegal el envío y recepción de dicho contenido. Esta funcionalidad puede ayudarle en sus esfuerzos por asegurar los correctos cumplimientos.

Para más acerca de la IWF, ver:

http://www.iwf.org.uk/

El contenido IWF debería ser...

bloqueado en tiempo real
Escoja esta opción si desea rechazar mensajes entrantes durante el proceso SMTP cuando tengan contenido IWF restringido.

aceptado por el filtrado
Escoja esta opción si desea incrementar la puntuación del Filtro de Spam en lugar de rechazarla cuando tiene contenido IWF restringido. La puntuación del Filtro de Spam se incrementará la cantidad especificada en la opción *Puntuación* siguiente.

Puntuación
Cuando se selecciona la opción anterior de *aceptado por el filtrado,* esta es la cantidad que se añadirá a la puntuación del Filtro de Spam cuando tenga contenido restringido por IWF.

Al bloquear el Spam, los mensajes bloqueados se clasifican como Spam "bloque" también
Algunas veces OP identificará ciertos mensajes que podrían ser considerados Spam, pero que no están siendo enviados desde un spammer o robot conocido—como sucede a veces con los correos masivos de lista y los newsletter. OP clasifica este tipo de mensajes como "*Spam (bulk)*" en lugar de *"Spam (confirmed)*". Haga clic en esta casilla si desea aplicar las funcionalidades de bloqueo de spam de OP también al correo "*Spam (bulk)*". Si esta opción se deshabilita, sólo los mensajes clasificados como "*Spam (confirmed)*" se verán afectados por las funcionalidades de bloqueo de spam de OP anteriores. Aceptar este tipo de spam para procesamiento posterior puede que sea necesario para los sitios que quieran recibir mensajes masivos de lista de correo, pero por alguna razón no pueden exentar el recurso o destinatario.

Actividad del procesamiento del registro al archivo de registros del complemento de MDaemon

Excepciones

Las sesiones SMTP autenticadas están excluidas del procesamiento de OP
Cuando esta opción está activada, las sesiones SMTP autenticadas están exentas del procesamiento OP. Esto significa que los mensajes enviados durante dicha sesión so estarán sujetos a las comprobaciones de Outbreak Protection.

Las sesiones SMTP de las IPs de confianza están excluidas del procesamiento de OP
Active esta opción si desea que las direcciones IP de confianza estén exentas de Outbreak Protection—los mensajes que llegan de un servidor de una dirección IP de confianza no están sujetos a las comprobaciones OP.

Los mensajes aprobados por SPF/DKIM están exentos de procesamiento OP
Haga clic en esta casilla si desea hacer exento del proceso OP a un mensaje cuando el dominio remitente aparezca en la Lista Aprobada[558] y esté validado por SPF o DKIM.

Las direcciones en lista de permitidos para los Honeypots de Spam y el Filtro de Spam están exentas de procesamiento OP
Habilite esta opción si desea incluir los Honeypots de Spam[707] y el Filtro de Spam en listas de permitidos de OP. La lista de permitidos aplica al destinatario o valor RCPT dado durante la sesión SMTP. La "Lista de Permitidos (De)" aplica al remitente o valor MAIL dado durante la sesión SMTP. Estas operaciones no se basan en los valores del encabezado del mensaje.

Falsos Positivos y Falsos Negativos

Los falsos positivos, o clasificar un correo legítimo incorrectamente como parte de un brote, debería suceder raramente si llegara a suceder. Si ocurriera un falso positivo, de todos modos, puede mandar dicho mensaje a **spamfp@mdaemon.com** para falsos positivos de Spam/phishing o a **virusfp@mdaemon.com** para falsos positivos de virus, para que lo podamos usar para refinar y mejorar nuestra detección y procesos de clasificación.

Los falsos negativos, o la clasificación de un mensaje como no parte de un brote, aunque siga siendo Spam o un ataque, sucederá con mayor frecuencia que los falsos positivos. Sin embargo, se debe destacar que OP no está diseñado para capturar todos los ataques de Spam, virus y similares—es simplemente una capa más de protección que se orienta específicamente a brotes. Los mensajes antiguos, específicamente orientados y similares, que no son parte de un brote en curso, pueden pasar la validación de OP. Este tipo de mensajes deberían ser capturados por las otras funcionalidades de Antivirus de MDaemon más adelante en la cadena de procesamiento. Si ocurriera un falso negativo, aun así, puede enviarnos el mensaje a **spamfn@mdaemon.com** para falsos negativos de Spam/phishing o a **virusfn@mdaemon.com** para falsos negativos de virus, para que podamos usarlo para refinar y mejorar los procesos de detección y clasificación.

Cuando nos envíe mensaje erróneamente clasificados, el mensaje original deberá ser enviado como adjunto MIME en lugar de reenviado. De no ser así, las cabeceras y otra información crítica para el proceso de clasificación se perderán.

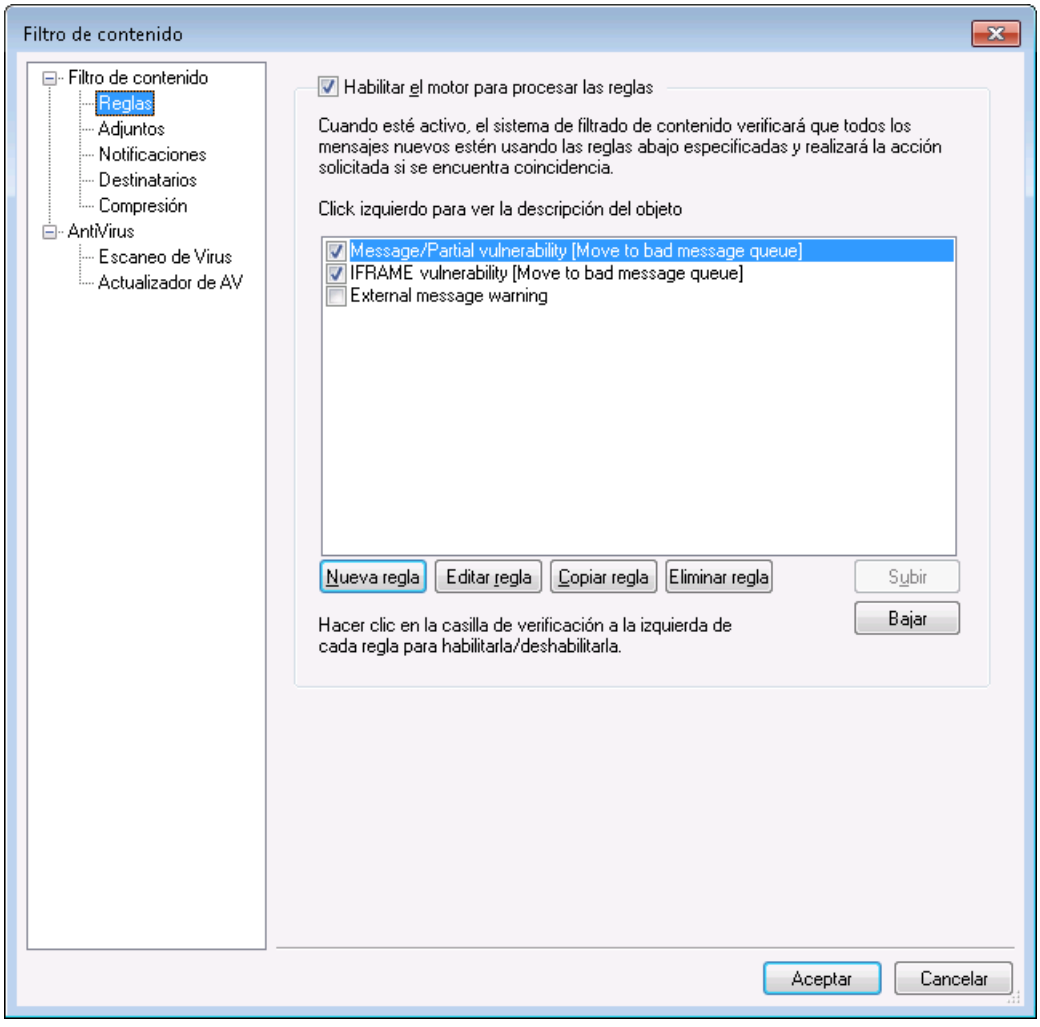
4.6 Filtro de Contenido y AntiVirus

Filtro de Contenido

El Filtro de Contenido 645 (Seguridad » Filtro de Contenido) se puede usar para un gran número de funciones, tal como: prevenir el correo Spam, interceptar mensajes que contengan virus antes de que lleguen a su destino final, copiar algunos correos a uno o más usuarios adicionales, añadir una nota o aviso al final de los mensajes, añadir y borrar encabezados, quitar adjuntos de mensajes, eliminar mensajes, y más. Dado que las reglas individuales de Filtro de Contenido son creadas por el administrador, y dado a su diversidad, pueden ser usadas en muchas situaciones y están en su mayor parte limitadas únicamente por la creatividad de la persona que las esté creando. Con un poco de observación y experimentación, esta funcionalidad puede ser muy útil.

4.6.1 Editor del Filtro de Contenido

4.6.1.1 Reglas



Todos los mensajes procesados por MDaemon residirán, en algún punto, temporalmente en una de las colas de mensajes. Cuando el Filtro de Contenido está habilitado, antes de que a un mensaje se le permita dejar la cola, éste será

procesado a través de las reglas del Filtro de Contenido. El resultado de este procedimiento determinará lo que se hace con el mensaje.

Los mensajes con un nombre de archivo que empiece con la letra "P" serán ignorados por el proceso de filtro de contenido. El resto de los mensajes serán procesados por el sistema de filtro de contenido. Una vez procesado, MDaemon cambiará el primer carácter del nombre del archivo a "P". De esta manera un mensaje sólo puede ser procesado por el sistema de filtro de contenido una vez.

Reglas de Filtro de Contenido

Habilitar el motor para procesar las reglas
Haga clic en esta casilla para habilitar el filtro de contenido. Todos los mensajes procesados por MDaemon serán filtrados a través de las reglas de filtro de contenido antes de ser enviados.

Reglas Existentes del Filtro de Contenido

Este cuadro lista todas las reglas de Filtro de Contenido, con una casilla de verificación cada una para que pueda habilitarlas/deshabilitarlas a voluntad. Para ver una descripción de cualquier regla en su formato interno de script, haga clic en la regla y pose su cursor encima (si mueve el cursor desaparecerá la descripción). Siempre que un mensaje se procesa a través del filtro de contenido, estas reglas se aplicarán en el orden en que se lista. Esto hace posible que ordene las reglas para conseguir un mayor nivel de versatilidad.

Por ejemplo: Si tiene una regla que borra los mensajes que contengan las palabras "Esto es Spam" y una regla similar que envíe dichos mensajes al Postmaster, entonces poniéndolas en el orden correcto hará que ambas reglas puedan aplicarse al mensaje. Esto asume que no existe una regla de "Parar de procesar reglas" que se aplique al mensaje y esté más arriba en la lista. Si fuera así, entonces puede usar los botones *Subir/Bajar* para mover la regla de "Paro" después de las otras dos. Después, cualquier mensaje que contenga "Esto es Spam" se copiaría al Postmaster y después sería borrada.

MDaemon tiene la capacidad de crear reglas que ejecutarán múltiples tareas y utilizan la lógica `and/or`. Considerando el ejemplo anteriormente citado, en lugar de utilizar múltiples reglas puede crear una única regla que cumpla con todas las tareas y más.

Nueva regla
Haga clic en este botón para crear una nueva regla de filtro de contenido. Esto abrirá el diálogo de Crear Regla 648.

Editar regla
Haga clic en este botón para abrir la regla seleccionada en el editor de Modificar Regla 653.

Copiar regla
Haga clic en este botón para clonar la regla de filtro de contenido seleccionada. Una regla idéntica se creará y se añadirá a la lista. La nueva regla se nombrará por defecto "Copy of [Nombre de la Regla Original]". Esto es útil si desea crear múltiples reglas similares. Puede crear una única regla, clonarla diversas veces, y luego modificar las copias según se necesite.

Eliminar regla
Haga clic en este botón para borrar la regla de filtro de contenido seleccionada. Se le pedirá que confirme su decisión de borrar la regla antes de que MDaemon lo haga.

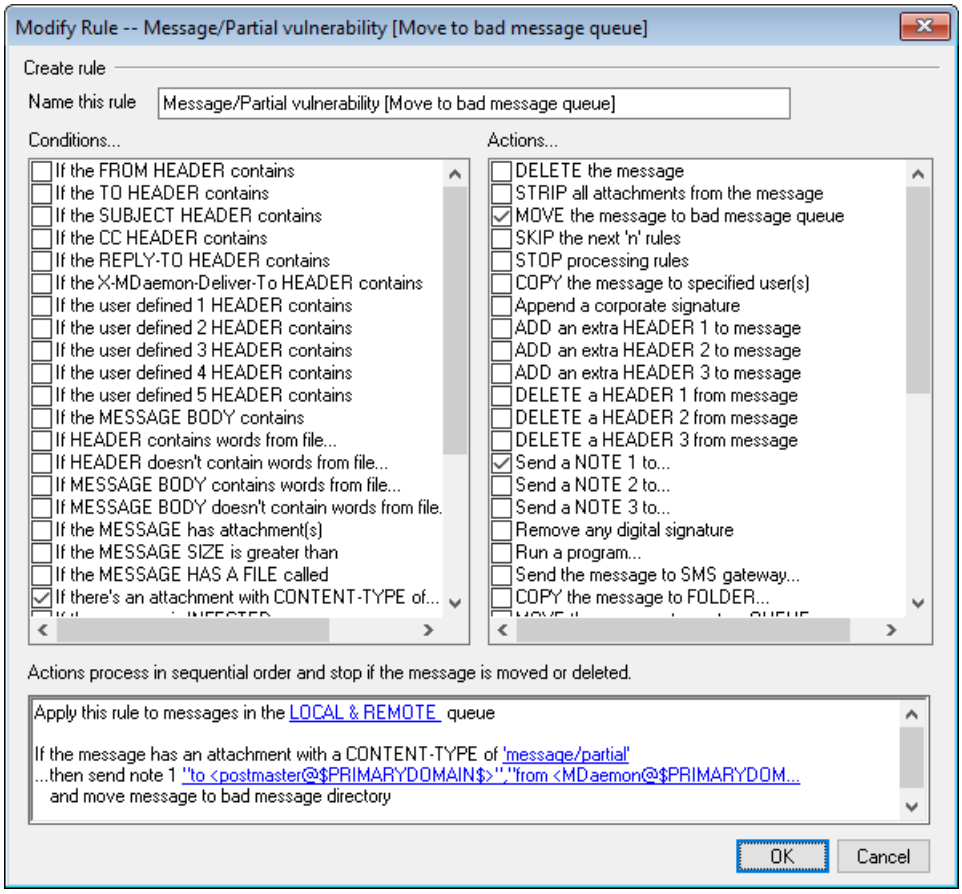
Subir
Haga clic en este botón para mover la regla seleccionada hacia arriba.

Bajar
Haga clic en este botón para mover la regla seleccionada hacia abajo.

Ver:

Crear una Nueva Regla de Filtro de Contenido 648
Modificar una Regla Existente de Filtro de Contenido 653
Usar Expresiones Regulares en sus Reglas de Filtro 653

4.6.1.1.1 Crear una Nueva Regla de Filtro de Contenido



Este diálogo se usa para crear nuevas Reglas de Filtro de Contenido. Se puede llegar a él haciendo clic en el botón *Nueva Regla* en el diálogo de Filtro de Contenido.

Crear Regla

Nombre esta regla
Teclee un nombre descriptivo para su nueva regla aquí. Por defecto se llamará "New Rule #n".

Condiciones...

Este cuadro lista las condiciones que se pueden aplicar a la nueva regla. Haga clic en la casilla correspondiente a cualquier condición que quiera aplicar a la nueva regla. Cada condición habilitada aparecerá en el cuadro de Descripción de la Regla a continuación. La mayoría de las Condiciones requieren información adicional que puede especificar haciendo clic en el enlace de Condiciones en el cuadro de Descripción de la Regla.

`If the [HEADER] contains`—Haga clic en cualquiera de estas opciones para basar su regla en el contenido de dichas cabeceras de mensaje particulares. Debe especificar el texto que desea escanear. Esta condición soporta ahora expresiones regulares. Vea Usar Expresiones Regulares en sus Reglas de Filtro 653.

`If the user defined [# HEADER] contains`—Haga clic en una o más de estas opciones para basar la regla en cabeceras de mensaje definidas por usted.

Debe especificar una nueva cabecera, y un texto para el que escanear. Esta condición ahora soporta expresiones regulares. Vea Usar Expresiones Regulares en sus Reglas de Filtro 653.

If the MESSAGE BODY contains—Esta opción hace que el contenido del cuerpo del mensaje sea una de las condiciones. Esta condición requiere que se especifique una cadena de texto a buscar. Esta condiciona ahora soporta expresiones regulares. Vea Usar Expresiones Regulares en sus Reglas de Filtro 653.

If the MESSAGE has Attachment(s)—Cuando esta opción se selecciona, la regla vigilará la presencia de uno o más Adjuntos de Mensaje. No se requiere información adicional.

If the MESSAGE SIZE is greater than—Haga clic en esta opción si quiere que la nueva regla se base en el tamaño del mensaje. El tamaño debe ser especificado en KB. Por defecto son 10 KB.

If the MESSAGE HAS A FILE called—Esta opción escaneará los adjuntos de mensaje con un nombre concreto. Debe especificar el nombre del archivo. Los comodines como *.exe y archivo*.* están permitidos.

If message is INFECTED...—Esta condición es VERDADERA cuando MDaemon determina que un mensaje está infectado con virus.

If the EXIT CODE from a previous run process is equal to—Si una regla previa de su lista utiliza la acción *Run Process,* puede usar esta condición para buscar códigos de salida específicos de dicho proceso.

If the MESSAGE IS DIGITALLY SIGNED—La condición se aplica a los mensajes que han sido firmados digitalmente. No se requiere información adicional para esta condición.

If SENDER is a member of GROUP...—Esta condición aplica a un mensaje cuando se envía por una cuenta que es miembro del Grupo de cuentas designado en la regla.

If RECIPIENT is a member of GROUP...—Esta condición aplica a un mensaje cuando su recipiente es un miembro del Grupo de cuentas designado en la regla.

If ALL MESSAGES—Haga clic en esta opción si quiere que la regla se aplique a todos los mensajes. No se requiere más información; esta regla afectará a todos los mensajes excepto aquellos con una acción de "Dejar de procesar reglas" o "Eliminar mensaje" aplicada en una regla anterior.

Acciones...

MDaemon puede ejecutar estas acciones si un mensaje concuerda con las condiciones de la regla. Unas cuantas acciones requerirán información adicional que se especificará haciendo clic en el enlace de Acción en el cuadro de Descripción de la Regla.

Delete Message—Seleccione esta acción para hacer que el mensaje se elimine.

Strip All Attachments From Message—Esta acción hace que todos los adjuntos se quiten del mensaje.

Move Message To Bad Message Queue—Haga clic en esta acción para hacer que el mensaje sea movido al directorio de mensajes erróneos. Se agregará un encabezado `X-MDBadQueue-Reason` al mensaje.

Skip n Rules—Seleccionar esta acción hará que un número específico de reglas no se ejecute. Esto es útil en situaciones donde puede que quiera que se aplique una regla en ciertas circunstancias pero no en otras.

Por ejemplo: puede querer eliminar mensajes que contengan la palabra "Spam", pero no aquellos que contengan "Spam bueno". Para conseguir eso puede crear una regla que elimine los mensajes que contengan la palabra "Spam" y luego crear encima de ésta otra regla que diga "si el mensaje contiene "Spam bueno" entonces saltar 1 Regla".

Stop Processing Rules—Esta acción se saltará todas las reglas siguientes.

Copy Message To Specified User(s)—Hace que se envíe un mensaje a uno o más recipientes. Puede especificar qué recipientes van a recibir el mensaje.

Append a corporate signature—Esta acción hace posible crear una pequeña cantidad de texto que se agregará como pie al mensaje. Alternativamente, puede añadir los contenidos de un archivo de texto. Se tiene disponible una casilla de verificación para *Utilizar HTML* si desea incluir código HTML en el texto de su firma. Esta Acción soporta las macros de firmas[143] `$CONTACT...$`.

Por ejemplo: puede utilizar esta regla para incluir una frase que diga "Este correo es originado por mi empresa, por favor dirija cualquier queja o cuestión a usuario1@ejemplo.com".

Add Extra Header Item To Message—Esta acción añadirá una cabecera adicional al mensaje. Debe especificar el nombre de la nueva cabecera y su valor.

Delete A Header Item From Message—Esta acción quitará una cabecera del mensaje. Debe especificar la cabecera que desee eliminar.

Send Note To... —Esta acción enviará un correo a una dirección concreta. Podrá especificar el remitente, destinatario, asunto, y una pequeña cantidad de texto. También puede configurar esta acción para adjuntar el mensaje original a la nota. **Nota:** Esta acción omite todos los mensajes que no cuentan con return-path. Por esto no puede ser detonada, por ejemplo, por mensajes DSN (Delivery Status Notification).

Por ejemplo: puede que desee crear una regla que mueva todos los mensajes que contengan "Esto es spam" al directorio de mensajes erróneos y otra regla que envíe una nota a alguien dejándoles saber que se ha realizado dicha acción.

Remove Digital Signature—Haga clic en esta acción para hacer que una firma digital sea eliminada del mensaje.

Run Process...—Esta acción se puede usar para ejecutar un programa concreto cuando un mensaje cumple con las condiciones de la regla. Debe especificar la ruta al programa que desea ejecutar. Puede utilizar la macro $MESSAGEFILENAME$ para pasar el nombre del mensaje al proceso, y puede especificar si MDaemon debe o no suspender temporalmente sus operaciones o de manera indefinida mientras espera que el proceso termine. Además, puede forzar que el proceso cierre y/o se ejecute en una ventana oculta.

Send Message Through SMS Gateway Server...—Haga clic en esta opción para enviar el mensaje a través de un servidor Gateway de SMS. Debe proveer de un host o dirección IP y del número de teléfono SMS.

Copy Message to Folder...—Use esta opción para colocar una copia del mensaje en una carpeta específica.

MOVE the messages to custom QUEUE...—Use esta acción para mover el mensaje en una o más previamente creadas colas de mensaje. Cuando se muevan mensajes a las colas remotas personalizadas, puede utilizar la programación personalizada del Programador de Eventos para controlar cuándo se procesarán dichos mensajes.

Add Line To Text File—Esta opción provoca que se agregue una línea de texto específica a un archivo. Cuando escoja esta acción deberá especificar la ruta al archivo y el texto que quiere le sea añadido. Puede utilizar algunas macros de MDaemon en el texto que hagan que el Filtro de Contenido añada dinámicamente información sobre el mensaje tal como el remitente, destinatario, ID de mensaje, y demás. Haga clic en el botón Macros en el diálogo "Add line to text file" para mostrar una lista de las macros permitidas.

[Copy|Move] Message to Public Folders...—Use esta acción para hacer que el mensaje se mueva a una o más Carpetas Públicas.

Search and Replace Words in a Header—Use esta opción para escanear encabezados específicos en busca de ciertas palabras y luego eliminarlas o reemplazarlas. Cuando se cree esta regla, haga clic en el enlace "especificar información" en la Descripción de la Regla para abrir el diálogo "Encabezado - Buscar y Reemplazar" en el que puede designar el encabezado y las palabras a reemplazar o eliminar. Esta acción ahora soporta expresiones regulares. Vea Usar Expresiones Regulares en sus Reglas de Filtro. 653

Search and Replace Words in the Message Body—use esta opción para escanear el cuerpo del mensaje y reemplazarlo por el texto deseado. Esta acción ahora soporta expresiones regulares. Vea Usar Expresiones Regulares en sus Reglas de Filtro. 653

Jump to Rule...—Use esta acción para saltar inmediatamente a una regla posterior en la lista, saltándose todas las reglas entre las dos..

Send an instant message...—Esta acción envía un mensaje instantáneo a alguien cuando un mensaje coincide con los criterios de la regla. Se especificará el campo **To:** dirección de correo, el **From:** dirección y el contenido del mensaje.

Add to Windows Event Log...—Utilice esta acción para agregar una cadena de texto al archivo de Eventos de Windows. Puede utilizar macros en esa cadena y hay un botón para desplegar las macros permitidas.

Extract attachments to folder...—Utilice esta acción para extraer adjuntos de un mensaje. Especificará la carpeta a la que se copiarán los archivos y puede elegir eliminar el adjunto del mensaje luego de la extracción. También puede establecer condiciones para determinar qué adjuntos serán extraídos, con base en el nombre del archivo, tipo de contenido y tamaño de los adjuntos.

Extract attachments to folder...—Utilice esta acción para extraer adjuntos de un mensaje. Puede especificar la carpeta a la que se copiarán los adjuntos y puede elegir que se elimine el adjunto del mensaje luego de la extracción. También puede establecer condiciones para determinar qué adjuntos serán extraídos, con base en el nombre de archivo, tipo de contenido y tamaño del adjunto.

Change message processing priority...—Esta acción se utiliza para definir la prioridad del procesamiento del mensaje, desde "10 (Urgente)" a "90 (Reintentar". El valor por omisión es "50 (normal)".

Sign with DKIM selector...—Utilice esta acción si quiere que la regla haga que un mensaje contenga una Firma de DKIM[532]. También puede utilizarlo si quiere firmar algunos mensajes utilizando un selector distinto del designado en el diálogo DKIM.**NOTA:** La Autenticación SMTP[523] siempre es requerida cuando se firman mensajes con DKIM.

Flag message for REQUIRETLS...—Indica que el mensaje debe utilizar REQUIRETLS[590].

[Sign|Encrypt|Decrypt] message with the user's [Private|Public] key...—Utilice estas acciones para firmar, encriptar o desencriptar un mensaje utilizando una llave privada o pública. Vea: MDPGP[629] para más información. **Nota**: estas acciones se ejecutarán aun cuando MDPGP esté deshabilitado.

Add a warning to the top of the message...—Utilice esta acción si desea agregar alguna clase de advertencia en la parte superior de un mensaje. Puede introducir una cadena de texto plano o código HTML, marcando la casilla "Utilizar HTML". Alternativamente, puede copiar el texto desde un archivo.

Add an attachment...—Utilice esta acción si desea adjuntar un archivo a un mensaje que coincida los criterios de la regla. El archivo debe estar contenido en la carpeta `./MDaemon/CFilter/Attachments/`.

Extract attachment and add link...—Utilice esta acción si desea extraer adjuntos de mensajes que coinciden con los criterios de la regla y les agrega una liga. Ver: Vinculación de Adjuntos[366].

Descripción de la Regla
Este cuadro muestra el formato interno de script de la nueva regla. Haga clic en cualquiera de las condiciones o acciones de la regla (listadas como hipervínculos) y el editor apropiado se abrirá para especificar cualquier información necesaria.

Ver:

Editor del Filtro de Contenido 645
Modificar una Regla Existente del Filtro de Contenido 653
Usar Expresiones Regulares en sus Reglas de Filtro 653

4.6.1.1.2 Modificar una Regla Existente de Filtro de Contenido

Para modificar una regla existente de filtro de contenido, seleccione la regla y haga clic en el botón *Editar Regla* en el diálogo de Filtro de Contenido. La regla se abrirá para edición en el editor de Modificar Regla. Los controles de este editor son idénticos a los del diálogo Crear Regla. 648

Ver:

Editor de Filtro de Contenido 645
Crear una Nueva Regla de Filtro de Contenido 648
Usar Expresiones Regulares en sus Reglas de Filtro 653

4.6.1.1.3 Usar Expresiones Regulares en sus Reglas de Filtrado

El sistema de Filtro de Contenido soporta las búsquedas por *expresión regular,* que es un sistema versátil que hace posible buscar no solamente cadenas específicas de texto, sino también *patrones*. Las expresiones regulares contienen una mezcla de texto llano y caracteres especiales que indican el tipo de comparación a realizar, y pueden por lo tanto hacer sus reglas de Filtro de Contenido más potentes y mejor orientadas.

¿Qué son las Expresiones Regulares?
Una expresión regular (regexp) es un patrón de texto que consiste en una combinación de caracteres especiales conocidos como *metacaracteres* y caracteres de texto alfanuméricos, o "*literales*" (abc, 123, y demás). El patrón se usa para comparar cadenas de texto—siendo el resultado de la comparación positivo o no. Las regexps se usan primariamente para comparaciones de texto regular y para búsquedas y sustituciones.

Los metacaracteres son caracteres especiales que tienen funciones específicas y usos dentro de expresiones regulares. La implementación regexp dentro del sistema de Filtro de Contenido de MDaemon permite los siguientes metacaracteres:

```
\ | () [] ^ $ * + ? . <>
```

Metacaracter	Descripción

**** Cuando se usa antes de un metacaracter, la barra invertida ("\") hace que el metacaracter se trate como carácter literal. Esto es necesario si quiere que la expresión regular busque uno de los caracteres especiales que se usan como metacaracteres. Por ejemplo, para buscar "+" su expresión debe incluir "\+".

| El carácter *alternación* (también llamado "*o*" o "*barra*") se usa cuando o bien quiere que cualquiera de las expresiones de al lado del carácter concuerden con la cadena objeto. La regexp "abc|zyz" comparará cualquier aparición de "abc" o "xyz" cuando busque una cadena de texto.

[...] Un conjunto de caracteres contenido entre corchetes ("[" y "]") significa que cualquier carácter en el conjunto puede concordar con la cadena de texto buscada. Un guion ("-") entre los caracteres en los corchetes denota un rango de caracteres. Por ejemplo, si busca la cadena "abc" con la regexp "[a-z]" encontrará tres resultados: "*a*", "*b*", y "*c*". Si utiliza la expresión "[az" sólo resultará en una coincidencia: "*a*".

^ Denota el principio de línea. En la cadena de destino "abc ab a" la expresión "^a" devolverá un único resultado —el primer carácter en la cadena objeto. La regexpr "^ab" también devolverá un resultado —los primeros *dos* caracteres en la cadena objeto.

[^...] El carácter ("^") inmediatamente después del corchete izquierdo ("[") tiene un significado distinto. Se usa para excluir los caracteres restantes dentro de los corchetes de coincidir con la cadena objeto. La expresión "[^0-9]" indica que el carácter objeto no debe ser un dígito.

(...) El paréntesis afecta al orden de la evaluación de los patrones, y también sirve como expresión *etiquetada* que se puede usar en expresiones de *búsqueda y reemplazo.*

Los resultados de una búsqueda con una expresión regular se guardan temporalmente y pueden ser usados en la expresión de *reemplazar* para construir una nueva expresión. En la expresión de *reemplazar* puede incluir un carácter "$0" o "\0", que será reemplazado por la sub-cadena encontrada por la expresión regular durante la búsqueda. Así, si la expresión de *búsqueda* "a(bcd)e" encuentra una sub-cadena coincidente, la expresión *reemplazar* de "123-$0-123" reemplazará el texto encontrado con "123-abcde-123".

Similarmente, también puede usar caracteres especiales "$1", "$2", "$3", y demás en la expresión *reemplazar.* Estos caracteres se reemplazarán sólo con los resultados de la expresión *etiquetar* en lugar de una coincidencia de sub-cadena completa. El número siguiente a la barra invertida denota cuál es la expresión etiquetada a la que quiere referenciar (en el caso de una regexp conteniendo más de

una expresión etiquetada). Por ejemplo, si su expresión *encontrar* es "(123)(456)" y su expresión *reemplazar* "a-\2-b-\1" entonces una sub-cadena coincidente se reemplazará con "a-456-b-123" mientras que una expresión *reemplazar* de "a-\0-b" se reemplazará con "a-123456-b"

**$** El símbolo del dólar ("$") denota el final de línea. En la cadena de texto "13 321 123" la expresión "3$" devuelve un resultado—el último carácter en la cadena. La regexp "123$" también devuelve un resultado —los últimos *tres* caracteres en la cadena objeto.

***** El cuantificador asterisco ("*") indica que el carácter a la izquierda debe resultar en *cero o más* ocurrencias del carácter en línea. Así, "1*abc" coincidirá con el texto "111abc" y "abc".

+ Similar al cuantificador asterisco, el cuantificador "+" indica que el carácter a la izquierda debe coincidir con *una o más ocurrencias* del carácter en línea. Así, "1+abc" coincidirá con el texto "111abc" pero no "abc".

? El cuantificador de interrogante ("?") indica que el carácter a su izquierda debe coincidir *una o cero* veces. Así, "1?abc" coincidirá con el texto "abc", y coincidirá con la porción "1abc" de "111abc".

. El metacaracter punto (".") coincidirá con cualquier carácter. Así pues ".+abc" coincidirá con "123456abc", y "a.c" coincidirá con "aac", "abc", "acc", y demás.

Condiciones y Acciones elegibles

Las expresiones regulares se pueden usar en cualquier *Condición* de regla de filtro de *Encabezado*. Por ejemplo, una regla que use la condición "`if the FROM HEADER contains`". Las expresiones regulares también se pueden usar en la condición "`if the MESSAGE BODY contains`".

Las expresiones regulares pueden ser usadas en dos *Acciones* de las reglas de Filtro de Contenido: "`Search and Replace Words in a Header`" y "`Search and Replace Words in the Message Body`."

Las expresiones regulares usadas en las *condiciones* del Filtro de Contenido no son sensibles a mayúsculas. Las mayúsculas no se tomarán en consideración.

La sensibilidad a mayúsculas en expresiones regulares usada en las *acciones* de las reglas del Filtro de Contenido es opcional. Cuando se crea la regexp dentro de la acción de la regla, tendrá la opción de activar/desactivar la sensibilidad a mayúsculas.

Configurar una Regexp en una Condición de Regla

Para configurar una condición de cabecera o cuerpo de mensaje para que use una expresión regular:

1. En el diálogo de Crear Regla, haga clic en la casilla que corresponde a la condición de encabezado o cuerpo de mensaje que desea insertar en su regla.

2. En el área de sumario al final del diálogo de Crear Regla, haga clic en el enlace "**contains specific strings**" que corresponde a la condición que ha seleccionado en el paso 1. Esto abrirá el diálogo de Especificar Texto de búsqueda.

3. Haga clic en el enlace "**contains**" en el área "Cadenas actualmente especificadas...".

4. Escoja "**Matches Regular Expression**" del cuadro de lista desplegable, y haga clic en **Aceptar**.

5. Si necesita ayuda cuando cree su regexp o quiere probarla entonces haga clic en "**Probar expresión regular**". Si no necesita usar el diálogo de Probar Expresión Regular entonces introduzca su regexp en el cuadro de texto proporcionado, haga clic en **Agregar** y luego vaya al paso 8.

6. Escriba su expresión regular en el cuadro de texto "Buscar expresión". Para simplificar el proceso hemos proveído un menú de acceso directo que se puede usar de manera sencilla para insertar los metacaracteres deseados en su regexp. Haga clic en el botón ">" para acceder a este menú. Cuando escoja una opción de este menú, su correspondiente metacaracter será insertado en la expresión y el punto de inserción de texto se moverá al lugar adecuado requerido por el carácter.

7. Teclee cualquier texto que desee usar para probar su expresión en el área de texto proporcionada, y haga clic en **Probar**. Cuando haya acabado de probar su expresión, haga clic en **Aceptar**.

8. Haga clic en **Aceptar**.

9. Continúe creando su regla normalmente.

Configurar una Regexp en una Acción de Regla

Para configurar una acción "Search and Replace Words in…" para que use una expresión regular:

1. En el diálogo Crear Regla, haga clic en la casilla que corresponde a la acción "*Search and Replace Words in...*" que desea insertar en su regla.

2. En el área de sumario al final del diálogo Crear Regla, haga clic en el enlace "**specify information**" que corresponde a la acción seleccionada en el paso 1. Esto abrirá el cuadro de Buscar y Reemplazar.

3. Si escoge la acción "*Search...header*" en el paso 1, entonces utilice la lista desplegable indicada para escoger el encabezado que desea buscar, o escriba un encabezado en el cuadro si el encabezado deseado no está listado. Si no escogió la acción "*Search...header*" en el paso 1, entonces sáltese este paso.

4. Teclee la expresión de *búsqueda* que desea utilizar en esta acción. Para simplificar el proceso hemos proveído un menú de acceso directo que se puede usar de manera sencilla para insertar los metacaracteres deseados en su regexp. Haga clic en el botón ">" para acceder a este menú. Cuando escoja una opción de este menú, su correspondiente metacaracter será insertado en la expresión y el punto de inserción de texto se moverá al lugar adecuado requerido por el carácter.

5. Teclee la expresión de *reemplazar* que desea usar en esta acción. Al igual que en la expresión de *búsqueda* hemos proveído de un menú de acceso directo de metacaracteres para esta opción también. Deje este cuadro en blanco si desea eliminar la sub-cadena coincidente en lugar de reemplazarla con más texto.

6. Haga clic en "**Coincidir con mayúsculas y minúsculas**" si desea que la expresión sea sensible a mayúsculas.

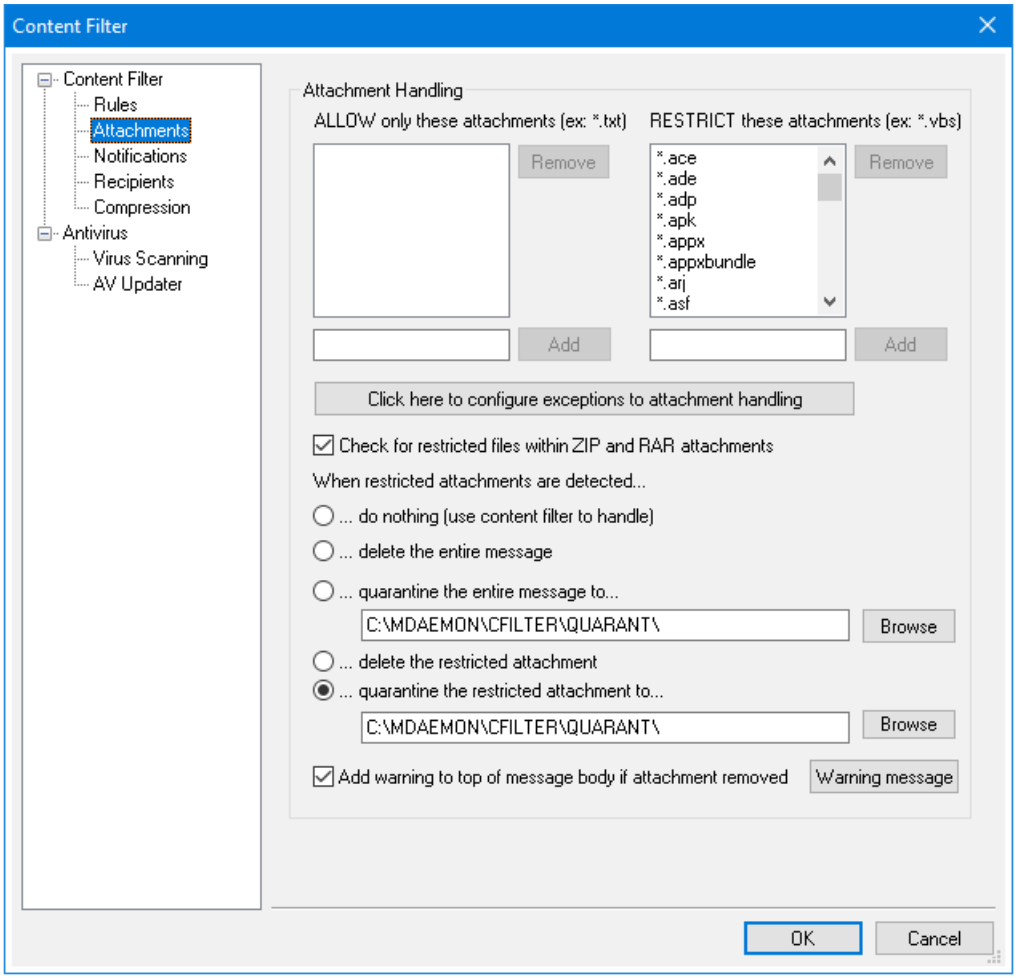
7. Haga clic en Expresión Regular si desea que las cadenas de buscar y reemplazar se traten como expresiones regulares. De otro modo cada una será tratada como una búsqueda y reemplazo simple de sub-cadena—buscará una coincidencia del literal exacto del texto en lugar de procesar la expresión regular.

8. Si no necesita comprobar su expresión puede saltarse este paso. Si necesita comprobar su expresión haga clic en "**Ejecutar prueba**." En el diálogo de comprobación de Buscar y Reemplazar, teclee sus expresiones de buscar y reemplazar y el texto con el que desea probarlas, luego haga clic en **Probar**. Cuando haya acabado de probar sus regexps haga clic en **Aceptar**.

9. Haga clic en **Aceptar**.

10. Continúe creando su regla normalmente.

4.6.1.2 Adjuntos



Utilice esta pestaña para especificar adjuntos que desee clasificar como permitidos o restringidos. Los adjuntos que no estén permitidos serán automáticamente eliminados de los mensajes.

Gestión de Adjuntos

Los nombres de archivo especificados en la lista *RESTRINGIR estos datos adjuntos* serán automáticamente arrancados de sus mensajes cuando MDaemon los localice. Si introduce cualquier tipo de archivo en la lista *PERMITIR sólo estos datos adjuntos,* entonces sólo dichos archivos serán permitidos — todos los demás adjuntos serán arrancados de los mensajes. Después de que un adjunto sea arrancado, MDaemon continuará normalmente y enviará el mensaje sin él. Puede usar las opciones en la pestaña de Notificaciones para provocar que un mensaje de notificación sea enviado a diversas direcciones cuando se encuentro uno de los adjuntos restringidos.

Los comodines están permitidos en las entradas de lista. Una entrada de por ejemplo "`*.exe`", hará que todos los adjuntos terminados en la extensión de archivo `EXE` sean permitidos o eliminados. Para añadir una entrada a cualquiera de las listas, teclee el nombre de archivo en el espacio proporcionado y luego haga clic en Agregar.

Haga clic aquí para configurar excepciones del control de datos adjuntos
Haga clic en este botón para especificar direcciones que desee excluir de la monitorización de restricción de adjuntos. Cuando un mensaje se direccione a

una de dichas direcciones MDaemon permitirá que el mensaje pase, aunque contenga un adjunto restringido.

Buscar archivos restringidos en los adjuntos tipo ZIP y RAR
Haga clic en esta opción si desea escanear los contenidos de archivos en formato comprimido Zip, 7-Zip y RAR para validar si contienen adjuntos restringidos. Adicionalmente, cualquier regla de Filtro de Contenido establecida para buscar un nombre de archivo concreto, será activada si se encuentra un archivo coincidente dentro de un adjunto comprimido.

Cuando se detectan adjuntos restringidos...
Dé clic en la acción deseada a ejecutar cuando un mensaje incluye un adjunto restringido.

...no hacer nada (utilizar el filtro de contenido para manejarlo)
Seleccione esta opción si no desea realizar una acción específica basada en los ajustes de Adjuntos, sino que desea basar las acciones en las Reglas del Filtro de Contenido 645.

...eliminar el mensaje completo
Esta opción eliminará el mensaje completo cuando contiene adjuntos restringidos.

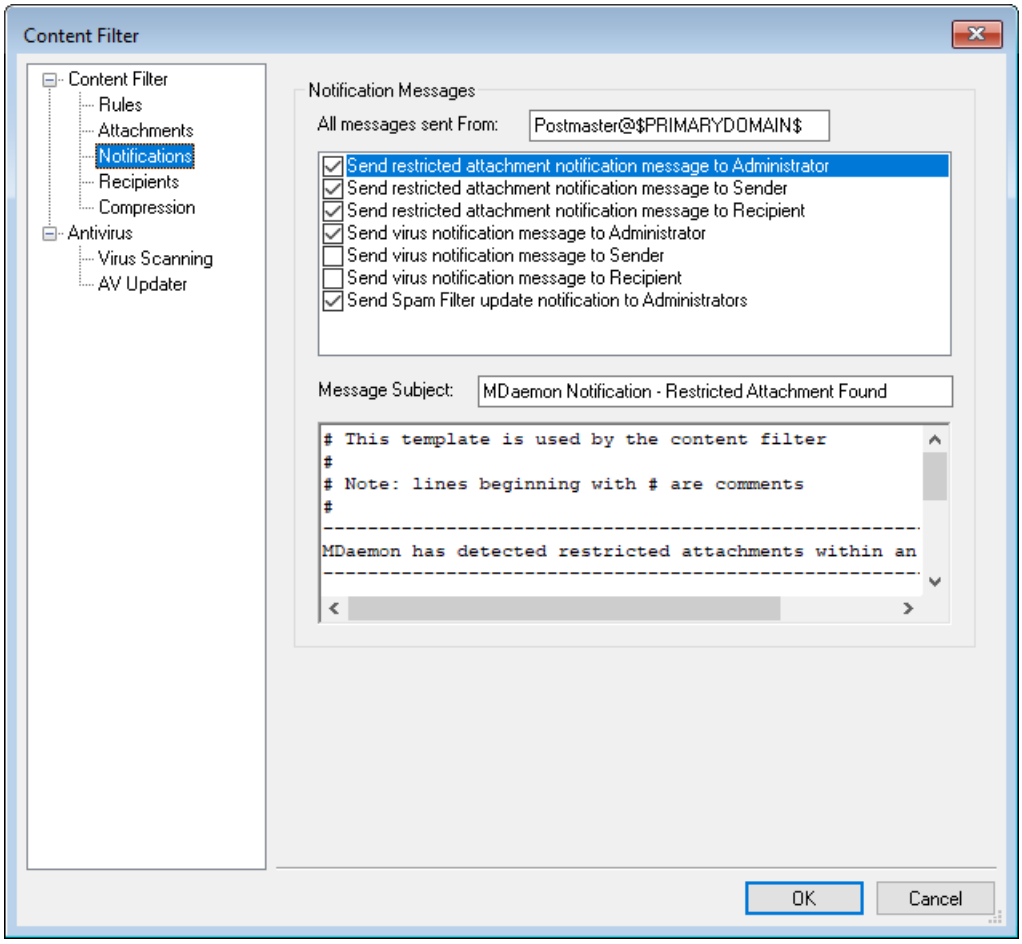
...poner en cuarentena el mensaje en...
Esta opción hará que los mensajes con adjuntos restringidos se pongan en cuarentena en la ubicación especificada.

...eliminar el adjunto restringido
Seleccione esta opción si desea eliminar cualquier adjunto restringido en lugar de eliminar el mensaje completo.

...poner en cuarentena los adjuntos restringidos en:
Haga clic en esta opción y especifique una ubicación si desea colocar los adjuntos restringidos en cuarentena en una ubicación específica en lugar de simplemente eliminarlos. Este es el ajuste por omisión.

Agregar advertencia en la parte superior del cuerpo del mensaje si el adjunto es removido
Cuando MDaemon remueve un adjunto de un mensaje, por ejemplo porque se detectó un virus, agregará un mensaje de advertencia en la parte superior del cuerpo del mensaje. Dé clic en el botón **Aviso** si desea revisar o modificar la plantilla del mensaje. Esta opción está habilitada por omisión.

4.6.1.3 Notificaciones



Use esta pantalla para definir quienes deberán recibir mensajes de notificación cuando se detecte un virus o un adjunto restringido o cuando se actualicen el Antivirus o los archivos del Filtro AntiSpam.

Mensajes de Notificación

Todos los mensajes enviados Desde:
Use este cuadro para especificar la dirección desde la que desea que se envíen los mensajes de notificación.

Enviar notificación de virus al...
Cuando un mensaje llega con un archivo adjunto que contenga virus, un mensaje de aviso se enviará a los individuos designados en esta sección. Un mensaje de aviso personalizado puede ser enviado al remitente, destinatario y a los administradores que haya designado en la pestaña Destinatarios. Para personalizar el mensaje para cualquiera de las tres entradas, seleccione una de ellas de la lista y edite el mensaje que aparece en la mitad inferior de esta pestaña. Cada entrada tiene su propio mensaje, aunque por defecto no es obvio puesto que los tres son idénticos.

Enviar mensaje restringido de notificación de datos adjuntos al...
Cuando llega un mensaje con un adjunto que coincide con una entrada de adjunto restringido (listada en la pestaña Adjuntos), un mensaje de aviso se enviará a los individuos designados en esta sección. Un mensaje de aviso personalizado puede ser enviado al remitente, destinatario y a los administradores que haya designado en la pestaña Destinatarios. Para

personalizar el mensaje para cualquiera de las tres entradas, seleccione una de ellas de la lista y edite el mensaje que aparece en la mitad inferior de esta pestaña. Cada entrada tiene su propio mensaje, aunque por defecto no es obvio puesto que los tres son idénticos.

Enviar a los Administradores notificación de la actualización del Filtro de Spam
Utilice esta opción si desea enviar un mensaje a los administradores siempre que se actualice el Filtro de Spam, conteniendo los resultados de la operación. Esta opción es la misma que "*Enviar mensaje de notificación con los resultados de las actualizaciones*" que se localiza en: Filtro de Spam » Actualizaciones.

Asunto del Mensaje:
Este texto se mostrará en el encabezado "Asunto:" del mensaje de notificación que se envíe.

Mensaje
Este es el mensaje que se enviará a la entrada seleccionada de la lista superior cuando la casilla correspondiente a dicha entrada esté habilitada. Puede editar directamente el mensaje en el cuadro en el que se muestra.

Los archivos reales que contienen este texto se ubican en el directorio `MDaemon\app\`. Son los siguientes:

`cfattrem[adm].dat` - Mensaje de Adjuntos Restringidos – Administradores
`cfattrem[rec].dat` - Mensaje de Adjuntos Restringidos – Destinatario
`cfattrem[snd].dat` - Mensaje de Adjuntos Restringidos – Remitente
`cfvirfnd[adm].dat` - Mensaje de Virus Encontrado – Administradores
`cfvirfnd[rec].dat` - Mensaje de Virus Encontrado – Destinatario
`cfvirfnd[snd].dat` - Mensaje de Virus Encontrado – Remitente

Si desea restaurar uno de estos mensajes a su configuración inicial, simplemente borre el archivo correspondiente y MDaemon lo recreará con sus estados por defecto.

Macros de Mensaje

Para su comodidad, pueden usarse algunas macros en los mensajes de notificación y otros mensajes que genera el Filtro de Contenido. Puede usar cualquiera de las siguientes macros:

`$ACTUALTO$`	Algunos mensajes pueden contener un campo "ActualTo" que generalmente representa el buzón de destino y host tal cual ha sido introducido por el usuario original antes de reformatearse o de realizar una traducción de alias. Esta macro se sustituye con dicho valor.

$AV_VERSION$	Lista la versión de Antivirus actualmente en uso.
$CURRENTTIME$	Esta macro se reemplaza con la hora actual cuando el mensaje está siendo procesado.
$ACTUALFROM$	Algunos mensajes pueden contener un campo "ActualFrom" que generalmente representa el buzón originario y host antes de cualquier reformateo o traducción de alias. Esta macro se sustituye con dicho valor.
$FILTERRULENAME$	Esta macro se sustituye por el nombre de la regla que ha coincidido con el mensaje.
$FROM$	Expande la dirección completa contenida en el encabezado "From:" del mensaje.
$FROMDOMAIN$	Esta macro insertará el nombre de dominio contenido en la dirección en el encabezado "From:" del mensaje (el valor a la derecha de "@" en la dirección de correo.
$FROMMAILBOX$	Enlista la porción del buzón de la dirección, contenido en el encabezado "From:" del mensaje (el valor a la izquierda de "@" en la dirección de correo.
GEN_GUID	Genera un ID único con 11 caracteres alfanuméricos. Ejemplo: 0XVBASADTZC
$HEADER:XX$	Esta macro hará que el valor del encabezado especificado en lugar de "xx" se expanda en el mensaje reformateado. Por ejemplo, si el mensaje original tiene "TO: usuario1@ejemplo.com" entonces la macro $HEADER:TO$ expandirá "usuario1@ejemplo.com". Si el mensaje original tiene "Subject: Este es el asunto" entonces la macro $HEADER:SUBJECT$ se sustituirá con el texto "Este es el asunto"
$HEADER:MESSAGE-ID$	Al igual que con el $HEADER:XX$ anterior, esta macro expande el valor de la cabecera Message-ID.
$LIST_ATTACHMENTS_REMOVED$	Cuando uno o más adjuntos se eliminan del mensaje, esta macro los listará.
$LIST_VIRUSES_FOUND$	Cuando uno o más virus se encuentran en un mensaje, esta macro las listará.
$MESSAGEFILENAME$	Esta macro expande el valor de nombre de archivo del mensaje que está siendo procesado.
$MESSAGEID$	Igual que en $HEADER:MESSAGE-ID$, excepto en que esta macro obvia "<>" del valor del ID de mensaje.
$PRIMARYDOMAIN$	Muestra el nombre del Dominio por Defecto de

	MDaemon definido en el Administrador de Dominios[190].
$PRIMARYIP$	Esta macro expande la dirección IPv4[192] del Dominio por Omisión[190].
$PRIMARYIP6$	Esta macro expande la dirección IPv6[192] de su Dominio por Omisión[190].
$RECIPIENT$	Esta macro resuelve la dirección completa del destinatario del mensaje.
$RECIPIENTDOMAIN$	Esta macro insertará el nombre de dominio para el destinatario del mensaje.
$RECIPIENTMAILBOX$	Muestra el buzón del destinatario (el valor a la izquierda de la "@" en la dirección de correo).
$REPLYTO$	Esta macro se expande con el valor del encabezado "Reply-to".
$SENDER$	Expande la dirección completa desde la que el mensaje ha sido enviado.
$SENDERDOMAIN$	Esta macro insertará el nombre del dominio del remitente del mensaje (el valor a la derecha de la "@" en la dirección de correo).
$SENDERMAILBOX$	Muestra el buzón del remitente (el valor a la izquierda de la "@" en la dirección de correo).
$SUBJECT$	Muestra el texto contenido en el asunto del mensaje.

4.6.1.3.1 Macros de Mensajes

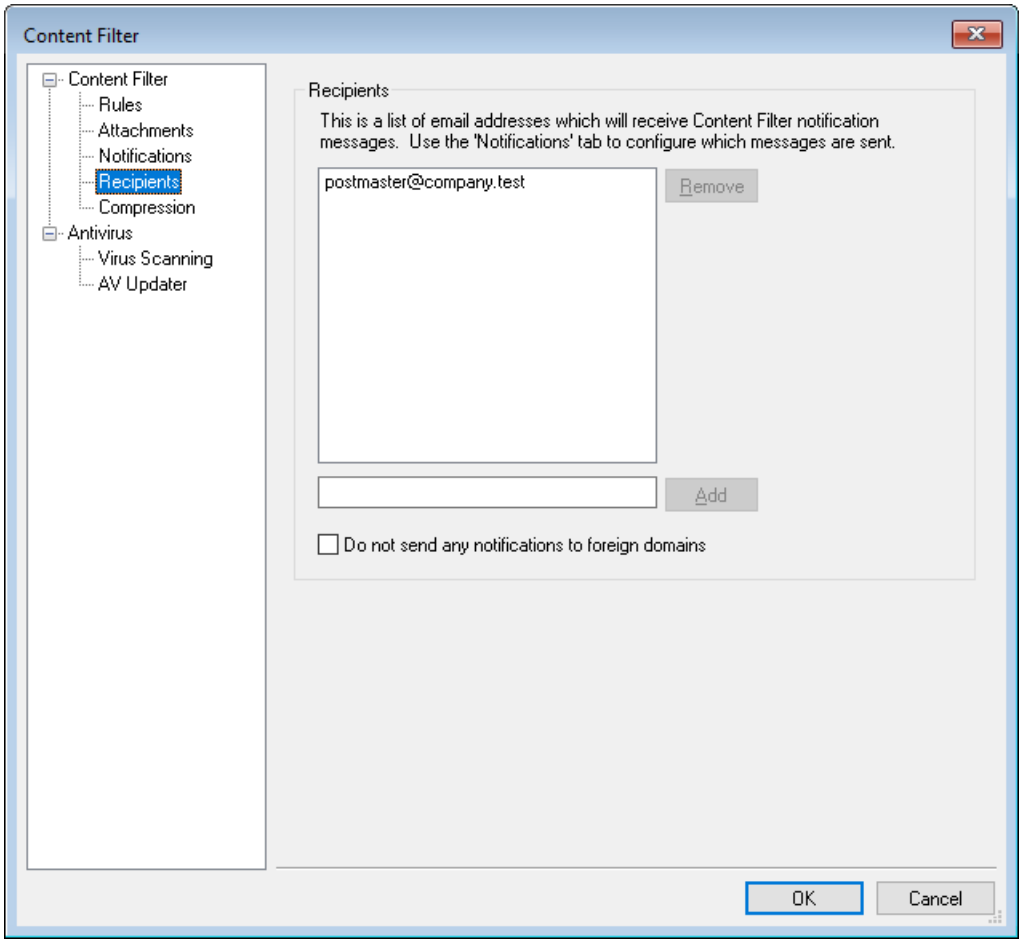
Para su comodidad, pueden usarse algunas macros en los mensajes de notificación y otros mensajes que genera el Filtro de Contenido. Puede usar cualquiera de las siguientes macros:

$ACTUALTO$	Algunos mensajes pueden contener un campo "ActualTo" que generalmente representa el buzón de destino y host tal cual ha sido introducido por el usuario original antes de reformatearse o de realizar una traducción de alias. Esta macro se sustituye con dicho valor.
$AV_VERSION$	Lista la versión de Antivirus actualmente en uso.
$CURRENTTIME$	Esta macro se reemplaza con la hora actual cuando el mensaje está siendo procesado.
$ACTUALFROM$	Algunos mensajes pueden contener un campo "ActualFrom" que generalmente representa el buzón originario y host antes de cualquier

	reformateo o traducción de alias. Esta macro se sustituye con dicho valor.
$FILTERRULENAME$	Esta macro se sustituye por el nombre de la regla que ha coincidido con el mensaje.
$FROM$	Expande la dirección completa contenida en el encabezado "From:" del mensaje.
$FROMDOMAIN$	Esta macro insertará el nombre de dominio contenido en la dirección en el encabezado "From:" del mensaje (el valor a la derecha de "@" en la dirección de correo.
$FROMMAILBOX$	Enlista la porción del buzón de la dirección, contenido en el encabezado "From:" del mensaje (el valor a la izquierda de "@" en la dirección de correo.
GEN_GUID	Genera un ID único con 11 caracteres alfanuméricos. Ejemplo: 0XVBASADTZC
$HEADER:XX$	Esta macro hará que el valor del encabezado especificado en lugar de "xx" se expanda en el mensaje reformateado. Por ejemplo, si el mensaje original tiene "TO: usuario1@ejemplo.com" entonces la macro $HEADER:TO$ expandirá "usuario1@ejemplo.com". Si el mensaje original tiene "Subject: Este es el asunto" entonces la macro $HEADER:SUBJECT$ se sustituirá con el texto "Este es el asunto"
$HEADER:MESSAGE-ID$	Al igual que con el $HEADER:XX$ anterior, esta macro expande el valor de la cabecera Message-ID.
$LIST_ATTACHMENTS_REMOVED$	Cuando uno o más adjuntos se eliminan del mensaje, esta macro los listará.
$LIST_VIRUSES_FOUND$	Cuando uno o más virus se encuentran en un mensaje, esta macro las listará.
$MESSAGEFILENAME$	Esta macro expande el valor de nombre de archivo del mensaje que está siendo procesado.
$MESSAGEID$	Igual que en $HEADER:MESSAGE-ID$, excepto en que esta macro obvia "<>" del valor del ID de mensaje.
$PRIMARYDOMAIN$	Muestra el nombre del Dominio por Defecto de MDaemon definido en el Administrador de Dominios 190.
$PRIMARYIP$	Esta macro expande la dirección IPv4 192 del Dominio por Omisión 190.
$PRIMARYIP6$	Esta macro expande la dirección IPv6 192 de su Dominio por Omisión 190.

$RECIPIENT$	Esta macro resuelve la dirección completa del destinatario del mensaje.
$RECIPIENTDOMAIN$	Esta macro insertará el nombre de dominio para el destinatario del mensaje.
$RECIPIENTMAILBOX$	Muestra el buzón del destinatario (el valor a la izquierda de la "@" en la dirección de correo).
$REPLYTO$	Esta macro se expande con el valor del encabezado "Reply-to".
$SENDER$	Expande la dirección completa desde la que el mensaje ha sido enviado.
$SENDERDOMAIN$	Esta macro insertará el nombre del dominio del remitente del mensaje (el valor a la derecha de la "@" en la dirección de correo).
$SENDERMAILBOX$	Muestra el buzón del remitente (el valor a la izquierda de la "@" en la dirección de correo).
$SUBJECT$	Muestra el texto contenido en el asunto del mensaje.

4.6.1.4 Destinatarios

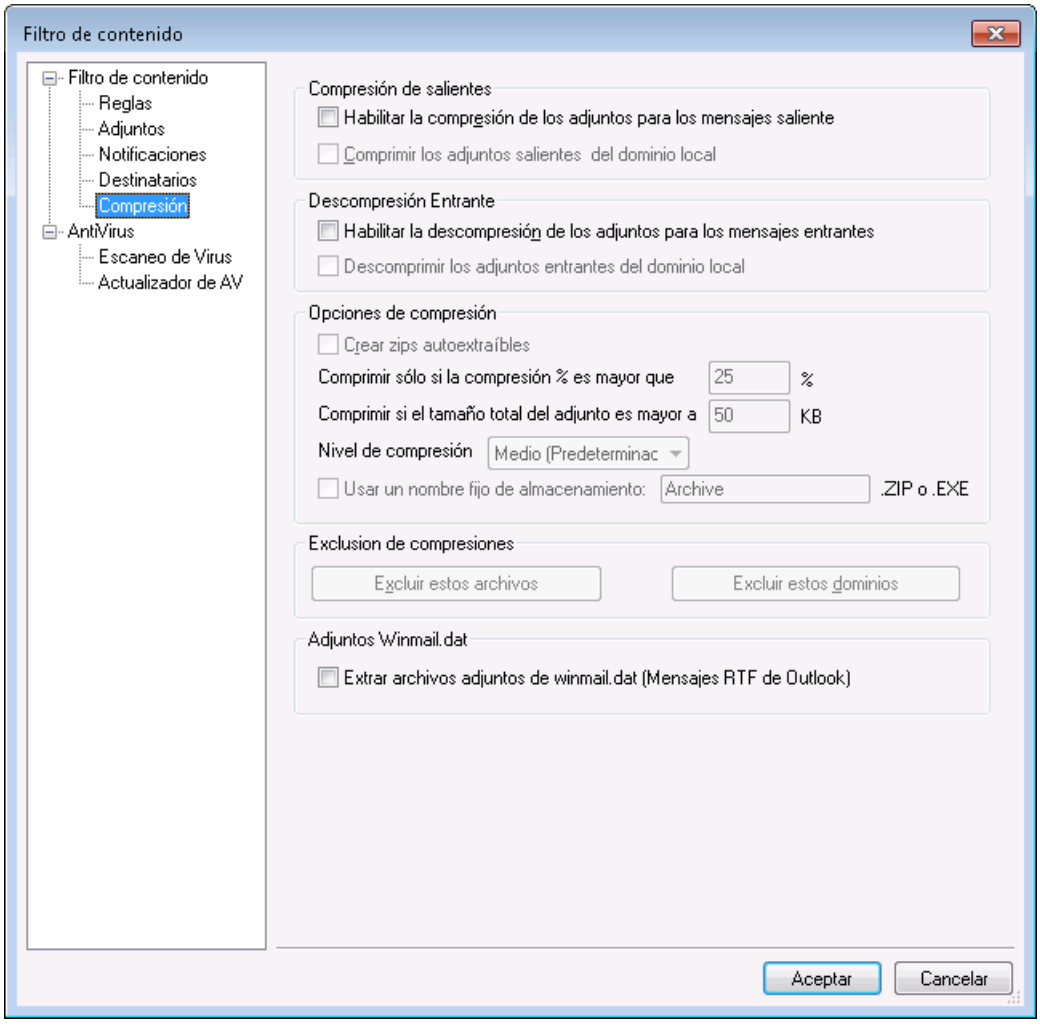


Destinatarios

Esta lista de destinatarios corresponde a las diversas opciones "*enviar...al administrador*" ubicadas en la pestaña Notificaciones. Estas direcciones recibirán mensajes de notificación cuando una de las opciones de Administrador se seleccione en dicha pestaña. Para añadir una dirección a esta sección, introdúzcala en el espacio proporcionado y luego pulse *Agregar*. Para quitar una dirección, selecciónela de la lista y luego pulse *Quitar.*

No enviar notificaciones a dominios externos
Marque esta casilla si desea restringir los mensajes de notificación del Filtro de Contenido a destinatarios del dominio local. Esta opción se encuentra deshabilitada por omisión.

4.6.1.5 Compresión



Con los controles de esta pestaña puede hacer que los adjuntos de mensajes sean automáticamente comprimidos o descomprimidos antes de que el mensaje se envíe. El nivel de compresión también se puede controlar, así como muchos otros parámetros y exclusiones. Esta funcionalidad puede reducir significativamente la cantidad de ancho de banda y salida requerida para enviar los mensajes salientes.

Compresión de salientes

Habilitar la compresión de los adjuntos para los mensajes saliente
Haga clic en esta casilla si quiere habilitar la compresión automática de adjuntos de mensajes para los mensajes de correo remoto salientes. Activando este control no se consigue que todos los adjuntos de mensaje se compriman; simplemente activa dicha funcionalidad. Si un mensaje se comprime o no será determinado por el resto de las configuraciones de esta pestaña.

Comprimir los adjuntos salientes del dominio local
Activando este control se consigue que las configuraciones de compresión de archivo se apliquen a todos los mensajes de salida - incluso aquellos cuya destinación es otra dirección local.

Compresión de entrantes

Habilitar la descompresión de los adjuntos para los mensajes entrantes
Haga clic en esta casilla si quiere activar la descompresión automática para adjuntos de mensajes remotos entrantes. Cuando un mensaje llegue con un adjunto comprimido, MDaemon lo descomprimirá antes de enviarlo al buzón local del usuario.

Descomprimir los adjuntos entrantes del dominio local
Active este control si quiere que se aplique la descompresión automática también al correo local.

Opciones de Compresión

Crear zips autoextraíbles
Haga clic en esta casilla si quiere que los archivos de compresión que cree MDaemon sean archivos zip autoextraíbles con una extensión de archivo `EXE`. Esto es útil si le preocupa que los recipientes del mensaje puedan no tener acceso a utilidades de descompresión. Los archivos zip autoextraíbles pueden descomprimirse simplemente haciendo doble-clic en ellos.

Comprimir solamente si la compresión % es mayor que XX%
MDaemon no comprimirá los adjuntos de mensaje antes de enviarlos a menos que puedan se comprimidos un porcentaje superior al valor especificado en este control. Por ejemplo, si se designa un valor de 20 y un adjunto concreto no puede ser comprimido al menos un 21% entonces MDaemon no lo comprimirá antes de enviar el mensaje.

MDaemon debe comprimir primero un archivo para determinar qué porcentaje puede ser comprimido. Además, esta funcionalidad no previene que los archivos sean comprimidos – simplemente previene que los adjuntos sean enviados en un formato de compresión cuando no pueden ser comprimidos más de un determinado valor. En otras

palabras, si después de comprimir el archivo MDaemon encuentra que no ha podido ser comprimido más que el valor indicado, la compresión será deshecha y el mensaje se enviará con sus adjuntos sin cambios.

Comprimir si el tamaño total del adjunto es mayor a XX KB
Cuando está activada la compresión automática de adjuntos, MDaemon sólo intentará comprimir los adjuntos de mensaje cuando su tamaño total exceda del valor especificado aquí. Los mensajes con tamaños totales de adjunto más allá de este umbral se enviarán normalmente con el adjunto sin cambios.

Nivel de compresión
Utilice la lista desplegable para escoger el nivel de compresión que quiere que MDaemon aplique a los adjuntos comprimidos automáticamente. Puede escoger tres niveles de compresión: mínimo (proceso de compresión más rápido con menos compresión), medio (valor por defecto), o máximo (proceso de compresión más lento pero mayor valor de compresión).

Usar un nombre fijo de almacenamiento: [nombre de archivo]
Haga clic en esta casilla y escoja un nombre si quiere que los adjuntos comprimidos automáticamente tengan un nombre de archivo específico.

Exclusión de compresiones

Excluir estos archivos...
Haga clic en este botón para especificar archivos que quiere excluir de las funciones de compresión automática. Cuando un adjunto de mensaje coincida con uno de estos nombres de archivos, no será comprimido, independientemente de la configuración de compresión. Los comodines están permitidos en estas entradas. Así pues, puede especificar por ejemplo "*.exe", y todos los archivos que acaben en ".exe" permanecerían sin comprimir.

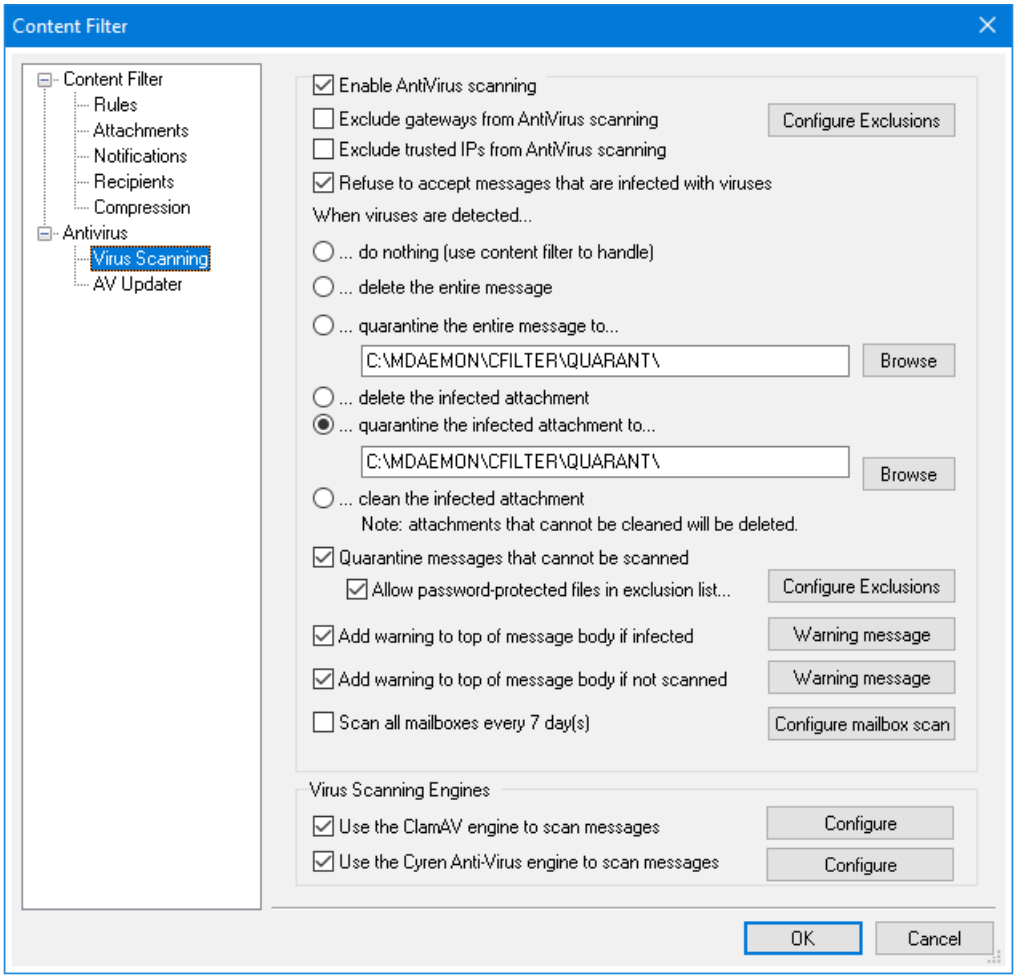
Excluir estos dominios...
Haga clic en este botón para especificar los dominios destinatarios cuyos mensajes desea excluir de la compresión automática. Los mensajes destinados a dichos dominios no tendrán compresión en sus archivos adjuntos, independientemente de las configuraciones de compresión.

Adjuntos Winmail.dat

Extraer archivos adjuntos de winmail.dat (mensajes Outlook RTF)
Habilite esta opción si desea extraer archivos adjuntos de winmail.dat y convertirlos a adjuntos de mensaje en formato estándar MIME.

4.6.2 AntiVirus

4.6.2.1 Escaneo de Virus



Las opciones en esta pantalla solo estarán disponibles al utilizar la funcionalidad opcional MDaemon AntiVirus 668. Al habilitar MDaemon AntiVirus por primera vez, se habilitará un periodo de prueba de 30 días. Si desea adquirir esta funcionalidad, contacte a su distribuidor autorizado de MDaemon o visite: www.mdaemon.com.

Habilitar el escaneo Antivirus

Haga clic en esta casilla para habilitar el escaneo de mensajes con el Antivirus. Cuando MDaemon recibe un mensaje con adjuntos, los escaneará en busca de virus antes de entregarlos a su destino final.

Excluir puertas de enlace del escaneo Antivirus

Haga clic en esta casilla si quiere que un mensaje asociado a uno de los dominios de puerta de enlace de MDaemon sea excluido de los escaneos de virus. Esto puede ser deseable para aquellos que quieran dejar el escaneo de dichos mensajes al servidor de correo del propio dominio. Para más información acerca de los dominios de puerta de enlace, vea Administrador de Puertas de Enlace 255.

Configurar Exclusiones

Haga clic en el botón Configurar Exclusiones para especificar las direcciones de destino a excluir del escaneo de virus. Los mensajes dirigidos a estas direcciones

no serán escaneados en busca de virus. Se permiten comodines en estas direcciones. Puede por lo tanto utilizar esta funcionalidad para excluir un dominio entero o buzones de correo específicos para todos los dominios. Por ejemplo, "*@ejemplo.com" o "ArchivosVirus@*".

Excluir IPs confiables del escaneo de AntiVirus
Dé clic en esta casilla si desea exentar de escaneo de Antivirus los mensajes que provienen de una de sus Direcciones IP Confiables 520.

Rechazar la aceptación de mensajes que están infectados con virus
Haga clic en esta opción si desea escanear los mensajes entrantes para virus durante la sesión SMTP en lugar de después de que la sesión concluya, y rechazar aquellos mensajes que se encuentre que contengan virus. Dado que cada mensaje entrante se escanea antes de que MDaemon lo acepte oficialmente y concluya la sesión, el servidor de envío sigue siendo responsable de éste—el mensaje no ha sido técnicamente enviado todavía. Así, el mensaje puede ser rechazado en el momento cuando se encuentra un virus. Además, dado que el mensaje fue rechazado, no se requiere tomar acciones adicionales de Antivirus definidas en este diálogo. No se tomarán procedimientos de limpieza o de cuarentena, y no se enviarán mensajes de notificación, esto puede reducir sustancialmente la cantidad de mensajes infectados y notificaciones de virus que recibirán usted y sus usuarios.

El registro log SMTP-(entrante) mostrará el resultado del proceso AV. Los posibles resultados que podrá observar son:

- el mensaje se escaneó y se encontró infectado con virus
- el mensaje se escaneó y no se encontró virus
- el mensaje no pudo ser escaneado (normalmente porque un archivo ZIP u otro tipo de adjunto no pudo ser abierto/accedido)
- el mensaje no pudo ser escaneado (excede el límite de tamaño máximo)
- ocurrió un error durante el escaneo

Cuando se detectan virus...
Haga clic en una de las opciones en esta sección para designar la acción que MDaemon tomarán cuando AntiVirus detecte un virus.

...no hacer nada (usar el filtro de contenido para gestionar)
Escoja esta opción si no desea tomar ninguna de las acciones mencionadas, y quiere establecer reglas de filtro de contenido para tomar acciones alternativas en su lugar.

...borrar el mensaje entero
Esta opción borrará el mensaje entero en lugar de sólo el adjunto cuando se encuentre un virus. Dado que esto borra todo el mensaje, la opción "*Agregar mensaje de advertencia...*" no aplica. De todos modos, puede aun así enviar un mensaje de notificación al destinatario usando los controles de la pestaña de Notificaciones.

...poner en cuarentena el mensaje entero en...
Esta opción es como la opción anterior "*Borrar el mensaje entero*", pero el mensaje será puesto en cuarentena en la ubicación especificada en lugar de ser eliminado.

...borrar el adjunto infectado
Esta opción borrará el adjunto infectado. El mensaje se enviará igualmente al destinatario, pero sin el adjunto infectado. Puede usar el control "*Agregar un mensaje de advertencia...*" al final de este diálogo para añadir texto al mensaje informando al usuario que ha sido eliminado un adjunto infectado.

...poner en cuarentena el adjunto infectado en...
Escoja esta opción y especifique una ubicación en el lugar indicado si quiere que los adjuntos infectados sean puestos en cuarentena en dicha ubicación en lugar de ser eliminados o limpiados. Como en la opción "*Borrar el adjunto infectado*", el mensaje se seguirá enviando al destinatario, pero sin el adjunto infectado.

...limpiar el adjunto infectado
Cuando se escoge esta opción, AntiVirus intentará limpiar (deshabilitar) el adjunto infectado. Si el adjunto no puede ser limpiado, será eliminado.

Poner en Cuarentena los mensajes que no pueden ser analizados
Cuando se habilita esta opción, MDaemon pondrá en cuarentena cualquier mensaje que no pueda analizar, tal como los que contienen archivos protegidos con contraseña.

Permitir archivos protegidos con contraseña en la lista de exclusiones...
Utilice esta opción si desea permitir que algún mensaje no verificable, conteniendo archivos protegidos con contraseña, pase por el motor del antivirus si el nombre de archivo o su tipo se encuentran en la lista de exclusiones.

Configurar Exclusiones
Dé clic en este botón para abrir y administrar la lista de exclusión de archivos. Los nombres y tipos de archivo incluidos en esta lista no serán escaneados.

Agregar advertencia en la parte superior del cuerpo del mensaje si está infectado
Cuando una de las anteriores opciones de "*...adjunto*" es seleccionada, haga clic en esta opción si quiere añadir algún mensaje de advertencia en la parte superior del mensaje anteriormente infectado antes de que éste sea enviado a su destinatario. Así puede informar al destinatario que el adjunto fue arrancado y por qué.

Mensaje de advertencia...
Haga clic en este botón para mostrar el texto de advertencia que se añadirá a los mensajes cuando la funcionalidad "*Agregar un mensaje de advertencia...*" se utilice. Después de hacer los cambios deseados al texto, haga clic en **OK** para cerrar el diálogo y guardar los cambios..

Agregar advertencia en la parte superior del mensaje si éste no fue escaneado
Cuando se habilita esta opción, MDaemon agregará un texto de advertencia en la parte superior de cualquier mensaje que no pueda escanear.

Mensaje de advertencia...
Dé clic en este botón para desplegar el texto de advertencia que se agregará a los mensajes que no se puedan escanear. Luego de hacer los cambios

requeridos al texto, dé clic en **OK** para cerrar el diálogo y guardar los cambios.

Escanear todos los buzones cada *n* día(s)
Marque esta casilla si desea escanear periódicamente todos los mensajes almacenados, para detectar algún mensaje infectado que haya pasado el sistema antes de que estuviera la actualización de antivirus para detectarlo. Los mensajes infectados serán movidos a la carpeta de cuarentena y se les agregará el encabezado `X-MDBadQueue-Reason`, de manera que se pueda ver una explicación cuando se visualice en MDaemon. Los mensajes que no puedan ser escaneados no se pondrán en cuarentena.

Configurar escaneo de buzones.
Dé clic en este botón para especificar la frecuencia con la que desea escanear los mensajes y si desea escanearlos todos o solo aquellos con menos de ciertos días de antigüedad. También puede ejecutar manualmente un escaneo de algún buzón, de manera inmediata.

Motores de Escaneo de Virus

MDaemon AntiVirus está equipado con dos motores de escaneo de virus: ClamAV y IKARUS AntiVirus. Cuando ambos se habilitan, los mensajes serán escaneados por los dos motores; primero IKARUS AntiVirus y luego ClamAV. Esto proporciona una capa extra de protección, dado que un virus potencialmente puede ser identificado por un motor antes de que las definiciones de virus del otro motor hayan sido actualizadas.

Utilice el motor ClamAV para escanear mensajes
Dé clic en esta casilla si desea utilizar el motor ClamAV para escanear mensajes buscando virus.

Configurar
Dé clic en este botón para tener acceso a la opción para activar el registro para depuración de ClamAV. El archivo de registro se localizará en la carpeta de registros de MDaemon.

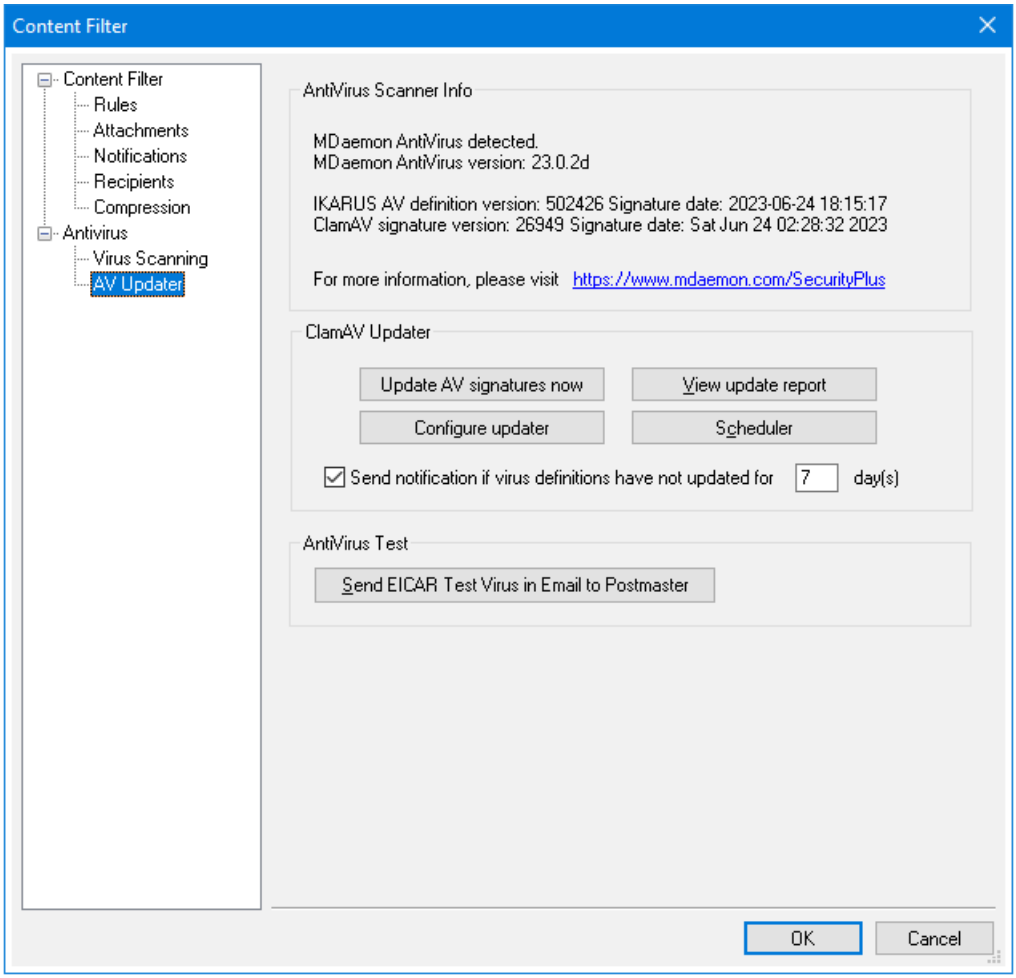
Utilice el motor IKARUS AntiVirus para escanear mensajes
Dé clic en esta casilla si desea utilizar el motor IKARUS Antivirus para escanear mensajes buscando virus..

Configurar
Utilice esta opción si desea marcar como virus, archivos adjuntos con documentos que contienen macros. Puede establecer un nivel heurístico de -1 a 5. "-1" es auto, "0" es deshabilitado y del 1 al 5 son el nivel heurístico de menor a mayor.

Ver:

Actualizador AV 673
Filtro de Contenido y AntiVirus 645

4.6.2.2 Actualizador AV



Las opciones en esta pantalla solo estarán disponibles al utilizar la funcionalidad opcional MDaemon AntiVirus 668. Al habilitar MDaemon AntiVirus por primera vez, se otorgará un periodo de prueba de 30 días. Si desea adquirir esta funcionalidad, contacte a su distribuidor autorizado de MDaemon o visite: www.mdaemon.com.

Utilice los controles en esta pantalla para actualizar manual o automáticamente sus definiciones de virus. Hay un programador para actualizar automáticamente, un visor de reportes para que pueda saber cuándo y cuales actualizaciones se han descargado y una funcionalidad de prueba utilizada para confirmar que el escaneo de virus está operando adecuadamente.

Info del Escaner de AntiVirus

Esta sección le dice si AntiVirus está disponible y qué versión se está ejecutando. También presenta la fecha de su última actualización de definiciones de virus.

Actualizador de ClamAV

Actualizar las firmas AV ahora
Dé clic en este botón para actualizar manualmente las definiciones de virus. El actualizador se conectará inmediatamente después de que se presione el botón.

Configurar el actualizador
Dé clic en este botón para abrir el diálogo de Configuración del Actualizador. Este diálogo contiene las pestañas siguientes:

Proxy
La pestaña Proxy contiene las opciones para configurar cualquier ajuste HTTP o FTP que requiera la configuración actual de su red a fin de conectarse a los sitios de actualización.

Misc
La pestaña Misc contiene opciones que administran el registro del actualizador. Puede elegir si se registran las acciones del actualizador en un archivo y puede especificar el tamaño máximo de ese archivo.

Ver reporte de actualización
El visor de registros de Antivirus se abre dando clic en el botón *Ver reporte de actualizaciones*. El visor enlista la hora, acciones tomadas y otra información sobre cada actualización.

Programador
Dé clic en este botón para abrir la pantalla de Programación de Antivirus 378, utilizada para programar verificaciones de actualizaciones de firmas de virus en horarios y días específicos o a intervalos regulares.

Enviar notificación si las definiciones de virus no se han actualizado durante xx día(s)
Por omisión el administrador será notificado si las definiciones de virus de ClamAV no han sido actualizadas durante el número especificado de días.

Prueba de AntiVirus

Enviar Test EICAR para Virus en Mail a Postmaster
Haga clic en este botón para enviar un mensaje de prueba al postmaster, con el archivo del virus EICAR adjunto. Este adjunto es inofensivo - se usa simplemente para probar el antivirus. Si mira la ventana de registro del Filtro de Contenido en la pantalla principal de MDaemon puede ver lo que hace MDaemon con este mensaje cuando se recibe. Por ejemplo, dependiendo de sus configuraciones, puede ver un extracto de registro que se parezca en algo al siguiente:

```
Mon 2008-02-25 18:14:49: Processing C:
\MDAEMON\LOCALQ\md75000001128.msg
Mon 2008-02-25 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2008-02-25 18:14:49: > Message from: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message to: postmaster@example.com
Mon 2008-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2008-02-25 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@example.com>
Mon 2008-02-25 18:14:49: Performing viral scan...
Mon 2008-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
```

```
Mon 2008-02-25 18:14:50: > eicar.com was removed from message
Mon 2008-02-25 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 2008-02-25 18:14:50: > Total attachments scanned    : 1
(including multipart/alternatives)
Mon 2008-02-25 18:14:50: > Total attachments infected   : 1
Mon 2008-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2008-02-25 18:14:50: > Total attachments removed    : 1
Mon 2008-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (sender)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (recipient)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2008-02-25 18:14:50: > Virus notification sent to
postmaster@example.com (admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

Ver:

AntiVirus 668
Filtro de Contenido y AntiVirus 645

4.7 Filtro de Correo Basura

4.7.1 Filtro de Correo Basura

El Filtro de Spam es una de las funciones principales en el extensivo paquete de herramientas de prevención de Spam de MDaemon. Incorpora heurística para examinar los mensajes entrantes para poder calcular una "puntuación" basada en un complejo sistema de reglas. La puntuación se usa para determinar la probabilidad de que un mensaje sea Spam, y se pueden tomar ciertas acciones basándonos en dicha puntuación — puede rechazar el mensaje, marcarlo como posible Spam, y demás.

Las direcciones pueden ser permitidas o bloqueadas, o designarlas como completamente exentas de ser examinadas por el Filtro de Spam. Puede tener un informe de Spam insertado en los mensajes, que muestre cómo se han conseguido las puntuaciones de Spam y de qué tipo son, o puede generar un informe como un correo separado y tener el correo Spam original incluido en él como adjunto. Además, puede incluso usar aprendizaje Bayesiano 680 para ayudar al Filtro de Spam a identificar el Spam más acertadamente a través del tiempo, así pues, incrementando su confiabilidad.

Finalmente, examinando muchos miles de mensajes de Spam conocidos, las reglas han sido optimizadas a través del tiempo y son muy fiables detectando las huellas

de un mensaje Spam. Puede, sin embargo, personalizar y añadir nuevas reglas editando los archivos de configuración del Filtro de Spam para que se ajusten a sus necesidades específicas.

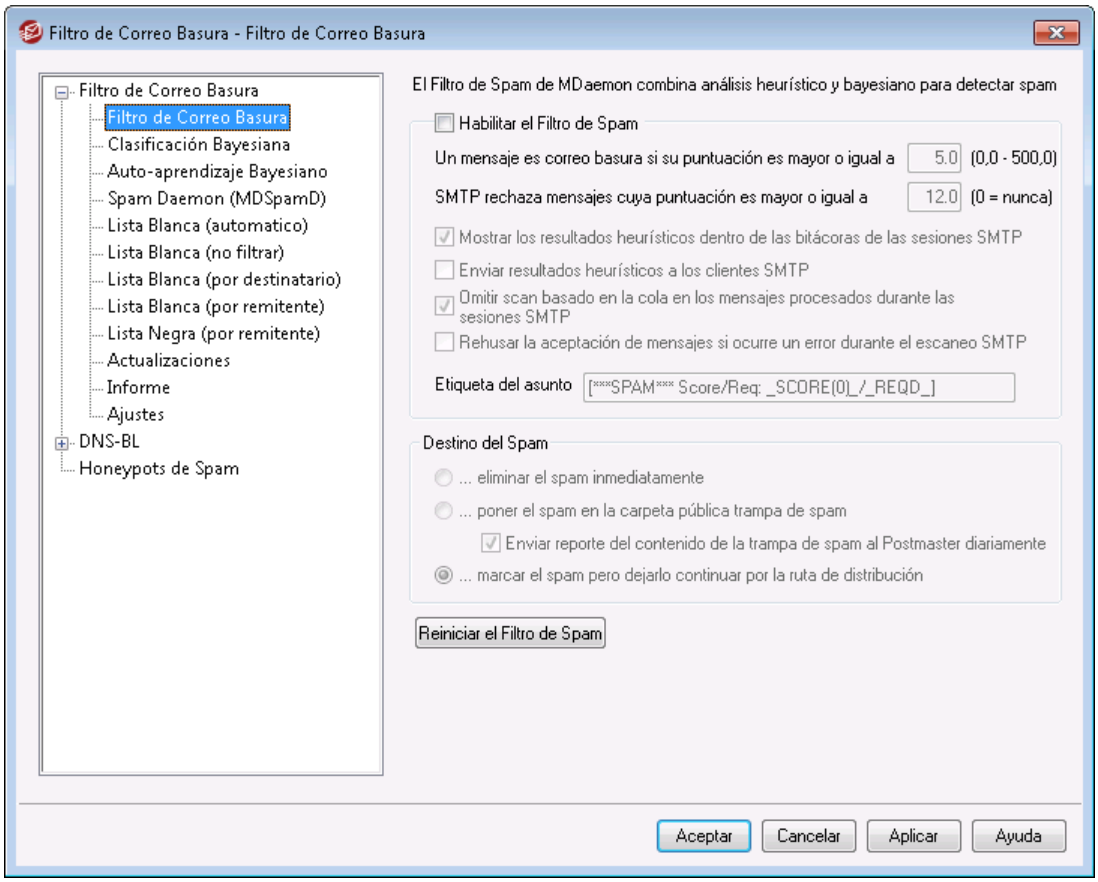
El Filtro de Spam de MDaemon una conocida tecnología integrada de código abierto. La página principal para el proyecto de código abierto es:

```
http://www.spamassassin.org
```

Ver:

Filtro de Correo Basura 676
Listas de Bloqueo de DNS 701

4.7.1.1 Filtro de Correo Basura



Habilitar el Filtro de Spam

Marque esta casilla para activar el sistema de filtrado de Spam a través de puntuación heurística de mensajes. Ninguna de las otras Opciones del Filtro de Spam en esta pantalla estará disponible hasta que esta opción esté habilitada.

Un mensaje es correo basura si su puntuación es mayor o igual a [XX] (0.0-500.0)
El valor que especifique aquí es el umbral de Spam requerido para que MDaemon compare cada puntuación de Spam de mensaje. Cualquier mensaje con una

puntuación de Spam superior o igual a esta cantidad se considerará Spam, y luego las acciones apropiadas se tomarán basándose en sus otras configuraciones de Filtro de Spam.

SMTP rechaza mensajes cuya puntuación es mayor o igual a XX (0=nunca)
Use esta opción para designar un umbral de rechazo de puntuación Spam. Cuando la puntuación Spam sea mayor o igual a esta puntuación se rechazará completamente en lugar de ser procesado a través del resto de las opciones y ser posiblemente enviado. El valor de esta opción debe ser siempre superior al de la opción anterior *"Un mensaje es correo basura si..."*. De otro modo, un mensaje no se consideraría nunca como Spam y ni se aplicarían el resto de las opciones de Filtro de Spam—seria simplemente rechazado durante el envío. Use "0" en esta opción si desea deshabilitar el escaneo durante el proceso SMTP, y si no quiere que MDaemon rechace ningún mensaje a pesar de sus puntuaciones. Si el escaneo SMTP se deshabilita, entonces un escaneo basado en cola se seguirá ejecutando en los mensajes después de que éstos sean aceptados. La configuración por defecto para esta opción es "12.0".

Ejemplo,

Si tiene un umbral de Spam establecido en 5.0 y un umbral de rechazo establecido en 10.0, entonces cualquier mensaje con una puntuación de Spam superior o igual a 5.0 pero menor que 10.0 se considerará Spam y se gestionará de acuerdo con el resto de sus configuraciones de Filtro de Spam. Cualquier mensaje con una puntuación de Spam superior o igual a 10.0 será rechazado por MDaemon durante el proceso de envío.

Debería monitorear el rendimiento de su filtro de Spam a lo largo del tiempo y refinar tanto los umbrales de detección como de rechazo para adaptarlos a sus necesidades. Para la mayoría de persones, sin embargo, un umbral de puntuación Spam de 5.0 capturará la mayoría del Spam, con una cantidad relativamente baja de falsos negativos (Spam que se cuela sin ser reconocido) y raramente ningún falso positivo (mensajes marcados como Spam que no lo son). Un umbral de rechazo de 10-15 hará que sólo los mensajes que es casi seguro que sean Spam sean rechazados. Es extremadamente raro que un mensaje legítimo tenga una puntuación tal alta. El umbral de rechazo por defecto es 12.

Mostrar resultados heurísticos en la bitácora de las sesiones SMTP
Haga clic en esta opción para registrar en la bitácora de las sesiones SMTP los resultados del proceso heurístico.

Enviar resultados heurísticos a clientes SMTP
Dé clic en esta opción para desplegar los resultados del procesamiento heurístico en línea con las transcripciones de las sesiones SMTP. Esta opción no está disponible cuando tiene su umbral de rechazo de Puntuación Spam establecido en "0", lo que significa que el Spam no será nunca rechazado por su puntuación. Para más información vea la opción anterior "*SMTP rechaza mensajes cuya puntuación es mayor o igual a XX (0=nunca)*".

Omitir escaneo basado en la cola en los mensajes procesados durante las sesiones SMTP
Por defecto, MDaemon escanea mensajes durante la sesión SMTP para determinar si deberían o no ser rechazados por tener una puntuación de Spam superior al umbral de rechazo anterior. Para mensajes que sean aceptados MDaemon realizará otro escaneo basado en cola y tratará a los mensajes de acuerdo con éste, basándose en sus puntuaciones y en su configuración de filtro de Spam. Haga clic en esta opción si quiere que MDaemon omita el escaneo basado en cola y trate los resultados del escaneo del Filtro de Spam iniciales como definitivos. Esto puede reducir considerablemente el uso de la CPU y aumentar la eficiencia del sistema AntiSpam. Aun así, sólo se añadirán a los mensajes las cabeceras SpamAssassin por defecto cuando se omita el escaneo basado en cola. Si ha realizado algún cambio a las cabeceras de SpamAssassin o a cabeceras personalizadas especificadas en su archivo `local.cf`, dichos cambios y modificaciones serán ignorados.

Rechazar la aceptación de correo si ocurre un error durante el escaneo SMTP
Haga clic en esta opción si quiere que un mensaje sea rechazado cuando se encuentre un error mientras está siendo escaneado durante el proceso SMTP.

Etiqueta del asunto
Esta etiqueta se insertará al principio del encabezado de Asunto de todos los mensajes que encuentren o excedan el umbral de puntuación de Spam requerido. Puede contener información acerca de la puntuación de Spam, y puede usar sus filtros de IMAP para buscar y filtra un mensaje de acuerdo con ello (asumiendo que tenga el Filtro de Spam configurado para continuar la entrega de los mensajes Spam). Este es un método sencillo para enrutar mensajes Spam automáticamente a una carpeta "Spam" designada. Si quiere insertar dinámicamente la puntuación Spam del mensaje y la puntuación requerida del umbral de Spam, utilice la etiqueta "`_HITS_`" para la puntuación de mensajes y "`_REQD_`" para el umbral requerido. Alternativamente, puede usar "`_SCORE(0)_`" en lugar de "`_HITS_`"— esto insertará un cero delante de las puntuaciones bajas, que puede asegurar una correcta ordenación cuando se ordenen los mensajes por asunto en algunos clientes de correo.

Ejemplo,

Una etiqueta de asunto puede establecida como: `***SPAM*** Puntos/Req: _HITS_/_REQD_ -`
hará que un mensaje de Spam con una puntuación de 6.2 y el asunto: "Hey, aquí hay Spam!" sea cambiada a "***SPAM*** Puntos/Req: 6.2/5.0 – Hey, aquí hay Spam!"

Si se sustituye "`_SCORE(0)_`" por "`_HITS_`" se cambiaría a "***SPAM*** Puntos/Req: 06.2/5.0 – Hey, aquí hay spam!"

Si no desea alterar la cabecera de asunto deje esta opción en blanco. No se insertará etiqueta en el asunto.

Esta opción no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. La configuración de etiquetado del Asunto la

determinarán las configuraciones del otro servidor. Vea: Spam Daemon 686, para más información.

Destino del Spam

El Filtro de Spam ejecutará la acción seleccionada abajo si el puntaje de Spam de un mensaje es igual o mayor al puntaje arriba especificado.

...eliminar el Spam inmediatamente
Seleccione esta opción si desea simplemente eliminar cualquier mensaje entrante cuyo puntaje de Spam exceda el límite designado.

...poner el Spam en la carpeta de la trampa pública de Spam
Seleccione esta opción si desea marcar los mensajes como Spam y luego moverlos a la carpeta de la trampa pública de Spam en lugar de permitir que sean entregados.

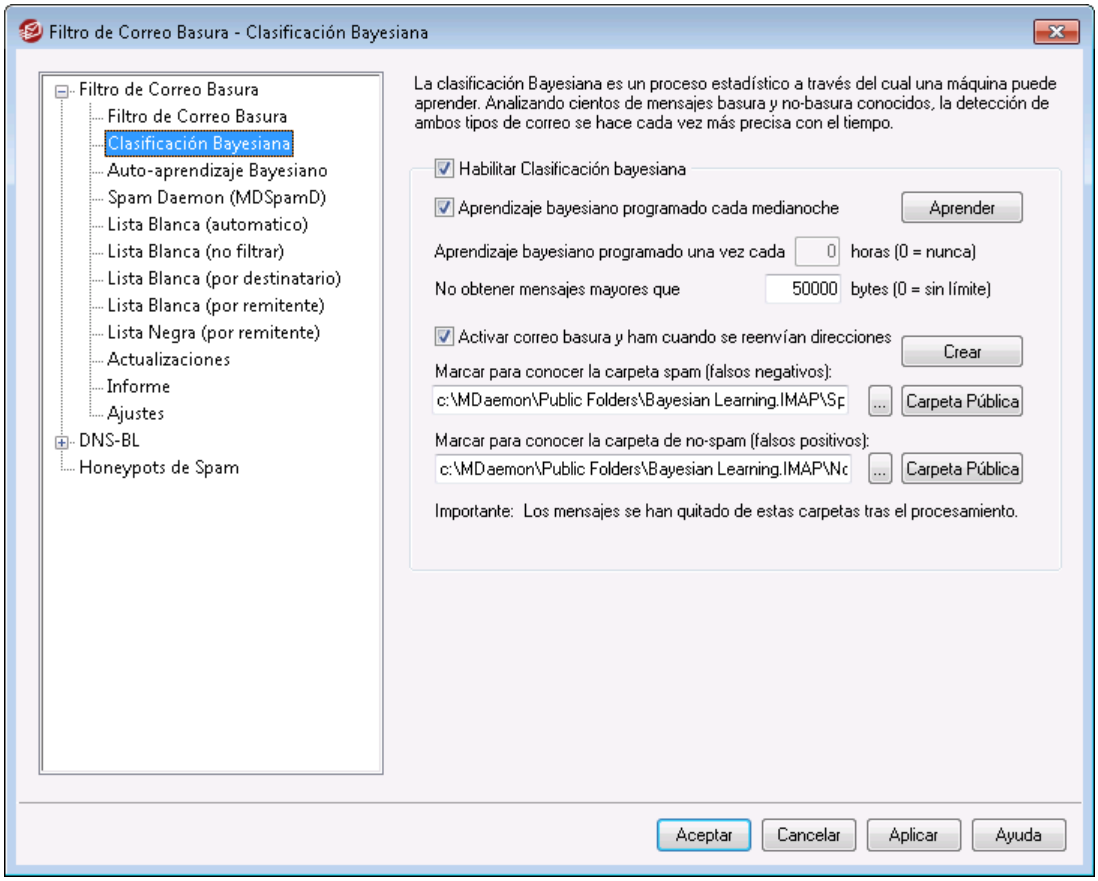
Enviar reporte del contenido de la trampa de Spam al Postmaster diariamente
Al utilizar la opción *...poner el Spam en la carpeta de la trampa pública de Spam*, habilite esta opción si desea que el postmaster reciba diariamente un mensaje contenido el resumen del contenido de la carpeta.

...marcar el Spam, pero permitirle continuar en el proceso de entrega
Elija esta opción si desea permitir la entrega de los mensajes de Spam a sus destinatarios, pero marcándolos como Spam, insertando los encabezados y/o etiquetas definidos arriba y en la pantalla de Informes 697. Esta es la opción por omisión, que permite a los usuarios aprovechar opciones tales como el filtrado de correo a la carpeta de Spam para su revisión y así evitar perder mensajes que se hayan etiquetado erróneamente como Spam (i.e., falsos positivos).

Reiniciar el Filtro de Spam

Dé clic en este botón para reiniciar el motor del Filtro de Spam.

4.7.1.2 Clasificación Bayesiana



La Clasificación Bayesiana no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. Todo el aprendizaje Bayesiano se realizará en el otro servidor. Vea: Spam Daemon 686, para más información.

El Filtro de Spam soporta el aprendizaje Bayesiano, que es un proceso estadístico que puede ser utilizado opcionalmente para analizar los mensajes de Spam y no-Spam para poder incrementar la fiabilidad del reconocimiento de Spam en el tiempo. Puede designar una carpeta para los mensajes Spam y no-Spam que serán escaneados manual o automáticamente a intervalos regulares. Todos los mensajes en dichas carpetas se analizarán e indexarán para que los nuevos mensajes puedan ser comparados estadísticamente para poder determinar si es posible que sean Spam. El Filtro de Spam puede incrementar o reducir la puntuación Spam de un mensaje basándose en los resultados de la comparación Bayesiana.

El Filtro de Spam no aplicará la clasificación Bayesiana a los mensajes hasta que se haya realizado un análisis Bayesiano en el número de correos Spam y no-Spam designados en la

pantalla Aprendizaje Automático 684. Esto es necesario para que el Filtro de Spam tenga una base de estadísticas suficiente cuando haga una comparación Bayesiana. Una vez que le haya dado al sistema estos mensajes para el análisis, estará suficientemente equipado para empezar a aplicar los resultados de la comparación Bayesiana para cada puntuación de cada mensaje entrante. Si continúa analizando más mensajes las clasificaciones Bayesianas serán, con el tiempo, más precisas.

Clasificación Bayesiana

Habilitar Clasificación Bayesiana
Haga clic en esta casilla si quiere que cada puntuación Spam de cada mensaje se ajuste basado en una comparación de las estadísticas Bayesianas conocidas actualmente.

Aprendizaje bayesiano programado cada media noche
Cuando esta opción está activa, una vez al día a medianoche el Filtro de Spam analizará y luego borrará todos los mensajes contenidos en las carpetas de Spam y no-Spam especificadas a continuación. Si desea programar el aprendizaje Bayesiano para algún otro intervalo, entonces desmarque esta opción y use la opción siguiente de *Aprendizaje bayesiano programado una vez cada XX horas*. Si no desea que el aprendizaje Bayesiano ocurra automáticamente, desactive esta opción y especifique "0" en la opción siguiente.

Aprendizaje bayesiano programado una vez cada XX horas (0=nunca)
Si desea que el aprendizaje Bayesiano ocurra en un intervalo de tiempo distinto de una vez a medianoche, desmarque la opción anterior y especifique el número de horas en esta opción en su lugar. Cada vez que hayan pasado el número de horas indicado, el Filtro de Spam analizará y luego borrará todos los mensajes contenidos en las carpetas de Spam y no-Spam especificadas a continuación. Si no desea que nunca ocurra automáticamente el aprendizaje Bayesiano, despeje la opción anterior y especifique "0" horas en esta opción.

Si por alguna razón no quiere que los mensajes se borren después de que sean analizados, puede prevenirlo copiando `LEARN.BAT` a `MYLEARN.BAT` en la subcarpeta `\MDaemon\App\` y luego borrando las dos líneas que empiezan con "`if exist`" cerca del final de dicho archivo. Cuando el archivo `MYLEARN.BAT` se encuentra en dicha carpeta, MDaemon lo usará en lugar de `LEARN.BAT`. Vea `SA-Learn.txt` en su subcarpeta `\MDaemon\SpamAssassin\` para más información.

Para información más detallada acerca de la tecnología de filtrado heurístico de Spam y aprendizaje Bayesiano, visite:

http://www.spamassassin.org/doc/sa-learn.html.

No obtener mensajes mayores que XX bytes (0=sin límite)
Use esta opción para designar un tamaño máximo de mensaje para el análisis Bayesiano. Los mensajes mayores a este valor no serán analizados. Especifique "0" en esta opción si no desea implementar ninguna restricción de tamaño.

Aprender
Haga clic en este botón para iniciar el análisis Bayesiano manual de las carpetas designadas en lugar de esperar al análisis automático.

Activar correo basura y ham cuando se reenvían direcciones
Haga clic en esta casilla si desea permitir a los usuarios que reenvíen mensajes Spam y no-Spam (ham) a las direcciones designadas para que el sistema Bayesiano pueda aprender de ellas. Las direcciones por defecto que MDaemon usará son "SpamLearn@<dominio>" y "HamLearn@<dominio>". Los mensajes enviados a estas direcciones deben recibirse vía SMTP desde una sesión autenticada usando SMTP AUTH. Además, MDaemon espera que los mensajes sean reenviados a las direcciones anteriores como adjuntos del tipo "message/rfc822". Cualquier mensaje de cualquier otro tipo que se envíe a estas direcciones de correo no será procesado.

Puede cambiar las direcciones que MDaemon usar añadiendo las siguientes claves en el archivo CFilter.INI:

```
[SpamFilter]
SpamLearnAddress=MiDireccionSpam@
HamLearnAddress=MiDireccionNoSpam@
```

Nota: el último carácter de estos valores debe ser "@".

Crear
Haga clic en este botón para crear las Carpetas Públicas IMAP de Spam y no-Spam automáticamente, y para configurar MDaemon para que las use. Las siguientes carpetas serán creadas:

\Bayesian Learning.IMAP\	Carpeta IMAP raíz.
\Bayesian Learning.IMAP\Spam.IMAP\	Esta carpeta es para falsos negativos (Spam que no ha puntuado suficiente como para ser marcado como tal).
\Bayesian Learning.IMAP\Non-Spam.IMAP\	Esta carpeta es para falsos positivos (mensajes no-Spam que han puntuado erróneamente suficientemente alto como para ser marcados como Spam).

Por defecto, los permisos de acceso a dichas carpetas sólo se conceden a usuarios locales de dominios locales y están limitados a Buscar e Insertar. Los permisos por defecto del postmaster son Buscar, Leer, Insertar y Eliminar.

Marcar para conocer la carpeta Spam (falsos negativos):
Esta es la ruta a la carpeta que se usará para el análisis Bayesiano de correos Spam conocidos. Sólo copie mensajes a esta carpeta si considera que son Spam. No debería automatizar el proceso de copiado de mensajes a esta carpeta a

menos que se haga a través del Aprendizaje Automático 684 o las opciones de Capturas de Spam 707. Automatizar este proceso por otros métodos puede causar potencialmente que se analicen mensajes no-Spam como Spam, lo cual reduciría la fiabilidad de las estadísticas Bayesianas.

Marcar para conocer la carpeta de no-Spam (falsos positivos):
Esta es la ruta a la carpeta que se usará para el análisis Bayesiano de mensajes que definitivamente **no** son Spam. Sólo los mensajes que **no** considere que sean Spam deberían ser copiados a esta carpeta. No debería automatizar el proceso de copiado de mensajes a esta carpeta a menos que lo haga a través de las opciones de Aprendizaje Automático 684. Automatizar este proceso por otros métodos puede causar potencialmente que se analicen mensajes Spam como no-Spam, lo que reduciría la fiabilidad de las estadísticas Bayesianas.

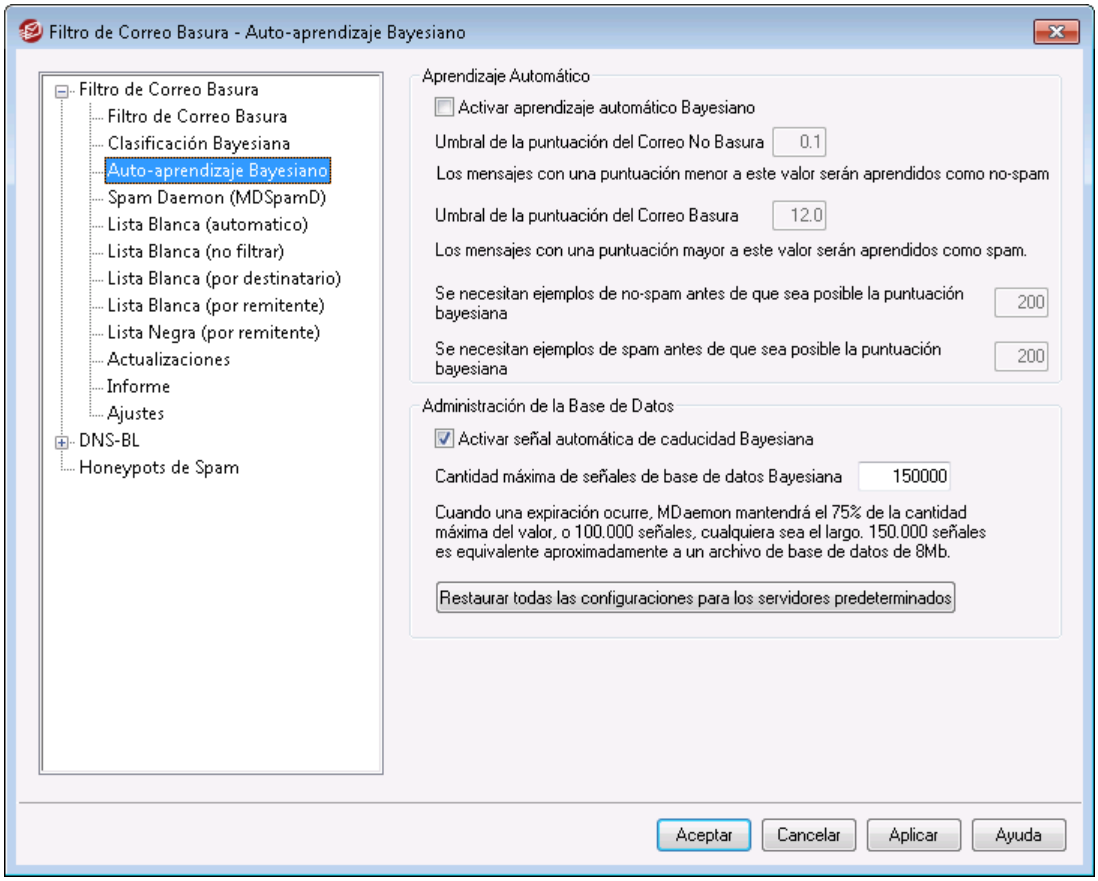
Carpeta Pública
Haga clic en uno de estos botones para designar una de las Carpetas Públicas existentes como directorio Bayesiano. Esta es una manera sencilla para sus usuarios de colocar sus mensajes erróneamente clasificados como Spam o no-Spam en sus directorios Bayesianos para el análisis. Note, aun así, que dar acceso a más gente incremente la posibilidad de que algunos mensajes se coloquen en los directorios erróneos así pues engañando las estadísticas y reduciendo la fiabilidad.

Si renombra una Carpeta Pública a través de un cliente de correo, el Explorador de Windows, o de otra manera, deberá restablecer esta ruta manualmente al nuevo nombre de carpeta. Si renombra la carpeta, pero no cambia su ruta aquí, el Filtro de Spam continuará usando esta ruta para la carpeta Bayesiana en lugar de la nueva.

Ver:

Aprendizaje Automático 684
Honeypots de Spam 707

4.7.1.3 Auto-aprendizaje Bayesiano



El Aprendizaje Bayesiano Automático no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. El aprendizaje bayesiano lo realizará el otro servidor. Vea: Spam Daemon 686, para más información.

Aprendizaje Automático

Activar aprendizaje automático Bayesiano
Con el aprendizaje Bayesiano automático puede designar umbrales de puntuación de Spam y no-Spam, lo que hará posible para el sistema de aprendizaje Bayesiano aprender de los mensajes automáticamente en lugar de requerir que coloque manualmente dichos mensajes en las carpetas de Spam y no-Spam. Cualquier mensaje que puntúe por debajo del umbral de puntuación de no-Spam será tratado por el aprendizaje automático como no-Spam y cualquier mensaje que puntúe por encima del umbral de Spam será tratado como Spam. Con el aprendizaje automático, las señales antiguas ya expiradas que se eliminan de la base de datos (vea *Administración de la base de datos* a continuación pueden ser sustituidas automáticamente. Esto le resguarda de la necesidad de reestructuración manual de las señales expiradas. El aprendizaje automático

puede ser útil y beneficioso mientras tenga cuidado a la hora de poner los umbrales, para evitar colocar mensajes clasificados erróneamente en las carpetas.

Umbral de la puntuación del Correo No Basura
Los mensajes con una puntuación de Spam por debajo de este valor se tratarán como mensajes no-Spam por el sistema de Clasificación Bayesiana.

Umbral de la puntuación del Correo Basura
Los mensajes con una puntuación de Spam por encima de este valor serán tratados como mensajes de Spam por el sistema de Clasificación Bayesiana.

Se necesitan ejemplos de no-Spam antes de que sea posible la puntuación bayesiana
El Filtro de Spam no aplicará una clasificación Bayesiana a los mensajes hasta que este número de mensajes no-Spam (y mensajes Spam especificados en la opción siguiente) hayan sido analizados por el sistema Bayesiano. Esto es necesario para proporcionarle al sistema estos mensajes suficientes para realizar un conjunto de estadísticas que utilizar para la comparación Bayesiana. Una vez le haya dado al sistema estos mensajes para analizar, estará suficientemente equipado para empezar a aplicar los resultados de una comparación Bayesiana en cada puntuación de Spam de cada mensaje entrante. Si continúa analizando más mensajes las clasificaciones Bayesianas serán más precisas con el tiempo.

Se necesitan ejemplos de Spam antes de que sea posible la puntuación bayesiana
Al igual que la opción anterior aplica a los mensajes no-Spam, esta opción es para designar el número de mensajes *Spam* que deben ser analizados antes de que el Filtro de Spam empiece a aplicar la clasificación Bayesiana a los mensajes.

Administración de la Base de Datos

Activar señal automática de caducidad Bayesiana
Haga clic en esta opción si quiere que el sistema Bayesiano automático expire las señales de base de datos siempre que el número de señales especificadas a continuación sea alcanzado. Si establece un límite de señales puede prevenir que su base de datos sea excesivamente grande.

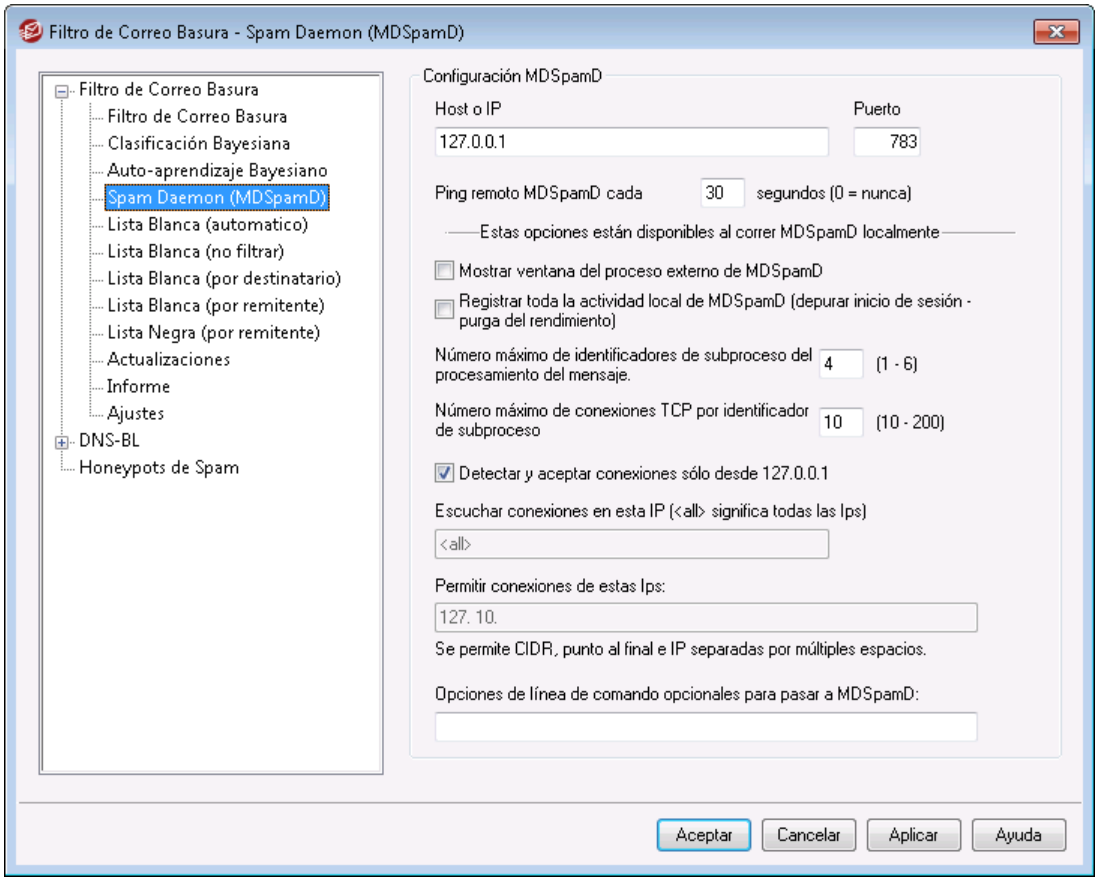
Cantidad máxima de señales de base de datos Bayesiana
Este es el máximo número de señales de base de datos Bayesianas permitidas. Cuando se alcanza este número de señales, el sistema Bayesiano elimina las más antiguas, reduciendo el número al 75% de su valor, o a 100,000 señales, lo que sea lo más alto. El número de señales nunca caerán por debajo de dichos dos valores a pesar de cuantas señales hayan expirado. Nota: 150,000 señales son aproximadamente 8Mb.

Restaurar todas las configuraciones para los servidores predeterminados
Haga clic en este botón para restaurar todas las opciones Bayesianas avanzadas a sus valores por defecto.

Ver:

Clasificación Bayesiana 680
Trampas de Miel de Spam 707

4.7.1.4 Spam Daemon (MDSpamD)



El sistema de filtrado de Spam de MDaemon se ejecuta como un daemon separado—el MDaemon Spam Daemon (MDSpamD), al que se le proveen mensajes a través de TCP/IP para su escaneo. Esto incrementa el rendimiento del Filtro de Spam sustancialmente y hace posible ejecutar MDSpamD localmente, en un ordenador separado, o hacer que MDaemon use otro MDSpamD (o cualquier otro Daemon de Spam que tenga soporte) ejecutándose en otra ubicación. Por defecto MDSpamD se ejecuta localmente y recibe mensajes por el puerto 783 en 127.0.0.1, pero puede configurar un puerto e IP diferentes si desea mandar mensajes a otro daemon de Spam que se ejecute en una ubicación o puertos diferentes.

Configuración de MDSpamD

Host o IP
Este es el host o dirección IP a la cual MDaemon enviará los mensajes para que sean escaneados por MDSpamD. Use `127.0.0.1` si MDSpamD se ejecuta localmente.

Puerto
Este es el puerto al que se enviarán los mensajes. El puerto por defecto de MDSpamD es 783.

Ping MDSpamD remoto cada XX segundos (0=nunca)
Si está usando un daemon de Spam que se ejecuta en una ubicación remota, puede usar esta opción para hacer ping a dicha ubicación de manera periódica. Use "0" si no desea hacer ping en dicha ubicación.

Estas opciones están disponibles cuando MDSpamD funciona localmente

Mostrar ventana del proceso externo de MDSpamD
Cuando MDSpamD se ejecuta localmente, active esta opción si quiere ejecutarlo en una ventana externa de proceso. Esta opción hará que la salida de MDSpamD se enlace a la ventana externa de proceso en lugar de a la interfaz interna de MDaemon o sistema de registro. Si usa esta opción se incrementará el rendimiento puesto que los datos de MDSpamD no tendrán que ser registrados ni controlados por MDaemon. Sin embargo, no se creará archivo de registro puesto que esta opción no se puede usar junto con la opción de registro siguiente, ni tampoco aparecerán datos en la pestaña *Seguridad»MDSpamD* de la interfaz principal de MDaemon.

Registrar en bitácora toda la actividad local de MDSpamD (para rastrear errores—degrada el rendimiento)
Haga clic en esta opción si desea registrar en bitácora toda la actividad de MDSpamD. Esta opción no está disponible si utiliza la opción anterior de *Mostrar ventana del proceso externo de MDSpamD*. Además, si usa credenciales de usuario en el diálogo Servicios de Windows 505 en lugar de ejecutar MDaemon bajo la cuenta SYSTEM, no se registrará actividad de MDSpamD.

Cuando se usa esta opción de registro, puede ver reducido el rendimiento de su sistema de correo, dependiendo del sistema y del nivel de actividad. Generalmente sólo debería usar esta opción para procesos de depuración.

Número máximo de subprocesos (threads) de mensajes (1-6)
Este es el máximo número de subprocesos (threads) que MDaemon usará para procesamiento interno. Puede establecer este valor de 1 a 6.

Número máximo de conexiones TCP por subproceso (thread) (10-200)
Este es el máximo número de conexiones TCP aceptadas por un subproceso de MDSpamD antes de que pase a otro subproceso. Puede establecer este valor entre 10 y 200.

Detectar y aceptar las conexiones sólo desde 127.0.0.1
Haga clic en esta opción si no desea permitir a su MDSpamD local aceptar conexiones de ningún recurso externo. Sólo las conexiones de la misma máquina en la que se ejecuta serán permitidas.

Detectar conexiones en esta IP
Si la opción anterior se deshabilita, puede usar esta opción para enlazar o restringir conexiones a una dirección IP específica. Sólo las conexiones a la IP designada serán permitidas. Utilice "`<all>`" si no desea restringir MDSpamD a ninguna dirección IP en particular.

Permitir conexiones desde estas IPs
Estas son las direcciones IP desde las cuales MDSpamD aceptará conexiones entrantes. Las conexiones de otras direcciones IP se rechazarán. Esto es útil si desea permitir conexiones desde otro servidor para poder compartir procesamiento del Filtro de Spam.

Opciones de línea de comando opcionales para pasar a MDSpamD:

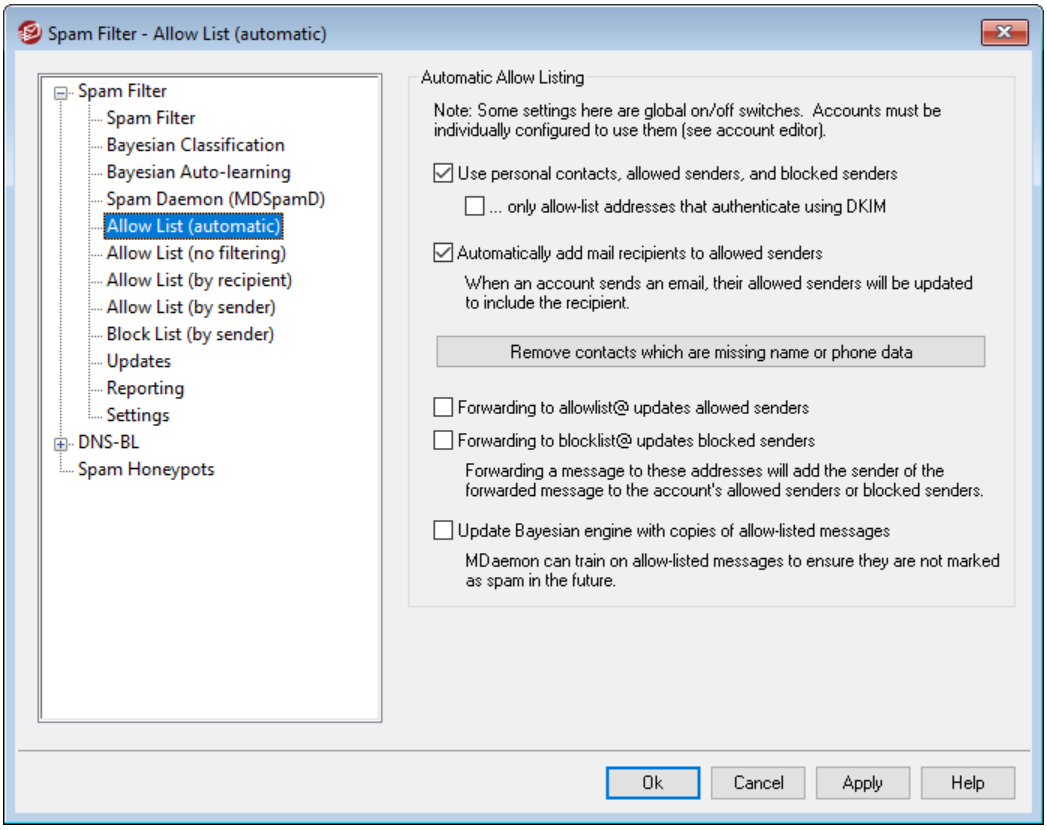
MDSpamD puede aceptar muchas opciones de línea de comandos, documentadas en:

http://spamassassin.apache.org/

Si desea utilizar alguna de estas opciones, construya una cadena que contenga las opciones deseadas y colóquela aquí.

Algunas de estas opciones pueden ser configuradas a través de las especificaciones en esta pantalla y no necesitan ser establecidas manualmente usando opciones de línea de comandos.

4.7.1.5 Lista de Permitidos (automática)



Lista automática de Permitidos

Utilizar los contactos personales y remitentes permitidos y bloqueados
Haga clic en esta opción para permitir que la carpeta de Contactos de cada usuario y sus carpetas de remitentes permitidos y bloqueados, se utilicen para el filtrado de spam de ese usuario. Para cada mensaje entrante, MDaemon verificará los contactos, la de permitidos y bloqueados del destinatario, buscando al

remitente del mensaje. Si este se encuentra en cualquiera de las carpetas entonces el mensaje se considerará permitido o bloqueado automáticamente. Si no desea aplicar esta opción a todos los usuarios de MDaemon la puede deshabilitar para usuarios individuales desactivando la opción *El Filtro de Spam utiliza contactos personales y remitentes permitidos y bloqueados* en la pantalla Lista de Permitidos 758 en el Editor de Cuentas.

...colocar en lista de permitidos solo direcciones que se autentifiquen utilizando DKIM
Cuando esta opción está habilitada, MDaemon no podrá el mensaje en lista de permitidos a menos que el remitente se haya autentificado vía DomainKeys Identified Mail 529 (DKIM). Esta opción ayuda a evitar incluir en lista blanca mensajes con direcciones apócrifas. Esta opción se encuentra deshabilitada por omisión.

Actualizar automáticamente los contactos en lista de permitidos
Cuando esta opción está habilitada, MDaemon añadirá automáticamente cualquier dirección de correo no local a la que envíe correo a su carpeta de lista personal de permitidos. Cuando se usa conjuntamente con la opción "*Usar contactos personales y remitentes permitidos y bloqueados*", el número de falsos positivos del Filtro de Spam puede verse reducido drásticamente.

Si no desea aplicar la actualización automática de la lista blanca a cada usuario de MDaemon la puede deshabilitar para usuarios individuales desmarcando la casilla *"Actualizar contactos en lista blanca con los destinatarios de correo"* en la pantalla Lista de Permitidos 758 del Editor de Cuentas.

Esta opción se deshabilita para las cuentas que utilicen autorespuestas.

Eliminar contactos que carecen de nombre o número telefónico
Dé clic en este botón si desea eliminar todos los contactos que contienen solamente la dirección de correo en la carpeta por omisión de Contactos de cada usuario. Si un contacto no tiene por lo menos nombre y número telefónico será eliminada. Esta opción pretende ayudar a aquellos que han estado utilizando las listas automáticas de permitidos en versiones de MDaemon previas a la 11, con esto se purgarán los contactos que se agregaron con la función de lista de permitidos. En versiones previas de MDaemon las direcciones se agregaban a los contactos principales en lugar de incorporarse a la carpeta de lista de remitentes permitidos. Esto podría originar que los usuarios tuvieran muchos registros en sus contactos que preferirían no tener ahí.

Considere esta opción cuidadosamente antes de utilizarla, ya que los contactos que solo tienen cuenta de correo podrían ser legítimos de todas formas.

Reenviar a allowlist@ actualiza los remitentes permitidos
Cuando se habilita esta opción, las cuentas que usan "*El Filtro de Spam utiliza contactos personales y remitentes permitidos y bloqueados*" en la pantalla de Ajustes del Editor de Cuentas, pueden reenviar mensajes a `allowlist@<dominio>` y hacer que MDaemon añada al remitente del mensaje

original a la lista blanca de la cuenta. La dirección a incluir en lista de permitidos se toma del encabezado `From` del mensaje reenviado.

Los mensajes reenviados a `allowlist@<dominio>` deben ser reenviados como adjuntos del tipo `message/rfc822`, y deben ser recibidos por MDaemon vía SMTP de una sesión autentificada. Los mensajes reenviados que no cumplan estos requisitos no serán procesados.

Puede cambiar la dirección que usa MDaemon editando la siguiente llave en el archivo `CFILTER.INI`:

```
[SpamFilter]
WhiteListAddress=MiListaBlanca@
```

Nota: el último carácter debe ser "@".

Reenviar a blocklist@ actualiza los remitentes bloqueados
Cuando se habilita esta opción, las cuentas que usan "*El Filtro de Spam utiliza contactos personales y remitentes permitidos y bloqueados*" en la pantalla de Ajustes del Editor de Cuentas, pueden reenviar mensajes a `blocklist@<dominio>` y hacer que MDaemon agregue el remitente original del mensaje a la lista de bloqueados de la cuenta. La dirección incorporada a lista de bloqueados se toma del encabezado `From` del mensaje reenviado.

Los mensajes reenviados a `blocklist@<dominio>` deben ser reenviados como adjuntos del tipo `message/rfc822` y deben ser recibidos por MDaemon vía SMTP desde una sesión autentificada. Los mensajes reenviados que no cumplan con estos requerimientos no serán procesados

Actualizar el motor Bayesiano con copias de los mensajes en lista de permitidos
Haciendo clic en esta casilla los mensajes en lista de permitidos serán copiados automáticamente a la carpeta de aprendizaje Bayesiano no-Spam (designada en la pantalla Bayesiano 680). Esto ayuda a automatizar el proceso de proveer al motor Bayesiano de muestras de mensajes no-Spam. Si se provee al motor Bayesiano regularmente con nuevos ejemplos de no-Spam del que aprender se incrementará su fiabilidad con el tiempo y ayudará a reducir el número de falsos positivos (i.e. mensajes que se clasifican erróneamente como Spam).

Para calificar para esta opción, el mensaje entrante debe ir dirigido a un usuario local y el remitente debe ser alguien en su libreta de direcciones o en su carpeta de remitentes permitidos. Si el mensaje es saliente, entonces es el destinatario quien debe estar en la libreta de direcciones o en los remitentes permitidos. Si no desea que los mensajes salientes puedan utilizarse, utilice el Bloc de Notas y edite las siguientes configuraciones del archivo `MDaemon.ini`:

```
[SpamFilter]
UpdateHamFolderOutbound=No (por defecto = Yes)
```

Cuando un mensaje cumple, se copia en la carpeta de aprendizaje Bayesiano de no-Spam, aunque la programación de aprendizaje bayesiano esté deshabilitada en la pantalla de Bayesiano. Así, cuando el aprendizaje bayesiano se activa posteriormente, o cuando el aprendizaje se activa manualmente, un conjunto de mensajes no-Spam estarán ya listos para el análisis. No todos los mensajes que cumplan, sin embargo, se copiarán a la carpeta de aprendizaje. Cuando la funcionalidad se activa, MDaemon copiará los mensajes que cumplan hasta que se alcance un número determinado. Subsecuentemente copiará mensajes únicos a intervalos designados. Por defecto, los primeros 200 mensajes que cumplan se

copiarán y luego pasará a copiar cada diez mensajes. El número inicial por copiar lo define la opción *"Se necesitan ejemplos de no-Spam antes de que sea posible la puntuación bayesiana"* de la pantalla Aprendizaje Automático 684. Si cambia esta configuración también cambiará este valor. Si desea cambiar el intervalo por el que los mensajes subsiguientes son copiados, puede hacerlo editando la siguiente configuración en el archivo `MDaemon.ini`:

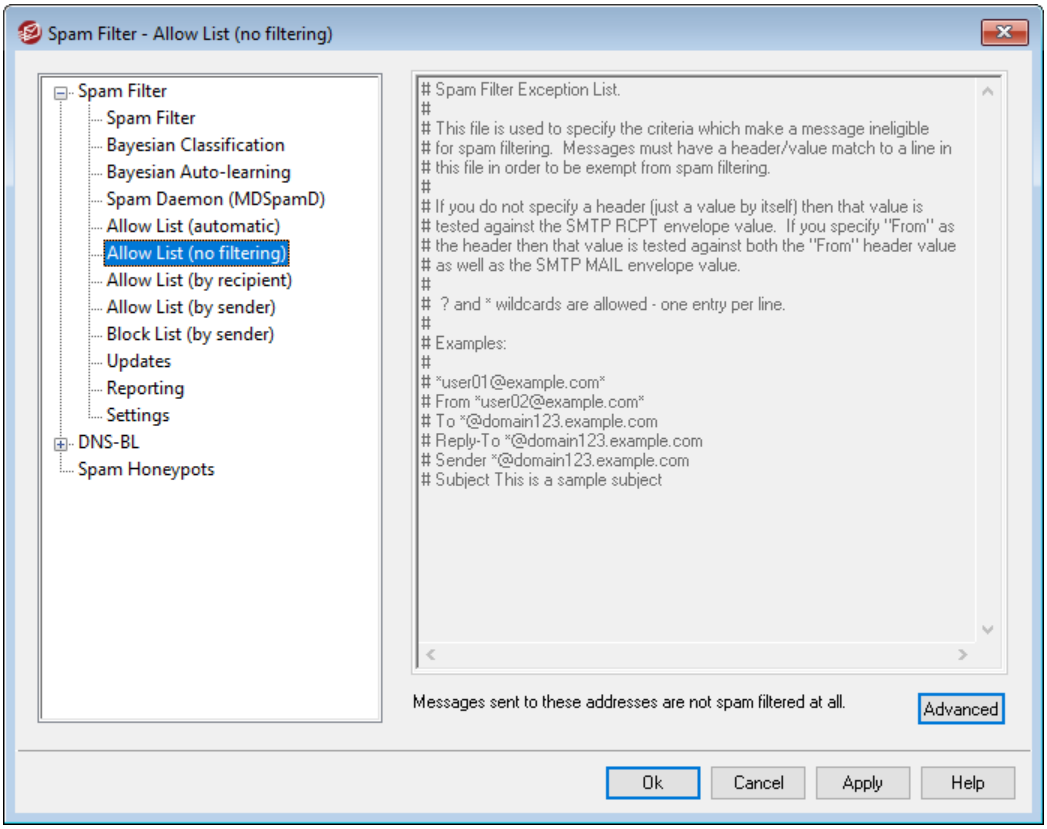
```
[SpamFilter]
HamSkipCount=10 (por defecto = 10)
```

Finalmente, una vez el número total designado de mensajes se haya copiado, el proceso empezará nuevamente — se copiarán 200 y luego uno de cada diez (o el valor alternativo si ha cambiado dicha configuración). Por defecto, el proceso se restablecerá después de que se hayan copiado 500 mensajes cualificados. Puede cambiar este valor editando la siguiente configuración en el archivo `MDaemon.ini`:

```
[SpamFilter]
HamMaxCount=500 (por defecto = 500)
```

Esta opción no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. La actualización de estas Listas se realizará en el otro servidor. Vea: Spam Daemon 686, para más información.

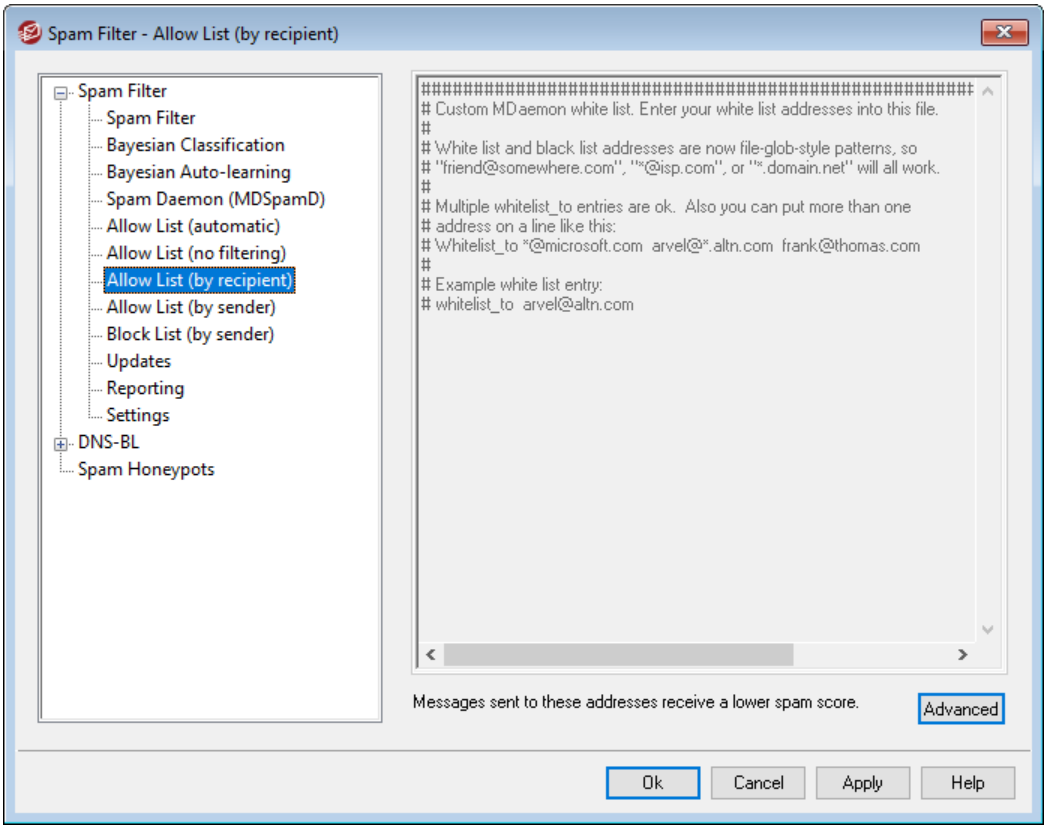
4.7.1.6 Lista de Permitidos (no filtrar)



Los mensajes enviados a estas direcciones no son filtrados
Dé clic en **Avanzado** en esta pantalla para definir los destinatarios que desea estén exentos del filtro de spam. Los mensajes destinados a estas direcciones no serán procesados por el filtro de spam.

Esta pantalla no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. La actualización de Listas Blancas se realizará en el otro servidor. Vea: Spam Daemon 686, para más información.

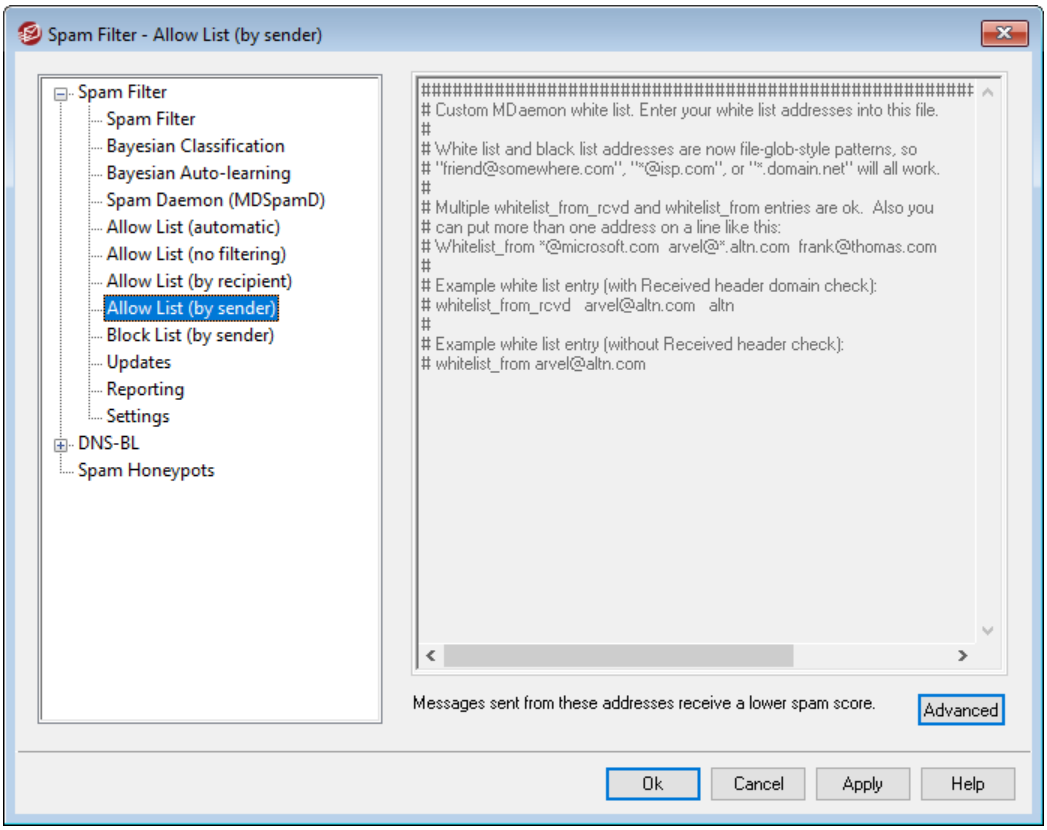
4.7.1.7 Lista de Permitidos (por destinatario)



Los mensajes enviados a estas direcciones reciben puntos positivos
Dé clic en **Avanzado** para agregar direcciones a esta lista. Esta lista es similar a *Lista de Permitidos (no filtrar)* 692, excepto que en lugar de exentar los mensajes al destinatario del procesamiento del Filtro de Spam, serán procesados pero su Puntaje de Filtro de Spam 676 se reducirá por la cantidad especificada en la pantalla Ajustes del Filtro de Spam 698. Por esto, el incluir una dirección en esta lista blanca no garantiza que un mensaje hacia esa dirección no sea considerado como Spam. Por ejemplo, si su umbral de puntaje de Spam está configurado en 5.0, el valor de lista blanca se define en 100 y llega un mensaje que alcanza un puntaje de Spam de 105.0 o más antes de que se reste el valor de lista blanca, entonces el puntaje final de Spam del mensaje será de por lo menos 5.0, con lo que se considerará como Spam. Sin embargo, esto es muy poco probable, porque rara vez el Spam tiene un valor tan alto a menos que contenga otros elementos que le generen un puntaje excepcionalmente alto, tal como una dirección en lista de bloqueados.

Esta pantalla no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. La actualización de Listas de Filtro de Spam se realizará en el otro servidor. Vea: Spam Daemon 686, para más información.

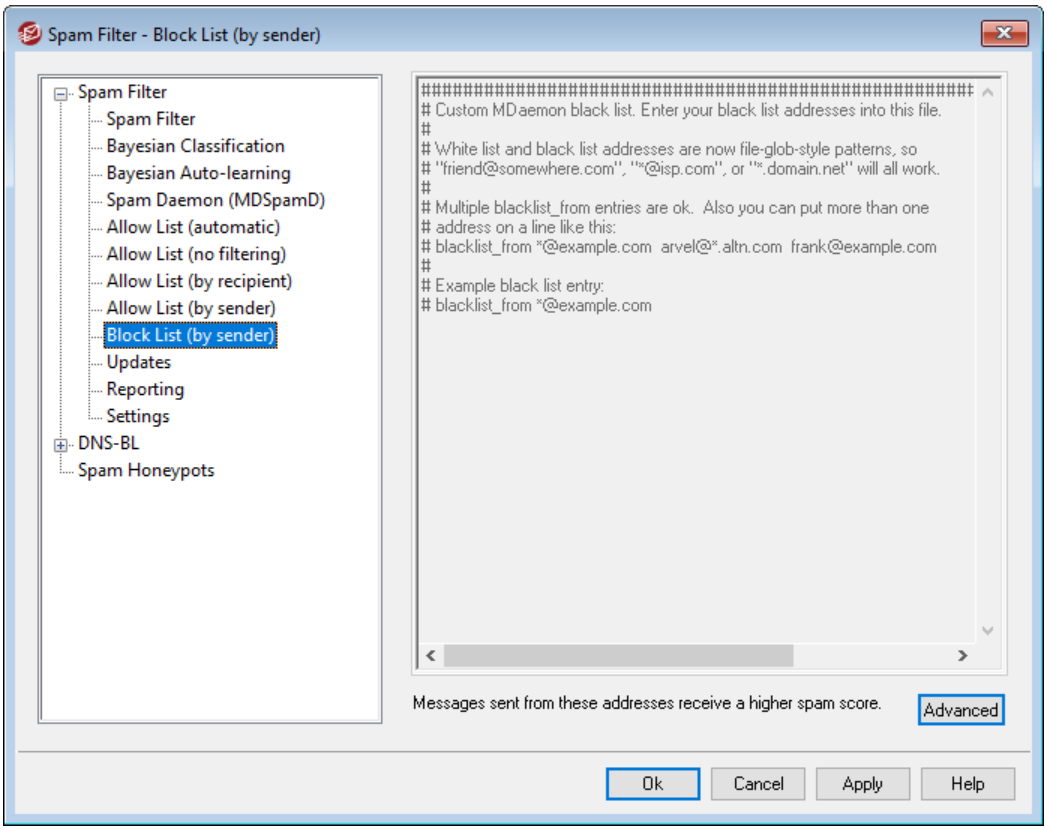
4.7.1.8 Lista de Permitidos (por remitente)



Los Mensajes enviados desde estas direcciones reciben un puntaje favorable
Dé clic en **Avanzado** para agregar direcciones a esta lista. Esta lista de permitidos es similar a *Lista de Permitidos (por destinatario)* 693, excepto que la reducción del puntaje de Spam se basa en *el remitente* del mensaje en lugar del destinatario. Los mensajes de estos remitentes verán su Puntaje de Filtro de Spam 676 reducido por la cantidad especificada en la pantalla Ajustes del Filtro de Spam 698. Por esto, el incluir una dirección en la lista blanca no garantiza en automático que un mensaje enviado a esa dirección no será considerado Spam. Por ejemplo, si su umbral de puntaje de Spam se establece en 5.0 y el valor de lista blanca es 100 y posteriormente llega un mensaje con contenido particularmente alto de Spam y obtiene un puntaje de 105.0 o superior antes de que se reste el valor de lista blanca, entonces el puntaje final de Spam del mensaje será de por lo menos 5.0 lo que lo identificará como Spam. Esto es muy poco probable, sin embargo, porque rara vez el Spam tiene un valor tan alto a menos que contenga elementos que eleven excepcionalmente el puntaje tales como direcciones en lista de bloqueados.

Esta pantalla no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. Esta Lista se actualizaré en el otro servidor. Vea: Spam Daemon 686, para más información.

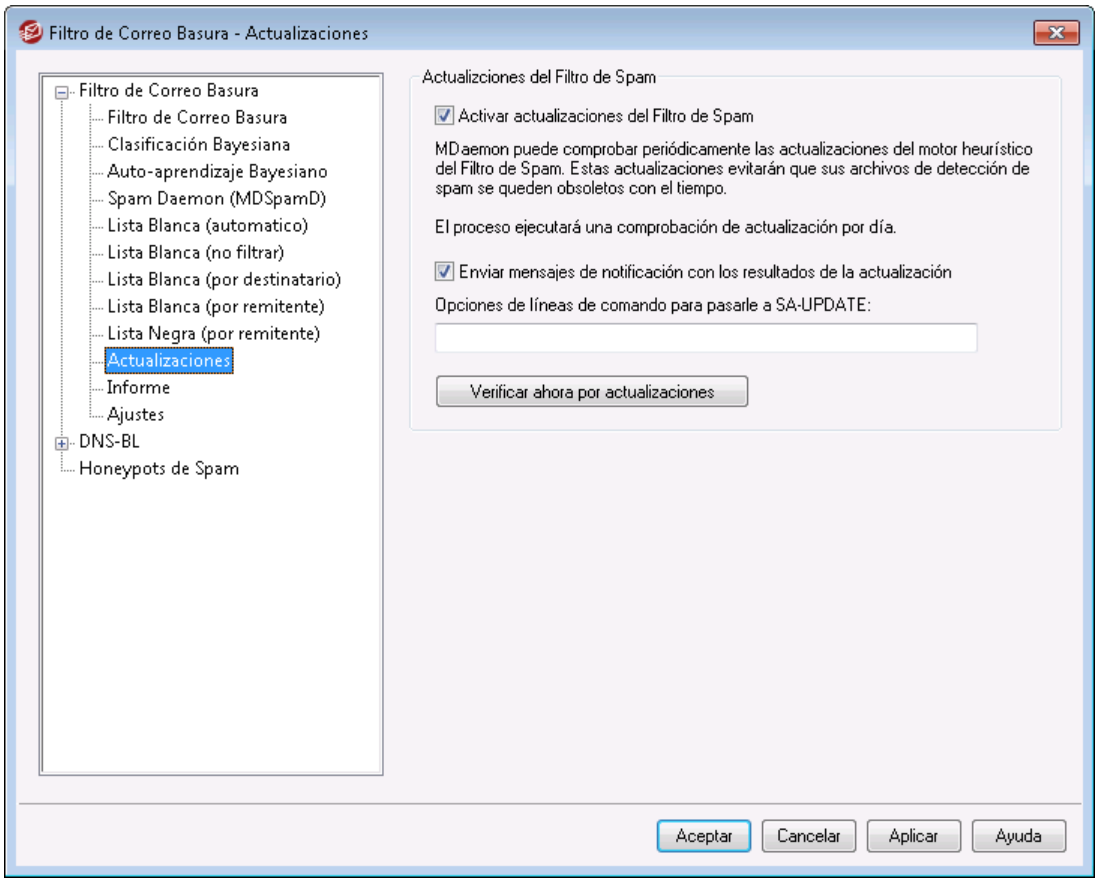
4.7.1.9 Lista de Bloqueados (por remitente)



Los mensajes enviados desde estas direcciones reciben una puntuación en detrimento
Dé clic en **Avanzado** para agregar direcciones a esta lista. Los mensajes provenientes de direcciones en esta lista de bloqueados verán incrementado su Puntaje de Filtro de Spam 676 con la cantidad especificada en la pantalla Ajustes del Filtro de Spam 698, haciendo típicamente que sean marcados como Spam. Por ejemplo, si llega un mensaje de un remitente en lista de bloqueados, pero va dirigido a un destinatario en lista de permitidos, entonces los modificadores de puntaje pueden neutralizarse y hacer que el mensaje tenga un puntaje final inferior al umbral de puntaje de Spam. Esto también puede suceder si ha definido el puntaje de lista de bloqueados en una cantidad particularmente baja.

Esta pantalla no está disponible cuando se configura MDaemon para que use otro Daemon de Spam de MDaemon de otro servidor (MDSpamD) para el proceso de Filtrado Spam. El Filtro de Spam será actualizado en el otro servidor. Vea: Spam Daemon 686, para más información.

4.7.1.10 Actualizaciones



Actualizaciones del Filtro de Spam

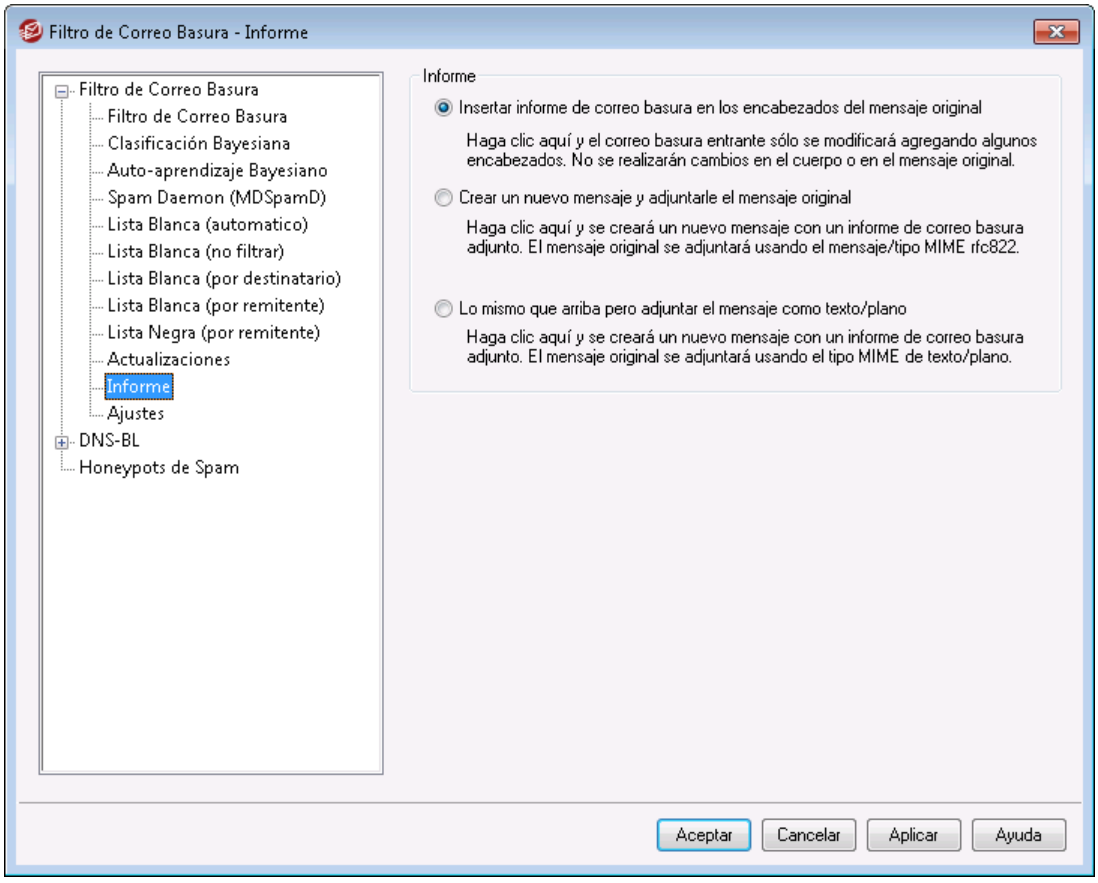
Activar actualizaciones del Filtro de Spam
Haga clic en esta casilla si quiere que el Filtro de Spam se actualice automáticamente. Una vez al día MDaemon verificará si existen actualizaciones disponibles para el motor heurístico del Filtro de Spam, y si es así las descargará e instalará automáticamente.

Enviar mensaje de notificación con los resultados de la actualización
Utilice esta opción si desea enviar un mensaje de correo a los administradores siempre que se actualice el Filtro de Spam, conteniendo los resultados de la actualización. Esta opción es la misma que "*Enviar notificaciones de Actualización del Filtro de Spam a los Administradores*" que se localiza en: Filtro de Contenido » Notificaciones.

Opciones adicionales por línea de comando para SA-UPDATE
Utilice esta opción avanzada si desea pasar opciones por línea de comando a SA-UPDATE.

Comprobar si hay una actualización ahora
Haga clic en este botón para comprobar inmediatamente si existen actualizaciones de las reglas del Filtro de Spam.

4.7.1.11 Informe



Los Reportes del Filtro de Spam no están disponibles si ha configurado a MDaemon para utilizar el Daemon de Spam de otro servidor para el proceso de Filtrado de Spam. Los Reportes del Filtro de Spam serán controlados por los parámetros del otro servidor. Vea la pantalla del Daemon de Spam para más información.

Informe

Inserte el reporte de Spam en los encabezados del mensaje original
Esta es la opción de reportes por omisión. Utilícela si desea que el Filtro de Spam inserte un reporte de Spam en el encabezado de cada mensaje. El ejemplo siguiente muestra un reporte de Spam sencillo:

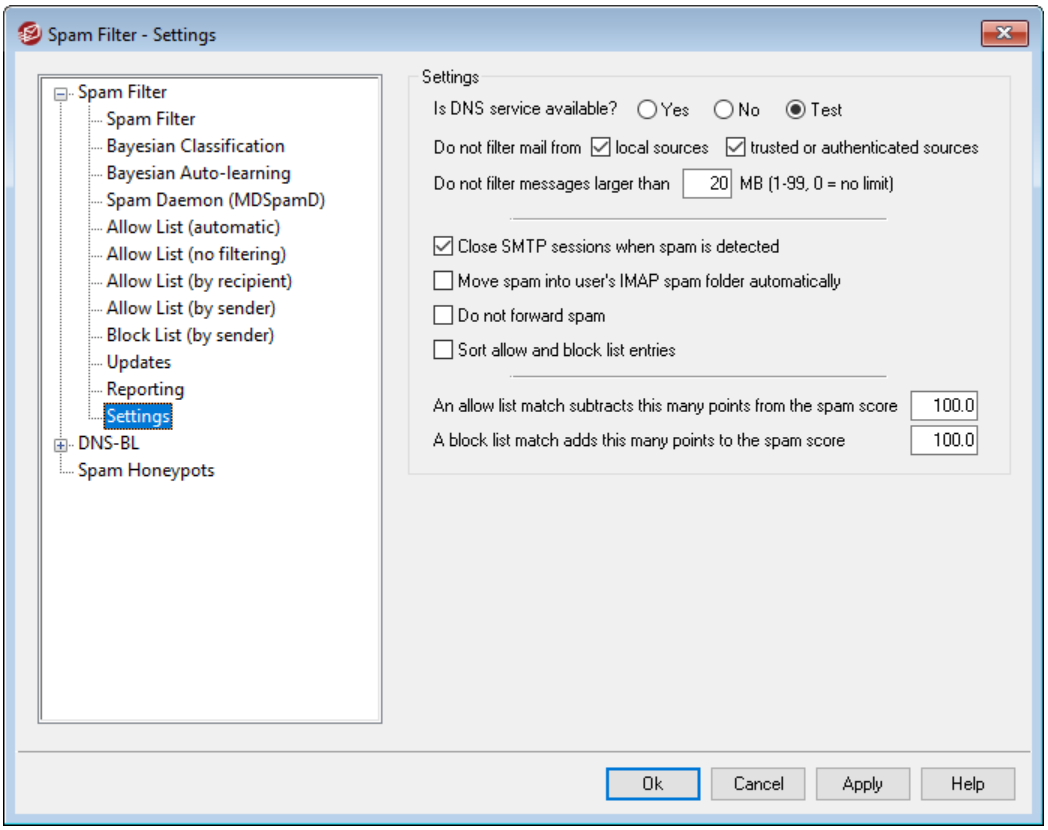
```
X-Spam-Report: ---- Start Spam Filter results
  5.30 points, 5 required;
  * -5.7 -- Message-Id indicates the message was sent from MS
Exchange
  *  2.0 -- Subject contains lots of white space
  * -3.3 -- Has a In-Reply-To header
```

```
  *  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
```

Crear un mensaje nuevo e incluir el mensaje original como adjunto
Seleccione esta opción de reportes si desea que el spam genere un nuevo mensaje de correo que se generará conteniendo el reporte de spam. El mensaje original de spam será incluido en el mensaje como archivo adjunto.

Igual que arriba, pero adjuntar el mensaje en archivo de texto plano
Al igual que la opción previa, en este caso se generará el reporte de spam como un mensaje nuevo incluyendo el mensaje de spam original como adjunto. La diferencia es que el mensaje original será incluido utilizando texto plano o tipo MIME. Dado que en ocasiones el spam contiene código HTML que es único para cada mensaje y que potencialmente puede revelar al spammer la dirección de correo y dirección IP que lo abrió, este método puede impedir que ocurra esto convirtiendo el código HTML en texto plano.

4.7.1.12 Ajustes



Ajustes

¿El servicio DNS está disponible?
Estas opciones le permiten seleccionar si el servicio DNS está disponible para el Filtro de Spam durante el procesamiento de mensajes. Puede escoger una de las opciones siguientes:

Si - El DNS está disponible. SURBL/RBL y otras reglas que requieren conectividad DNS serán utilizadas.

No - El DNS no está disponible. Las reglas de Filtrado de Spam que requieren DNS no serán utilizadas.

Prueba - Se probará la disponibilidad del DNS y si se detecta será utilizado. Este es el valor por omisión.

No filtrar correo de...

recursos locales
Dé clic en esta casilla si desea que los mensajes de usuarios y dominios locales estén exentos de filtrado.

recursos confiables o autentificados
Habilite esta opción si desea que los mensajes enviados desde dominios confiables o remitentes autentificados estén exentos de filtrado de spam.

No filtrar mensajes mayores de [XX] MB (1-99, 0 = sin límite)
Es típico que los mensajes de spam sean relativamente pequeños dado que el objetivo de los spammers es entregar tantos mensajes como sea posible en el menor lapso. Si desea que los mensajes mayores de cierto tamaño estén exentos del filtrado de spam, especifique aquí esa cantidad (en MB). Utilice "0" si no desea limitar el tamaño del mensaje en el filtro de spam.

Cerrar sesiones SMTP cuando se detecte SPAM
Esta opción está habilitada por omisión y cerrará una sesión SMTP si el escaneo en línea detecta un mensaje de spam.

Mover automáticamente el spam a la carpeta IMAP de spam del usuario
Dé clic en esta opción y MDaemon automáticamente colocará cada mensaje que el Filtro de Spam determine que es spam, en la carpeta IMAP denominada "`Spam`" (si tal carpeta existe). También creará automáticamente la carpeta para cada nueva cuenta de usuario que se dé de alta.

Cuando le dé clic a esta opción también se le preguntará si desea que MDaemon genere esta carpeta para cada uno de los usuarios existentes Si selecciona "Si", la carpeta será creada para todos los usuarios. Si selecciona "No" entonces solamente se creará la carpeta para los usuarios nuevos. Las carpetas que ya existen para algunos o todos los usuarios no serán alteradas o afectadas por esta opción de ninguna forma.

No reenviar spam
Verifique esta casilla si no quiere permitir que los mensajes de spam sean reenviados.

Ordenar registros de lista de permitidos y de bloqueados
Utilice esta opción si desea mantener sorteados los registros de Lista Blanca y Negra del Filtro de Spam. **Nota**: si ha agregado comentarios al archivo (líneas

que inician con #), cuando habilite esta opción se ordenarán estas líneas al inicio del archivo. Esta funcionalidad está deshabilitada por omisión. Si la habilita, el ordenamiento tendrá lugar cuando ocurra la siguiente modificación a la lista blanca o negra.

Las opciones restantes de esta pantalla no están disponibles cuando ha configurado MDaemon a utilizar el Daemon de Spam de MDaemon (MDSpamD) para procesar el Filtrado de Spam. Vea la pantalla Daemon de Spam 686 para más información.

Una coincidencia en lista de permitidos resta esta cantidad de puntos del puntaje de spam
Colocar una dirección en la Lista Blanca (por destinatario) 693 o la Lista Blanca (por remitente) 694 no garantiza automáticamente que un mensaje de o para esa dirección no sea considerado spam. En lugar de esto, a esas direcciones simplemente se les restará la cantidad especificada en este control de su puntaje de spam. Por ejemplo, si el umbral del puntaje de spam se define como 5.0 y este valor se fija en 100, al momento que llega un mensaje particularmente excesivo de spam, obtiene un puntaje de 105.0 o mayor antes de que el valor de la lista de permitidos sea substraído, entonces el puntaje final de spam para el mensaje será de por lo menos 5.0 — indicando que es spam. Esto pasaría en raras ocasiones, sin embargo, porque no es frecuente que el spam alcance valores tan altos a menos que contenga elementos que generen puntajes excepcionalmente altos tales como una dirección en lista de bloqueados. Por supuesto, si configura muy bajo el valor a restar por estar en lista de permitidos, la situación descrita ocurrirá con mayor frecuencia.

Si desea que los mensajes dirigidos a ciertos destinatarios no pasen por el Filtro de Spam en lugar de ajustar sus puntajes, incluya esos destinatarios en la pantalla Lista de Permitidos (no filtrar) 692. También puede excluir a los mensajes del puntaje del Filtro de Spam con base en el remitente utilizando las opciones en la pantalla Lista de Permitidos (automática) 688.

Una coincidencia en lista de bloqueados agrega esta cantidad de puntos al puntaje de spam
Este valor se agrega al puntaje de spam de los mensajes provenientes de direcciones registradas en la pantalla Lista de Bloqueados (por remitente) 695. Al igual que en la opción de lista de permitidos arriba mencionada, el incluir una dirección en la lista negra del Filtro de Spam no garantiza que el mensaje proveniente de esa dirección será considerado spam. En lugar de esto, el valor definido en esta opción será agregado al puntaje de spam del mensaje, que a su vez será utilizado para determinar si el mensaje es o no spam.

4.7.2 Listas de Bloqueados por DNS (DNS-BL)

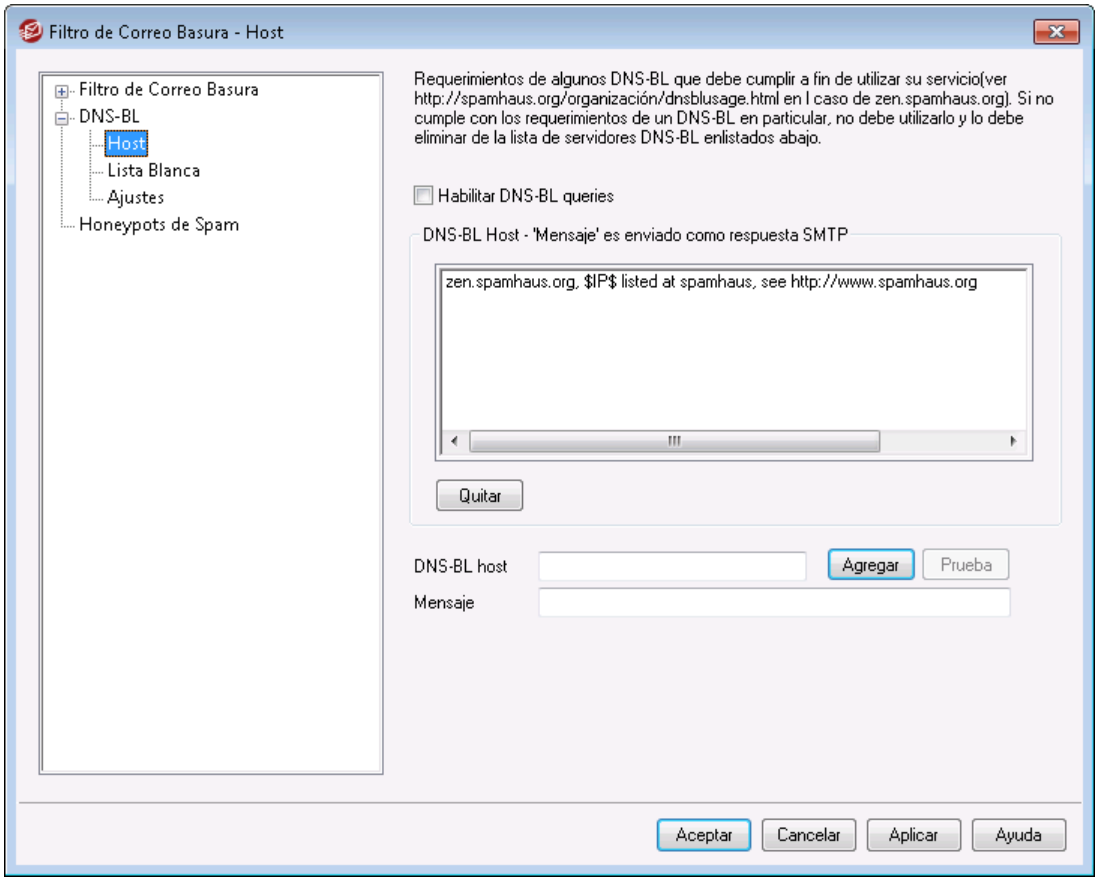
Las Listas de Bloqueados por DNS (DNS-BL) pueden usarse para ayudar a prevenir que correo Spam llegue a sus usuarios. Esta funcionalidad de seguridad le permite especificar diversos servicios de listas de DNS bloqueados (que mantienen listas de servidores conocidos como retransmisores de Spam) que serán verificados cada vez que alguien intente enviar un mensaje a su servidor. Si la IP de conexión se encuentra en la lista de bloqueados de alguno de dichos servicios, el mensaje(s) será rechazado o marcado de acuerdo con las configuraciones de la pantalla Ajustes 704.

Las Listas de bloqueados por DNS incluyen una Lista de Permitidos para designar direcciones IP que desea hacer exentas de consultas DNS-BL. Antes de activar DNS-BL debería asegurarse que su rango de IP local esté en la lista de permitidos para prevenir búsquedas en dichas direcciones. "127.0.0.1" está exenta y por lo tanto no necesita ser añadida a la lista.

Ver:

Hosts DNS-BL 701
Ajustes DNS-BL 704
Lista de Permitidos DNS-BL 703

4.7.2.1 Hosts



Hosts DNS-BL

Habilitar consultas DNS-BL

Active esta opción si desea comprobar los mensajes entrantes con Listas de Bloqueados por DNS. MDaemon consultará cada uno de los hosts listados cuando realice una búsqueda DNS-BL en la IP de envío. Si el host contesta que la consulta da un resultado positivo, MDaemon puede marcar el menaje o rechazar su aceptación, dependiendo de qué opciones tenga habilitadas en la pantalla Ajustes de DNS-BL 704.

Quitar

Seleccione una entrada de la lista de servicios DNS-BL y haga clic en este botón para quitarla de la lista.

DNS-BL host

Si desea añadir un nuevo host al que consultar para direcciones IP bloqueadas, introdúzcalo aquí.

Probar

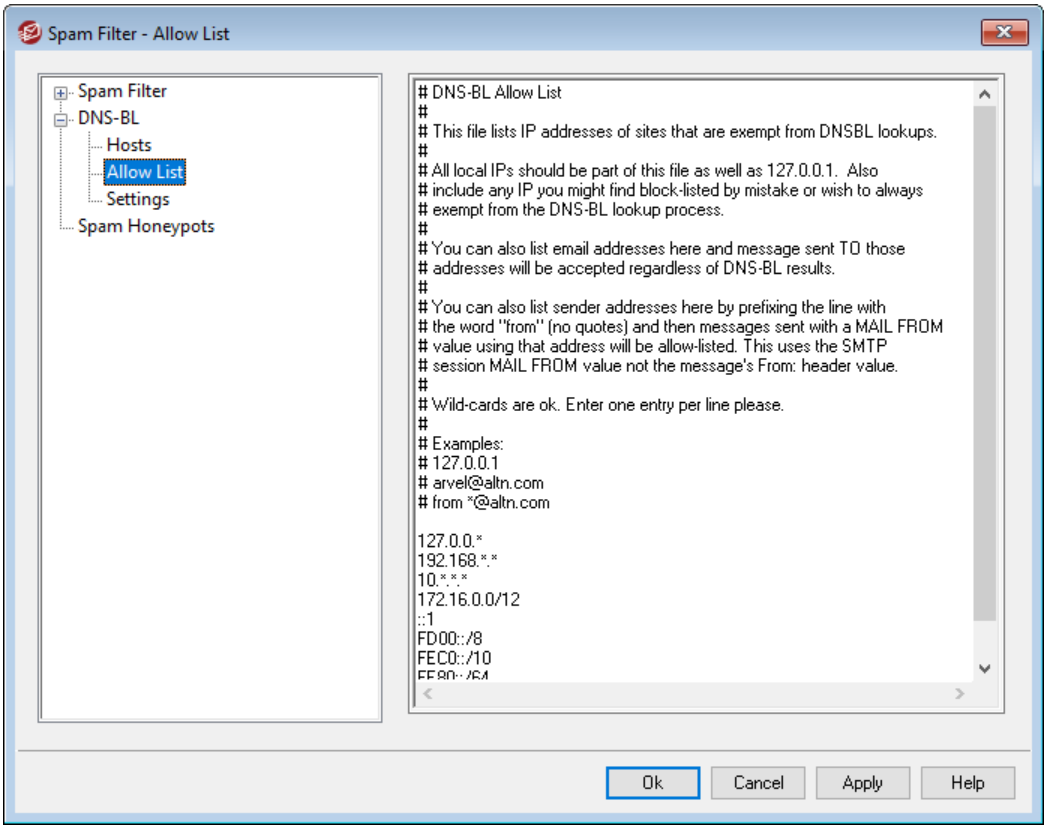
Registre un host en la opción *DNS-BL host* y dé clic en este botón para probar consultando 127.0.0.2.

Mensaje

Este es el mensaje que se puede enviar durante la sesión SMTP cuando una dirección IP ha sido bloqueada por el host DNS-BL listado arriba. Este mensaje corresponde a la opción *...y responder con 'Mensaje' en vez de 'usuario desconocido'* ubicada en la pantalla Ajustes de DNS-BL 704.

Agregar
Después de introducir un host y un mensaje de retorno, haga clic en este botón para añadirlo a la lista de hosts de DNS-BL.

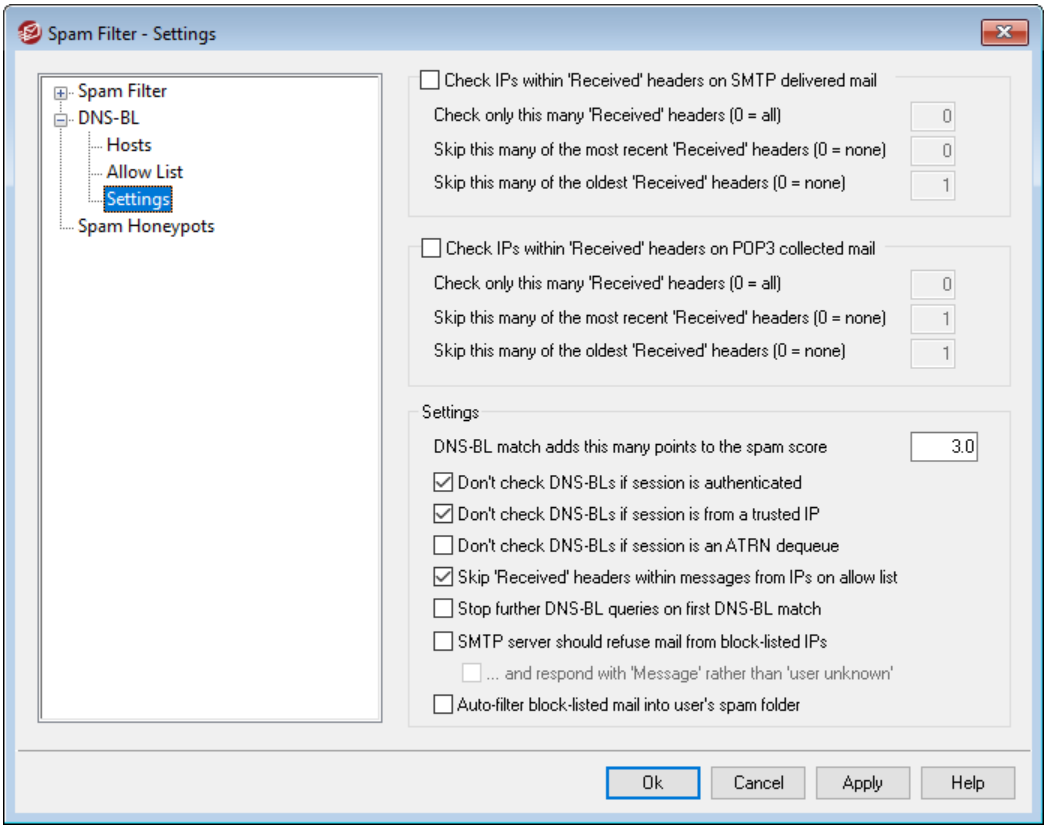
4.7.2.2 Lista de Permitidos



Use esta pantalla para definir direcciones IP que estarán exentas de las consultas de bloqueados por DNS . Deberá incluir siempre su rango de IPs locales para evitar que DNS-BL valide mensajes originados desde usuarios y dominios locales (p. ej. `127.0.0.*`, `192.168.*.*`, y demás). También puede incluir en la lista direcciones de correo. Cuando un mensaje es dirigido a una de ellas, entonces ese mensaje se aceptará sin importar los resultados de la consulta DNS-BL. Finalmente, también puede exentar remitentes específicos ingresando "From *sender@example.com*" en la lista. Esta dirección debe coincidir con el valor "MAIL FROM" de la sesión SMTP, no el encabezado "From:".

Coloque solo una dirección en cada línea. Se permiten comodines.

4.7.2.3 Ajustes



Comprobar IP en los encabezados 'Recibido' en el correo SMTP entregado
Haga clic en esta opción si desea que las Listas de Bloqueados por DNS comprueben la dirección IP estampada en los encabezados "`Received`" de los mensajes recibidos vía SMTP.

Verificar sólo esta cantidad de encabezados 'Recibido' (0=todos)
Especifique el número de encabezados "`Received`" que quiere que DNS-BL compruebe, empezando por el más reciente. Un valor de "0" significa que todos los encabezados "`Received`" serán comprobados.

Omitir estos de los encabezados 'Recibido' más recientes (0=ninguno)
Use esta opción si quiere que DNS-BL se salte uno más de los encabezados `Received` recientes cuando compruebe los mensajes SMTP.

Saltar estas de las cabeceras de 'Recibidos' más antiguas (0=ninguna)
Use esta opción si quiere que DNS-BL se salte uno o más de los encabezados Received antiguos cuando compruebe los mensajes SMTP.

Comprobar IPs de las cabeceras 'Recibido' del correo POP3 recogido
Cuando este control está activado, DNS-BL comprobará las direcciones IP estampadas en los encabezados "`Received`" de los mensajes recolectados vía DomainPOP o MultiPOP.

Verificar sólo esta cantidad de encabezados 'Recibido' (0=todos)
Especifique el número en encabezados '`Received`' que quiere que DNS-BL compruebe, empezando con el más reciente. Un valor de "0" significa que todos los encabezados 'Received' serán comprobados.

Omitir estos de los encabezados 'Recibido' más recientes (0=ninguno)
Use esta opción si quiere que DNS-BL se salte uno o más de los encabezados `Received` recientes cuando compruebe los mensajes DomainPOP y MultiPOP. Dado que a veces es necesario saltarse el encabezado más reciente `Received` en el correo recolectado por POP3, como por ejemplo DomainPOP, la opción se establece por defecto en "1".

Saltar estas de las cabeceras de 'Recibidos' más antiguas (0=ninguna)
Use esta opción si quiere que DNS-BL se salte uno o más de los encabezados Received cuando compruebe mensajes DomainPOP y MultiPOP:

Ajustes

Coincidencia en DNS-BL agrega estos puntos al puntaje de Spam
Utilice esta opción para especificar el valor que se agregará al puntaje de Spam 676 del mensaje cuando exista una coincidencia en una Lista Negra DNS (DNS-BL). En ocasiones, la revisión heurística de un mensaje por el Filtro de Spam puede no dar un puntaje suficientemente alto para considerarlo como spam, pero una consulta DNS-BL puede indicar que sí lo es. Por esto, al agregar este valor al puntaje de spam se ayuda a interceptar algunos mensajes de spam que de otra manera podrían pasar sin ser detectados. Por omisión, la coincidencia en DNS-BL agrega 3.0 puntos al puntaje de spam

No ejecutar el proceso DNS-BL si la sesión es...

autentificada
Haga clic en esta casilla si quiere que las sesiones que autenticadas usando el comando AUTH estén exentas de las consultas de DNS-BL.

de IPs confiables
Haga clic en esta casilla si quiere que las direcciones que estén listadas en la pantalla de Hosts de Confianza 519 estén exentas de las consultas DNS-BL.

un desencolamiento ATRN
Habilite esta opción si no desea realizar consultas DNS-BL sobre correo recolectado desde sesiones de desencolamiento ATRN. Este ajuste se encuentra deshabilitado por omisión pero usted lo puede habilitar si, por ejemplo, su host inteligente ya está realizando verificaciones DNS-BL en su correo almacenado.

Omitir los encabezados 'Recibido' de los mensajes enviados desde los sitios de la lista de permitidos
Cuando esta opción está habilitada, DNS-BL no comprobará los encabezados "Received" dentro de los mensajes que provengan de direcciones IP que estén listadas en la Lista de Permitidos de DNS-BL 703.

Detener las consultas DNS-BL subsecuentes al ocurrir la primera coincidencia DNS-BL
A veces existen múltiples hosts contenidos en las cabeceras de cada mensaje que DNS-BL procesa, y se ejecutan múltiples consultas a servicios DNS-BL. Por defecto, DNS-BL continuará consultando a dichos servicios para todos los hosts en el mensaje independientemente del número de coincidencias encontradas. Haga clic en esta opción si quiere que DNS-BL pare de consultar a los servicios para un mensaje determinado tan pronto como encuentre una coincidencia.

El servidor SMTP debe rechazar correo de las IPs en lista de bloqueados
Por defecto esta casilla está desmarcada, lo que significa que los mensajes de las direcciones IP de lista de bloqueados no serán rechazados durante la sesión SMTP, pero tendrán una cabecera X-MDDNSBL-Result insertada. Puede usar el Filtro de Contenido después para buscar mensajes con esta cabecera y hacer con ellos lo que le parezca. También puede usar la opción siguiente de "*Auto-filtrar el correo en lista de bloqueados en la carpeta de Spam*" para filtrar mensajes automáticamente en la carpeta de spam de cada usuario. Marque esta casilla si desea que MDaemon rechace mensajes de direcciones IP en lista de bloqueados en lugar de marcarlos.

Dado que algunas direcciones pueden estar en lista de bloqueados por error, deberá actuar con precaución antes de escoger rechazar mensajes en lugar de simplemente marcarlos. Tampoco sirve de nada que hacerlo además de marcar un mensaje, puede en su lugar ajustar la puntuación de Spam basado en los resultados de DNS-BL vía la opción *Una coincidencia de DNS-BL suma muchos puntos a la puntuación de correo basura* ubicada en el Filtro de Spam 676.

...y responder con 'Mensaje' en vez de 'usuario desconocido'
Haga clic en esta opción si quiere que el mensaje específico que haya designado en el Host DNS-BL 701 se transmita durante la sesión SMTP siempre que una dirección IP resulte en lista de bloqueados. De otro modo se pasará un mensaje de "usuario desconocido" en su lugar. Esta opción sólo está disponible si ha seleccionado la opción anterior de "*El servidor SMTP debe rechazar correo de las IPs de la lista de bloqueados*".

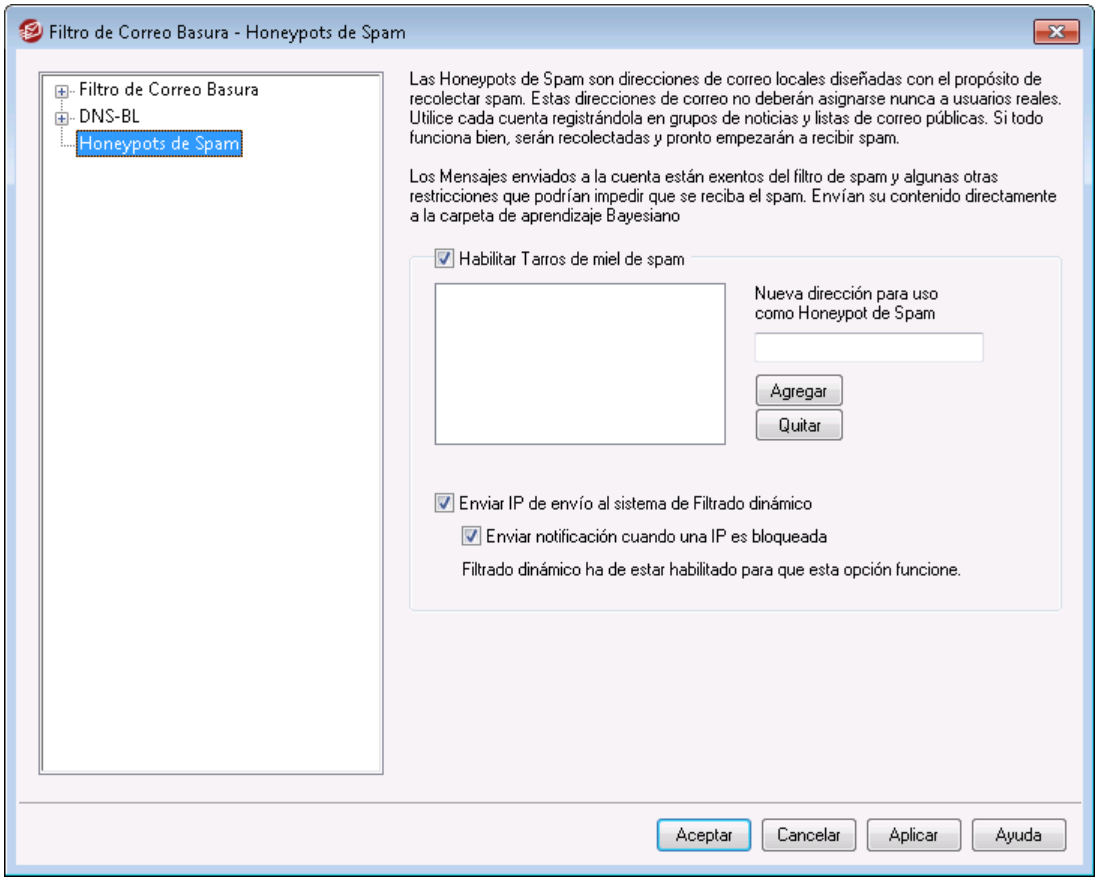
Autofiltrar el correo en lista de bloqueados en la carpeta de Spam
Haga clic en esta opción y una carpeta IMAP "Junk E-mail" se creará para todas las futuras cuentas de usuario que le añada a MDaemon. MDaemon también creará un filtro de correo para cada uno de dichos usuarios, que buscará el encabezado X-MDDNSBL-Result y colocará los mensajes que contengan dicho encabezado en la carpeta de Spam del usuario. Cuando haga clic en esta opción también se le preguntará si quiere o no que MDaemon cree dicha carpeta y filtre cada una de las ya existentes cuentas de usuario. Vea *Autogenerar una carpeta de Spam y filtro para cada cuenta*.

Autogenerar una Carpeta de Spam y Filtro para Cada Cuenta

MDaemon puede crear automáticamente una carpeta IMAP "Junk E-mail" para cada cuenta y generar un filtro de correo que moverá los mensajes a dicha carpeta siempre que encuentre un encabezado X-MDDNSBL-Result. Siempre que haga clic en la opción *Auto-filtrar el correo en lista de bloqueados en la carpeta de Spam*, se le presentará la opción de crear la carpeta y acompañarla de un filtro para todas las cuentas. Simplemente escoja "sí" en el diálogo para crear las carpetas y filtros. Aunque no es a prueba de tontos, esta es una manera sencilla y generalmente confiable de ayudar a que sus usuarios identifiquen rápidamente los mensajes de Spam—puede prevenir efectivamente que el Spam se mezcle con todo el correo legítimo. Sólo necesitarán revisar ocasionalmente los contenidos de su carpeta de Spam para asegurarse que no se ha colocado accidentalmente un mensaje importante allí (lo que puede suceder a veces). Cuando se crean las carpetas y los filtros para sus cuentas, si MDaemon encuentra que una cuenta ya tiene un filtro

que comprueba la existencia del encabezado X-MDDNSBL-Result no se tomará ninguna acción y no se creará ningún filtro para dicha cuenta. Si quiere que el nombre de la carpeta IMAP sea otro que "Junk E-mail", puede cambiar la configuración por defecto editando la opción *Nombre de la carpeta de correo basura predeterminado* ubicada en la pantalla Sistema 494 bajo Configurar » Preferencias.

4.7.3 Honeypots de Spam



Los Honeypots de Spam (Tarros de Miel de Spam) (ubicados en Seguridad » Filtro de Correo Basura » Honeypots de Spam) se utilizan para definir direcciones de correo locales designadas con el propósito para recolectar Spam. Estos Honeypots de Spam no son cuentas válidas de MDaemon o alias de direcciones y nunca deberán usarse para enviar o recibir correo legítimo. Pero, publicando una dirección del honeypot de Spam en un grupo de noticias, lista pública de correo, u otro recurso del que los spammers recolecten habitualmente direcciones, deberá empezar a ver mensajes entrantes dirigidos al Honeypot de Spam — también puede crear direcciones a partir de otro Spam que ya haya recibido dirigido a otras direcciones locales inválidas. Dado que los Honeypots de Spam nunca reciben correo legítimo, todos los mensajes entrantes dirigidos a ellos se enrutarán directamente a la Carpeta de Aprendizaje Bayesiano 680 para procesamiento. Además, las direcciones IP de los servidores de envío pueden añadirse opcionalmente al sistema de Monitoreo Dinámico 566, bloqueando futuras conexiones de dichas direcciones

durante un período designado de tiempo. Todo esto ayuda a aumentar la probabilidad de identificar y bloquear Spam en un futuro.

Honeypots de Spam

Esta lista contiene todas las direcciones que haya designado como Honeypot de Spam.

Habilitar Honeypots de Spam
Esta opción está habilitada por omisión. Desactive esta caja si desea deshabilitar la funcionalidad de Honeypots de Spam.

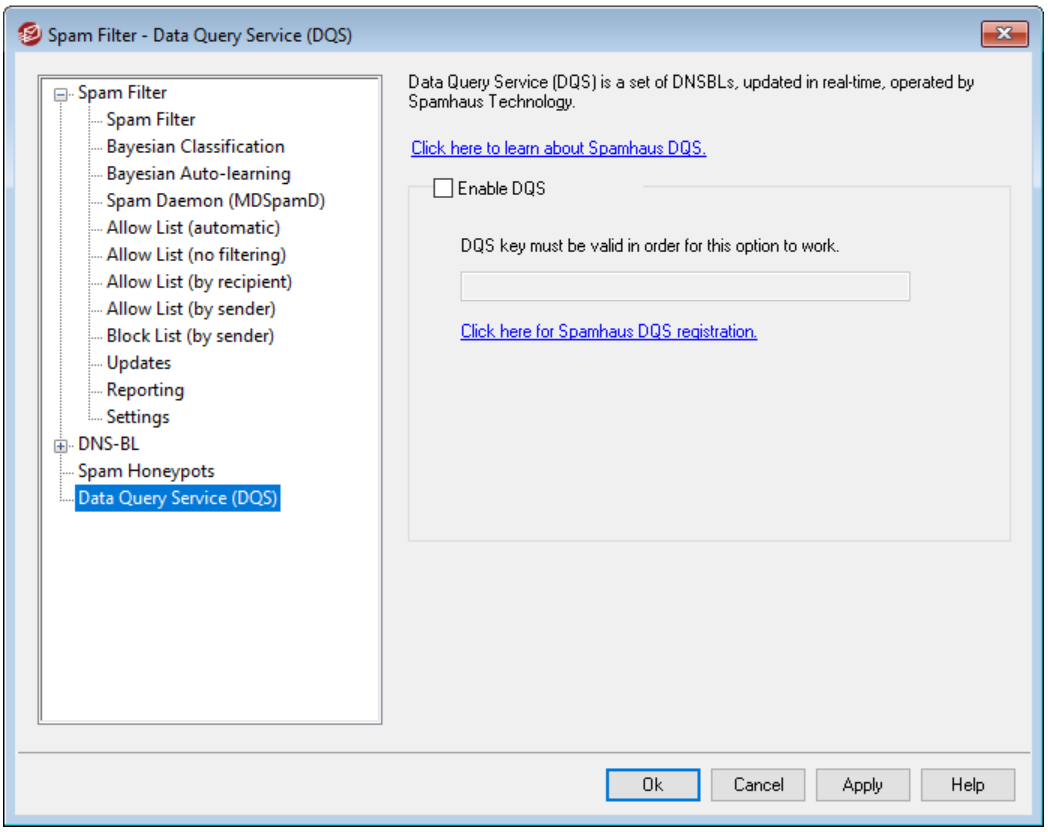
Nuevo Honeypot de Spam
Para agregar un Honeypot de Spam, introduzca las direcciones aquí y pulse *Agregar.*

Eliminar
Para eliminar un Honeypot de Spam, seleccione la dirección deseada y luego pulse Eliminar.

Enviar IP remitente al sistema de Monitoreo Dinámico
Haga clic en esta casilla si desea enviar al sistema de Monitoreo Dinámico 566 todas las direcciones IP de las que han llegado mensajes hacia los Honeypots de Spam. El Monitoreo Dinámico (localizado en Seguridad » Ajustes de Seguridad » Monitoreo » Monitoreo Dinámico) debe estar habilitando.

Enviar notificación cuando se bloquea una IP
Por omisión, cuanto una dirección IP es bloqueada por el sistema de Monitoreo Dinámico, se utilizarán las opciones *Reportes de Bloqueo de Direcciones IP* 619 del Monitoreo Dinámico para notificarle dicha acción. Deshabilite esta casilla si no desea recibir notificaciones cuando se bloquea una dirección IP debido a la funcionalidad de los Honeypots de Spam.

4.7.4 Data Query_Service



Servicio de Consulta de Datos o Data Query Service (DQS) es un conjunto de DNSBLs[701], actualizadas en tiempo real, operado por Spamhaus Technology a fin de bloquear más del 99% de las amenazas provenientes del correo electrónico. DQS requiere de una suscripción válida y uso de una llave proporcionada por Spamhaus Technology. Para utilizar el servicio DQS:

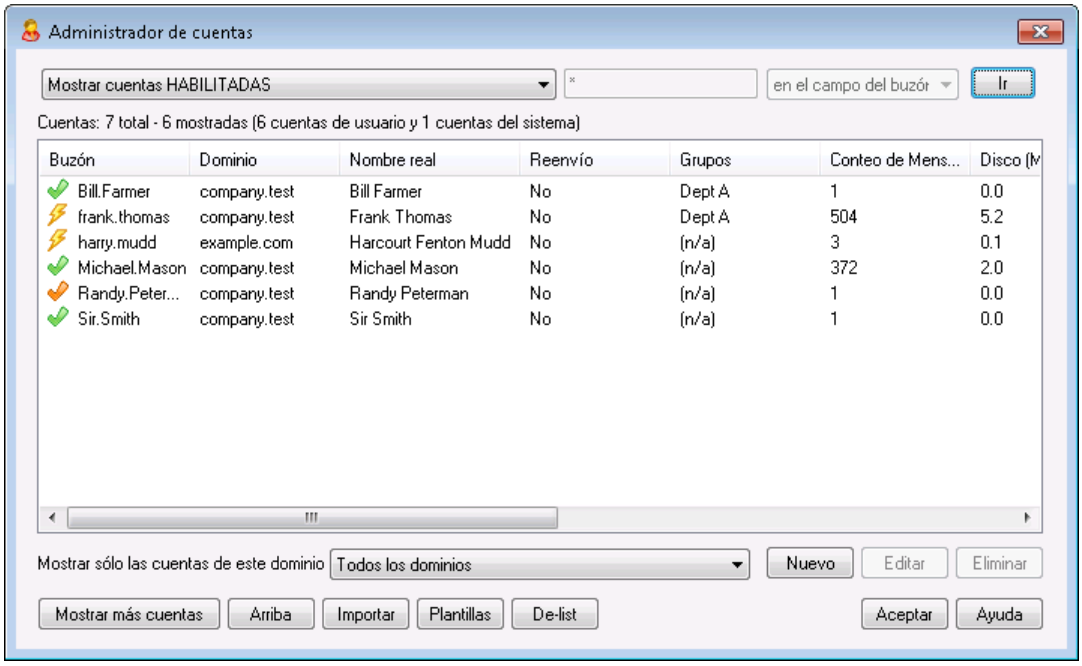
1. Active su prueba gratis de Data Query Service.
2. Dé clic en **Habilitar DQS**.
3. Registre su **Llave DQS de Spamhaus**.
4. Dé clic en **Ok**.

Sección

5 Menú Cuentas

5.1 Administración de Cuentas

Para administrar mejor la selección, adición, eliminación, o modificación de sus cuentas, MDaemon contiene el Administrador de Cuentas. Este diálogo da acceso a la información de las cuentas y puede usarse para ordenar las cuentas por buzón, dominio, nombre real, o carpeta de correo. El Administrador de Cuentas está ubicado en el menú de cuentas en: Cuentas » Administrador de Cuentas...



Administración de Cuentas

Arriba de la lista de cuentas verá dos estadísticas con respecto a la lista. El primer número es el número total de cuentas de usuario de MDaemon que existen actualmente en su sistema. El segundo número es el número de dichas cuentas que se muestra actualmente en la lista. Las cuentas que se mostrarán dependerán de lo que se haya escogido en la opción siguiente de *Mostrar sólo las cuentas para este dominio*. Si ha seleccionado "Todos los dominios" entonces se mostrarán todas las cuentas de MDaemon en la lista. Existe una opción de búsqueda al principio del diálogo que puede usar para definir exactamente qué cuentas se mostrarán con más precisión que simplemente el dominio al que pertenecen.

Cada registro en la lista contiene un Icono de Estatus de Cuenta (ver a continuación), el buzón, el dominio al que pertenece, el "nombre real" del propietario de la cuenta, cualquier grupo al que la cuenta pertenezca, el conteo de mensajes, el espacio en disco utilizado (en MB), la última vez que la cuenta fue accesada y la carpeta de correo en la que se almacenan los mensajes de la cuenta. Esta lista puede ordenarse en orden ascendente y descendente por la columna que prefiera. Haga clic en cualquier encabezado de columna para ordenar la lista en orden ascendente por dicha columna. Haga clic de nuevo en la columna para ordenarla en orden descendente.

Por defecto, sólo se mostrarán 500 cuentas a la vez en esta lista. Si quiere ver más cuentas del dominio actualmente seleccionado (o de Todos los Dominios, si ha seleccionado dicha opción) entonces debe hacer clic en el botón *Mostrar más cuentas* para mostrar las siguientes 500. Si quiere poder mostrar más de 500 cuentas a la vez entonces abra el archivo `MDaemon.ini` y cambie la clave `MaxAccountManagerEntries=500` al valor que prefiera.

Icono de Estatus de Cuentas

La cuenta es un administrador global o de dominio.

Cuenta con acceso total. Están habilitados tanto el acceso IMAP como POP.

Cuenta con acceso restringido. Ya sea POP o IMAP o ambos están deshabilitados.

Cuenta congelada. MDaemon aceptará correo para la cuenta, pero el usuario no puede enviar o verificar correo.

Cuenta deshabilitada. Todos los accesos de la cuenta están deshabilitados.

Nuevo
Haga clic en este botón para abrir el Editor de Cuentas[715] para poder crear una nueva cuenta.

Editar
Seleccione una cuenta de la lista y luego haga clic en este botón para abrir la en el Editor de Cuentas[715]. También puede dar doble clic en la cuenta para abrirla.

Eliminar
Seleccione una cuenta de la lista y luego haga clic en este botón para eliminarla. Se le pedirá que confirme su decisión de eliminar la cuenta antes de que MDaemon lo procese.

Mostrar solo las cuentas de este dominio
Selecciones "Todos los Dominios" de esta lista desplegable para desplegar todas las cuentas de MDaemon. Seleccione un dominio en específico para mostrar solo las cuentas de ese dominio.

Mostrar más cuentas
La lista de cuentas sólo mostrará 500 cuentas a la vez. Si existen más de 500 cuentas en el dominio que ha escogido entonces haga clic en este botón para mostrar las siguientes 500. Vea la nota anterior para instrucciones sobre cómo incrementar el número máximo de cuentas que pueden mostrarse.

Arriba
Haga clic en este botón para moverse arriba de la lista de cuentas.

Importar
Haga clic en este botón si desea importar cuentas de un archivo de texto separado por comas. Este botón es idéntico a la selección de menú Cuentas » Importar » Importar cuentas de un archivo de texto delimitado por comas.

Plantillas
Dé clic en este botón para abrir el diálogo Grupos & Plantillas 781, desde el que se pueden administrar los parámetros por omisión para las Cuentas Nuevas 792 y controlar la membresía de cuentas en grupos.

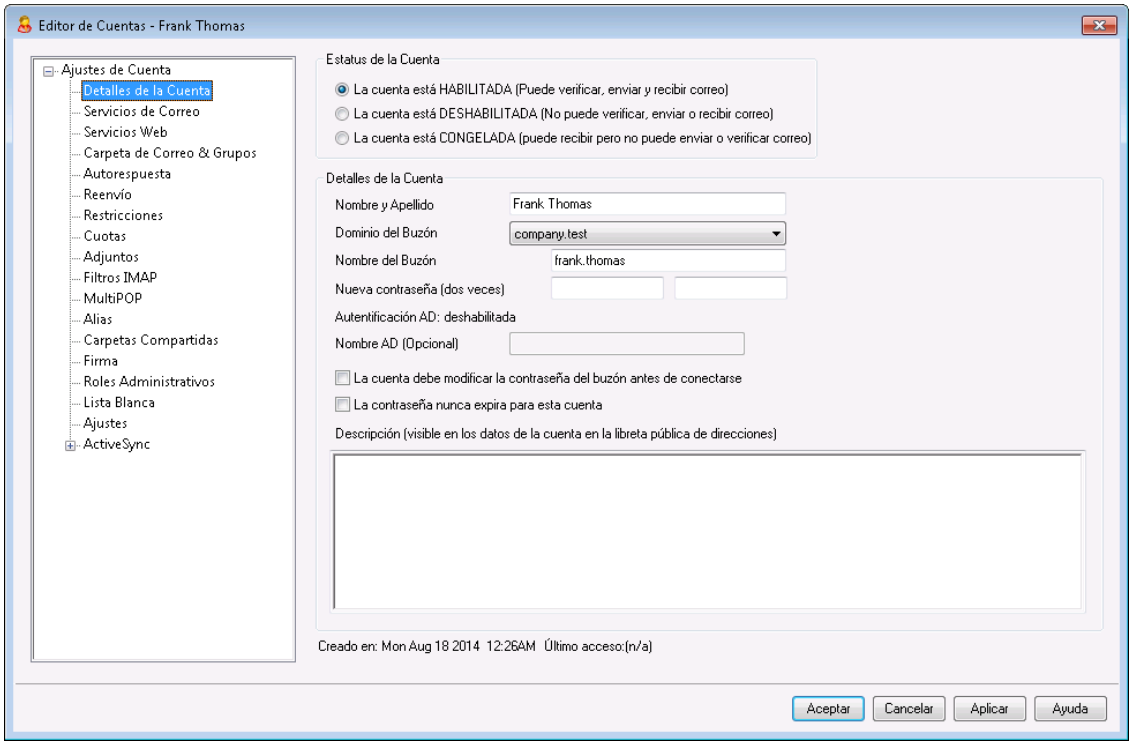
Desenlistar
Seleccione una o más cuentas y haga clic en este botón si desea desuscribirlas de todas las Listas de Distribución 280 hospedadas en el servidor. Se abrirá una caja solicitando su confirmación para remover esas direcciones de las listas.

Ver:

Editor de Cuentas 715
Plantilla para Cuentas Nuevas 792

5.1.1 Editor de Cuentas

5.1.1.1 Detalles de la Cuenta



Estatus de la Cuenta

La cuenta se encuentra HABILITADA (puede verificar, enviar y recibir correo)
Esta es la opción por omisión; la cuenta puede verificar, enviar y recibir correo.

La cuenta se encuentra DESHABILITADA (no puede verificar, enviar o recibir correo)
Seleccione esta opción si desea deshabilitar el acceso de la cuenta. El usuario no tendrá acceso a la cuenta por ningún medio, ni MDaemon aceptará correo para él. No se eliminará y todavía contará como parte del número de cuentas utilizadas de acuerdo con el límite de su licencia, pero MDaemon funcionará como si la cuenta no existiera, con una excepción - cualquiera de las carpetas de la cuenta que haya sido compartida con otros usuarios aun podrá ser accesada por esos usuarios, de acuerdo a los L Permisos ACL 316 de la carpeta.

La cuenta está CONGELADA (puede recibir, pero no puede enviar o verificar)
Seleccione esta opción si desea permitir que la cuenta reciba mensajes entrantes, pero impedir que se encuentre habilitada para verificar o enviar mensajes. Esto es útil cuando, por ejemplo, se sospecha que la cuenta ha sido secuestrada. Al congelar la cuenta se previene que algún usuario malicioso tenga acceso a sus mensajes o la utilice para enviar correo, pero se seguirá recibiendo su correo entrante.

Detalles de Cuentas

Nombre y Apellido
Introduzca el Nombre y Apellido del usuario aquí. Cuando se crea una nueva cuenta, la mayoría de los campos de las pantallas anteriores del editor de cuenta serán automáticamente completados mientras se teclea el nombre y apellido del usuario. Esta información autogenerada se basa en las plantillas y

configuraciones encontradas en Valores predeterminados de la nueva cuenta. El campo de nombre y apellido no pueden contener " ! " o " | ".

Dominio del Buzón
Utilice esta lista desplegable para especificar el domino al que pertenece esta cuenta y que será utilizado en su dirección de correo. El Dominio por Omisión 190 de MDaemon aparecerá en la lista desplegable por omisión.

Nombre del Buzón
Esta es la porción de la dirección de correo de la cuenta que la distingue de las otras cuentas del dominio. La dirección de correo completa (i.e. [*Nombre del buzón*]@[*Dominio del Buzón*]) se utiliza como identificador único de la cuenta y como su credencial de ingreso para los servicios POP3, IMAP, Webmail y demás. Las direcciones de correo no pueden contener espacios o caracteres como "!" o "|". No utilice "@" en esta opción. Por ejemplo, utilice "juan.perez", no utilice "juan.perez@".

Nueva Contraseña (dos veces)
Si desea modificar la contraseña de la cuenta, teclee la nueva aquí, una vez en cada caja. Esta es la contraseña que la cuenta usará cuando conecte a MDaemon para enviar o recibir correo vía POP3 o IMAP, cuando se autentifique usando el proceso SMTP, o cuando use Webmail, MDaemon Administración Remota o MDaemon Connector. Ambas cajas se iluminarán en rojo si las contraseñas no coinciden o violan las restricciones de contraseñas 855. De otra forma se iluminarán en verde.

Se está utilizando la Autentificación de Active Directory 866 para esta cuenta, debe registras dos barras inversas seguidas del dominio de Windows al que pertenece el usuario, en lugar de registrar la contraseña (por ejemplo \\ALTN en lugar de `123Password`). Bajo los campos de contraseña se muestra una frase corta indicando si se encuentra habilitada o no la autentificación dinámica para la cuenta.

La cuenta deberá tener contraseña aun cuando no desee permitir acceso POP3/IMAP a la cuenta de correo. Además de la verificación de la sesión de correo, los valores *Dirección de correo* y *Contraseña de correo* se usan para permitir la manipulación remota de la cuenta y la solicitud remota de archivos. Si desea prevenir el acceso POP/IMAP, use las opciones localizadas en la pantalla Servicios de Correo 719. Si desea prevenir todo acceso, entonces utilice las opciones *La Cuenta está DESHABILITADA* o *La Cuenta está CONGELADA* mencionadas arriba.

Nombre AD (opcional)
Utilice este ajuste si desea especificar opcionalmente un nombre de cuenta de Active Directory para acceso de la cuenta.

La cuenta debe modificar su contraseña antes de conectarse
Marque esta casilla si desea requerir que la cuenta modifique la *Contraseña del buzón* antes de que pueda tener acceso a los servicios POP, IMAP, SMTP, Webmail o MDaemon Administración Remota. El usuario se puede conectar a Webmail o MDaemon Administración Remota, pero se le solicitará que modifique su contraseña antes de proceder. Nótese, sin embargo, que a fin de que los

usuarios puedan modificar su contraseña vía Webmail o MDaemon Administración Remota, primero deben tener habilitada la opción vía web "*...editar contraseña*" en la pantalla Servicios Web 720. Luego de que se modifica la contraseña, esta opción se desactivará.

Dado que modificar la contraseña puede no ser fácil o posible para algunos usuarios, deberá tener mucho cuidado antes de activar esta opción.

La contraseña nunca expira para esta cuenta
Marque esta casilla si desea exentar la cuenta de la opción de expiración de la contraseña, localizada en el diálogo Contraseñas 855.

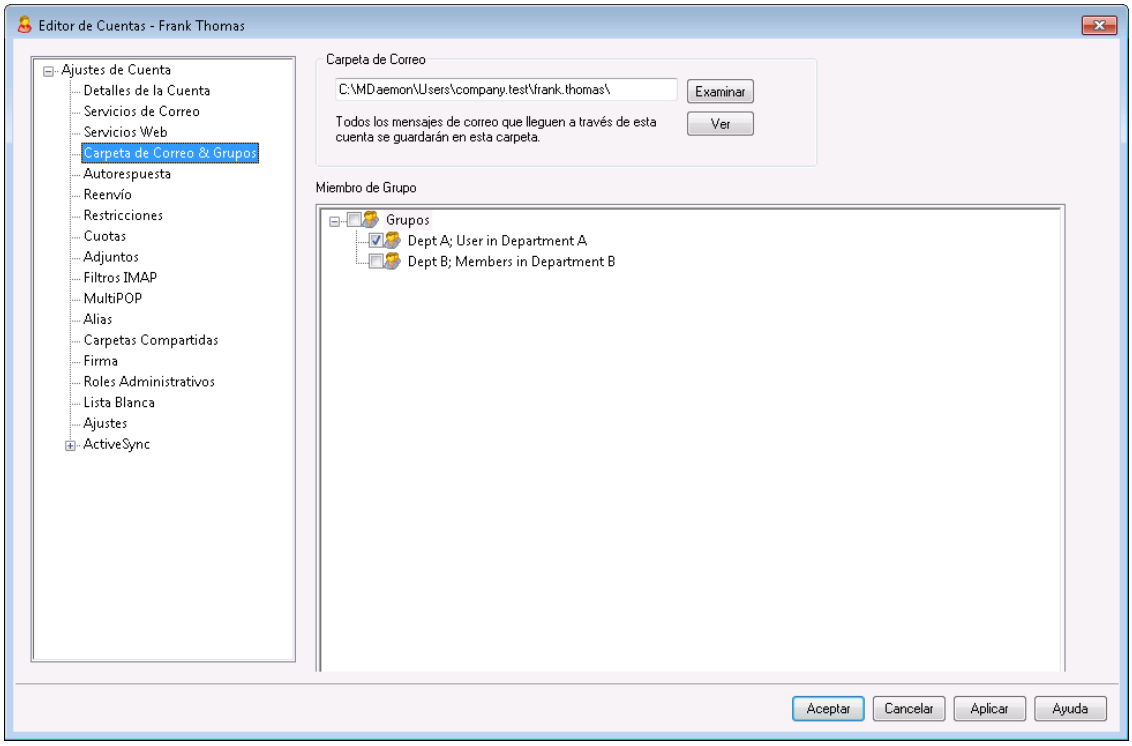
Descripción
Utilice esta área de texto para detallar cualesquiera notas o comentarios respecto a la cuenta.

Esta descripción está incluida en el registro de cuentas públicas y es visible por otros. No incluya información privada o sensible en este campo. Para registrar notas o comentarios privados respecto a esta cuenta, utilice el espacio proporcionado en la pantalla Roles del Administrador 757.

Ver:

Autentificación AD 866
Contraseñas 855
Editor de Cuentas » Servicios Web 720

5.1.1.2 Carpeta de Correo & Grupos



Carpeta de Correo

Registre aquí la carpeta donde desea que se almacenen los mensajes de correo de esta cuenta. Al crear una cuenta nueva la ubicación por omisión de esta carpeta se basa en la configuración de *Carpeta de Correo* definida en la Plantilla de Cuentas Nuevas[793].

Ver

Dé clic en este botón para abrir el Administrador de Colas/Estadísticas[884] en la *Carpeta de Correo* del usuario.

Membresía en Grupos

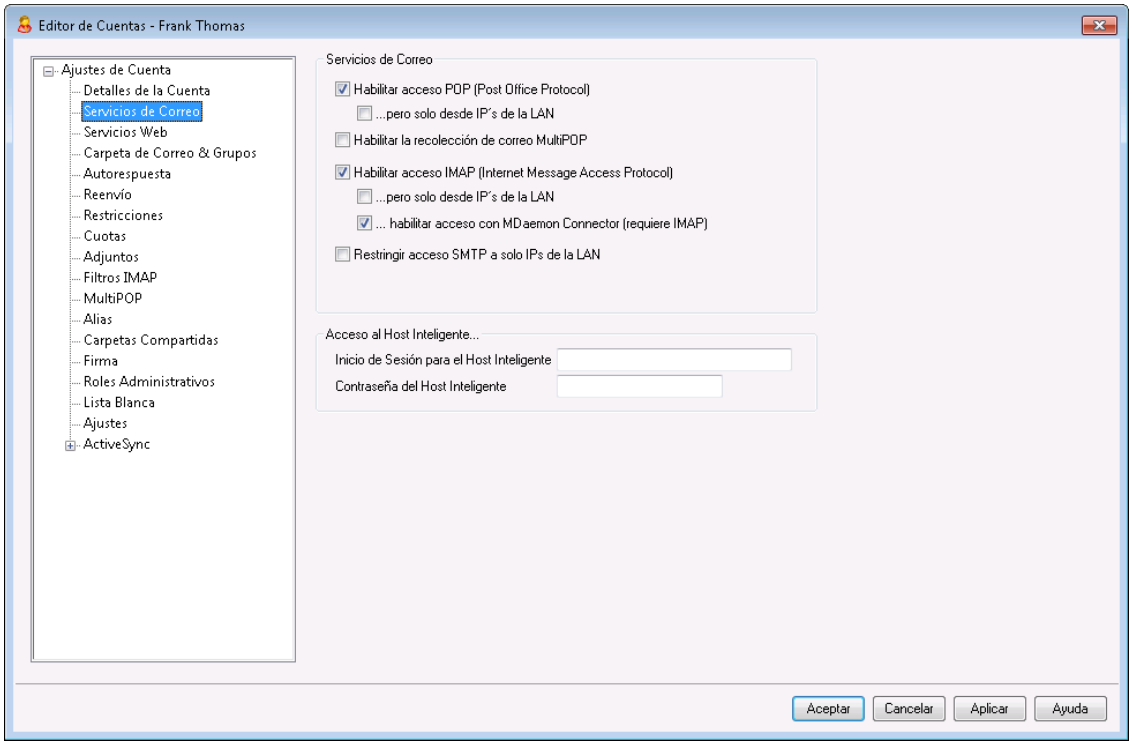
Utilice esta caja para agregar una cuenta a uno o más Grupos[781]. Marque la caja junto a cada grupo al que desee que pertenezca la cuenta.

Ver:

Plantilla de Cuentas Nuevas[793]

Grupos[781]

5.1.1.3 Servicios de Correo



Las opciones en esta pantalla controlan qué servicios de correo puede utilizar la cuenta: POP3, IMAP, MultiPOP y MDaemon Connector. El acceso al correo electrónico vía Webmail se controla en la pantalla de la opción Servicios Web[720]. También contiene campos para especificar opcionalmente las credenciales de acceso al Host Inteligente para la cuenta.

Servicios de Correo

Habilitar acceso POP3 (Post Office Protocol v3)
Cuando se selecciona esta casilla, la cuenta de correo se puede accesar vía Post Office Protocol v3 (POP3). Virtualmente todos los clientes de correo soportan este protocolo.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que la cuenta sea accesada vía POP3 solamente cuando el usuario se conecta utilizando direcciones IP de la LAN[608].

Habilitar recolección de correo MultiPOP
Marque esta casilla si desea permitir que la cuenta utilice MultiPOP[739]. MultiPOP permite al usuario recolectar mensajes de otras cuentas de correo, mantenidas en otros servidores de correo.

Habilitar acceso IMAP (Internet Message Access Protocol)
Cuando se selecciona esta casilla, la cuenta de correo se puede accesar vía Internet Message Access Protocol (IMAP). IMAP es más versátil que POP3, permitiendo que el correo se maneje en el servidor y se accese utilizando múltiples clientes. La mayor parte de los clientes de correo soportan este protocolo.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que la cuenta sea accesada vía IMAP solamente cuando el usuario se conecta utilizando direcciones IP de la LAN[608] .

...habilitar acceso desde Outlook Connector (requiere IMAP)

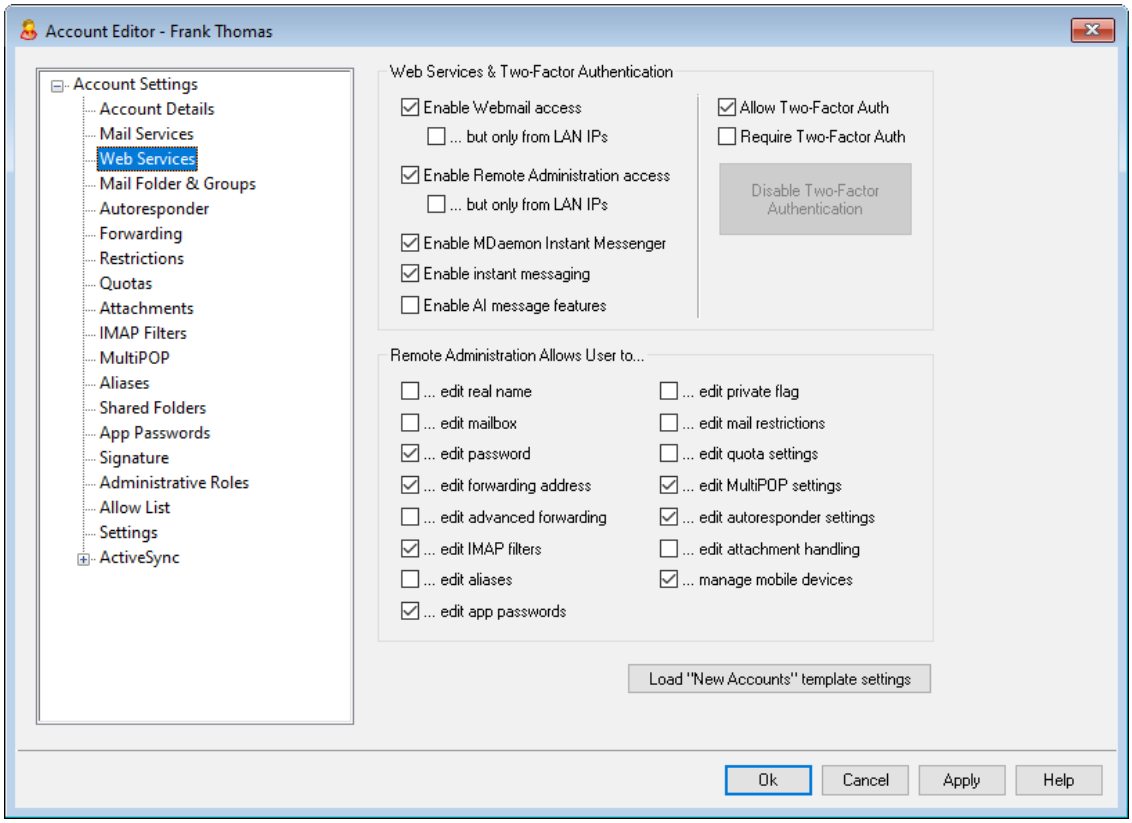
Dé clic en esta opción si desea permitir que la cuenta se conecte utilizando MDaemon Connector[387]. **Nota:** esta opción solo estará disponible cuando se haya activado soporte para MDaemon Connector en su servidor.

Restringir acceso SMTP a solo IPs de la LAN
Marque esta casilla si desea restringir el acceso solamente a IPs de la LAN. Esto impedirá que las cuentas envíen correo a menos que se encuentren conectada a su red. Si la cuenta intenta enviar correo desde una IP externa la conexión será rehusada y cerrada.

Acceso a Host Inteligente

Login/contraseña del host inteligente
Si se encuentra habilitada la opción *Permitir autentificación por cuenta* en la pantalla Entrega[102] en Configuración » Ajustes de Servidor y desea utilizar autentificación por cuenta con esta cuenta en lugar de utilizar las credenciales especificadas en esa pantalla, entonces defina aquí la credenciales opcionales para el host inteligente. Si no desea utilizar autentificación por cuenta para esta cuenta, deje esta opción en blanco.

5.1.1.4 Servicios Web



Servicios Web

Habilitar acceso vía Webmail
Habilite esta casilla si desea que la cuenta tenga acceso al servidor Webmail[321], que permite a los usuarios tener acceso a su correo, calendarios y otras funciones usando un navegador Web.

...pero solo desde IPs de la LAN
Marque esta casilla si desea permitir que la cuenta tenga acceso a Webmail solamente cuando se conecte desde direcciones IP de la LAN[608].

Habilitar el acceso a la Administración Remota
Marque esta casilla si desea conceder al usuario permisos para modificar la configuración de su cuenta a través de la Administración Remota[354]. El usuario solo podrá editar aquellas configuraciones que active a continuación.

Cuando esta funcionalidad está habilitada y el servidor de Administración Remota está activo, el usuario podrá acceder a la Administración Remota introduciendo en un navegador el dominio designado de MDaemon y el puerto asignado a la Administración Remota[356] (p. ej. `http://ejemplo.com:1000`). Primero se le presentará una pantalla de acceso que contiene las configuraciones a las que se le ha dado permiso para editar. Todo lo que necesita hacer es editar las configuraciones que escoja y luego hacer clic en el botón *Guardar cambios*. Luego puede salir de sesión y cerrar el navegador. Si tiene acceso a Webmail, también puede acceder a MDaemon Administración Remota desde las Opciones Avanzadas en el menú de Webmail.

Si el usuario es un Administrador Global o de Dominio (designado en la pantalla Roles Administrativos[757] del Editor de Cuentas) verá una pantalla diferente después de que acceda a la Administración Remota.

...pero solo desde IPs de la LAN
Marque esta casilla si desea permitir que la cuenta tenga acceso a la Administración Remota solamente cuando se conecte desde direcciones IP de la LAN[608].

Habilitar MDaemon Mensajería Instantánea
Dé clic en esta casilla si desea habilitar el soporte a MDIM[322] para esta cuenta.

Habilitar Mensajería Instantánea
Cuando se habilita el soporte a MDIM para la cuenta, dé clic en esta opción si también desea habilitar el soporte a la mensajería instantánea de MDIM. Cuando esta casilla está deshabilitada, podrá acceder a las otras funcionalidades de MDIM, pero no a la mensajería instantánea.

El Usuario puede editar categorías
Marque esta casilla si desea permitir que este usuario de Webmail edite categorías. Esta opción está habilitada por omisión. **Nota:** Esta opción solo está disponible en la interface web MDaemon Administración Remota (MDRA)[354].

Omitir verificación de Persistencia de IP para sesiones de Webmail
Cuando se habilita la opción del Servidor Web Webmail[326] de "Requerir persistencia de IP durante la sesión de Webmail", puede marcar esta casilla si desea exentar a este usuario del requerimiento de persistencia de IP. **Note:** **Nota:** Esta opción solo está disponible en la interface web MDaemon Administración Remota (MDRA)[354].

Habilitar funcionalidades IA en mensajes
Si está activada la opción *Habilitar funcionalidades de IA en mensajes* en el diálogo del dominio de esta cuenta en Webmail[201], marque esta casilla si desea permitir a la cuenta utilizar esas funcionalidades en MDaemon Webmail; las funcionalidades solo estarán disponibles para el usuario cuando está habilitada la opción a nivel dominio. **Nota:** Puede utilizar las funcionalidades de Plantillas de Cuentas[791] y Grupos[781] para asignar usuarios a un grupo que tenga acceso a las funcionalidades IA en mensajes. Ver: "Funcionalidades de IA en mensajes, en Webmail[724]" abajo para obtener información importante y precauciones sobre el uso de estas funciones.

Autenticación de Dos Factores

MDaemon soporta la Autenticación de Dos Factores (2FA) para usuarios que se firman en Webmail o en la Administración Remota de MDaemon. Las cuentas que se firman en Webmail vía HTTPS pueden activar la Autentificación de Dos Factores en la pantalla **Opciones » Seguridad** en Webmail. Así, el usuario deberá ingresar un código de verificación al firmarse a Webmail o a la Administración Remota. El código se obtiene de una app autentificadora instalada en el dispositivo móvil del usuario o en su tableta. Esta funcionalidad está diseñada para cualquier cliente que soporte el Autentificador de Google. Vea la ayuda de Webmail para más información sobre como configurar 2FA para una cuenta.

Permitir Autenticación de Dos Factores
Por omisión a las cuentas nuevas[798] se les permite configurar y utilizar la Autenticación de Dos Factores de Webmail. Deshabilite esta casilla si no desea permitir a esta cuenta utilizar 2FA.

Requerir Autenticación de Dos Factores
Habilite esta opción si desea forzar la cuenta a utilizar la Autenticación de Dos Factores al firmarse en Webmail. Si 2FA no se ha configurado para la cuenta, la próxima vez que la cuenta se firme a Webmail el usuario será redirigido a la página para configurarla. Vea la ayuda de Webmail para más información sobre como configurar 2FA para una cuenta.

Deshabilitar Autentificación de Dos Factores
Dé clic en este botón si necesita deshabilitar la Autentificación de Dos Factores para la cuenta. Esto podría ser necesario, por ejemplo, si el usuario extravió su dispositivo y no puede accesar sus datos del autentificador.

Administración Remota permite al usuario...

...editar su nombre real
Activar esta funcionalidad permitirá al usuario modificar la configuración de *Nombre y Apellido*.

...editar el buzón
Si activa esta funcionalidad permitirá al usuario modificar el Nombre de buzón[715] de su cuenta.

Dado que el *Nombre de buzón* es parte de la dirección de correo de la cuenta y es un identificador único y valor de acceso para la cuenta, cambiarlo significa que el usuario estará cambiando su dirección de correo real. Esto podría hacer que cualquier mensaje futuro dirigido a la dirección antigua sea rechazado o eliminado.

...editar la contraseña
Haga clic en esta casilla si desea permitir al usuario que modifique la *Contraseña de su cuenta.* Para más información sobre requerimientos de la contraseña, vea: Contraseñas[855].

...editar dirección de reenvío
Cuando se habilita esta funcionalidad, el usuario podrá modificar la configuración de reenvío[729] de dirección.

...editar reenvío avanzado
Cuando se activa esta opción, el usuario podrá modificar las *Ajustes avanzados de Reenvío.*

...editar filtros IMAP
Use este control para habilitar al usuario para que cree y administre sus propios Filtros IMAP[737].

...editar alias
Habilite esta opción si desea permitir al usuario editar los Alias[742] asociados con su cuenta.

...editar contraseñas de apps
Por omisión los usuarios pueden editar sus Contraseñas de Apps[751]. Deshabilite esta casilla si no desea permitir a los usuarios editarlas.

...editar marca de privada
Esta opción define si el usuario podrá o no utilizar la Administración Remota para editar la opción "*La Cuenta está oculta de las listas "Everyone", calendarios compartidos y VRFY*" que se localiza en la pantalla Ajustes 760 del Editor de Cuentas

...editar las restricciones de correo
Esta casilla controla si la cuenta podrá o no editar las restricciones de correo Entrante/Saliente, ubicada en la pantalla Restricciones 731.

...editar las configuraciones de cuota
Haga clic en esta casilla si desea permitir a la cuenta que modifique las configuraciones de cuota 733.

...editar las configuraciones MultiPOP
Haga clic en esta casilla si desea dar permiso a la cuenta para añadir nuevas entradas MultiPOP 739 y para habilitar/deshabilitar la recolección MultiPOP para dichas entradas en MDRA 354. Cuando están habilitadas esta opción y *Habilitar MultiPOP* 739, estará disponible la página Buzones en Webmail 321 para que el usuario administre sus ajustes de buzones MultiPOP. Finalmente, la opción global para habilitar/deshabilitar el servidor MultiPOP se localiza en: Configuración » Ajustes de Servidor » MultiPOP 151.

...editar las configuraciones de la respuesta automática
Haga clic en esta casilla si desea dar al usuario permiso para agregar, editar, o eliminar Autorespuestas 726 para esta cuenta.

...editar manejo de adjuntos
Haga clic en esta casilla si desea permitir al usuario editar las opciones de manejo de adjuntos de la cuenta, localizadas en la pantalla Adjuntos 735.

...administrar dispositivo móvil
Utilice esta opción si desea permitir al usuario utilizar Administración Remota para administrar los parámetros específicos de configuración de sus dispositivos móviles o dispositivos ActiveSync.

Cargar la configuración de la plantilla de "Cuentas Nuevas"

Dé clic en este botón para regresar los parámetros en esta pantalla a los valores por omisión definidos en la pantalla Servicios Web 798 de la plantilla de *Cuentas Nuevas*.

Funcionalidades IA en Mensajes de Webmail

Al igual que MDaemon 23.5.0, el tema Pro en el cliente Webmail de MDaemon incluye varias funcionalidades de Inteligencia Artificial (IA para ayudar a sus usuarios a administrar su correo e incrementar la productividad. Estas funcionalidades son opcionales y están deshabilitadas por omisión, pero se pueden habilitar para cualquier usuario.

Con estas funcionalidades, en MDaemon Webmail puede utilizar IA :

- Generar un resumen de los contenidos de un mensaje de correo.

- Sugerir una respuesta al mensaje, de acuerdo a varios lineamientos que le puede indicar a la IA. También puede definir el *Tono* de la respuesta ya sea profesional respetuoso o casual. La *Posición*, o sentido de la respuesta puede definirse como interesado, no interesado, de acuerdo, en desacuerdo o escéptico. La respuesta con *Actitud* podrá definirse como confiado, emocionado, calmado o arrepentido. Por último, puede definir la *Longitud* de la respuesta, que puede ser desde muy breve a detallada.
- Puede ayudar a redactar un nuevo mensaje de correo, con base en algún texto que ya se haya incluido. Al igual que en la opción mencionada *Sugerir Respuesta*, también se puede definir el Tono, Posición, Actitud y Longitud como criterios a utilizar por la IA al redactar el mensaje.

La opción *Habilitar funcionalidades de IA en Mensajes* en la pantalla Ajustes de Webmail 345 controla si está o no habilitado el soporte a las funcionalidades de IA por omision para sus dominios. Existe una opción con el mismo nombre localizada en el diálogo Webmail 201 del Administrador de Dominios, que se puede utilizar para ignorar el ajuste principal para dominios específicos. **Nota:** el habilitar el soporte a Funcionalidades IA en Mensajes no garantiza acceso a ellas para todos los usuarios del dominio. Se deberá activar la opción *Habilitar funcionalidades IA en mensajes* en la pantalla Servicios Web 720 del editor de cuentas para los usuarios a los que desee dar permiso. Alternativamente, puede utilizar las opciones de Plantillas de Cuentas 791 y Grupos 781 para asignar usuarios a un grupo que tenga acceso a funcionalidades IA en mensajes.

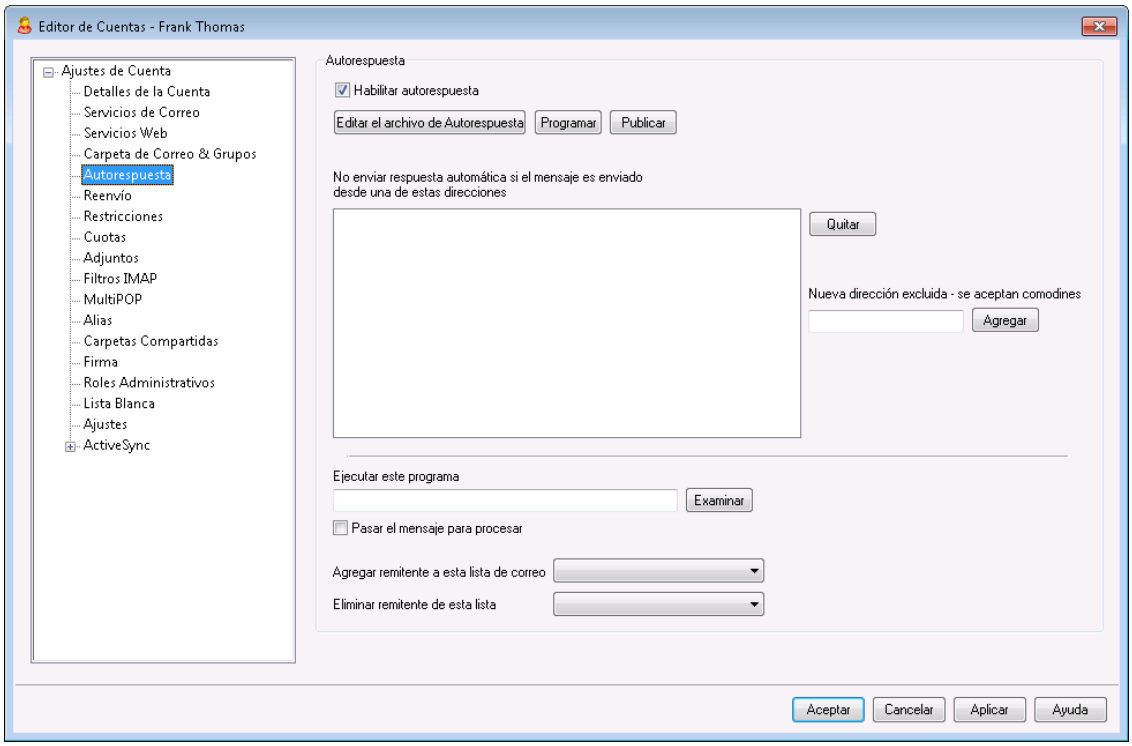
Cuando se habilitan en MDaemon las cuentas para utilizar las funcionalidades IA en mensajes se permite a los usuarios enviar y recibir información para y de servicios generativos IA de terceros, específicamente ChatGPT de OpenAI. Los Administradores y usuarios deberán estár conscientes de que esto introduce varios temas de privacidad debido a la habilidad de la funcionalidad de procesar datos personales y generar información potencialmente sensitiva. Para resolver los temas de privacidad, es vital que las organizaciones capaciten a sus empleados para usar IA con responsabilidad. **Nota:** Los datos enviados para/de Open AI no se almacenan en el servidor local o en nuestra red.

Puede encontrar la Política de Uso de MDaemon Technologies en la Página Artifical Intelligence (AI) Information. En esa misma página existe una liga a los Terminos de Uso de OpenAI.

Ver:

Webmail 321
Administración Remota 354
Administrador de Plantillas » Servicios Web 798

5.1.1.5 Autorespuestas



Las autorespuestas son herramientas útiles que hacen que los mensajes entrantes detonen algunos eventos automáticamente, tales como ejecutar un programa, añadir al remitente a una lista de correo, responder con un mensaje generado automáticamente, y más. El uso más común de las autorespuestas es responder a los mensajes entrantes automáticamente con un mensaje definido por el usuario indicando que el destinatario está de vacaciones, no está disponible, contestará lo antes posible, o similar. Los usuarios de MDaemon con Acceso Web 720 a Webmail 321 o Administración Remota 354 pueden usar las opciones ofrecidas para redactar mensajes de autorespuesta por sí mismos y programar las fechas en que estarán en uso. Finalmente, los mensajes de respuesta automática se basan en los contenidos del archivo `OOF.mrk`, que se encuentra en la carpeta raíz `\data\` de cada usuario. Este archivo soporta un gran número de macros, que se pueden utilizar para generar dinámicamente gran parte del contenido de los mensajes, haciendo las autorespuestas muy versátiles.

Los eventos de Autorespuesta son siempre respetados cuando el mensaje que los detona es de un origen remoto. Sin embargo, para los mensajes originados en el dominio del usuario, las autorespuestas sólo se activarán si habilita la opción *Las respuestas automáticas se generan por el correo del dominio interno*, ubicada en la pantalla Autorespuestas » Ajustes 842. Puede usar también una

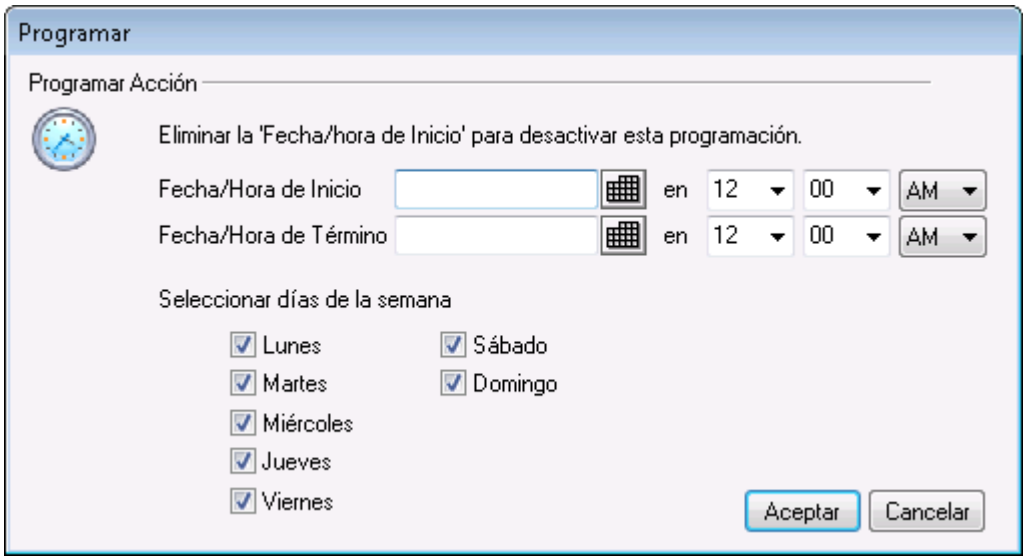
opción en dicha pantalla para limitar los mensajes de autorespuesta a uno por remitente por día.

Autorespuesta

Activar autorespuesta
Habilite este control para activar una autorespuesta para esta cuenta. Para más información sobre autorespuestas vea: Autorespuestas 838.

Editar archivo de autorespuesta
Dé clic en este botón para editar el archivo de autorespuesta de la cuenta. Este es el archivo `oof.mrk`, localizado en la carpeta `\data\`de la cuenta.

Programar
Haga clic en este botón para abrir el diálogo de programación donde puede establecer una fecha de inicio y de fin y la hora y definir los días de la semana en que la Autorespuesta debe estar activa. Deje el programador en blanco si quiere que la Autorespuesta esté activa continuamente.



Publicar

Dé clic en este botón si desea copiar el archivo de autorespuesta y los ajustes de esta cuenta a una o más cuentas. Seleccione las cuentas a las que desea copiar la autorespuesta y dé clic en **OK**.

No enviar respuesta automática si el mensaje es enviado desde una de estas direcciones
Aquí puede listar las direcciones que desea que estén excluidas de las respuestas iniciadas por este autorespuesta.

Ocasionalmente los mensajes de autorespuesta pueden ser enviados a una dirección que les devuelve a su vez una autorespuesta. Esto puede crear un efecto "ping-pong" haciendo que los servidores se respondan continuamente unos a otros. Si se encuentra con una de dichas

> direcciones, introdúzcala aquí para prevenir que eso suceda. También existe una opción ubicada en la pantalla de Autorespuesta » Ajustes 842, que puede usarse para limitar el número de mensajes de respuesta a uno por día.

Quitar
Haga clic en este botón para eliminar cualquier entrada seleccionada de la lista de direcciones excluidas.

Nueva dirección excluida—se aceptan comodines
Si desea agregar una dirección a la lista de direcciones excluidas, introdúzcala aquí y luego haga clic en el botón **Ejecutar un Programa**

Ejecutar este programa
Use este campo para especificar la ruta y el nombre de archivo a un programa que desea ejecutar cuando llega nuevo correo para esta cuenta. Se debe tener cuidado para asegurarse que este programa termina apropiadamente y puede ejecutarse en modo desatendido. Puede introducir parámetros de línea de comandos opcionales inmediatamente después de la ruta de ejecución si así lo desea.

Pasar el mensaje para procesar
Seleccione esta opción y al proceso especificado en el campo *Ejecutar este programa* se le pasará el nombre del mensaje desencadenante como el primer parámetro disponible de línea de comando. Cuando la autorespuesta se configura para una cuenta que está reenviando correo a otra ubicación y **no** retiene copia local en su propio buzón (vea Reenvío 729) entonces esta función se deshabilitará.

Por defecto, MDaemon colocará el nombre del archivo de mensaje como el último parámetro en la línea de comando. Puede sobrescribir este comportamiento usando la macro `$MESSAGE$`. Use esta macro en lugar donde debería colocarse el nombre del archivo de mensaje. Esto permite más flexibilidad en el uso de esta funcionalidad puesto que puede usarse una línea de comando compleja tal como esta: `logmail /e /j /message=$MESSAGE$ /q`.

Listas de Distribución

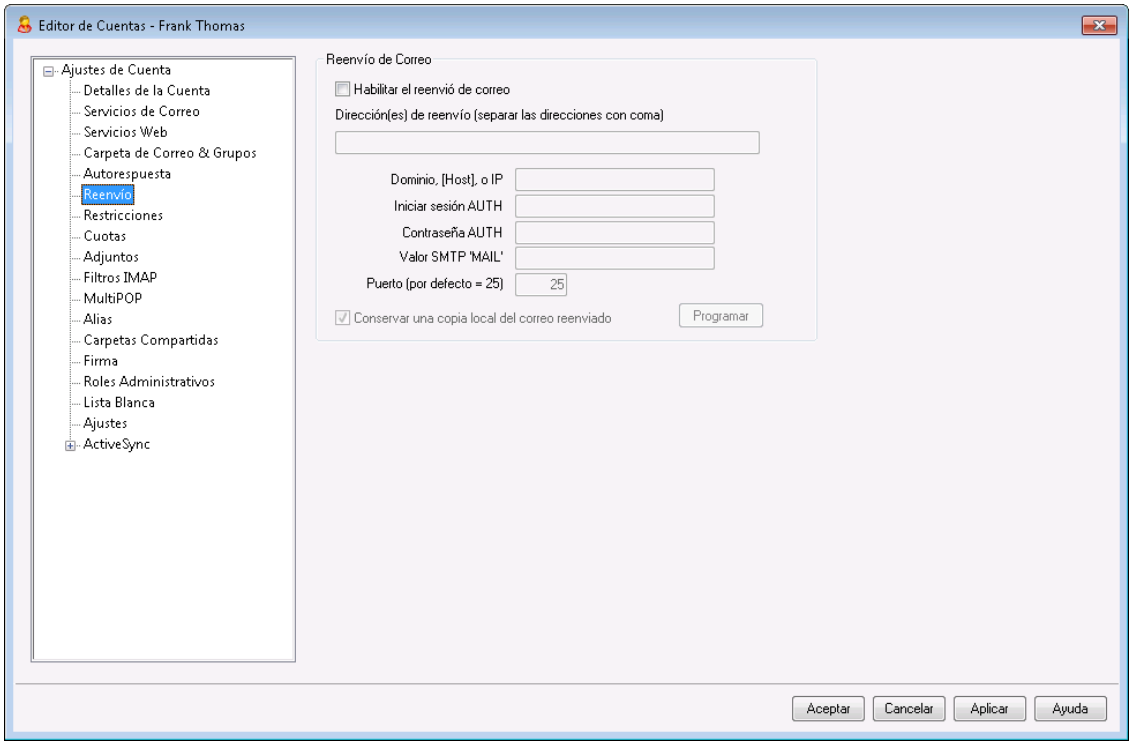
Agregar remitente a esta lista de correo
Si se introduce una lista de correo en este campo el remitente del mensaje entrante será automáticamente añadido como miembro de dicha lista. Esta es una función útil para construir listas automáticamente.

Quitar el remitente de esta lista
Si se introduce una lista de correo en este campo el remitente del mensaje entrante será automáticamente eliminado como miembro de la lista especificada.

Ver:

Autorespuesta » Cuentas 838
Autorespuesta » Lista de Exentos 840
Autorespuesta » Ajustes 842
Crear Scripts de Autorespuesta 843

5.1.1.6 Reenvío



Reenvío de Correo

Habilitar reenvío de correo
Marque esta casilla si desea reenviar los mensajes entrantes de esta cuenta a la dirección o direcciones especificadas en la opción siguiente de *Direcciones de envío.* Los usuarios de MDaemon con Acceso Web 720 a Webmail 321 o MDaemon Administración Remota 354 pueden usar las opciones proporcionadas para establecer las opciones de reenvío ellos mismos en lugar de requerir que lo haga un administrador.

Dirección(es) de reenvío (separar las direcciones con coma)
Use este campo para designar cualquier dirección de correo a la que quiera reenviar copias de los mensajes entrantes de esta cuenta tal cual lleguen. Una copia de cada nuevo mensaje que llegue al servidor será automáticamente generada y reenviada a las direcciones especificadas en este campo, si la opción

anterior de *Habilitar reenvío de correo* está marcada. Cuando reenvíe a direcciones múltiples, separe cada una con una coma.

Dominio, [Host], o IP
Si desea enrutar mensajes reenviados a través de otro servidor, tal como un servidor MX particular del dominio, especifique el dominio o dirección IP aquí. Si desea enrutar los mensajes a un host específico, cierre el valor en corchetes (ej. `[host1.example.com]`).

Inicio de Sesión/Contraseña AUTH
Registre aquí las credenciales requeridas por el servidor al que está reenviando el correo del usuario.

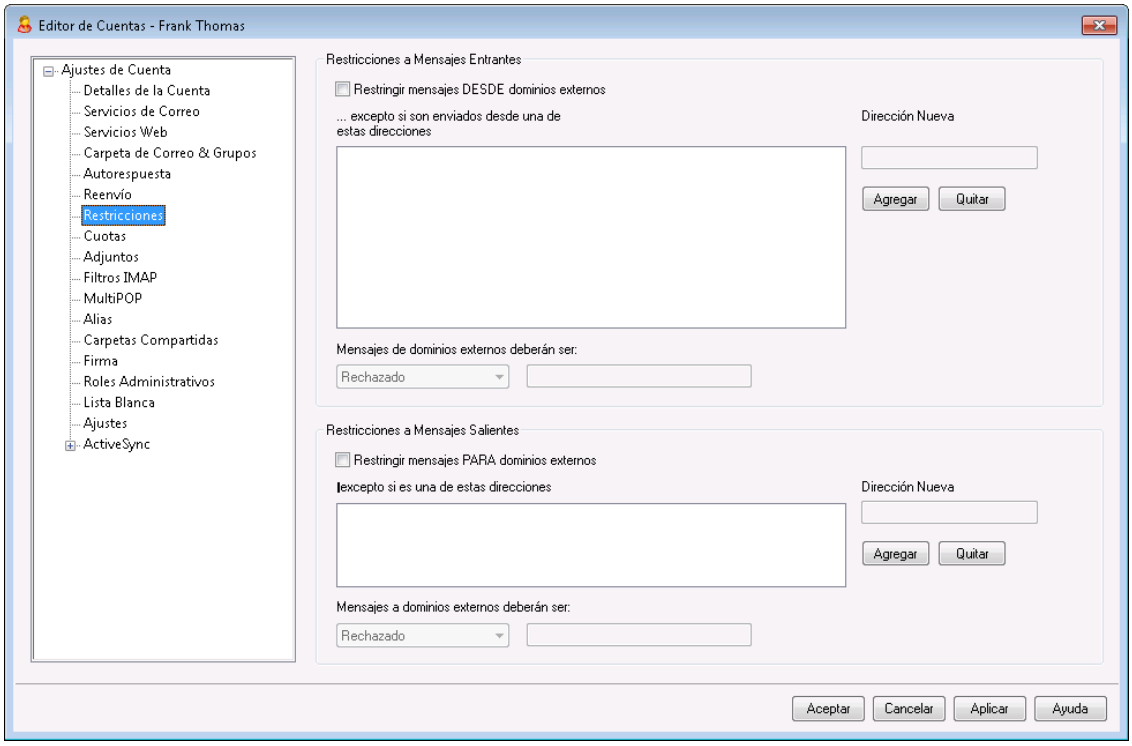
Valor SMTP 'MAIL'
Si se especifica una dirección aquí, se utilizará en la sentencia "`MAIL From`" enviada durante la sesión SMTP con el host destino, en lugar de utilizar el remitente del mensaje. Si requiere una sentencia SMTP con valor vacío para "`MAIL From`" (ej. "`MAIL From`" <>") entonces registre "[trash]" en esta opción.

Puerto (omisión = 25)
MDaemon enviará los mensajes reenviados utilizando el puerto TCP especificado aquí. El puerto SMTP por omisión es 25.

Retener una copia local del correo reenviado
Por omisión, una copia de cada mensaje reenviado se entrega normalmente al buzón del usuario local. Si deshabilita esta casilla no se retendrá una copia local.

Programación
Dé clic en este botón para crear una programación para el reenvío del correo de la cuenta. Puede configurar la fecha y hora de inicio, la fecha y hora de término y especificar los días de la semana en que se reenviará correo.

5.1.1.7 Restricciones



Use las opciones en esta pantalla para determinar si la cuenta podrá o no enviar o recibir correo a dominios no-locales.

Restricciones de Mensajes Entrantes

Restringir mensajes DE dominios externos
Haga clic en esta casilla si quiere impedir que esta cuenta reciba mensajes de dominios no-locales.

...excepto si son enviados desde una de estas direcciones
Las direcciones especificadas en esta área son excepciones a las Restricciones de Mensajes Entrantes. Se permiten comodines. Así, si designa "*@altn.com" como excepción, todos los mensajes entrantes de cualquier dirección en altn.com serán aceptados y enviados a la cuenta.

Nuevas direcciones
Si desea añadir una dirección de excepción a la lista de Restricciones de Mensajes Entrantes regístrela aquí y luego haga clic en el botón *Agregar*.

Agregar
Después de introducir una dirección en la opción *Nuevas direcciones*, haga clic en este botón para agregarla a la lista de excepciones.

Quitar
Si desea quitar una dirección de la lista de restricciones, seleccione la dirección y luego haga clic en este botón.

Los mensajes de dominios externos deben...
Estas opciones en la lista desplegable gobiernan lo que hará MDaemon con los mensajes destinados a esta cuenta, pero originados de no locales. Puede

escoger cualquiera de las siguientes opciones:

Rechazado – Los mensajes restringidos serán rechazados por MDaemon.

Devuelto al remitente – Los mensajes de dominios restringidos se devolverán al remitente.

Enviado al administrador de correo – Los mensajes restringidos serán aceptados pero enviados al postmaster en lugar de a esta cuenta.

Enviado a... - Los mensajes restringidos serán aceptados pero entregados a la dirección que especifique en la casilla de texto a la derecha.

Restricciones de Mensajes Salientes

Restringir mensajes A dominios externos
Haga clic en esta casilla si desea prevenir que la cuenta envíe mensajes a dominios no-locales.

...excepto si son enviados a una de estas direcciones
Las direcciones especificadas en esta área son excepciones a las Restricciones de Mensajes Salientes. Se permiten comodines. Así, si designa "*@altn.com" como excepción, todos los mensajes salientes dirigidos a cualquier dirección en altn.com serán entregados normalmente por MDaemon.

Nuevas direcciones
Si desea añadir una dirección de excepción a la lista de Restricciones de Mensajes Salientes tecléela aquí y luego haga clic en el botón agregar.

Agregar
Después de introducir una dirección en la opción *Nuevas direcciones*, haga clic en este botón para agregarla a la lista de excepciones.

Quitar
Si desea quitar una dirección de la lista de restricciones, seleccione la dirección y luego haga clic en este botón.

Los mensajes hacia dominios externos deben ser...
Estas opciones en la lista desplegable controlan lo que hará MDaemon con los mensajes originados por esta cuenta, pero destinados a un dominio no-local. Puede escoger cualquiera de las siguientes opciones:

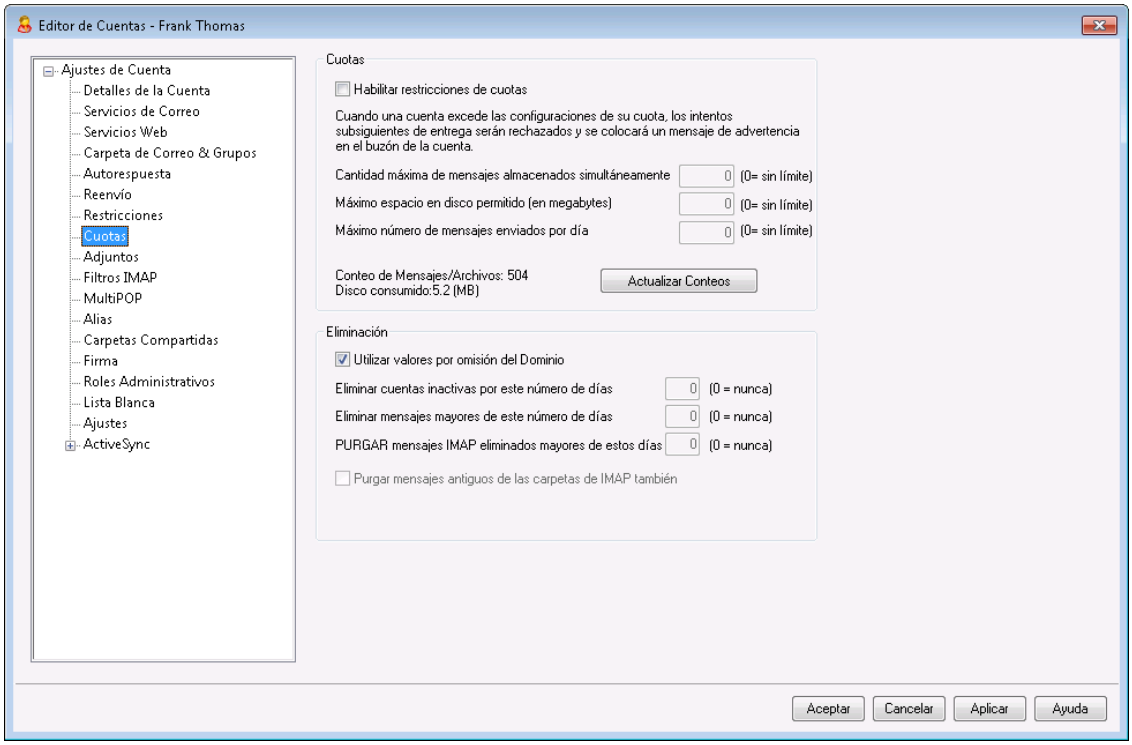
Rechazado – Los mensajes restringidos serán rechazados por MDaemon.

Devuelto al remitente – Los mensajes hacia dominios restringidos se devolverán al remitente.

Enviado al postmaster – Los mensajes restringidos serán aceptados pero enviados al postmaster en lugar de al destinatario.

Enviado a... - Los mensajes restringidos serán aceptados pero entregados a la dirección que especifique en la casilla de texto a la derecha.

5.1.1.8 Cuotas



Cuotas

Habilitar restricciones de cuotas
Marque esta caja si desea especificar un número máximo de mensajes que la cuenta puede almacenar o establecer un máximo de espacio en disco que la cuenta puede usar (incluyendo cualquier archivo adjunto en la carpeta Documentos de la cuenta) o definir un número máximo de mensajes que la cuenta puede enviar por día vía SMTP. Si se intenta un envío de correo que exceda el máximo de mensajes o el límite de espacio, el mensaje será rechazado y se colocará un mensaje de advertencia adecuado en el buzón del usuario. Si una recolección MultiPOP 739 provoca que se supere el máximo de la cuenta, se emitirá una advertencia similar y los registros MultiPOP de la cuenta se desactivarán automáticamente (pero no se eliminarán de la base de datos).

Use la opción *Enviar un mensaje de advertencia al usuario con el porcentaje de su cuota que se ha alcanzado* en "Cuentas » Ajustes de Cuentas » Cuotas 812" para hacer que se envíe un mensaje de advertencia cuando una cuenta se acerque a cuota límite. Cuando la cuenta exceda el porcentaje designado en las restricciones *Cantidad máxima de mensajes almacenados simultáneamente* o *Espacio máximo permitido en disco,* se enviará un mensaje de advertencia a la cuenta, a medianoche. El mensaje listará el número de mensajes almacenados, el tamaño del

buzón, y el porcentaje usado y restante. Además, si existe una advertencia en el buzón de la cuenta, se reemplazará con un mensaje actualizado.

Cantidad máxima de mensajes almacenados simultáneamente
Use esta opción para designar el máximo número de mensajes que se pueden almacenar para la cuenta. Si usa "0" en esta opción significa que no habrá límite al número de mensajes permitidos.

Espacio máximo permitido en disco (en megabytes)
Use esta opción para definir la máxima cantidad de espacio en disco que la cuenta puede usar, incluyendo cualquier archivo adjunto que esté almacenado en la carpeta Documentos de la cuenta. Si usa "0" en la opción significa que no habrá límite a la cantidad de espacio en disco que la cuenta puede usar.

Número máximo de mensajes a enviar por día
Utilice esta opción para definir el número máximo de mensajes que una cuenta puede enviar diariamente vía SMTP. Si la cuenta alcanza este límite entonces los correos nuevos de la cuenta se rechazarán hasta que el contador se restablezca a medianoche. Utilice "0" en la opción si no desea limitar el número de mensajes que la cuenta puede enviar.

Actualizar conteos
Dé clic en este botón para actualizar las estadísticas *Conteo de Mensajes/Archivos* y el *Espacio en disco consumido* que se despliega a la izquierda.

Eliminación

Las opciones en esta sección se usan para designar cuándo o si esta cuenta será eliminada por MDaemon si permanece inactiva. Puede designar también si los mensajes antiguos pertenecientes o no a la cuenta serán eliminados después de una cantidad de tiempo. Cada día a medianoche, MDaemon eliminará todos los mensajes que hayan excedido el límite de tiempo establecido, o eliminará la cuenta completamente si ha alcanzado el límite de inactividad.

Usar los valores por omisión del Dominio
Las configuraciones de Eliminación por defecto, son específicas de cada dominio y se ubican en la pantalla Ajustes 219 en el Administrador de Dominios. Si desea sobrescribir los valores por defecto del dominio para esta cuenta, desmarque esta casilla y establezca los valores deseados en las opciones siguientes.

Eliminar la cuenta si ha estado inactiva por este número de días (0 = nunca)
Especifique el número de días que desea permitir que la cuenta esté inactiva antes de ser eliminada. Un valor de "0" en este control significa que la cuenta nunca será eliminada debido a la inactividad.

Eliminar mensajes de más de este número de días (0 = nunca)
Este es el número de días que un mensaje dado puede residir en el buzón de la cuenta antes de que sea eliminado por MDaemon automáticamente. Un valor de "0" significa que los mensajes nunca se eliminarán debido a su edad.
Nota: El ajuste de esta opción no aplica a mensajes contenidos en carpetas IMAP a menos que también habilite la opción siguiente "*DEPURAR también mensajes antiguos de carpetas IMAP*".

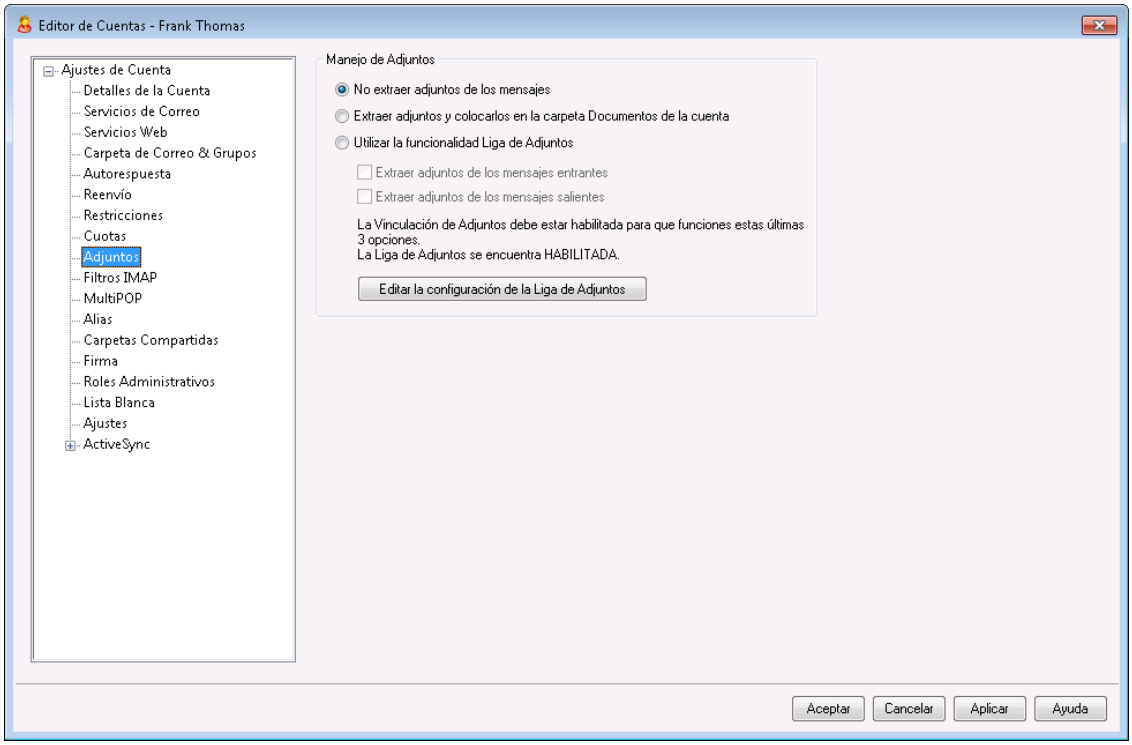
DEPURAR mensajes IMAP eliminados mayores de este número de días (0 = nunca)
Use este control para especificar el número de días que desea permitir que los mensajes IMAP que están marcados para eliminación permanezcan en las carpetas de este usuario. Los mensajes marcados para eliminación por un tiempo superior a este número de días serán purgados. Un valor de "0" significa que los mensajes marcados para eliminación nunca serán purgados debido a su edad.

DEPURAR mensajes antiguos de las carpetas IMAP también
Haga clic en esta casilla si desea que la opción anterior "*Eliminar mensajes de más de...*" se aplique también a los mensajes en carpetas IMAP. Cuando este control está deshabilitado, los mensajes regulares contenidos en carpetas IMAP no se eliminarán debido a su antigüedad.

Ver:

Administrador de Plantillas » Cuotas 812
Ajustes de Cuentas » Cuotas 860

5.1.1.9 Adjuntos



Manejo de Adjuntos

Esta pantalla se utiliza para controlar si MDaemon extraerá o no los archivos adjuntos de los mensajes de correo de la cuenta. Puede utilizar el Administrador de Plantillas 815 para definir los parámetros por omisión de estas opciones.

No extraer adjuntos de los mensajes
Si se selecciona esta opción, los adjuntos no serán extraídos de los mensajes de la cuenta. Los mensajes con adjuntos se manejarán normalmente, dejando los adjuntos intactos.

Extraer adjuntos y colocarlos en la carpeta Documentos de la cuenta
Si se habilita, esta opción hace que MDaemon automáticamente extraiga cualquier archivo adjunto Base64 MIME que encuentre en los mensajes de correo entrantes para la cuenta. Los archivos extraídos serán eliminados del mensaje entrante, decodificados y colocados en la carpeta Documentos de la cuenta. Se coloca entonces una nota en el cuerpo del mensaje, informando los nombres de los archivos que fueron extraídos. Esta opción no proporciona una liga a los adjuntos almacenados, pero los usuarios pueden utilizar Webmail 321 para tener acceso a su carpeta Documentos.

Utilizar la Vinculación de Adjuntos
Seleccione esta opción si desea utilizar la Vinculación de Adjuntos para los mensajes entrantes y salientes que contienen archivos adjuntos.

Si se selecciona esta opción, pero la Vinculación de Adjuntos está deshabilitada en el diálogo Vinculación de Adjuntos 366, los archivos adjuntos no serán extraídos.

Extraer adjuntos de los mensajes entrantes
Cuando se encuentra habilitada, los adjuntos serán extraídos de los mensajes entrantes de la cuenta y sean almacenados en la ubicación definida en el diálogo Vinculación de Adjuntos 366. Se colocan ligas URL en el cuerpo del mensaje, sobre las que el usuario puede dar clic para descargar los archivos. Por razones de seguridad estas ligas URL no contienen rutas directas de archivo. En lugar de esto, contienen un identificador único (GUID) que el servidor utiliza para mapear el archivo a la ruta actual. Este mapeo GUID se almacena en el archivo `AttachmentLinking.dat`. Esta opción se encuentra habilitada por omisión.

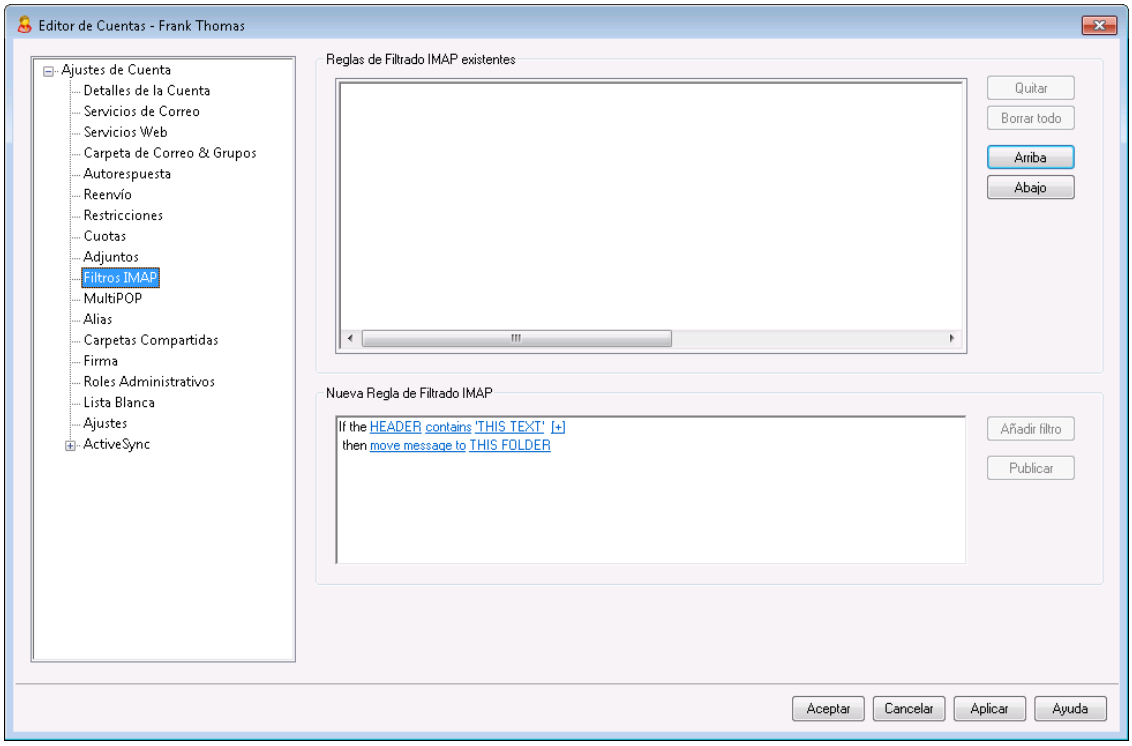
Extraer adjuntos de los mensajes salientes
Marque esta casilla si desea utilizar la Vinculación de Adjuntos para extraer adjuntos de los mensajes salientes de la cuenta. Cuando la cuenta envía correo, la Vinculación de Adjuntos extraerá el archivo, lo almacenará y reemplazará con una URL para descargarlo.

Editar la configuración de Vinculación de Adjuntos
Dé clic en este botón para abrir el diálogo Vinculación de Adjuntos 366.

Ver:

Vinculación de Adjuntos 718
Administrador de Plantillas » Adjuntos 815

5.1.1.10 Filtros IMAP



Los usuarios de Webmail[321] y IMAP pueden enrutar automáticamente su correo a carpetas específicas en el servidor usando filtros. De manera similar a los Filtros de Contenido[645], MDaemon examinará los encabezados de cada mensaje entrante de la cuenta y los comparará con los filtros de la cuenta. Cuando un mensaje para la cuenta coincida con uno de sus filtros, MDaemon lo moverá a la carpeta especificada en dicho filtro, eliminará el mensaje o lo redireccionará o enviará a la dirección de correo que se haya seleccionado. Este método es mucho más eficiente (tanto para el cliente como para el servidor) que intentar filtrar los mensajes en el cliente y dado que algunos clientes de correo ni siquiera aceptan reglas locales o filtrado, los filtros IMAP les proporcionarán dichas opciones.

Los administradores pueden crear filtros a través de la pantalla Filtros IMAP del Editor de Cuentas, o usando MDaemon Administración Remota[354]. Sin embargo, también pueden otorgar permiso a sus usuarios para crear y gestionar los filtros ellos mismos desde Webmail o Administración Remota. Estos permisos pueden establecerse en la pantalla de Servicios Web[720].

Reglas de filtrado IMAP existentes

Este cuadro muestra la lista de todos los filtros creados para la cuenta del usuario. Los filtros se procesan en el orden en que están listados hasta que se encuentra una coincidencia. Así pues, tan pronto como un mensaje coincide con uno de los filtros, será movido a la carpeta especificada en el filtro y el filtro de proceso para dicho mensaje terminará. Use los botones *Arriba* y *Abajo* para mover los filtros a diferentes posiciones en la lista.

Quitar
Haga clic en un filtro de la lista y luego haga clic en *Quitar* para quitarlo de ella.

Borrar todo
Haga clic en este botón para eliminar todos los filtros del usuario.

Arriba
Haga clic en un filtro de la lista y luego en este botón para moverlo a una posición superior en la lista.

Abajo
Haga clic en un filtro en la lista y luego en este botón para moverlo en una posición inferior en la lista.

Nueva regla de filtrado IMAP

Utilice las ligas en esta área para construir una nueva regla de filtrado. Cuando su regla esté terminada, dé clic en **Agregar Filtro** para agregarla a las *Reglas de Filtrado IMAP existentes*.

Condiciones de Filtro

Dé clic en las ligas en la primera sección de la regla de filtrado para definir las condiciones del filtro. Cuando un mensaje coincide con las condiciones del filtro entonces la Acción de Filtrado se ejecutará.

HEADER
Dé clic en "**HEADER"** para seleccionar el encabezado u otro componente del mensaje que desea examinar como parte de la regla de filtrado. Puede elegir: **TO**, **CC**, **FROM**, **SUBJECT**, **SENDER**, **LIST-ID**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE, MESSAGE BODY u Otro...** Si selecciona "Otro..." se abrirá una caja de Condición de Filtro para que especifique el nombre del encabezado que no está enlistado. Si da clic en MESSAGE SIZE, las ligas "contiene" y 'ESTE TEXTO' serán reemplazadas por "es mayor que" y "0 KB" respectivamente.

contiene / es mayor que
Dé clic en "**contiene**" o **es mayor que** para seleccionar el tipo de condición a definir cuando se examina el encabezado. Por ejemplo, si el encabezado existe o no existe, contiene o no contiene cierto texto, inicia o termina con cierto texto o algo similar. Puede elegir de las condiciones siguientes: **starts with**, **ends with**, **is equal to**, **is not equal to**, **contains**, **does not contain**, **exists**, **does not exist**, **is greater than**, o **is less than**. Las condiciones "is greater than" y "is less than" solo están disponibles cuando la liga HEADER se configura a "MESSAGE SIZE."

ESTE TEXTO / 0 KB
Ingrese el texto que desea que busque MDaemon cuando revise el encabezado que seleccionó para filtrar. Cuando la opción HEADER se configura a MESSAGE SIZE, la liga dirá "0 KB" y el diálogo Condición del Filtro tendrá una caja para definir el valor "Message size in KB."

[+] [x] and
Dé clic en **[+]** si desea definir dos o más condiciones para la regla de filtrado. Esto agregará otra línea conteniendo los componentes "HEADER," "contains," y "THIS TEXT" para expandir el filtro.

Al probar un mensaje con múltiples condiciones contra una regla de filtrado, por omisión el mensaje debe pasar cada una de las condiciones para que cumpla la regla. Dé clic en "**and**" y luego seleccione "**or**" si desea que el mensaje coincida con la regla cuando pasa cualquiera de las condiciones.

Cuando una regla de filtrado contiene múltiples líneas, puede dar clic en **[x]** al lado de cualquier línea que desee eliminar.

Acciones de Filtrado

Dé clic en las ligas en la sección de abajo de la regla de filtrado para definir la acción a tomar cuando un mensaje coincide con las condiciones del filtro.

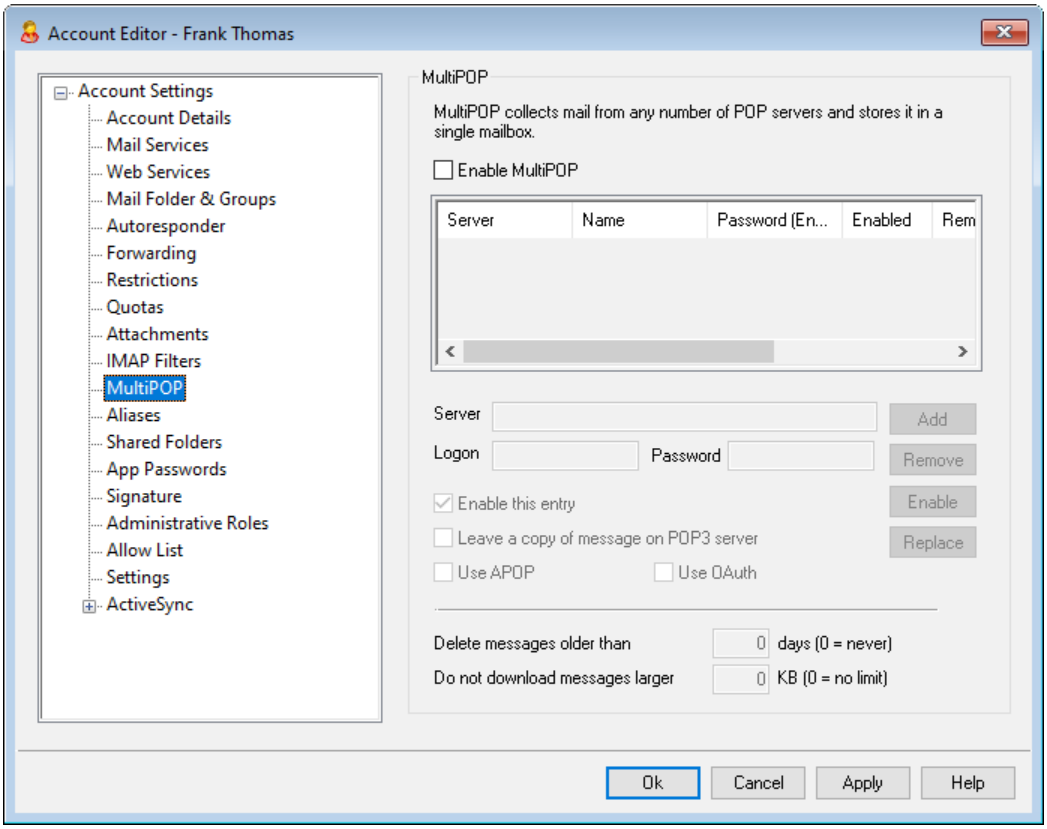
mover mensaje a
Dé clic en "**move message to**" para definir la acción de filtrado. Puede elegir: **move message to**, **delete message**, **redirect message to**, o **forward message to**.

THIS FOLDER / EMAIL
Si selecciona la acción "move message to", dé clic en **THIS FOLDER** para definir la carpeta a la que se deberá mover el mensaje. Si selecciona redirigir o reenviar el mensaje, dé clic en **EMAIL** y registre la dirección de correo del destinatario. Para mensajes redirigidos, no se harán cambios al encabezado o cuerpo del mensaje. Lo único que se modifica es el destinatario en el sobre SMTP. Para mensajes reenviados, se creará y reenviará un nuevo mensaje, con el encabezado Subject y el contenido del cuerpo tomados del mensaje original.

Agregar filtro
Cuando termine de crear su nueva regla, dé clic en este botón para agregarla a las *Reglas IMAP de Filtrado* existentes.

Publicar
Luego de crear una regla, dé clic en **Publicar** si desea copiar esa regla a los usuarios pertenecientes al dominio de esa cuenta. Se le solicitará que confirme su decisión de copiar la regla a las otras cuentas.

5.1.1.11 MultiPOP



La funcionalidad de MultiPOP permite crear un número ilimitado de combinaciones POP3 de host/usuario/contraseña para recolección de mensajes de correo desde múltiples orígenes. Esto es útil para usuarios que tienen cuentas de correo en múltiples servidores, pero prefieren recolectar y agrupar su correo junto en un sólo sitio. Antes de ser colocados en el buzón de usuario, el correo recolectado MultiPOP primero se coloca en la cola local para que sea procesado como el resto del correo, teniendo Filtros de Contenido y autorespuestas aplicados. Las opciones de programación para MultiPOP están ubicadas en: Configuración » Programación de Eventos » Programación de Correo » Recolección MultiPOP 383.

Habilitar MultiPOP
Haga clic en esta casilla para habilitar el procesamiento MultiPOP para esta cuenta. Si desea permitir que el usuario edite sus ajustes MultiPOP en MDRA 354, habilite la opción "*...editar ajustes MultiPOP*" en la página Servicios Web 720 de la cuenta. Cuando están habilitadas esta y la opción de servicios web, estará disponible la página Buzones en Webmail 321 para que el usuario administre sus ajustes de correo MultiPOP. La opción global para habilitar/deshabilitar el servidor MultiPOP se localiza en: Configuración » Ajustes de Servidor » MultiPOP 151. Si esta opción está deshabilitada, MultiPOP no se puede utilizar aún cuando esta opción en la cuenta esté habilitada.

Crear o Editar una Entrada MultiPOP

Servidor
Introduzca el servidor POP3 desde el que desea recolectar correo. Si este servidor requiere que usted se conecte a un puerto específico distinto al puerto POP3 estándar, agregue "`:[port]`" al nombre del servidor. Por ejemplo, "`mail.example.com:1000`". Al recolectar desde Gmail o Microsoft (Office) 365,

utilice "pop.gmail.com:995" o "outlook.office365.com:995", respectivamente.

Inicio de sesión
Introduzca el usuario POP3 o inicio de sesión asociado a la cuenta de correo del servidor especificado arriba.

Contraseña
Introduzca la contraseña POP3 o APOP usada para acceder a la cuenta de correo del servidor especificado.

Usar APOP
Haga clic en esta casilla si quiere que las entradas de MultiPOP usen el método de autentificación APOP cuando descarguen correo de su host correspondiente.

Usar OAuth
Seleccione este método de autentificación al recolectar correo desde Gmail o de Office365. Vea las Instrucciones MultiPOP OAuth 2.0 151 en la página Ajustes de Servidor » MultiPOP para obtener más información. **Nota:** la opción "*...editar ajustes MultiPOP*" en la página Servicios Web 720 de la cuenta debe estar habilitada para que el usuario pueda utilizar OAuth con Gmail u Office 365, porque él/ella debe iniciar sesión en Webmail e ir a la página **Buzones** a fin de autentificar el registro del buzón Gmail u Office 365.

Dejar una copia del mensaje en el servidor POP3
Haga clic en esta casilla si quiere dejar una copia de los mensajes recolectados en el servidor. Esto es útil cuando planea descargar estos mensajes posteriormente desde una ubicación diferente. Si desea ignorar esta opción para todos los usuarios, lo que significa que los mensajes siempre serán eliminados del servidor POP luego de ser descargados de MDaemon, puede hacerlo habilitando la opción "*MultiPOP siempre elimina correo de todos los servidores luego de la recolección*" en Configuración » Servidor Ajustes » MultiPOP 151.

Agregar
Después de introducir toda la información para la nueva entrada MultiPOP, haga clic en este botón para agregarlo a la lista.

Quitar
Si desea eliminar una de sus entradas MultiPOP, seleccione la entrada deseada y luego haga clic en este botón.

Habilitar/Deshabilitar
Este botón alterna el estado de los registros MultiPOP seleccionados, dándole control sobre si MDaemon recolectará correo para ese registro o lo omitirá cuando realice el proceso MultiPOP.

Reemplazar
Para editar un registro, haga clic en él sobre la lista, realice los cambios deseados y haga clic en este botón para aplicar dichos cambios.

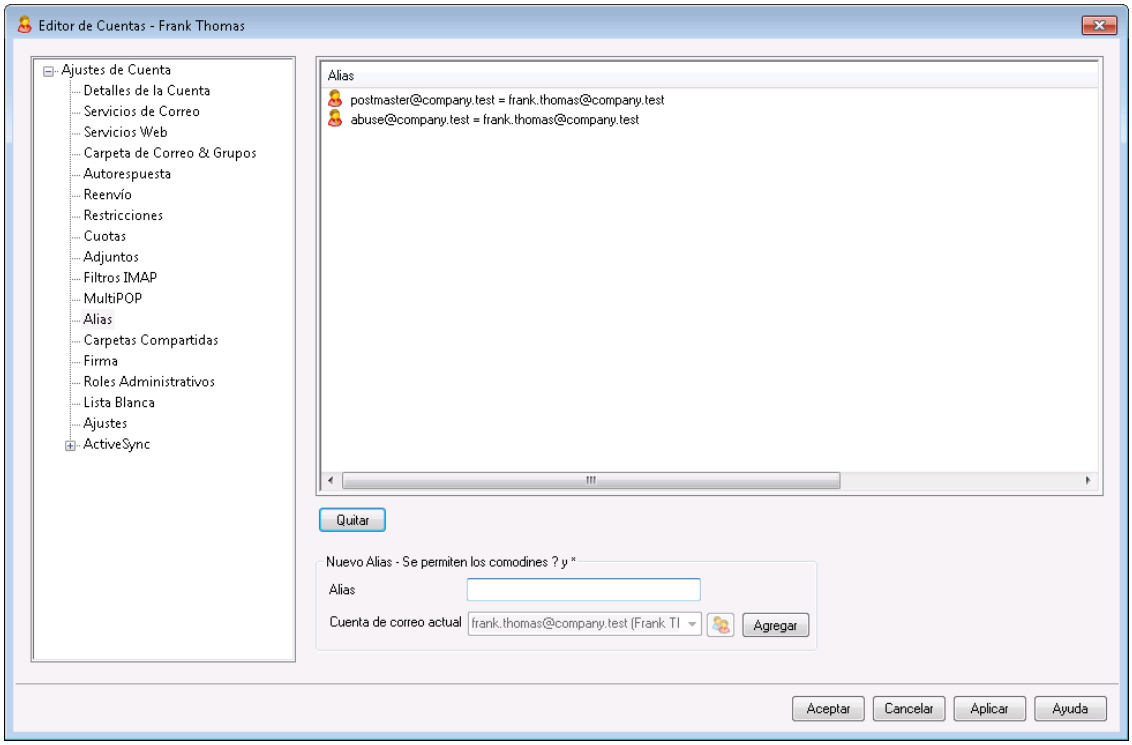
Eliminar los mensajes más antiguos de [XX] días (0 = nunca)
Este es el número de días que un mensaje puede permanecer en el host MultiPOP antes de ser eliminado. Use "0" si no desea eliminar mensajes antiguos.

No descargar mensajes que tengan más de [XX] KB (0 = sin límite)
Introduzca el valor aquí si desea limitar el tamaño de los mensajes que se descarguen.

Ver:

Ajustes de Servidor » MultiPOP 151
Programación de Eventos » Recolección MultiPOP 383

5.1.1.12 Alias



Esta pantalla enlista todos los alias 834 de direcciones asociados con la cuenta y puede ser utilizada para agregarlos o removerlos.

Eliminar un Alias

Para eliminar un alias de una cuenta, selecciónelo en la lista y dé clic en **Remover**.

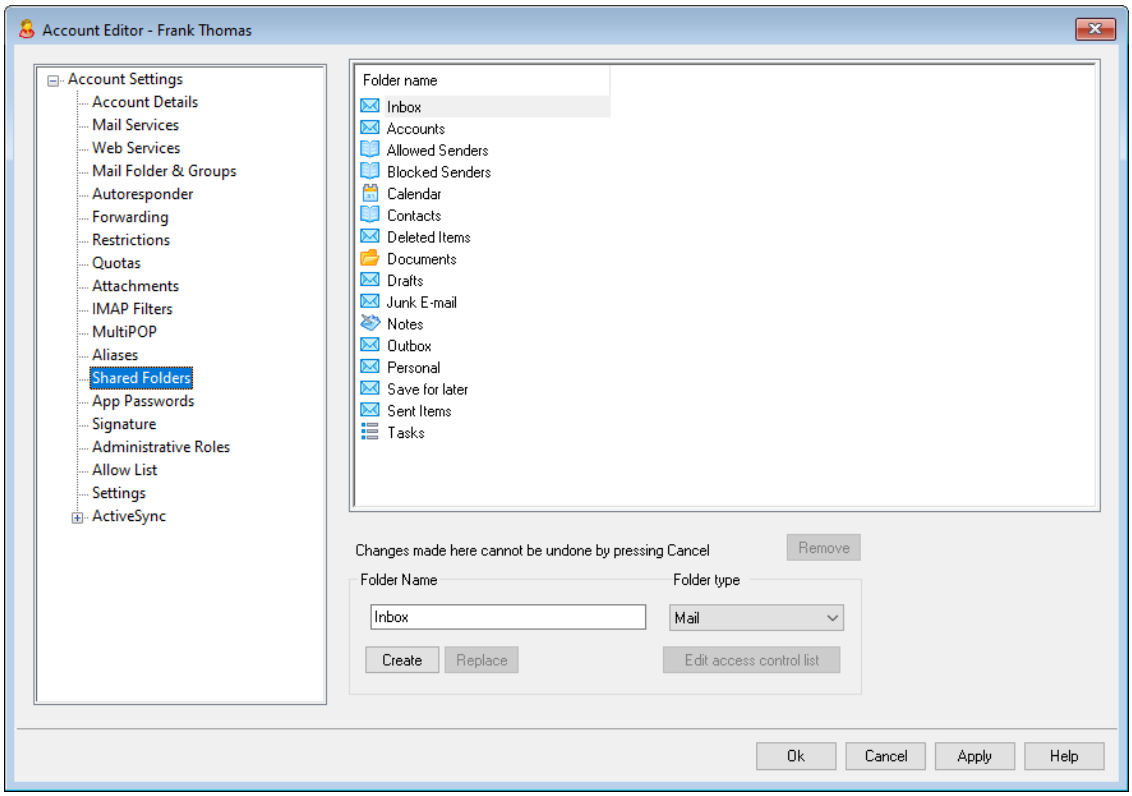
Agregar un Alias

Para agregar un nuevo alias a la cuenta, en la ventana *Alias* teclee la dirección que desea asociar con la cuenta y dé clic en **Agregar**. Se permiten los comodines "?" y "*", representando caracteres únicos o palabras únicas, respectivamente.

Ver:

Ajustes de Cuentas » Alias 834

5.1.1.13 Carpetas Compartidas



Esta pantalla sólo está disponible cuando la opción *Activar carpetas públicas* está activada en la pantalla Carpetas Públicas y Compartidas 128, ubicada en Configurar » Configuración de Servidor » Carpetas Públicas y Compartidas. Las Carpetas Públicas se pueden administrar desde Administrador de Carpetas Públicas 314

La sección superior muestra todas las carpetas IMAP del usuario y puede ser usada para compartir el acceso a ellas con otros usuarios de MDaemon o Grupos 781. Cuando la cuenta se crea por primera vez, esta área sólo tendrá la Bandeja de entrada listada hasta que use las opciones *Nombre de la carpeta y Crear* (o las opciones de Filtros IMAP 737) para añadir carpetas a ésta. Las

subcarpetas en esta lista tendrán los nombres de carpeta y subcarpeta separados por una barra.

Quitar
Para quitar una carpeta compartida IMAP de la lista, seleccione la carpeta deseada y luego pulse el botón *Quitar.*

Nombre de la carpeta
Para añadir una nueva carpeta a la lista, especifique un nombre para ella en esta opción y haga clic en *Crear.* Si quiere que la nueva carpeta sea una subcarpeta de una de las carpetas en la lista, entonces ponga delante del nombre el nombre de la carpeta superior y una barra. Por ejemplo, si la carpeta superior es "Mi carpeta" entonces la nueva subcarpeta sería "Mi Carpeta/Mi nueva carpeta". Si no quiere que sea una subcarpeta, simplemente llame a la nueva carpeta "Mi nueva carpeta" si ningún prefijo.

Anidar Abajo
Utilice este menú desplegable para elegir la carpeta padre bajo la cual se anidará esta carpeta compartida.**Nota:** Esta opción solo está disponible en la interface web de MDRA 354.

Tipo de carpeta
Use esta lista desplegable para escoger el tipo de carpeta que desea crear: correo, Calendario, Contactos, y demás.

Crear
Después de especificar el nombre de carpeta haga clic en este botón para añadir la carpeta a la lista.

Reemplazar
Si desea editar una de las Carpetas Compartidas, haga clic en la entrada, haga el cambio deseado, y luego haga clic en *Remplazar.*

Editar la lista del control de acceso
Escoja esta carpeta y luego haga clic en este botón para abrir el diálogo de Lista de Control de Acceso 316 para dicha carpeta. Use esta Lista de Control de Acceso para designar a los usuarios o grupos que podrán acceder a la carpeta y a los permisos de carpeta para cada usuario y grupo.

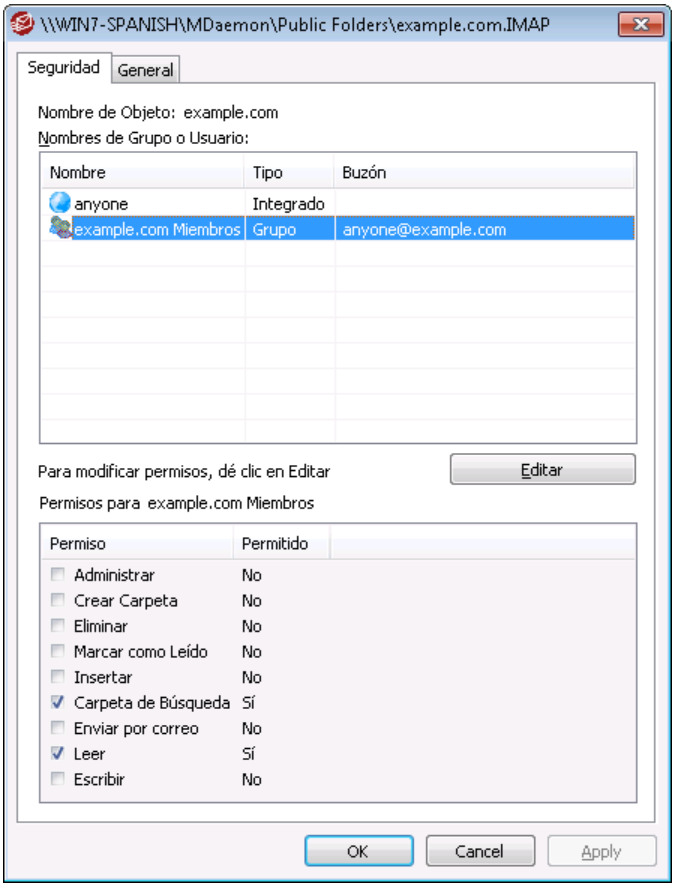
Ver:

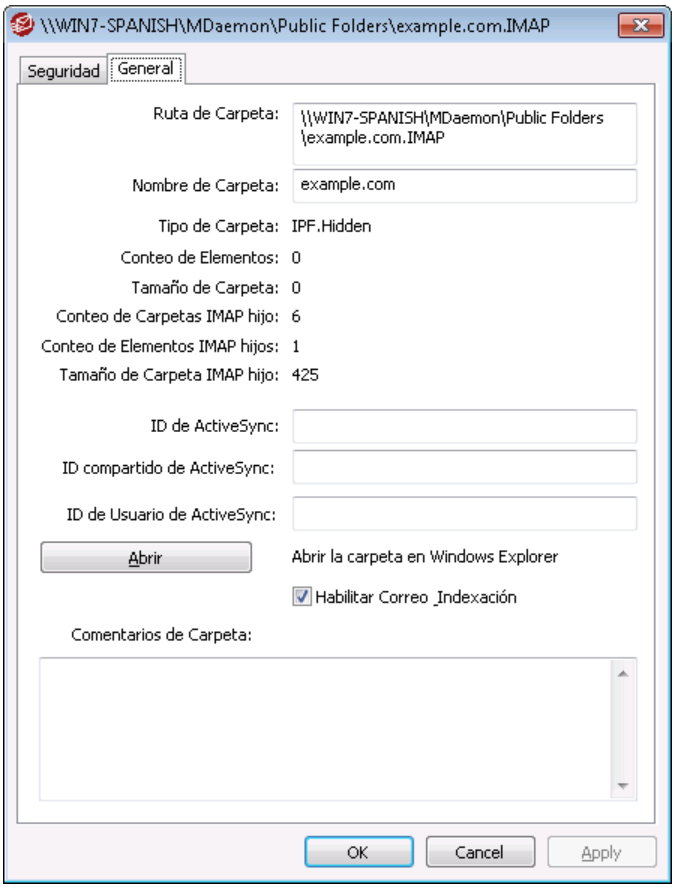
Lista de Control de Acceso 316
Administrador de Carpetas Públicas 314

5.1.1.13.1 Lista de Control de Acceso

La Lista de Control de Acceso (Access Control List - ACL) se utiliza para asignar permisos de acceso a usuarios o grupos para sus carpetas públicas y compartidas 125. Se ingresa a través del botón *Editar ACLs* en el Administrador de

Carpetas Públicas 314 o con el botón *Editar lista de control de acceso* en la pantalla Carpetas Compartidas 743 del Editor de Cuentas.





Seguridad

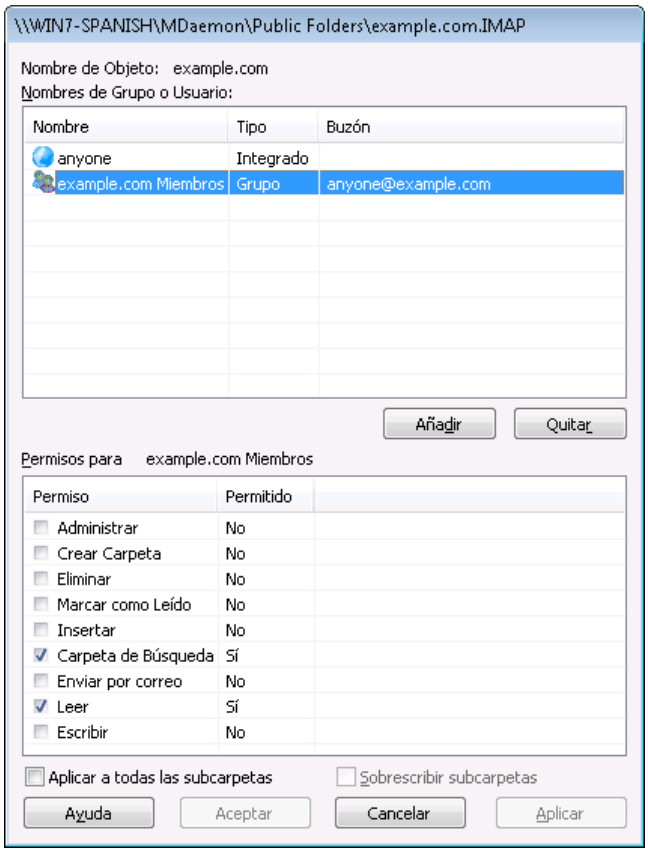
Esta pestaña despliega la lista de grupos o usuarios asociados con la carpeta y los permisos de acceso específicos otorgados a cada uno. Seleccione un grupo o usuario en la lista para desplegar sus permisos 319 y revisarlos en la ventana de Permisos abajo. Para editar los permisos, dé clic en **Editar** 318.

General

Esta pestaña despliega las propiedades de la carpeta, tales como su ruta, nombre, tipo, tamaño y demás.

Editor de ACLs

De clic en **Editar** en la pestaña Seguridad de los ACLs para abrir el Editor de ACLs para modificar los permisos de acceso.



Nombre del Objeto
Este es el nombre del objeto o carpeta al que se aplicará los permisos ACL.

Grupo o nombres de usuarios
Estos son los grupos o usuarios para los que se pueden haber otorgado algún nivel de permisos de acceso. Seleccione un grupo o usuario para desplegar sus permisos en la ventaja abajo *Permisos para <grupo o usuario>*. Marque la casilla siguiente para seleccionar cualquier permiso de acceso que desee otorgar al grupo o usuario.

Agregar
Par otorgar permisos de acceso a un grupo o usuario que no aparezca en la lista arriba, dé clic en **Agregar**[320].

Remover
Para remover un grupo o usuario, seleccione su entrada en la lista arriba y dé clic en **Remover**.

Permisos para <grupo o usuario>
Marque la casilla siguiente para cualquier permiso de acceso que desee otorgar al grupo o usuario seleccionado arriba.

Puede otorgar los siguientes permisos de control de acceso:

Administrar – el usuario puede administrar los ACL para esta carpeta.

Crear – el usuario puede crear subcarpetas dentro de esta carpeta.

Eliminar – el usuario puede eliminar elementos de esta carpeta.

Marcar Leído – el usuario puede modificar el estatus leído/no leído de los mensajes en esta carpeta.

Insertar – el usuario puede agregar y copiar elementos a esta carpeta.

Carpeta de Búsqueda – el usuario puede ver esta carpeta en su lista personal de carpetas IMAP.

Postear – el usuario puede enviar correo directamente a esta carpeta (si la carpeta lo permite).

Leer – el usuario puede abrir esta carpeta y visualizar sus contenidos.

Escribir – el usuario puede modificar las banderas de los mensajes en esta carpeta.

Aplicar a todas las carpetas hijo
Marque esta casilla si desea aplicar los permisos de control de acceso de esta carpeta a cualquier subcarpeta que contenga. Agregará los permisos de usuario y de grupo a las carpetas hijo, reemplazando donde exista conflicto. Sin embargo, no eliminará los permisos de cualquier otro usuario o grupo que en ese momento tenga acceso a esas carpetas.

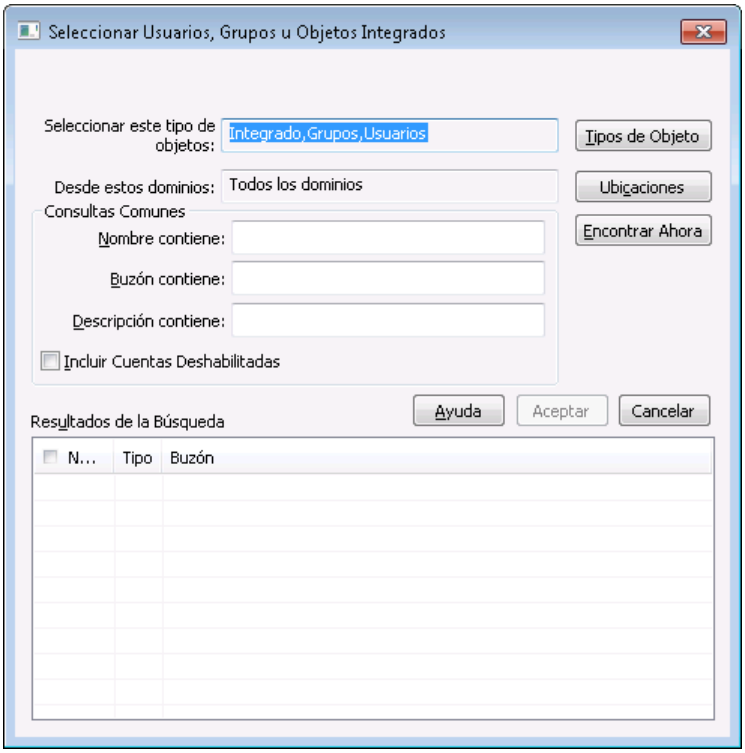
Ejemplo,

La carpeta padre otorga ciertos permisos a `Usuario_A` y `Usuario_B`. La carpeta hijo otorga permisos a `Usuario_B` y `Usuario_C`. Esta opción agregará los permisos de `Usuario_A` a la carpeta hijo, reemplazará los permisos en la carpeta hijo del `Usuario B` con los de la carpeta padre y no hará nada con los permisos del `Usuario C`. Por consiguiente, la carpeta hijo tendrá entonces permisos para `Usuario A`, `Usuario_B` y `Usuario C`.

Sobrescribir carpetas hijo
Marque esta casilla si desea reemplazar todos los permisos de acceso de las carpetas hijo con los permisos actuales de la carpeta padre. Los permisos de las carpetas hijo serán entonces idénticos a los de la carpeta padre.

Agregar un Grupo o Usuario

Dé clic en **Agregar** en el Editor ACL si desea agregar otro grupo o usuario a la Lista de Control de Acceso. Esto abre la pantalla Agregar Grupo o Usuario que puede utilizar para buscarlos y agregarlos.



Seleccionar esos tipos de objeto
Dé clic en **Tipos de Objeto...** para seleccionar los tipos de objeto que desea buscar para los grupos o usuarios que desea agregar. Puede seleccionar: Predeterminados, Grupos y Usuarios.

De estas ubicaciones
Dé clic en **Ubicaciones...** para seleccionar los dominios en los que desea buscar. Puede seleccionar todos sus dominios de MDaemon o algún dominio en específico.

Consultas Comunes
Utilice las opciones en esta sección para reducir su búsqueda especificando toda o una parte del nombre de usuario, dirección de correo o los contenidos de la Descripción[715] de la cuenta. Deje estos campos en blanco si desea que los resultados de la búsqueda contengan todo grupo y usuario que coincida con los Tipos de Objeto y Ubicaciones especificados arriba.

Incluir Cuentas Deshabilitadas
Marque esta casilla si desea incluir cuentas deshabilitadas[715] en su búsqueda.

Encontrar Ahora
Luego de que haya especificado todos los criterios de búsqueda, dé clic en **Encontrar Ahora** para ejecutar la consulta.

Resultados de la Consulta
Luego de ejecutar la búsqueda, seleccione cualquiera de los grupos o usuarios deseados en los Resultados de la Consulta y dé clic en **OK** para agregarlos al ACL.

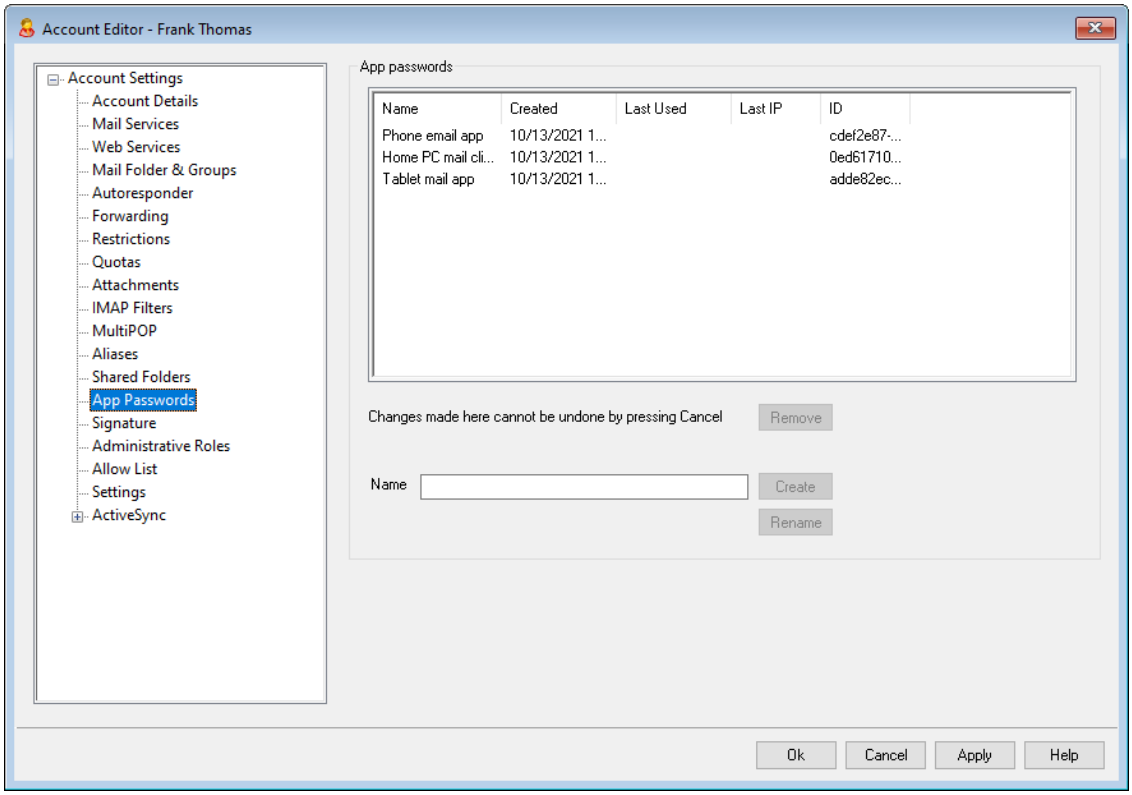
Los Permisos de Acceso se controlan a través del soporte de MDaemon para Listas de Control de Acceso (Access Control Lists - ACL). ACL es una extensión de Internet Message Access Protocol (IMAP4), que le permite crear una lista de acceso para cada una de sus carpetas IMAP de mensajes, otorgando permisos de acceso por carpeta a otros usuarios que también tengan cuentas en su servidor de correo. Si su cliente de correo no soporta ACL aún puede establecer los permisos vía los controles de este diálogo.

ACL se discute completamente en la RFC 2086, que se puede encontrar en: http://www.rfc-editor.org/rfc/rfc2086.txt.

Ver:

Administrador de Carpetas Públicas 314
Descripción General de Carpetas Públicas 125
Carpetas Públicas & Compartidas 128
Editor de Cuentas » Carpetas Compartidas 743
Listas de Distribución » Carpetas Públicas 304

5.1.1.14 Contraseñas de Apps



Contraseñas de Apps

Las Contraseñas de Apps son contraseñas muy fuertes, generadas aleatoriamente para ser utilizadas en clientes de correo y apps, para ayudar a hacer que sus apps de correo sean más seguras dado que no pueden ser protegidas por la Autentificación de Dos Factores 720 (2FA). 2FA es una manera segura para que el usuario inicie sesión en Webmail o en MDaemon Administración Remota (MDRA), pero una aplicación de correo no la puede utilizar porque la app debe poder tener acceso al correo en segundo plano sin que el usuario tenga que ingresar un código de su app de autentificación. La funcionalidad Contraseñas de Apps le permite crear contraseñas fuertes y seguras para utilizar en sus apps, manteniendo la contraseña de su cuenta asegurada por 2FA. Las Contraseñas de Apps solo se pueden utilizar en aplicaciones de correo, no se pueden utilizar para iniciar sesión en Webmail o en MDRA. Esto significa que aún si una de sus Contraseñas de App estuviera comprometida, el usuario no-autorizado no podría tener acceso a su cuenta para modificar la contraseña o algún otro ajuste, pero usted, sin embargo, podrá iniciar sesión en su cuenta con la contraseña de la cuenta y 2FA, para eliminar la Contraseña de App comprometida y crear una nueva si fuera necesario.

Si no desea permitir a algún usuario utilizar Contraseñas de Apps, lo puede hacer deshabilitando la opción *...editar contraseñas de apps* 720 en la página de Servicios Web del usuario. Si desea deshabilitar el soporte a las Contraseñas de Apps para todos los usuarios, lo puede hacer utilizando la opción *Habilitar Contraseñas de Apps* 855 en la página de Contraseñas.

Requerimientos y recomendaciones de las Contraseñas de Apps

- A fin de crear Contraseñas de Apps, 2FA debe estar habilitada para la cuenta (aunque puede deshabilitar este requerimiento 855 si así lo decide).

- Las Contraseñas de Apps solo se pueden utilizar en apps de correo—no se pueden utilizar para iniciar sesión en Webmail o en MDRA.
- Cada Contraseña de App se despliega una sola vez, cuando es creada. No hay manera de recuperarla después, de forma que los usuarios deberán estar listos para ingresarla en su app cuando sea creada.
- Los usuarios deberán utilizar una Contraseña de App distinta para cada app de correo y deberán revocar (eliminar) la contraseña siempre que dejen de utilizar la app o cuando el dispositivo se pierda o sea robado.
- Cada Contraseña de App enlista cuando fue creada, cuando fue utilizada por última vez y la dirección IP desde la que se tuvo acceso a la cuenta de correo. Si un usuario encuentra algo sospechoso sobre la última vez que fue utilizada o los datos de la última IP, deberá revocar la Contraseña de App y crear una nueva para su app.
- Cuando se modifica la contraseña de una cuenta, todas las Contraseñas de App se eliminan en automático—el usuario no puede continuar utilizando sus antiguas Contraseñas de Apps..

Crear y utilizar Contraseñas de Apps

Los usuarios típicamente crean y administrar sus propias Contraseñas de Apps desde Webmail siguiendo los pasos descritos abajo (esta información se incluye en el archivo de ayuda de Webmail). Antes de que el usuario inicie, deberá tener su app de correo o su cliente listo para ingresar la contraseña, porque la Contraseña de App solo se desplegará una vez cuando es creada.

1. Tenga su app o cliente de correo listo para ingresar la Contraseña de App.
2. Inicie sesión en Webmail y de clic en **Opciones » Seguridad**.
3. Ingrese la contraseña de la cuenta en **Contraseña Actual**.
4. Dé clic en **Nueva Contraseña de App**.
5. Registre el nombre de la app que utilizará esa contraseña (ej. App de correo del teléfono) y dé clic en **OK**.
6. Copie/pegue o capture manualmente la contraseña mostrada en la app de correo o péguela en un archivo de texto o anótela si es necesario. Si se copia la contraseña para utilizarla después, deberá eliminar la copia luego de registrar la contraseña en su cliente de correo. Cuando termine, dé clic en **OK**.

Si por alguna razón necesita crear o eliminar una Contraseña de App para uno de sus usuarios, lo puede hacer utilizando las opciones en esta página. Tal y como en Webmail, la Contraseña de App solo se desplegará una vez cuando es creada, así que deberá ser registrada inmediatamente en la app o copiada de alguna manera para dársela a usuario después.

Hay una opción de cuenta en la página Ajustes del Editor de Cuentas 760 que puede utilizar para "*Requerir contraseña de app para iniciar sesión en SMTP, IMAP, ActiveSync, etc.*"

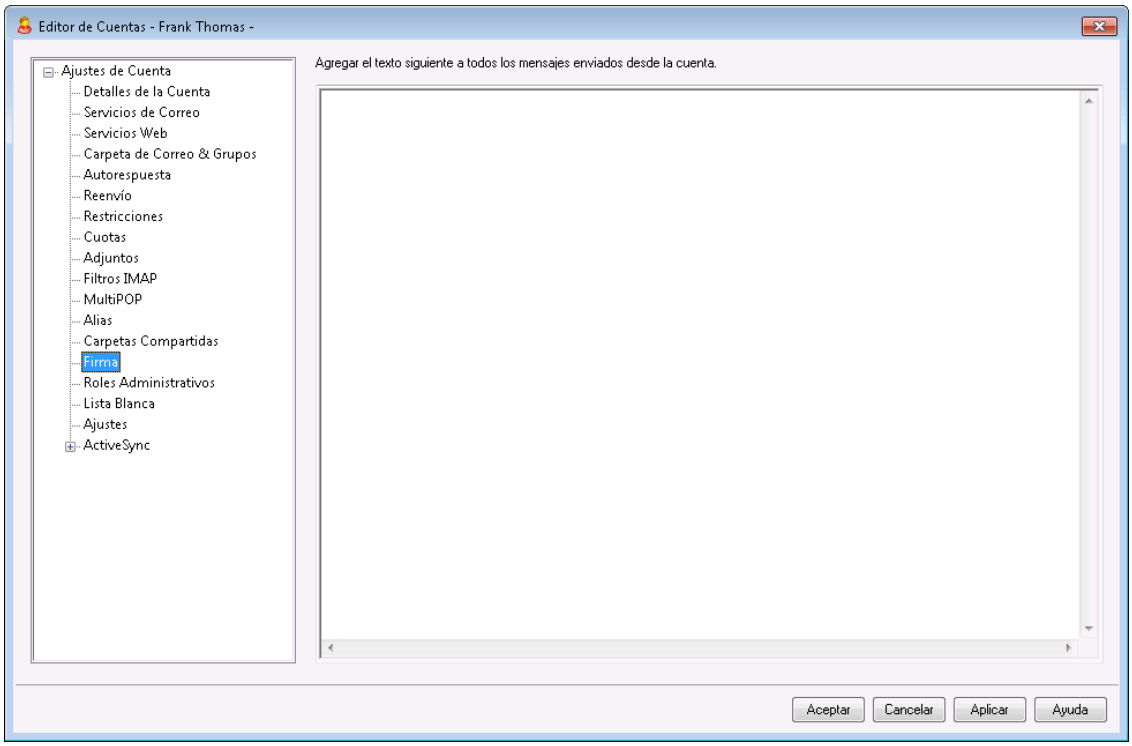
Requerir Contraseñas de Apps puede ayudar a proteger la contraseña de una cuenta de ataques de diccionario y de fuerza bruta vía SMTP, IMAP, etc. Esto es más seguro porque aún si un ataque de ese tipo pudiera adivinar la

contraseña actual de una cuenta, no funcionaría y el atacante no lo sabría, porque MDaemon solo aceptaría la Contraseña de App correcta. Adicionalmente, si sus cuentas en MDaemon están utilizando autentificación con Active Directory 822 y Active Directory bloquea la cuenta luego de un cierto número de intentos fallidos, esta opción puede ayudar a prevenir que las cuentas sean bloqueadas, porque MDaemon solo verificará la Contraseña de App y no intentará autentificar con Active Directory.

Ver:

Contraseñas 855
Editor de Cuentas » Ajustes 760

5.1.1.15 Firma



Firma de Cuenta

Use esta pantalla para definir una firma que se añadirá al final de cada mensaje que la cuenta envíe. Esta firma se añade en adición a cualquier otra firma o pie de página agregados por otras opciones, tales como la opción de firma incluida en Webmail y otros clientes de correo, las opciones Firma por Omisión 142 y Firma del Dominio 210 y el Pie de Página de Listas de Distribución 302. Estas tres opciones siempre se agregan debajo de la Firma de la Cuenta.

Los usuarios con acceso a Webmail o a Administración Remota 354 pueden editar sus propias firmas desde ahí.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje siempre que quieran que aparezca la firma,

Signature Selector	
$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.
$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**

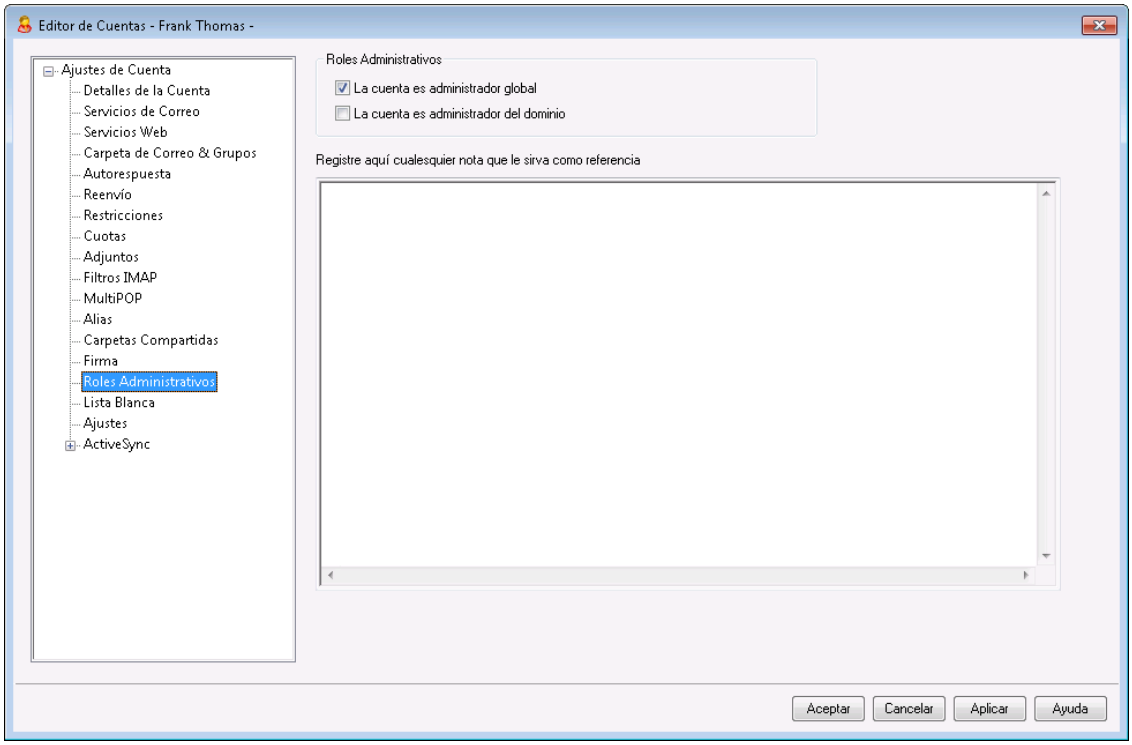
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**

Gerencia	$CONTACTBUSINESSMANAGER$
Asistente	$CONTACTBUSINESSASSISTANT$
Teléfono Asistente	$CONTACTBUSINESSASSISTANTPHONE$
Teléfono directo en la Empresa	$CONTACTBUSINESSMAINPHONE$
Teléfono de la Empresa	$CONTACTBUSINESSPHONE$
Teléfono 2 de la Empresa	$CONTACTBUSINESSPHONE2$
Teléfono IP de la Empresa	$CONTACTBUSINESSIPPHONE$
Fax de la Empresa	$CONTACTBUSINESSFAX$
Pager de la Empresa	$CONTACTBUSINESSPAGER$
Radio de la Empresa	$CONTACTBUSINESSRADIO$
Dirección de la Empresa	$CONTACTBUSINESSADDRESS$
Ciudad de la Empresa	$CONTACTBUSINESSCITY$
Estado de la Empresa	$CONTACTBUSINESSSTATE$
Código Postal de la Empresa	$CONTACTBUSINESSZIPCODE$
País de la Empresa	$CONTACTBUSINESSCOUNTRY$
Sitio web de la Empresa	$CONTACTBUSINESSWEBADDRESS$
Otros	
Esposo(a)	$CONTACTSPOUSE$
Hijos	$CONTACTCHILDREN$
Categorías	$CONTACTCATEGORIES$
Comentario	$CONTACTCOMMENT$

Ver:

Firmas por Omisión 142
Firma del Dominio 210
Pie de página de Listas de Distribución 302

5.1.1.16 Roles Administrativos



Roles Administrativos

La cuenta es administrador global
Habilite esta casilla para otorgar al usuario acceso administrativo a nivel servidor. Los administradores globales tienen:

- Acceso completo a la configuración del servidor, todos los usuarios y todos los dominios vía la Administración Remota
- Acceso a todos los usuarios de MDaemon de todos los dominios de MDaemon como contactos en la Mensajería Instantánea
- La facilidad de postear a todas las listas de distribución, aun las marcadas como de "Solo Lectura".
- La facilidad de postear a todas las listas de distribución aun sin ser miembro.

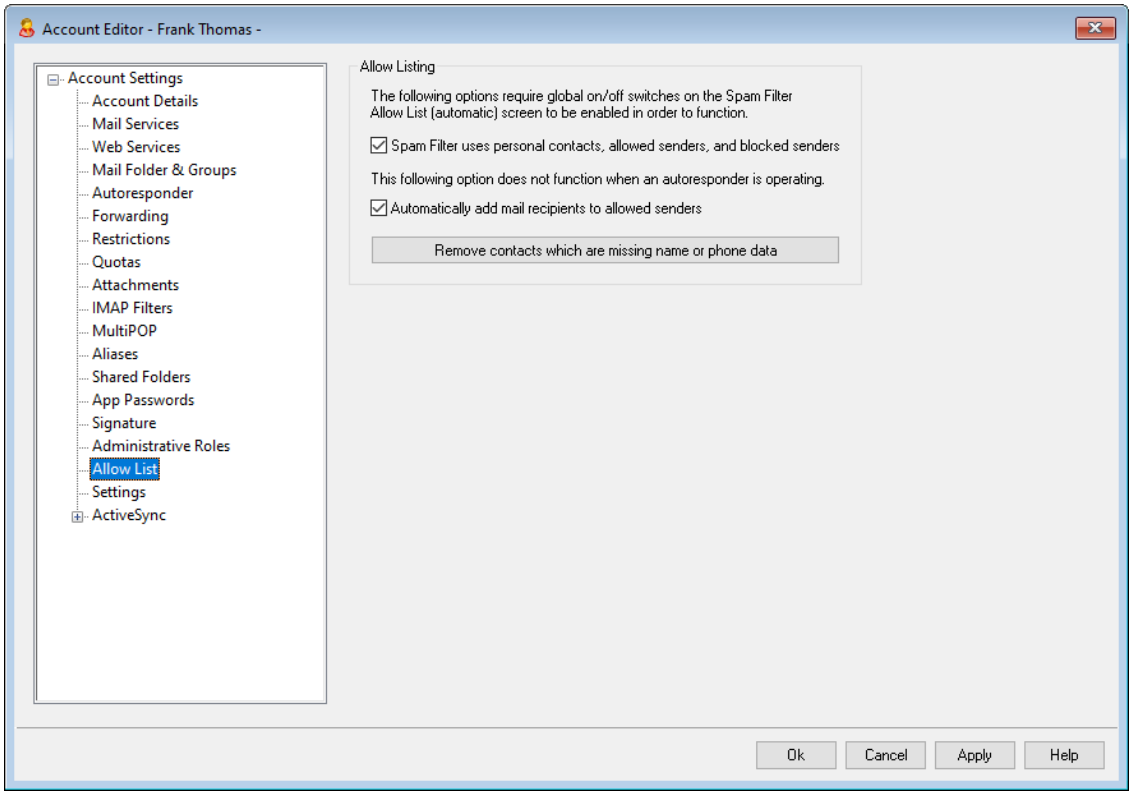
El usuario tendrá acceso completo a los archivos y opciones de MDaemon. Para más información sobre las opciones administrativas dentro de Administración Remota, vea la sección Administración Remota 354.

La cuenta es administrador del dominio
Dé clic en esta casilla para asignar al usuario como Administrador del Dominio. Los administradores de Dominio son similares a los administradores globales excepto que su acceso administrativo está limitado a este dominio y a los permisos otorgados en la página Servicios Web 720.

Si desea permitir que esta cuenta administre un dominio diferente, lo puede hacer desde la interface web Administración Remota 354, en la página del Administrador de Dominios » Admins.

Registre aquí notas que desee conservar como referencia
Utilice este espacio par anotaciones o cualquier otra información que desee conservar como referencia respecto a esta cuenta. A diferencia del campo *Descripción* en la pantalla Detalles de Cuenta 715, estas notas no se sincronizarán con los contactos públicos ni se mapearán con ningún campo en Active Directory.

5.1.1.17 Lista de Permitidos



Lista de Permitidos

El Filtro de Spam utiliza los archivos de contactos personales y listas de permitidos y bloqueados
La pantalla Lista de Permitidos (automática) 688 del Filtro de Spam contiene una opción global que se puede utilizar para hacer que el Filtro de Spam considere automáticamente en lista de permitidos un mensaje cuando el remitente del mensaje se encuentre en las carpetas de contactos personales o lista de permitidos personales del destinatario. También pondrá en automático en Lista de Bloqueados cualquier mensaje cuando el remitente se encuentre en el archivo de Lista de Bloqueados del usuario. Si ha habilitado la opción global del Filtro de Spam pero no desea aplicarla a esta cuenta deshabilite esta casilla para omitir la configuración global. Si la opción global se encuentra deshabilitada, entonces esta opción no estará disponible.

Agregar en automático destinatarios de correo en la lista de remitentes permitidos
De clic en esta opción si desea actualizar la carpeta de remitentes permitidos de la cuenta cada vez que envíe un mensaje saliente a direcciones de correo no locales. Cuando se utiliza junto con la opción anterior, E*l Filtro de Spam utiliza los archivos de contactos personales y listas de permitidos y bloqueados,* el número de falsos positivos del Filtro de Spam se puede reducir drásticamente. La opción *Automáticamente actualizar contactos en lista de permitidos* localizada en la pantalla Lista de Permitidos (automática) 688 debe estar habilitada antes de que pueda utilizar esta funcionalidad.

Esta opción se deshabilita cuando la cuenta está utilizando autorespuestas.

Eliminar contactos que no cuentan con nombre o número telefónico
Dé clic en este botón si desea eliminar los contactos que solo contengan la dirección de correo de la carpeta de Contactos de la cuenta. Si un contacto no tiene por lo menos nombre o número telefónico, será eliminado. Esta opción es principalmente para ayudar a aquellos que utilizaban la opción de lista de permitidos automática de MDaemon antes de la versión 11, a depurar contactos que fueron agregados solo por la funcionalidad de lista de permitidos. En versiones anteriores de MDaemon se agregaban las direcciones a los contactos en lugar de a la carpeta de lista de permitidos. Esto podría originar que la cuenta tuviera muchos registros en la carpeta de Contactos que el usuario preferiría no tener ahí.

Considere cuidadosamente esta opción antes de utilizarla, ya que los contactos que solo contienen la dirección de correo pueden ser legítimos.

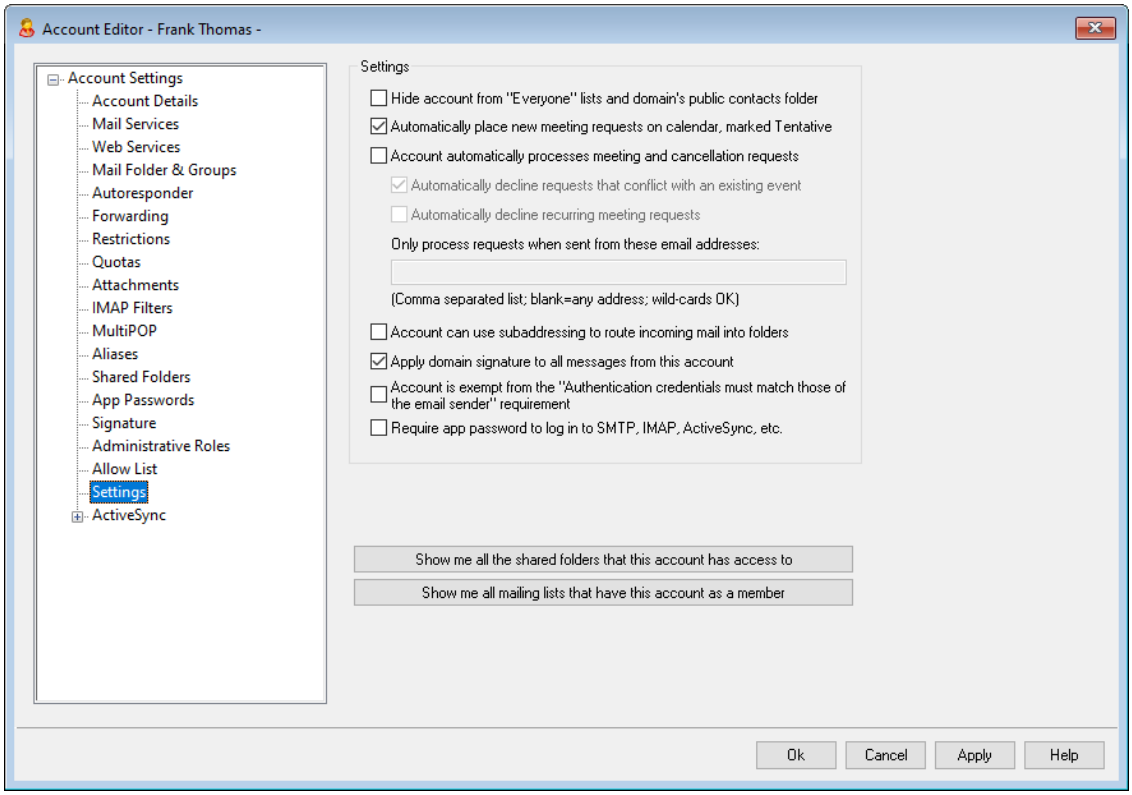
Establecer los valores por omisión para Cuentas y Grupos

Las opciones den esta pantalla corresponden a las que se localizan en la pantalla Propiedades de Plantillas » Lista de Permitidos 818, que se pueden utilizar para establecer los valores por omisión de cuentas nuevas 792 y los valores para cuentas que pertenecen a ciertos grupos 781.

Ver:

Lista de Permitidos (automática) 688
Administrador de Plantillas 791
Propiedades de Plantillas » Lista de Permitidos 818

5.1.1.18 Ajustes



Ajustes

Cuenta oculta de listas "Everyone"y de las carpetas públicas del dominio
MDaemon puede crear y mantener automáticamente listas de distribución "Everyone@" y "MasterEveryone@" 277, que se pueden utilizar para enviar mensajes a todos los usuarios del dominio y a todos los usuarios de MDaemon, respectivamente. Por omisión estas listas incluyen a todas las cuentas de cada dominio, pero usted puede marcar esta caja si desea ocultar esta cuenta de esas listas - los mensajes destinados a esas listas no se enviarán a la cuenta. Esto también ocultará la cuenta de la carpeta pública de contactos del dominio.

Colocar automáticamente nuevas peticiones de juntas en el calendario, marcadas como Tentativas
Por omisión, cuando una cuenta recibe una nueva petición de junta, esta se coloca en el calendario del usuario y se marca como *Tentativa*.

La cuenta procesa automáticamente solicitudes de reunión y cancelaciones de eventos
Haga clic en esta casilla si desea automatizar el procesamiento de solicitudes de reunión, cambios y cancelaciones para esta cuenta. Cuando la cuenta recibe un mensaje que contiene una solicitud de reunión, el calendario de la cuenta se actualizará automáticamente. Esta opción está deshabilitada para todas las cuentas por defecto.

Declinar en automático peticiones que entren en conflicto con un evento existente
Si se habilita el procesamiento automático de peticiones de reuniones y cancelaciones para la cuenta, esas peticiones se declinarán en automático

por omisión cuando entren en conflicto con un evento existente. Deshabilite esta casilla si desea permitir que el evento en conflicto sea creado.

Declinar en automático peticiones de reuniones recurrentes
Dé clic en esta casilla si el procesamiento automático de reuniones y cancelaciones está habilitado para la cuenta, pero desea declinar aquellas peticiones cuando sean para eventos recurrentes.

Solo procesar peticiones enviadas desde estas direcciones de correo
Si desea procesar en automático peticiones provenientes solo de ciertas direcciones de correo, enliste esas direcciones aquí. Separe cada dirección con una coma. Se permiten comodines en las direcciones (ej. *@example.com). Si deja esta casilla en blanco, se permitirá cualquier dirección.

La cuenta puede utilizar subdireccionamiento para enrutar el correo entrante a carpetas
Dé clic en esta casilla si desea permitir subdireccionamiento 762 para esta cuenta.

Aplicar la firma del dominio a todos los mensajes de esta cuenta
Cuando existe una Firma del Dominio 210 para el dominio al que pertenece esta cuenta, esta opción hace que sea la firma sea agregada a todos los mensajes enviados por la cuenta. Se encuentra habilitada por omisión.

La cuenta está exenta del requerimiento "Las credenciales de autentificación deben coincidir los del remitente del mensaje"
Use esta opción si desea exentar a la cuenta de la opción global "*Las credenciales de autentificación deben coincidir con las del remitente*" localizada en la pantalla Autentificación SMTP 523. Esta opción se encuentra deshabilitada por omisión.

Requerir contraseña de app para iniciar sesión en SMTP, IMAP, ActiveSync, etc.
Marque esta casilla si desea requerir que la cuenta utilice Contraseñas de Apps 751 en los clientes de correo, para iniciar sesión en SMTP, IMAP, ActiveSync, u otro protocolo de servicio de correo. Sin embargo, la contraseña 855 regular de la cuenta, aún debe utilizarse para iniciar sesión en Webmail o Administración Remota.

Requerir Contraseñas de Apps puede ayudar a proteger la contraseña de la cuenta de ataques de diccionario y fuerza bruta vía SMTP, IMAP, etc. Esto es porque MDaemon solo aceptará la Contraseña de App correcta. Adicionalmente, si sus cuentas en MDaemon están utilizando autentificación con Active Directory 822 y Active Directory está configurado para bloquear una cuenta luego de un número de intentos fallidos, esta opción puede ayudar a prevenir que las cuentas sean bloqueadas, dado que MDaemon solo verificará las Contraseñas de Apps y no intentará autentificar con Active Directory.

Habilitar la carpeta de Documentos en MDaemon Webmail
Marque esta casilla para habilitar la carpeta de Documentos para este usuario. Esta opción solo puede ser utilizada si está habilitada la opción correspondiente en la página de Ajustes de Webmail 201 del dominio. **Nota:** Esta opción y la de Ligas de Documentos abajo solo están disponibles en la interface web MDaemon Administración Remota (MDRA) 354.

Se permite que la cuenta comparta ligas temporales de sus documentos personales
Cuando está habilitada esta opción, el usuario podrá crear ligas en Webmail hacia documentos personales, que podrá compartir con cualquier persona. Las ligas mayores de 30 días se depuran en automático.

Ver Ligas de Documentos
Dé clic en este botó para desplegar la páginaLigas de Documentos, que contiene una lista de todas las ligas activas que ha creado el usuario. Desde esta página usted puede revocar cualquier liga que elija. Las ligas mayores de 30 días se revocarán automáticamente.

Mostrar las carpetas compartidas a las que esta cuenta tiene acceso
Dé clic en este botón para desplegar todas las carpetas compartidas a las que se le ha dado acceso a la cuenta.

Mostrar las listas de distribución en las que esta cuenta es miembro
Dar clic en este botón para abrir una lista de todas las Listas de Distribución 274 en las que esta cuenta es miembro.

Subdireccionamiento

El subdireccionamiento es un sistema para incluir un nombre de carpeta en el nombre de buzón de la dirección de correo de una cuenta. Usando este sistema, los mensajes direccionados a la combinación de *buzón+carpeta* serán enrutados automáticamente a la carpeta de la cuenta incluida en la dirección (asumiendo que exista), sin la necesidad de crear reglas de filtro específicas para hacer que suceda.

Por ejemplo, si `bill.farmer@ejemplo.com` tiene una carpeta IMAP llamada "varios," entonces si llega un correo para "bill.farmer`+varios@ejemplo.com`" será enrutado automáticamente a dicha carpeta. Las subcarpetas pueden ser designadas incluyendo los nombres de carpeta y subcarpeta separados por signo "+" adicional y los guiones bajos se utilizan para sustituir los espacios en los nombres de carpeta. Así, usando el ejemplo anterior, si la carpeta de Bill "varios" tuviera una subcarpeta llamada "`cosas antiguas`," los mensajes para "bill.farmer`+varios+cosas_antiguas@ejemplo.com`" serán enrutados automáticamente a la carpeta de correo de Bill "varios`\cosas antiguas`".

Puesto que la subdirección requiere el uso del carácter "+", los buzones que contienen "+" no pueden ser subdireccionados. Así, en el ejemplo anterior, sil a dirección fuera "bill`+farmer@ejemplo.com`" en lugar de "bill.farmer`@ejemplo.com`" no podría ser subdireccionada. Además, no puede usar alias de direcciones en las subdirecciones. Puede, sin embargo, crear un alias que use una subdirección. Así, aunque "`alias+varios@ejemplo.com`" no está permitido, usar "`alias@ejemplo.com`" para que apunte a "bill.farmer`+varios@ejemplo.com`" es correcto.

Para prevenir exploits o abusos, la carpeta IMAP incluida en la subdirección **debe** ser válida. Si el mensaje subdireccionado llega para una cuenta que no tiene una carpeta que coincida con el nombre de carpeta definido en la subdirección, entonces la subdirección será tratada como dirección de correo desconocida y gestionada acorde, según sus configuraciones de MDaemon. Por ejemplo, si `bill.farmer@ejemplo.com` no tiene una carpeta llamada "varios" y aun así llega

un mensaje para "bill.farmer+varios@ejemplo.com" entonces el mensaje será tratado como si fuera para un usuario desconocido y será rechazado.

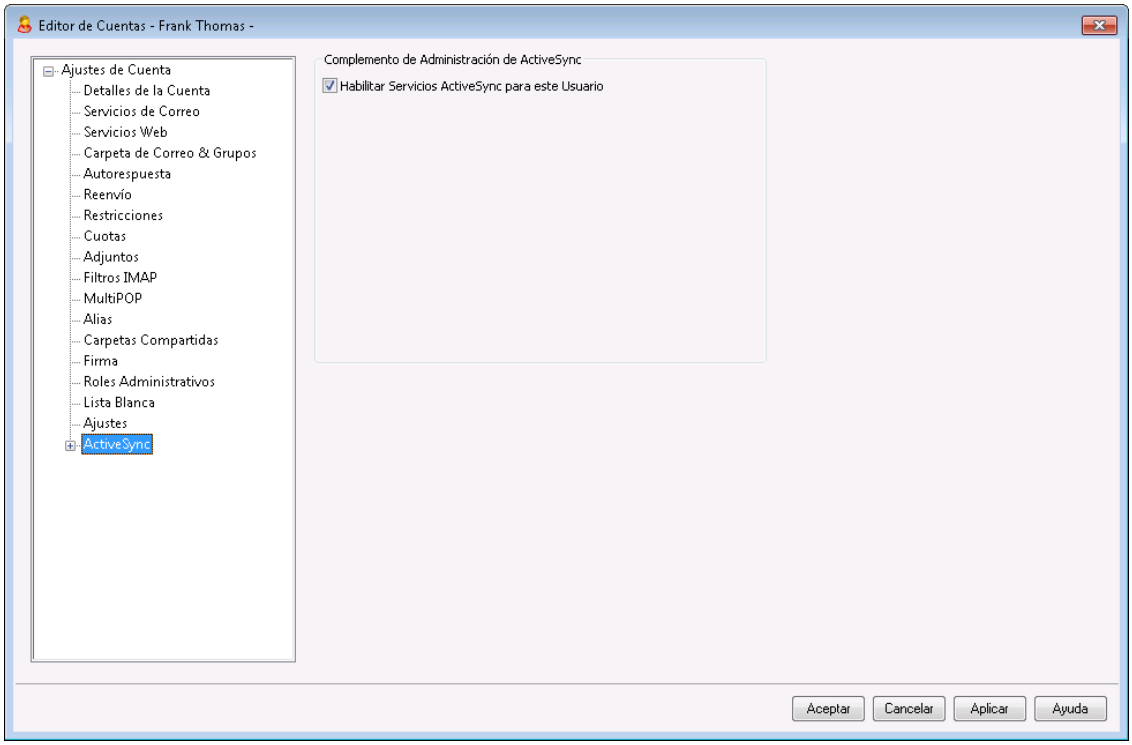
Habilitar el subdireccionamiento
Haga clic en esta casilla si desea permitir el subdireccionamiento para esta cuenta.

Por defecto, cada cuenta tiene la función de subdireccionamiento deshabilitada. Puede, sin embargo, deshabilitar esta funcionalidad globalmente a través de la opción *Deshabilitar el subdireccionamiento para todas las cuentas* ubicada en la pantalla Varios 503 del diálogo de Preferencias. Si se deshabilita el subdireccionamiento a través de dicha opción, no se permitirá para ninguna cuenta, independientemente de las configuraciones individuales de cuenta.

Ver:

Lista de Permitidos (automática) 688
Administración Remota 354
Administrador de Plantillas 791
Contraseñas 855

5.1.1.19 ActiveSync para MDaemon



Las pantallas de ActiveSync para MDaemon en el Editor de Cuentas se utilizan para habilitar o deshabilitar ActiveSync para las cuentas, configurar ajustes específicos de cuenta[765], asignar política por omisión[771] y administrar los clientes ActiveSync[772] de la cuenta.

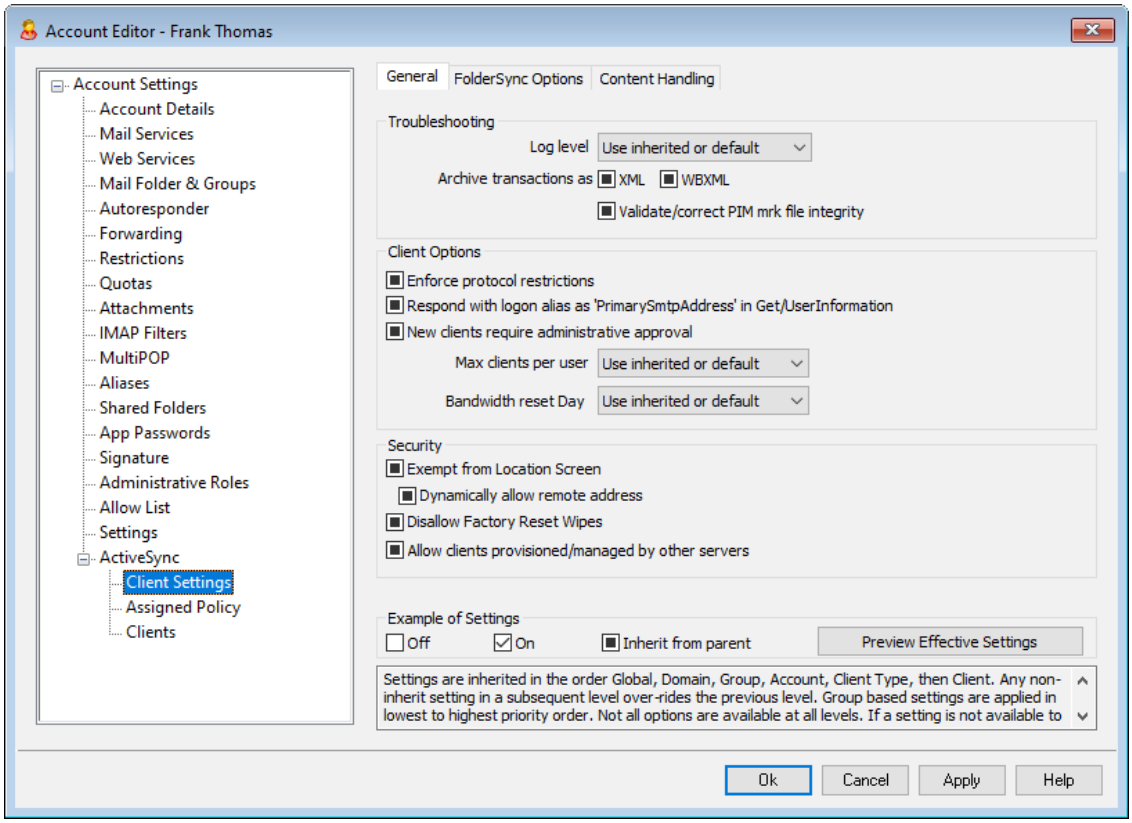
Habilitar/Deshabilitar ActiveSync para la cuenta

Si desea permitir que la cuenta utilice un cliente ActiveSync para accesar su correo y datos PIM, habilite esta opción.

Ver:

Editor de Cuentas » ActiveSync » Ajustes de Cliente[765]
Editor de Cuentas » ActiveSync » Política Asignada[771]
Editor de Cuentas » ActiveSync » Clientes[772]

5.1.1.19.1 Ajustes de Cliente



Las opciones en esta pantalla se utilizan para controlas los ajustes de cliente ActiveSync para clientes asociados con esta cuenta. Por omisión cada una de estas opciones está configurada para heredar su ajuste del valor correspondiente para el dominio al que pertenece la cuenta. Si se modifica cualquier valor en esta pantalla se omite el ajuste de dominio 434 para esta cuenta. Más aun, puede utilizar la opción *Ajustes* en la pantalla Clientes 772 si desea omitir los ajustes a nivel de cuenta para clientes específicos.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por

omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las

carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas[128] a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas[743] a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes[460] y tipos de clientes[475] que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS)[432] 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido[834] para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en

realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

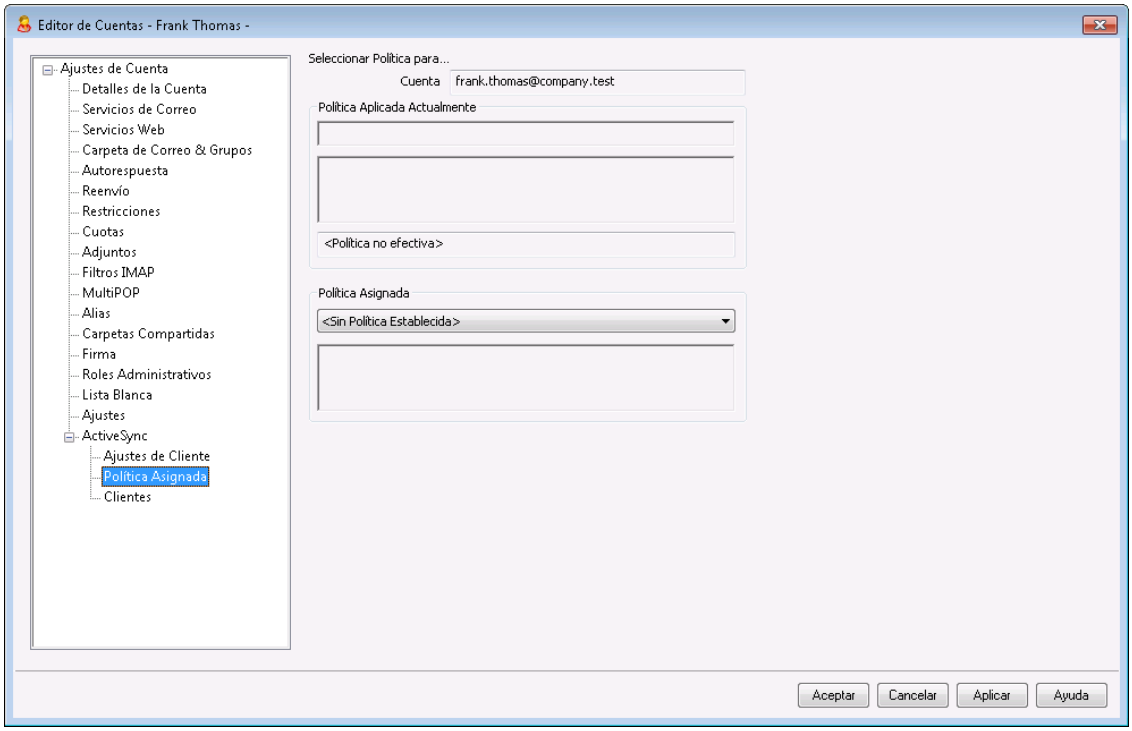
Vista Previa de Ajustes Efectivos

Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios 434, cuentas 451 y clientes 460). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Dominios 434
Editor de Cuentas » ActiveSync » Clientes 772

5.1.1.19.2 Política Asignada



Utilice esta pantalla para asignar la Política ActiveSync 442 por omisión que utilizará cualquier cliente ActiveSync que se conecte utilizando esta cuenta. Por omisión este ajuste de política se hereda del valor de la política de dominio 237, pero puede modificarla aquí para omitir ese valor para esta cuenta. Más aun, también puede omitir el valor del ajuste para la cuenta en específico y asignar una política diferente a Clientes 772 específicos.

Asignar una Política ActiveSync

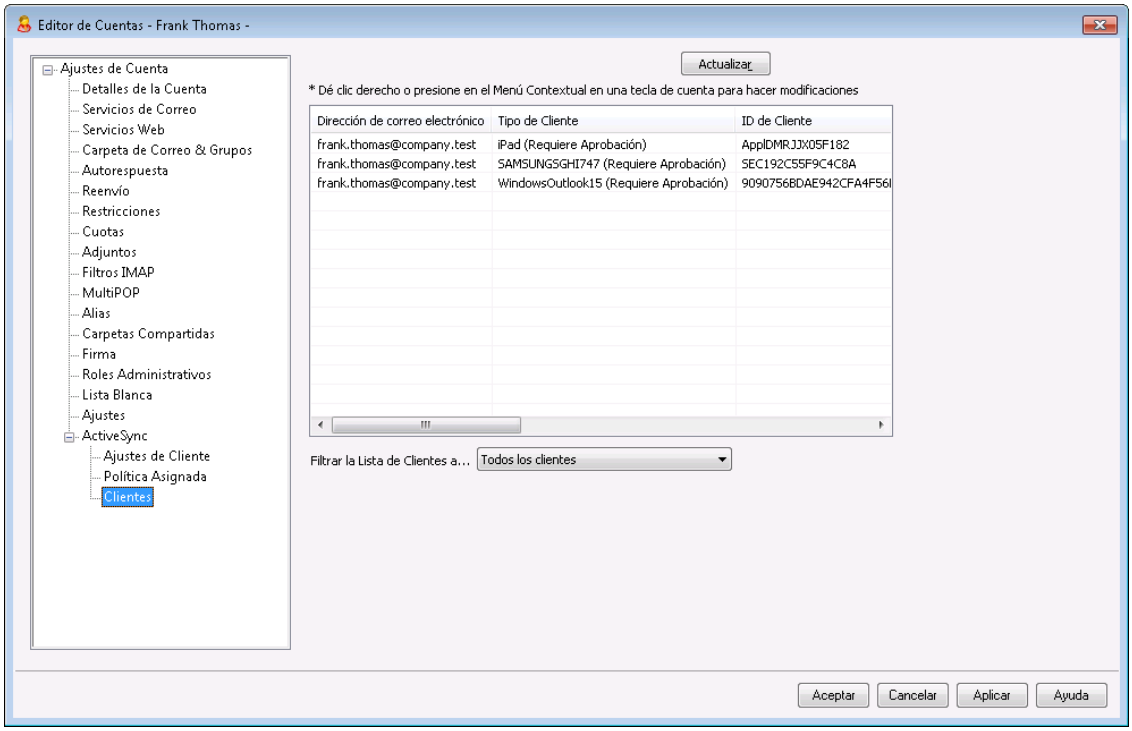
Para asignar una política a esta cuenta, dé clic en la lista desplegable **Política a Asignar**, seleccione la política y dé clic en **OK** o en **Aplicar**.

No todos los dispositivos ActiveSync reconocen o aplican políticas consistentemente. Algunos pueden ignorar las políticas o ciertos elementos de política por completo y otros pueden requerir un reinicio de dispositivo antes de que tengan efecto los cambios. Más aun, al intentar asignar una política nueva, no se aplicará al dispositivo hasta la siguiente ocasión en que se conecte por sí mismo al servidor ActiveSync; las políticas no pueden "entregar" a los dispositivos hasta que se conecten.

Ver:

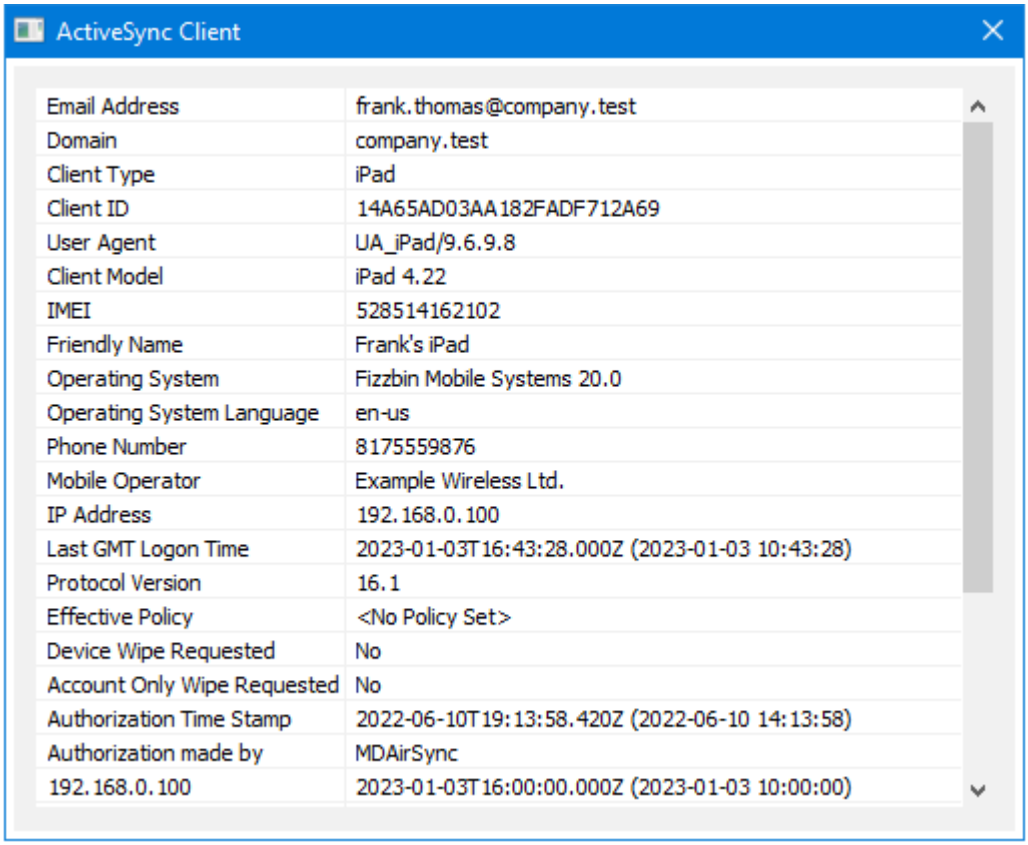
ActiveSync » Administrador de Políticas 442
ActiveSync » Dominios 434
Editor de Cuentas » ActiveSync » Clientes 772

5.1.1.19.3 Clientes



Esta pantalla despliega información sobre cualesquiera clientes ActiveSync asociados con la cuenta del usuario. Desde aquí puede asignar una Política ActiveSync 771 para cada cliente, controlar varios ajustes de cliente, remover clientes, borrarlos de manera remota y restablecer las estadísticas de cliente en MDaemon.

Detalles del Cliente ActiveSync



Seleccione una entrada y dé clic en **Ver Detalles del Cliente** para abrir el diálogo de Detalles del Cliente. Esta pantalla contiene información sobre el cliente, tal como su Tipo de Cliente, ID de Cliente, último inicio de sesión y más.

Ajustes de Cliente

dé clic derecho en un cliente y clic en **Personalizar Ajustes de Cliente** para administrar sus Ajustes de Cliente. Por omisión estos ajustes se heredan de la pantalla de Ajustes de Tipo de Cliente, pero se pueden ajustar si lo desea . Vea Administrar Ajustes del Cliente del Dispositivo abajo.

Asignar una Política ActiveSync

Para asignar una Política 442 al dispositivo:

1. Dé clic derecho en un dispositivo en la lista.
2. Dé clic en **Aplicar Política**. Esto abre el diálogo Aplicar Política.
3. Dé clic en **Política a Asignar** en la lista desplegable y seleccione la política deseada.
4. Dé clic en **OK**.

Estadísticas

Dé clic derecho en una entrada y luego clic en **Ver Estadísticas** para abrir el diálogo Estadísticas del Cliente, que contiene varias estadísticas de uso para el cliente.

Restablecer Estadísticas

Si desea restablecer las estadísticas del cliente, dé clic derecho en el cliente, luego clic en **Restablecer Estadísticas** y **OK** para confirmar la acción.

Remover un Cliente ActiveSync

Para remover un cliente ActiveSync, dé clic derecho en el cliente y clic en **Eliminar**, y luego en **Si**. Esto eliminará el cliente de la lista así como toda la información de sincronización relativa al cliente, en MDaemon. Por esto, si en el futuro la cuenta utiliza ActiveSync para sincronizar el mismo cliente, MDaemon lo tratará como si nunca antes hubiera sido utilizado en el servidor: todos los datos del cliente tendrán que resincronizarse con MDaemon.

Borrar por completo un Cliente ActiveSync

Cuando se ha aplicado una política 442 a un cliente ActiveSync seleccionado y el cliente la ha aplicado y respondido, entonces se dispondrá con una opción de Borrado Completo para ese cliente. Para hacer un Borrado completo, dé clic derecho en el cliente (o selecciónelo si está utilizado MDRA) y dé clic en **Borrado Completo**. La próxima vez que se conecte ese cliente, MDaemon le dirá que borre todos los datos o se restaure a sí mismo a sus valores de fábrica. Dependiendo del cliente, esto puede eliminar todo en el dispositivo incluyendo apps descargadas. Más aún, en tanto exista el registro en ActiveSync de ese cliente, MDaemon continuará enviando peticiones de borrado siempre que el dispositivo se conecte en el futuro. Si en algún momento desea eliminar el cliente, asegúrese de agregarlo primero a la Lista de Bloqueados 428, de manera que no se pueda conectar en el futuro. Finalmente, si un dispositivo borrado es recuperado y desea permitirle que se conecte de nuevo, deberá seleccionar el dispositivo y dar clic en **Cancelar Acciones de Borrado**. También deberá eliminarlo de la Lista de Bloqueados.

Borrado de Cuenta de un Cliente ActiveSync

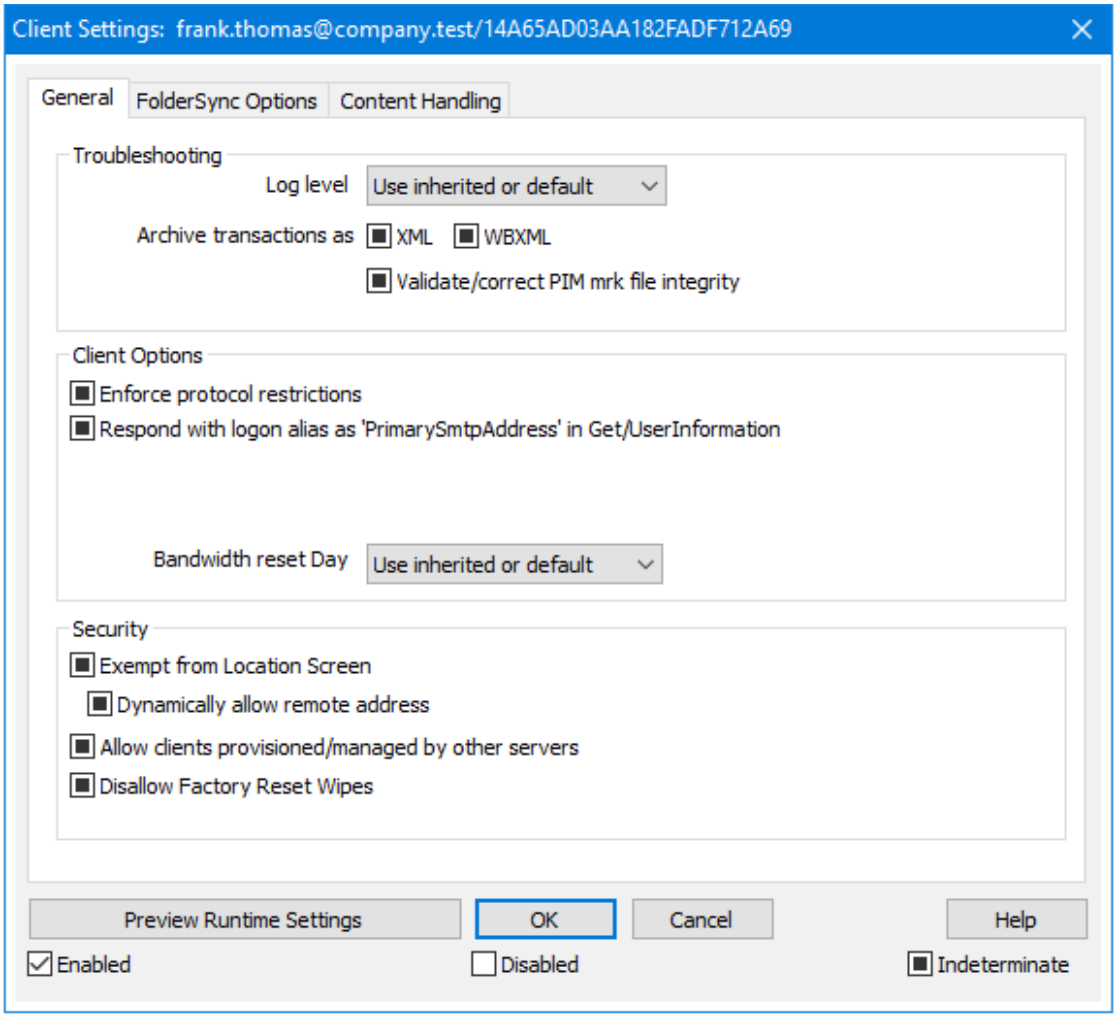
Para borrar la cuenta de correo y datos PIM de un cliente o dispositivo, dé clic derecho y clic en **Borrar Cuenta de Correo y datos PIM del Cliente.** La opción *Borrar Cuenta* es similar a la opción **Borrado Completo** explicada arriba, pero en lugar de borrar todos los datos, solo borrará los datos de la cuenta tales como correos, registros del calendario, contactos y demás. El resto, como son las apps, fotos o música quedarán intactos.

Autorizar un Cliente

Si está habilitada la opción "*Clientes nuevos requiere aprobación administrativa*" en la pantalla Ajustes de Cliente ActiveSync 421, seleccione un cliente y de clic en Aprobar cliente para sync, en este botón para autorizar su sincronización con el servidor.

Administrar los Ajustes del Cliente de un Dispositivo

La pantalla de Ajustes de Cliente a nivel dispositivo le permite administrar los ajustes para un dispositivo en particular.



Por omisión todas las opciones en esta pantalla se establecen como "Usar heredado o el de omisión", lo que significa que cada opción tomará sus ajustes de la opción correspondiente en la pantalla Ajustes de Cliente de la cuenta 451. Cualquier cambio hecho a los ajustes en esa pantalla se verá reflejado en esta pantalla. En correspondencia, cualquier cambio que realice en esta pantalla omitirá el ajuste a nivel de cuenta para este dispositivo.

General

Resolución de problemas

Nivel de Registro
ActiveSync soporta seis niveles de registro desde la mayor a menor cantidad de datos registrados:

Depurar Este es el nivel de registro más extenso. Registra toda la actividad y típicamente solo se utiliza cuando se está diagnosticando un problema.

Info Registro Moderado. Incluye operaciones generales sin detalle. Este es el nivel de registro por omisión.

Advertencia Se incluyen advertencias, errores, errores críticos y eventos de inicio/cierre de sesión.

Error Se registran Errores, errores críticos e inicios de sesión/cierre de sesión.

Crítico Se registran errores críticos y eventos de inicio/cierre de sesión.

Ninguno Solo se registran eventos de inicio/cierre de sesión.

Heredar Por omisión, el ajuste Nivel de Registro se hereda de la jerarquía de Ajustes de Cliente. De manera que los Clientes heredan su ajuste de los Tipos de Cliente, éstos heredan de las Cuentas, las Cuentas de los Grupos y así sucesivamente. El Ajuste Global de Cliente para estas opciones se determina por el ajuste Nivel de Registro en el diálogo Diagnósticos 430.

Archivar transacciones como [XML | WBXML]

Utilice las opciones *Archivar XML...* y *WBXML* si desea guardar estos datos, lo que en ocasiones puede ser útil para fines de depuración. Las opciones globales están deshabilitadas por omisión.

Validar/corregir integridad del archivo PIM mrk
Esta opción ejecuta un proceso de validación y corrección en los datos PIM del cliente para encontrar problemas conocidos que pueden impedir que sincronice correctamente, tal como duplicar UIDs iCal o dejar vacíos campos requeridos. La opción global está deshabilitada por omisión.

Opciones de Cliente

Forzar restricciones de protocolo
Habilite esta opción si desea denegar conexiones desde cualquier cliente que intente utilizar un protocolo distinto a los especificados en *Versiones de Protocolo Permitidas* definido para el cliente. Por omisión esta opción está deshabilitada, lo que significa que las restricciones de protocolo no impiden que el cliente utilice un protocolo diferente; simplemente le dicen al cliente qué protocolos utilizar. Si un cliente intenta utilizar de todas formas un protocolo restringido, MDaemon le permitirá la conexión. Ver: Restricciones de Protocolo 432 para más información.

Responder con alias de inicio de sesión como 'PrimarySmtpAddress' en Get/UserInformation
Esto le permite al servicio devolver una dirección alias/secundaria como dirección principal en respuesta a una petición Settings/Get/UserInformation. Esto resuelve un problema generado por una actualización a iOS9.x que hizo que los clientes no pudieran enviar correo utilizando un alias. Al utilizar esta opción se da una respuesta fuera de especificación a Settings/Get/UserInformation.

Los clientes nuevos requieren aprobación administrativa
Habilite esta opción si desea requerir que los clientes nuevos sean autorizados

por un administrador antes de que puedan sincronizar con una cuenta. La lista de Clientes 460 indica los clientes que esperan autorización y el administrador los puede autorizar desde la misma pantalla. Este ajuste está deshabilitado por omisión.

Max clientes por usuario
Si desea limitar el número de clientes o dispositivos ActiveSync que se pueden asociar con una cuenta MDaemon, especifique el número deseado en esta opción. La opción global se configura como "ilimitado" por omisión. Esta opción está disponible en las pantallas de ajustes Global, de Dominio y de Cuenta, no en las pantallas individuales de Clientes.

Día de reinicio del ancho de banda
Utilice esta opción si desea restablecer las estadísticas de uso del ancho de banda para ActiveSync un día específico de cada mes. El evento de reinicio tiene lugar como parte del proceso nocturno de mantenimiento normal y se registra en el registro del Sistema como otras rutinas de mantenimiento. La opción global se configura en "0 (Nunca)" por omisión, lo que significa que la estadísticas de uso nunca se restablecerán. Configure las opciones ahí contenidas a un día diferente si, por ejemplo, desea que el día de restablecimiento coincida con la fecha de reinicio del plan de facturación del proveedor de telefonía del usuario.

Seguridad

Exentar del Monitoreo de Localizaciones
Habilite esta opción en la pantalla de ajustes de cliente de ActiveSync si desea que el servicio pueda evitar el Monitoreo de Localizaciones 572. Esto permite que un usuario válido continúe teniendo acceso a su cuenta vía ActiveSync cuando, por ejemplo, se encuentren viajando a una ubicación que esté bloqueada para realizar intentos de autentificación. A fin de exentar el dispositivo, debe estar conectado y autentificado utilizando ActiveSync dentro de un rango de tiempo configurado en el ajuste Eliminar clientes inactivos después de este no. de días 418 localizado en la pantalla Ajustes.

Permitir dinámicamente la dirección remota
Al exentar un dispositivo del Monitoreo de Localizaciones, habilite esta opción si también desea agregar a lista de permitidos la dirección IP remota desde la que se conecta. Esto puede ser útil para permitir a otros clientes que pudieran conectarse desde la misma IP.

Permitir que se conecten cliente administrados por otros servidores
Por omisión, cuando el servidor ActiveSync envía datos/políticas de aprovisionamiento específicos para un cliente y reporta que también es administrador por otro servidor ActiveSync, de todas maneras se le permitirá al cliente conectarse a MDaemon. En esta circunstancia, sin embargo, no hay manera de asegurar que sus políticas específicas se apliquen cuando exista un conflicto con las políticas del otro servidor ActiveSync. Generalmente, se opta por aplicar las opciones más restrictivas cuando las políticas entran en conflicto. Deshabilite esta opción si no desea permitir que se conecten esos clientes.

No permitir Restablecimiento a Valores de Fábrica
Si se configura en Habilitado/Si no estará disponible la capacidad de un **Borrado Completo** en el Cliente ActiveSync. Si desea habilitar la facilidad de realizar un restablecimiento a valores de fábrica para un cliente, primero debe deshabilitar

esta opción. La opción se encuentra deshabilitada por omisión. Para más información, vea: **Borrar por Completo un Cliente ActiveSync** 460 en la página Clientes.

Opciones de FolderSync

Opciones FolderSync

Excluir

Carpeta de [Bloqueados/Permitidos] del usuario
Por omisión las carpetas de lista blanca y negra de contactos del usuario no se sincronizan con los dispositivos. Generalmente solo se utilizan por MDaemon para ayudar a la prevención automática del spam. Por esa razón no requieren ser desplegados en dispositivos como contactos.

Carpetas de correo personalizadas
Todas las carpetas de correo que se crean por omisión y generadas por el usuario se pueden sincronizar con el dispositivo. Habilite esta opción si desea permitir que solo se sincronicen las carpetas por omisión, ej. la Bandeja de Entrada, Enviados, Eliminados, Borradores y demás. No se incluyen las carpetas creadas por el usuario. Esta opción está deshabilitada por omisión.

Carpetas PIM personalizadas
Por omisión todas las carpetas PIM del usuario (ej. contactos, calendario, notas, tareas,

se sincronizarán con el dispositivo. Habilite esta opción si desea permitir que se sincronicen por omisión solo las carpetas PIM. Por ejemplo, si esta opción se habilita y un usuario tiene múltiples carpetas de calendario, solo se sincronizarán el calendario por omisión. Esta opción está deshabilitada por omisión.

Incluir

Jerarquía de Carpetas Públicas
Marque esta casilla si desea que las carpetas públicas 314 a que tiene acceso el usuario se incluyan en la lista de carpetas del usuario en dispositivos ActiveSync. Esto está habilitado por omisión.

Permitir consultas
Permitir a los clientes consultar las Carpetas Públicas 314 a las que tiene acceso. Esto se permite por omisión.

Permitir Carpetas Públicas transversales (expone nombres de carpetas)
Por omisión, a fin de que un cliente sincronice o tenga acceso a una subcarpeta pública, a cuenta debe tener Permisos de Consulta 316 para subcarpetas (ej. carpetas hijos) y todas las carpetas públicas 314 padre arriba de ellas. Si la cuenta no tiene permisos de ver las carpetas padre entonces no puede ver tampoco las carpetas hijos, aun cuando la cuenta tenga permiso para hacerlo. Habilite esta opción si desea permitir al cliente tener acceso a estas carpetas hijo. **Nota**: Si habilita esta opción necesariamente se revelan los nombre de las carpetas padre del cliente, lo que podría ser un riesgo de seguridad. Esta opción está deshabilitada por

omisión.

Máx. número de Carpetas Públicas
Utilice esta opción si desea limitar el número de Carpetas Públicas permitidas en el dispositivo. Cuando se configura un límite, el servidor itera a través de la lista de carpetas hasta alcanzar el límite y luego no envía más carpetas al dispositivo. No hay manera de asegurar el orden en que se procesarán las carpetas. Por omisión no se establece un límite global.

Carpetas compartidas
Marque esta casilla si desea que se incluyan las carpetas compartidas 128 a que tiene acceso el usuario, en la lista de carpetas del usuario en los dispositivos ActiveSync. Esto se encuentra habilitado por omisión.

Permitir búsquedas
Permite al cliente realizar búsqueda en las Carpetas Compartidas 743 a las que tiene acceso. Esto está permitido por omisión.

Manejo de Contenido

Opciones de Manejo de Correo

Crear tareas/recordatorios para elementos de correo cuando se marcan por el cliente
Esta opción permite que MDaemon recuerde al usuario sobre elementos marcados, creando una tarea por cada mensaje marcado cuando el cliente lo solicita. La opción global de este control se encuentra habilitada por omisión.

Enviar siempre actualizaciones de reuniones cuando se modifica un evento.
Algunos clientes no envían correctamente actualizaciones de reuniones cuando se modifica un evento. Esta opción indica al Servicio ActiveSync que envíe una actualización de la reunión cuando el organizador actualice un elemento de la reunión. Esto solo se deberá configurar en clientes 460 y tipos de clientes 475 que fallan al enviar correctamente actualizaciones de reuniones, de otra forma, se generarán actualizaciones duplicadas. Consecuentemente, esta opción solo está disponible en la página de ajustes para Clientes y Tipos de Clientes.

Solicitar confirmación de lectura para todos los mensajes enviados
Habilite esta opción si desea que el servidor solicite confirmaciones de lectura para todo el correo enviado por un cliente. La opción está deshabilitada por omisión.

Enviar confirmaciones de lectura desde el servidor cuando el correo se marque como leído y la confirmación haya sido solicitada por el remitente
Habilite esta opción si desea que el servidor soporte las peticiones de confirmación de lectura y envíe una confirmación de lectura cuando un mensaje sea leído por un cliente. Esta opción se encuentra deshabilitada por omisión.

Enviar como el Alias especificado en la dirección Responder a
Algunos clientes pueden no permitir que un remitente de correo utilice un Alias. Esta funcionalidad se agregó en el Protocolo Exchange ActiveSync (EAS) 432 16.x, pero algunos clientes no soportan esa versión. Por ejemplo, Outlook para Windows solo usa EAS 14.0 y en tanto no permite al usuario especificar una

dirección alterna para enviar, el mensaje generado no refleja las elecciones del usuario correctamente. Esta opción permite el uso del campo Responder a para enviar un mensaje, siempre y cuando esa dirección sea un alias válido[834] para ese usuario. La opción global está habilitada por omisión.

Combinar virtualmente los contactos públicos con los contactos por omisión
Habilite esta opción si desea combinar los contactos públicos con los contactos por omisión del usuario, en el dispositivo. Es solo una fusión virtual ya que en realidad no se copian a la carpeta de contactos del usuario. Esto puede ser útil para cliente que no soportan consultas en la Lista Global de Direcciones (Global Address List - GAL). Esta opción se encuentra deshabilitada por omisión.

Bloquear al Remitente al mover correo a la carpeta de Correo no Deseado
Al habilitar esta opción, si el cliente mueve un mensaje a la carpeta de Correo no deseado de la cuenta, el servicio agregará el Remitente o la dirección De de ese mensaje a la carpeta de Remitentes Bloqueados.

Forzar envío de respuestas a reuniones cuando una petición de reunión se acepta/declina.
Al habilitar esta opción, si el cliente acepta, declina o realiza una acción para responder a una petición de reunión, el servicio enviará una respuesta al organizador de la reunión. Esto es específico para clientes que no envían correctamente esas actualizaciones.

Vista Previa de Ajustes Efectivos

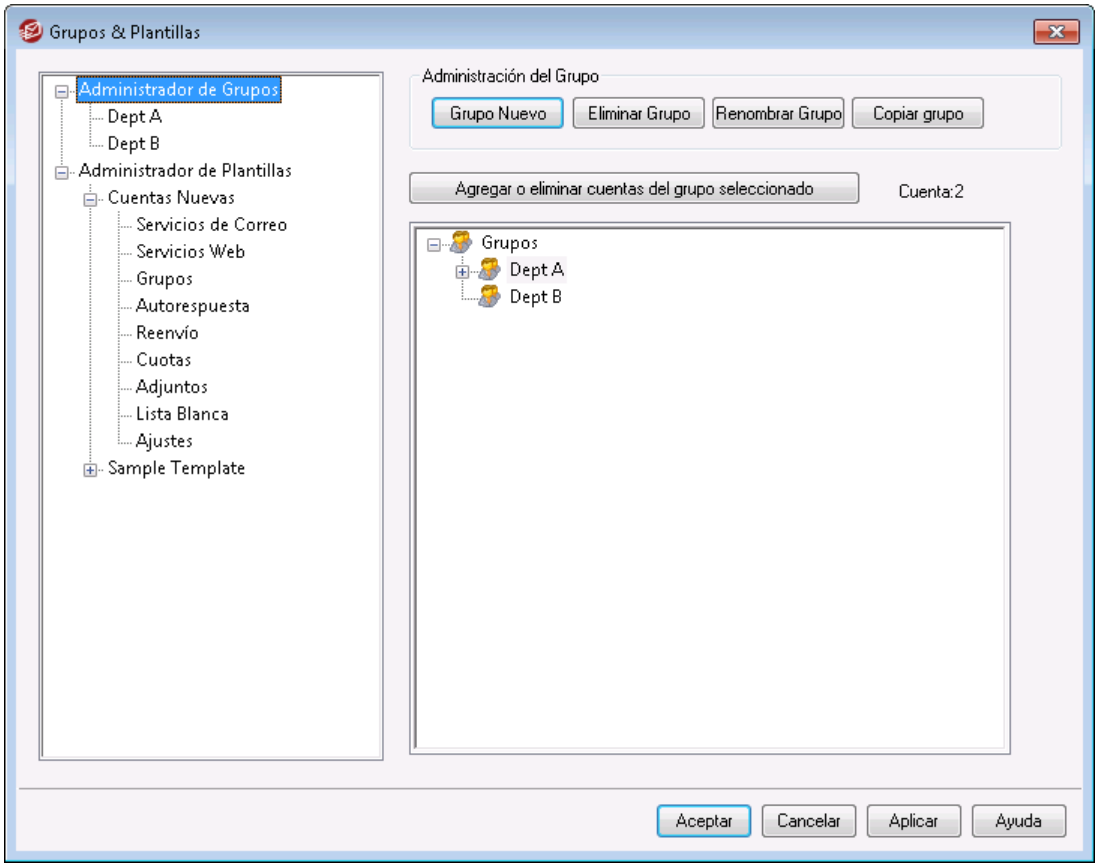
Este botón está disponible en todas las pantallas de Ajustes de Cliente anidadas (ej. dominios[434], cuentas[451] y clientes[460]). Dado que por omisión las opciones en esas pantallas se configuran para heredar los valores de la pantalla padre, utilice esta funcionalidad para ver qué ajustes se están aplicando en el momento en la pantalla desplegada.

Ver:

ActiveSync » Ajustes de Cliente[421]
ActiveSync » Dominios[434]
ActiveSync » Cuentas[451]

5.2 Grupos & Plantillas

5.2.1 Administrador de Grupos



El Administrador de Grupos (Cuentas » Grupos & Plantillas... » Administrador de Grupos) se utiliza para crear Grupos de cuentas y administrar qué cuentas pertenecen a ellos. Por ejemplo, al utilizar la pantalla Propiedades de Grupo 783, puede asignar una plantilla de cuenta 791 a un Grupo, permitiéndole controlar una serie de parámetros de cuenta para los miembros del Grupo. También puede controlar si los miembros del grupo tienen acceso a MDaemon Mensajería Instantánea 322 y a la mensajería instantánea. Más aun, el Filtro de Contenido soporta Grupos, lo que permite crear reglas 648 basadas en si el remitente o destinatario de un mensaje es miembro de un Grupo específico. Finalmente, para las Carpetas Compartidas 125 puede asignar permisos en la Lista de Control de Acceso 316, a Grupos específicos, lo que significa que todos los miembros del Grupo compartirán esos permisos.

Puede agregar cuentas a un Grupo seleccionándolo en la lista y luego dando clic en el botón "*Agregar o eliminar cuentas...*". También puede agregar usuarios a los Grupos desde la pantalla Carpetas de Correo & Grupos 718.

Administración de Grupos

Nuevo grupo
Para crear un nuevo Grupo de Cuentas, dé clic en *Nuevo grupo*, teclee un nombre y descripción para el grupo y dé clic en *OK*. El nuevo grupo aparecerá en la lista de grupos abajo y en el panel izquierdo.

Eliminar grupo
Para eliminar un grupo, seleccione el grupo de la lista, dé clic en *Eliminar grupo* y clic en *Si* para confirmar su decisión de eliminar el grupo.

Renombrar grupo
Para renombrar un grupo, seleccione el grupo de la lista y dé clic en *Renombrar grupo*. Teclee un nuevo nombre para el grupo y dé clic en *OK*.

Copiar grupo
Si desea crear un grupo con los mismos ajustes de otro grupo, seleccione el grupo original en la lista, dé clic en este botón y especifique un nombre y descripción para el nuevo grupo.

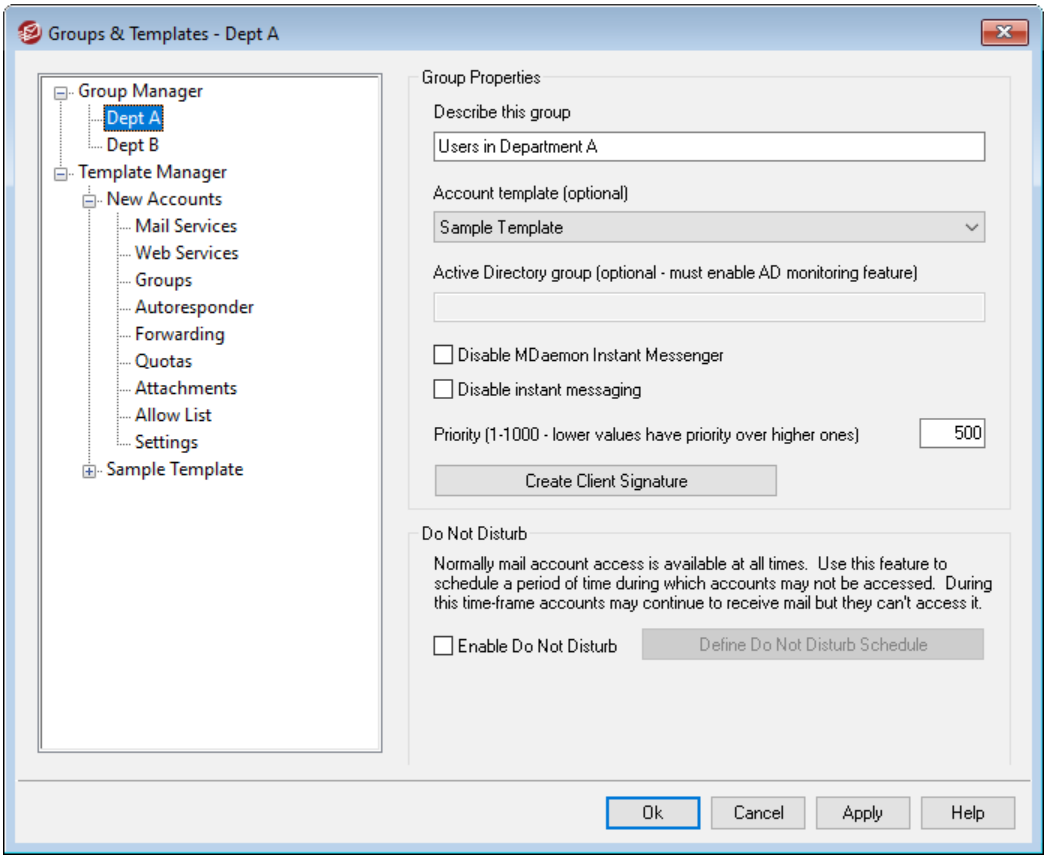
Agregar o eliminar cuentas del grupo seleccionado

Para administrar la membresía al grupo, seleccione el grupo y dé clic en este botón. Dé clic en la casilla contigua a las cuentas que desee agregar al grupo y quite la marca en la casilla de los miembros que desee remover. Dé clic en *OK*.

Ver:

Carpetas de Correo & Grupos 718
Creando una nueva Regla del Filtro de Contenido 648
Carpetas Compartidas 125

5.2.1.1 Propiedades de Grupo



La pantalla Propiedades de Grupo (Cuentas » Grupos & Plantillas... » [nombre de grupo]) se utiliza para configurar los parámetros para cada grupo que haya creado utilizando el Administrador de Grupos 781. Para abrir las Propiedades de Grupo en el Administrador de Grupos, dé doble clic en el grupo que desea editar o clic en el nombre de grupo en el panel izquierdo. En esta pantalla puede asignar una Plantilla de Cuenta 791 a un grupo, pudiendo controlar una variedad de parámetros de cuenta para los miembros del grupo. También puede ligar el grupo a un grupo de Active Directory, controlar si los miembros del grupo tienen acceso o no a MDaemon Mensajería Instantánea 322 y a la mensajería instantánea y definir un nivel de prioridad para el grupo. Para controlar la membresía a grupos, utilice el Administrador de Grupos y la pantalla Carpetas de Correo & Grupos 718 en el Editor de Cuentas.

Propiedades de Grupo

Describa este grupo
Registre aquí una descripción para el grupo, para su propia referencia. Esta información típicamente se registra cuando se crea el grupo, pero se puede editar en esta pantalla en cualquier momento.

Plantilla de Cuentas (opcional)
Si ha creado una Plantilla de Cuenta 791 que le gustaría utilizar para controlar algunos ajustes de cuenta para los miembros de un grupo, utilice esta lista desplegable para seleccionar la plantilla deseada. Cuando una plantilla de cuenta se liga a un grupo, cualquier categoría de ajustes de cuenta definida en Propiedades de Plantilla 793 se utilizará para todas las cuentas que pertenezcan al grupo. La plantilla se utilizará para controlar esos ajustes en lugar de los ajustes individuales de cuenta en el Editor de Cuentas. Si se elimina una cuenta de un

grupo que controlaba sus ajustes de cuenta, estos revertirán sus valores a los definidos en la Plantilla de Cuentas Nuevas 792.

Si una cuenta pertenece a múltiples grupos ligados a plantillas diferentes, entonces se utilizarán todas las plantillas siempre que no existan conflictos en las Propiedades de Plantilla 793 definidas. Si se establecen múltiples plantillas para controlar las mismas propiedades, entonces se utilizará la primera plantilla en la lista.

Grupo de Active Directory (opcional - requiere monitoreo AD)
Utilice esta opción si desea ligar el grupo a un grupo específico de Active Directory. Los miembros del grupo de Active Directory se agregarán al grupo de cuentas automáticamente. Pero para que esto funcione debe estar utilizando la funcionalidad Monitoreo de Active Directory 828.

Puede mapear cualquier atributo de Active Directory que desee utilizar como detonante para agregar cuentas a los Grupos, aunque el atributo "`memberOf`" es el que se utilizará más probablemente. Puede configurar esto editando el archivo `ActiveDS.dat` en el bloc de notas. Esta funcionalidad se encuentra deshabilitada por omisión. Para habilitarla, edite el archivo `ActiveDS.dat` y especifique el atributo a utilizar como detonante del grupo o quite el signo de comentario en la línea "`Groups=%memberOf%`" en el archivo `ActiveDS.dat` para utilizarlo.

Deshabilitar MDaemon Mensajería Instantánea
Dé clic en esta caja si desea deshabilitar soporte a MDIM para todos los miembros del grupo.

Deshabilitar la Mensajería Instantánea
Dé clic en esta caja si desea permitir soporte a MDIM, pero no a la Mensajería instantánea.

Prioridad (1-1000 - los valores inferiores tienen prioridad sobre los más altos)
Utilice esta opción para configurar un nivel de prioridad (1-1000) para sus grupos, que permiten a las cuentas ser miembros de múltiples grupos y evitar posibles conflictos entre las configuraciones de cada grupo. Por ejemplo, cuando una cuenta es miembro de varios grupos y cada uno tiene asociada una plantilla que controla los mismos parámetros de cuenta, se utilizará el valor del parámetro del Grupo con la mayor prioridad. En otras palabras, si la Prioridad de un Grupo es "1", se encontrará por arriba del Grupo con la Prioridad "10". Cuando no hay conflicto, se aplican colectivamente los parámetros de cada Grupo. En el caso de un empate, gana el grupo que se encuentre primero. Cuando se elimina una cuenta de un grupo ligado a una plantilla d cuenta, los parámetros de cuenta controlados previamente por la plantilla se modificarán a los parámetros definidos por el siguiente Grupo en Prioridad. Si no hay otro grupo controlando esos parámetros, entonces regresarán a la configuración definidas en la Plantilla de Cuentas Nuevas 792.

Crear Firma de Cliente
Haga clic en este botón si desea agregar una firma de cliente para que la usen los miembros del grupo. Ver: Firma de Cliente de Grupo 786

No Molestar

Utilice la funcionalidad No Molestar para programar un lapso de tiempo durante el cual una cuenta no podrá enviar correo o se accesada por sus usuarios. El Acceso durante el periodo No Molestar no se permite y devuelve una respuesta de error

adecuada a las peticiones de acceso IMAP, POP, SMTP, ActiveSync y Webmail. MDaemon aceptará correo entrante para las cuentas en este estado, pero dichas cuentas no pueden enviar correo ni ser accesadas por clientes de correo.

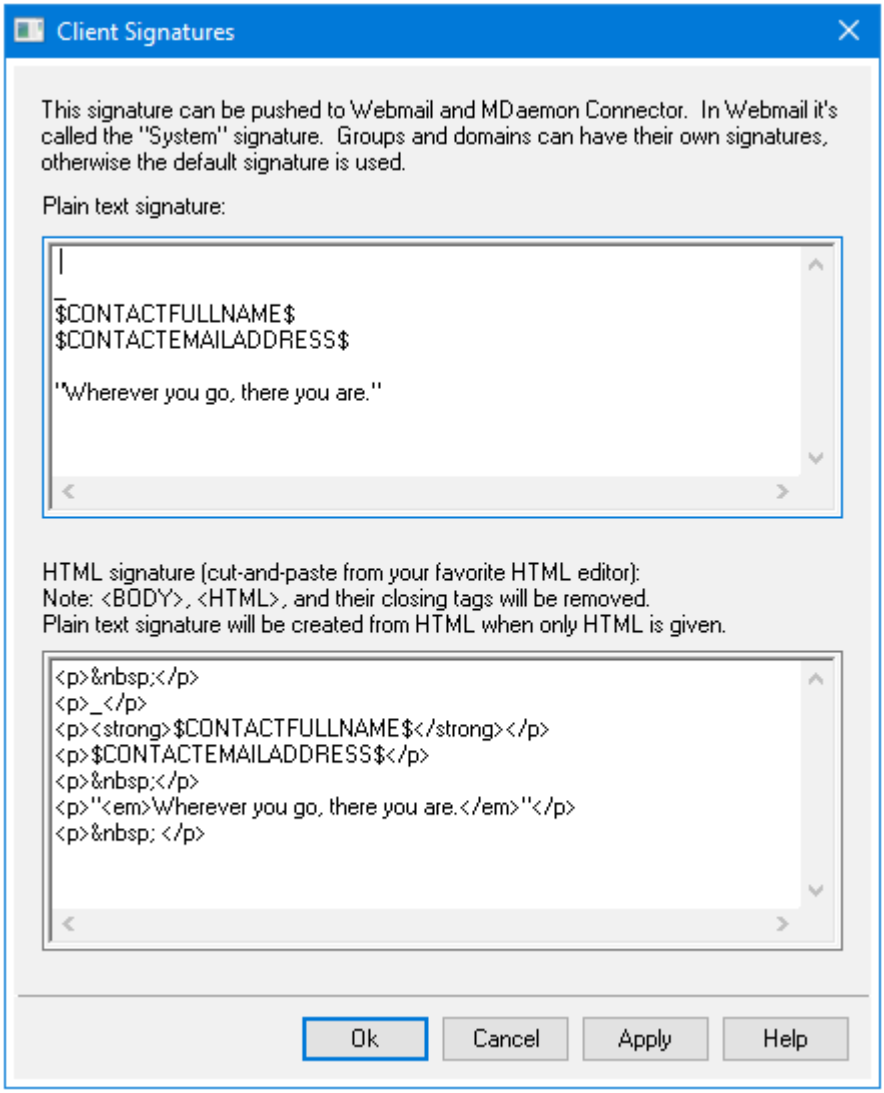
Para aplicar No Molestar a una o más cuentas:

1. Dé clic en **Habilitar No Molestar**.
2. Dé clic en **Definir la programación de No Molestar**.
3. Defina las fechas de inicio/fin y el horario de inicio/fin y los días de la semana en que se habilitará.
4. Dé clic en **OK**.
5. Utilice el Administrador de Grupos 781 para asignar a este grupo las cuentas que desee que utilicen esta funcionalidad.

Ver:

Administrador de Grupos 781
Carpetas de Correo & Grupos 718
Administrador de Plantillas 791
Propiedades de Plantilla 793

5.2.1.1.1 Firma de Cliente



Utilice esta pantalla para crear una firma de cliente para este grupo que puede entregar a MDaemon Webmail[345] y a MDaemon Connector[404], para ser utilizada por sus usuarios al redactar mensajes de correo. Puede utilizar las macros[787] listadas abajo para personalizar la firma, de manera que será única para cada usuario, incluyendo elementos como el nombre de usuario, dirección de correo, teléfono y demás. Si ha creado una Firma de Cliente por Omisión[147] o una Firma de Cliente por Dominio[215], esta firma se utilizará en lugar de aquellas, para los miembros del grupo. Utilice la opción *Entregar firma del cliente*[345] si desea entregar la firma de cliente a Webmail y la opción *Entregar firma del cliente a Outlook*[404] si desea entregarla a MDaemon Connector. En las opciones de redacción de Webmail, la firma de cliente entregada se denomina "Sistema". Para MDaemon Connector, puede asignar un nombre a la firma que aparecerá en Outlook.

Firma en Texto Plano

Este espacio es para insertar una firma en texto plano. Si desea definir en correspondencia una firma html a ser utilizada en la sección text/html de mensajes multiparte, utilice el área abajo *firma HTML*. Si una firma se incluye en ambos lugares, MDaemon utilizará la apropiada para cada parte del mensaje multiparte. Si

no se especifica firma html, entonces se utilizará la firma en texto plano en ambas partes.

Firma HTML (cortar &pegar desde su editor HTML favorito)

Esta área es para insertar una firma HTML a ser utilizada en la parte text/html de mensajes multiparte. Si se incluye una firma aquí y en el área *Firma en Texto Plano* arriba, MDaemon utilizará la apropiada para cada parte del mensaje multiparte. Si no se especifica firma en texto plano entonces se utilizará la firma html para crear una.

Para crear su firma html, teclee el código html aquí manualmente o copie & pegue directamente desde su editor HTML favorito. Si desea incluir imágenes en línea en su firma HTML, lo puede hacer utilizando la macro `$ATTACH_INLINE:path_to_image_file$`.

Por ejemplo:

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

También existen varias maneras en que puede insertar imágenes en línea en firmas desde la interface web de MDaemon Administración Remota 354:

- En la pantalla Firma de Cliente en Administración Remota, dé clic en el botón de la barra de herramientas "Imagen" en el editor HTML y seleccione la pestaña de carga.
- En la pantalla Firma de Cliente en Administración Remota, dé clic en el botón de la barra de herramientas "Agregar Imagen" en el editor HTML.
- Arrastre y suelte una imagen en la pantalla del editor HTML de la Firma de Cliente con Chrome, FireFox, Safari, o MSIE 10+
- Copie y pegue una imagen desde el portapapeles en la pantalla del editor HTML de la Firma de Cliente con Chrome, FireFox, MSIE 11+

Las etiquetas <body></body> y <html></html> no están permitidas en las firmas y serán eliminadas si se encuentran.

Macros de Firmas

Las firmas de MDaemon soportan macros que insertan la información de contacto del remitente en la firma, tomada del contacto del remitente en la Carpeta Pública de Contactos del dominio. Esto permite que se personalices con la información del remitente, las firmas por omisión y del dominio. Por ejemplo `$CONTACTFULLNAME$`, inserta el nombre completo del remitente y `$CONTACTEMAILADDRESS$` inserta la dirección de correo del remitente. Utilice Webmail, MDaemon Connector o ActiveSync para editar los contactos públicos. Se utilizan valores en blanco si no existe contacto para el remitente. Las macros disponibles se enlistan a continuación.

Los usuarios pueden controlar la ubicación de las firmas de MDaemon en sus mensajes colocando cualquiera de las macros **Signature Selector** en un mensaje

siempre que quieran que aparezca la firma,

Signature Selector	
$SYSTEMSIGNATURE$	Coloca la Firma por Omisión 142 o la Firma del Dominio 210 en un mensaje. Si existen ambas, se utilizará la Firma del Dominio.
$CLIENTSIGNATURE$	Coloca la Firma del Cliente por Omisión 147 o la Firma de Cliente del Dominio 215 en un mensaje. Si existen ambas, se utilizará la Firma de Cliente del Dominio.
$ACCOUNTSIGNATURE$	Coloca la Firma de la Cuenta 753 en el mensaje.
Nombres y IDs	
Nombre Completo	**$CONTACTFULLNAME$**
Nombre	**$CONTACTFIRSTNAME$**
Segundo Nombre	**$CONTACTMIDDLENAME$,**
Apellido	**$CONTACTLASTNAME$**
Puesto	**$CONTACTTITLE$**
Sufijo	**$CONTACTSUFFIX$**
Apodo	**$CONTACTNICKNAME$**
Nombre Yomi	**$CONTACTYOMIFIRSTNAME$**
Apellido Yomi	**$CONTACTYOMILASTNAME$**
Nombre de la Cuenta	**$CONTACTACCOUNTNAME$**
ID de Cliente	**$CONTACTCUSTOMERID$**
ID de Gobierno	**$CONTACTGOVERNMENTID$**
Guardar como	**$CONTACTFILEAS$**
Direcciones de Correo	
Dirección de Correo	**$CONTACTEMAILADDRESS$**
Dirección de Correo 2	**$CONTACTEMAILADDRESS2$**
Dirección de Correo 3	**$CONTACTEMAILADDRESS3$**
Teléfono y Fax	
Teléfono Móvil	**$CONTACTHOMEMOBILE$**
Teléfono Móvil 2	**$CONTACTMOBILE2$**
Teléfono del Auto	**$CONTACTCARPHONENUMBER$**
Teléfono Particular	**$CONTACTHOMEPHONE$**
Teléfono Particular 2	**$CONTACTHOMEPHONE2$**

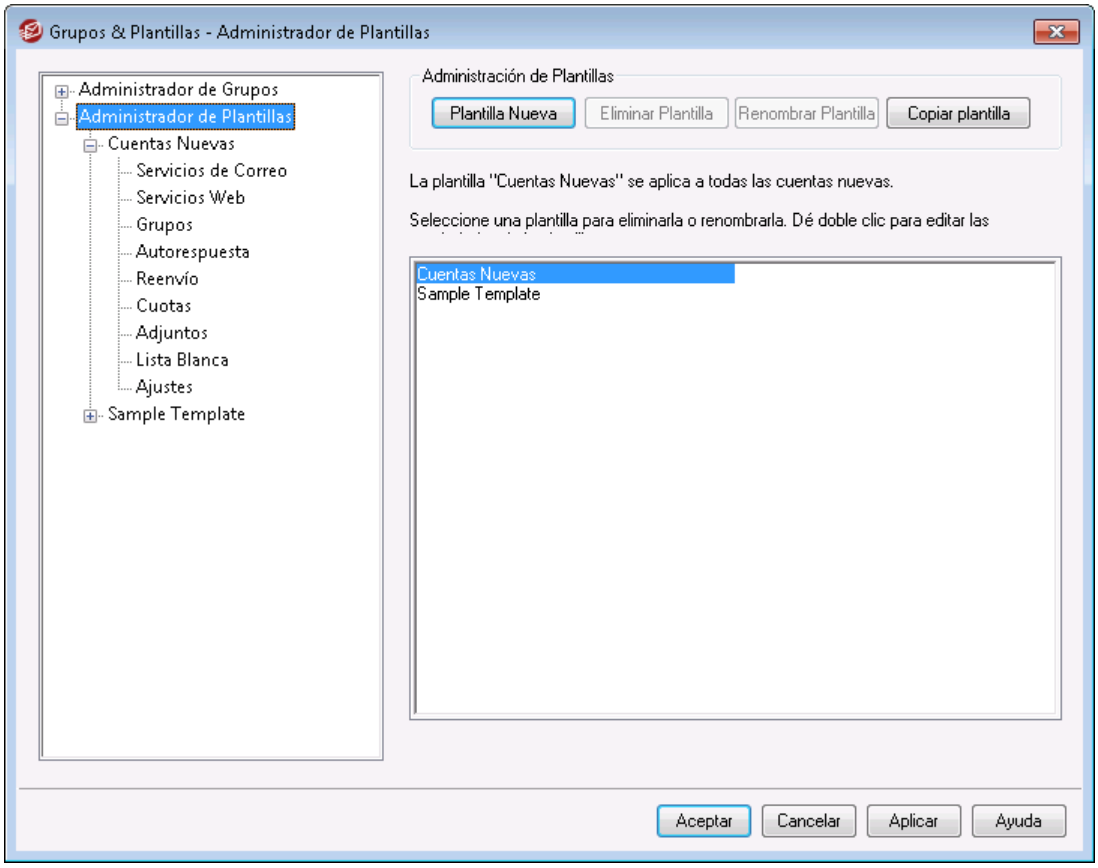
Fax Particular	**$CONTACTHOMEFAX$**
Otro teléfono	**$CONTACTOTHERPHONE$**
Mensajería Instantánea y Web	
Dirección IM	**$CONTACTIMADDRESS$**
Dirección IM 2	**$CONTACTIMADDRESS2$**
Dirección IM 3	**$CONTACTIMADDRESS3$**
Dirección MMS	**$CONTACTMMSADDRESS$**
Dirección web personal	**$CONTACTHOMEWEBADDRESS$**
Address	
Domicilio Particular	**$CONTACTHOMEADDRESS$**
Ciudad	**$CONTACTHOMECITY$**
Estado	**$CONTACTHOMESTATE$**
Código Postal	**$CONTACTHOMEZIPCODE$**
País	**$CONTACTHOMECOUNTRY$**
Otra Dirección	**$CONTACTOTHERADDRESS$**
Otra Ciudad	**$CONTACTOTHERCITY$**
Otro Estado	**$CONTACTOTHERSTATE$**
Otro Código Postal	**$CONTACTOTHERZIPCODE$**
Otro País	**$CONTACTOTHERCOUNTRY$**
Trabajo	
Empresa	**$CONTACTBUSINESSCOMPANY$**
Nombre Yomi de la Empresa	**$CONTACTYOMICOMPANYNAME$**
Puesto	**$CONTACTBUSINESSTITLE$**
Área	**$CONTACTBUSINESSOFFICE$**
Departamento	**$CONTACTBUSINESSDEPARTMENT$**
Gerencia	**$CONTACTBUSINESSMANAGER$**
Asistente	**$CONTACTBUSINESSASSISTANT$**
Teléfono Asistente	**$CONTACTBUSINESSASSISTANTPHONE$**
Teléfono directo en la Empresa	**$CONTACTBUSINESSMAINPHONE$**
Teléfono de la Empresa	**$CONTACTBUSINESSPHONE$**
Teléfono 2 de la Empresa	**$CONTACTBUSINESSPHONE2$**
Teléfono IP de la Empresa	**$CONTACTBUSINESSIPPHONE$**

Fax de la Empresa	$CONTACTBUSINESSFAX$
Pager de la Empresa	$CONTACTBUSINESSPAGER$
Radio de la Empresa	$CONTACTBUSINESSRADIO$
Dirección de la Empresa	$CONTACTBUSINESSADDRESS$
Ciudad de la Empresa	$CONTACTBUSINESSCITY$
Estado de la Empresa	$CONTACTBUSINESSSTATE$
Código Postal de la Empresa	$CONTACTBUSINESSZIPCODE$
País de la Empresa	$CONTACTBUSINESSCOUNTRY$
Sitio web de la Empresa	$CONTACTBUSINESSWEBADDRESS$
Otros	
Esposo(a)	$CONTACTSPOUSE$
Hijos	$CONTACTCHILDREN$
Categorías	$CONTACTCATEGORIES$
Comentario	$CONTACTCOMMENT$

Ver:

Firmas de Cliente por Omisión 147
Firmas por Omisión 142
Administrador de Dominios » Firmas 210
Editor de Cuentas » Firma 753
Administrador de Dominios » Ajustes de Webmail 201
Ajustes de Cliente OC » Firma 404

5.2.2 Administrador de Plantillas



Con el Administrador de Plantillas (Cuentas » Grupos & Plantillas... » Administrador de Plantillas) puede crear y administrar las Plantillas de Cuentas, que son conjuntos definidos de parámetros de cuentas que se pueden asignar a Grupos 781 específicos. Cualquier cuenta que pertenezca a uno o más de esos grupos tendrá bloqueados los parámetros incluidos en la plantilla y solo podrán alterarse a través de ésta y no desde el Editor de Cuentas. Las categorías de parámetros de cuentas que controla una plantilla se definen en la pantalla propiedades 793 de la plantilla, a la que se ingresa dando doble clic en el nombre de la plantilla en la lista abajo o dando clic en la plantilla en el panel izquierdo.

Administración de Plantillas

Plantilla Nueva
Para crear una nueva Plantilla de Cuentas, dé clic en *Plantilla Nueva*, teclee un nombre para la plantilla y dé clic en *OK*. La nueva plantilla aparecerá en la lista de plantillas abajo y en el panel izquierdo.

Eliminar Plantilla
Para eliminar una plantilla, selecciónela en la lista inferior, dé clic en *Eliminar Plantilla* y dé clic en *Si* para confirmar su decisión de eliminarla.

Renombrar Plantilla
Para renombrar una plantilla, selecciónela en la lista inferior y dé clic en *Renombrar Plantilla*. Teclee el nuevo nombre de la plantilla y dé clic en *OK*.

Copiar plantilla
Si desea crear una plantilla con los ajustes de otra ya existente, seleccione la plantilla de la lista, dé clic en este botón y especifique el nombre de la nueva plantilla.

Lista de Plantillas

La lista en la sección inferior del Administrador de Plantillas contiene todas sus plantillas. Dé clic en una de ellas y utilice los botones de la sección superior de la pantalla para eliminarla o renombrarla. Dé doble clic en una plantilla para abrir la pantalla de sus propiedades[793] desde la que puede definir las categorías de los parámetros de cuenta que controlará. Puede ir directamente a cualquier plantilla y sus parámetros de cuenta utilizando los controles del panel izquierdo. La plantilla *Cuentas Nuevas* es una plantilla especial que siempre aparece en primer lugar en la lista.

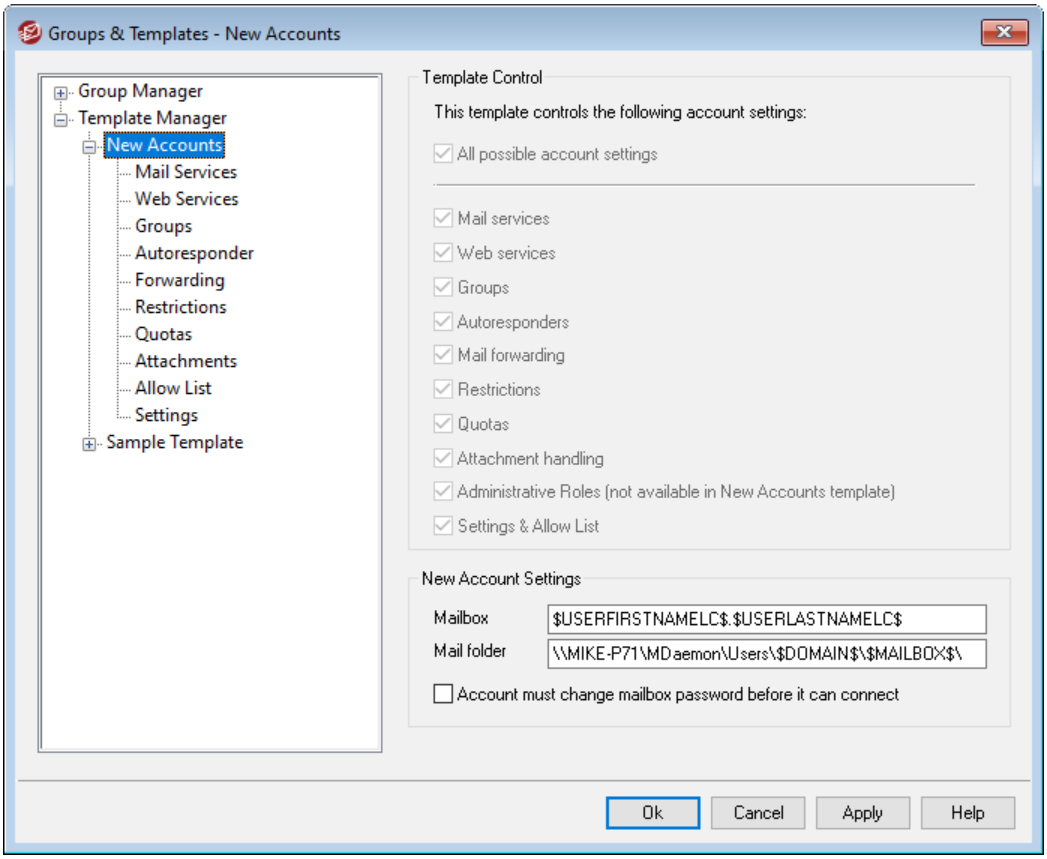
Plantilla de Cuentas Nuevas

La plantilla *Cuentas Nuevas* es una plantilla especial que se aplica a todas las cuentas nuevas cuando son creadas. En lugar de bloquear y controlar ciertos parámetros de cuenta como otras plantillas, *Cuentas Nuevas* se utiliza simplemente para definir los parámetros iniciales de las cuentas nuevas. Esos parámetros iniciales pueden entonces modificarse normalmente al utilizar el Editor de Cuentas para editar las cuentas individualmente. Algunas configuraciones de plantillas, tales como las opciones localizadas en la pantalla Roles Administrativos[817], no están disponibles en la plantilla de Cuentas Nuevas.

Ver:

Propiedades de Plantillas[793]
Administrador de Grupos[781]

5.2.2.1 Propiedades de Plantillas



Para ingresar a la pantalla de propiedades de plantillas, abra el Administrador de Plantillas 791 y dé clic en el nombre de la plantilla en el panel izquierdo. Utilice la pantalla de propiedades de cada plantilla para definir las categorías de parámetros de cuentas que controlará la plantilla. Cualquier cuenta que pertenezca a un Grupo 781 que utiliza una plantilla de cuentas tendrá bloqueadas las pantallas correspondientes en el Editor de Cuentas, dado que esos parámetros serán controlados por la plantilla. Si una cuenta pertenece a múltiples grupos ligados a diferentes plantillas, entonces todas esas plantillas se utilizarán siempre que no existan conflictos entre las propiedades de plantilla definidas. Si se establecen múltiples plantillas para controlar las mismas propiedades, entonces se utilizará la primera plantilla enlistada.

Control de Plantillas

Todos los posibles ajustes de cuentas
Dé clic en esta caja si desea que esta plantilla controle todos los ajustes de cuenta disponibles para los Grupos 781, utilizando la plantilla. Todas las pantallas de la plantilla se utilizarán para definir la configuración de las cuentas miembro del grupo en lugar de las pantallas correspondientes en el Editor de Cuentas. Deshabilite esta casilla si desea utilizar las opciones de *Configuración de Cuenta* abajo, para seleccionar los parámetros específicos de cuenta que desea controlar.

Ajustes de Cuentas
Esta sección enlista todas las categorías de ajustes de cuenta que puede controlar una plantilla para los Grupos que la utilizan. Cada opción corresponde a una pantalla de plantilla con el mismo nombre. Cuando se selecciona una opción,

se utilizarán los parámetros en esa pantalla de plantilla en lugar de los parámetros establecidos en la pantalla correspondiente del Editor de Cuentas, asociada a los miembros del grupo.

Ajustes de Cuentas Nuevas

Estas opciones solo están disponibles en la Plantilla de Cuentas Nuevas[792]. Utilizan una serie de macros especiales[795] para generar automáticamente la carpeta de almacenamiento de correo y la porción del buzón de la dirección de correo para cuentas nuevas.

Buzón
Utilice este campo para controlar la porción del *Nombre del Buzón*[715] de la dirección de correo que será generada para cuentas nuevas. Vea las Macros de Plantillas[795] abajo para obtener la lista de las Macros que se pueden utilizar en la cadena de esta plantilla. "`$USERFIRSTNAMELC$.$USERLASTNAMELC$`" es la plantilla por omisión de esta opción. Por esto, al crear una cuenta para "Juan Luna" bajo el dominio ejemplo.com se generará la dirección de correo como "`juan.luna@ejemplo.com`".

Carpeta de Correo
Utilice este campo para controlar la *Carpeta de Correo*[718] por omisión que se utilizará para cuentas nuevas. La *Carpeta de Correo* de cada cuenta es la ubicación donde se almacenarán los mensajes de correo en el servidor. Por ejemplo, "`...\$DOMAIN$\$MAILBOX$\`" creará la ruta, "`...\ejemplo.com\juan.luna\`" para el usuario, "juan.luna@ejemplo.com".

MDaemon soporta un sistema básico de hash para las carpetas. Bajo NTFS, el mantener muchas carpetas bajo la misma raíz en ocasiones puede generar problemas de desempeño. Si se tiene una gran cantidad de usuarios y desea subdividir las carpetas de usuario más allá del valor por omisión `$DOMAIN$\$MAILBOX$\`, puede utilizar la macro `$MAILBOXFIRSTCHARSn$` para hacerlo. Al utilizar esta macro, "`n`" es un número entre 1 y 10 y se expandirá a los primeros "`n`" caracteres del nombre del buzón. Al modificar su ruta por omisión de *Carpeta de Correo* a algo como lo siguiente, obtendrá un sistema decente de hash de carpetas:

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCH
ARS2$\$MAILBOX$\.
```

La cuenta debe cambiar su contraseña antes de conectarse
Esta opción controla si la cuenta debe modificar o no su *Contraseña del Buzón* antes de tener acceso POP, IMAP, SMTP, Webmail, o a la Administración Remota. El usuario puede conectarse a Webmail o a la Administración Remota, pero se le solicitará que modifique su contraseña antes de proceder. Note, sin embargo, que a fin de que los usuarios puedan modificar sus contraseñas vía Webmail o Administración Remota, primero se les debe otorgar permiso para "*...editar contraseña*" vía web en la pantalla Servicios Web[798]. Luego de que se modifique la contraseña esta opción se desactivará en la pantalla Detalles de la Cuenta[715].

Dado que puede no ser sencillo o posible que algunos usuarios modifiquen su contraseña, se deberá tener precaución antes de activar esta opción.

Macros de Plantillas

Abajo se presenta una referencia rápida a las macros disponibles para automatizar la configuración de cuentas.

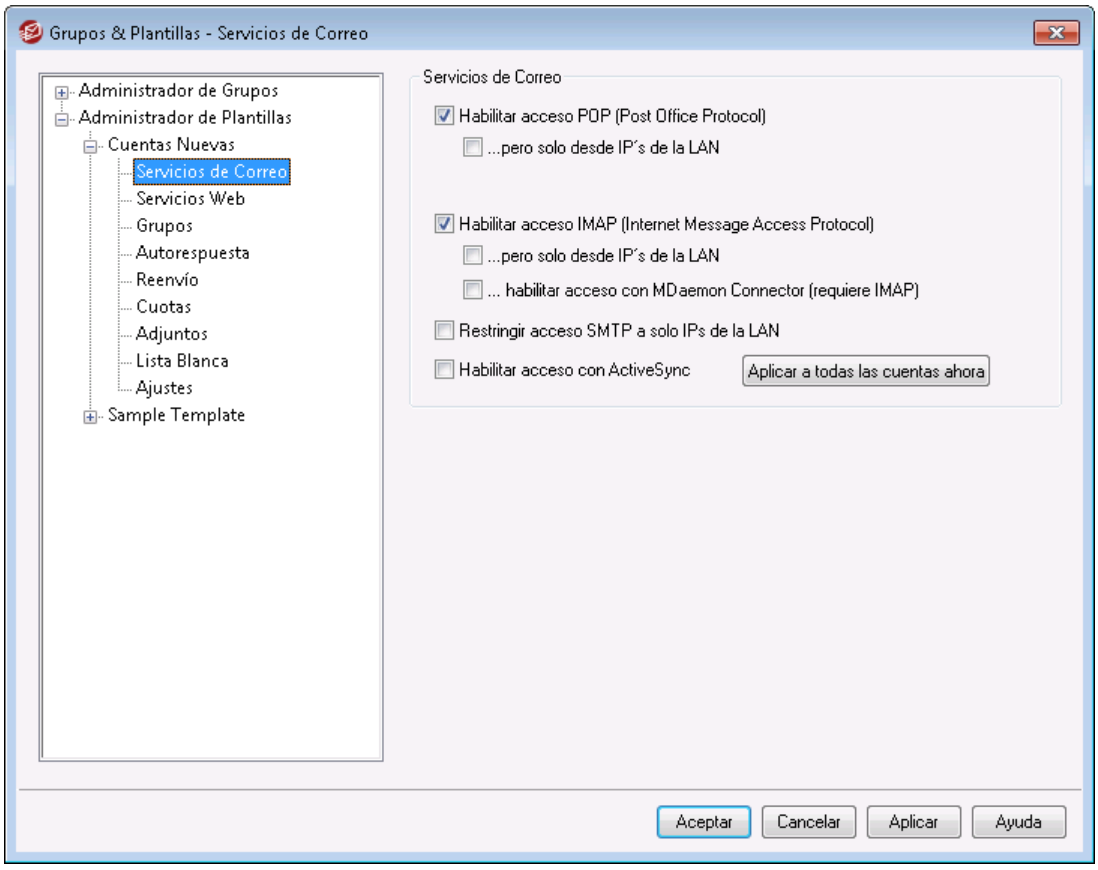
$DOMAIN$	Esta variable resolverá al nombre de dominio seleccionado para la cuenta.
$DOMAINIP$	Esta variable resolverá a la IP asociada con el dominio seleccionado para la cuenta.
$MACHINENAME$	Esta macro devuelve el nombre de host del Dominio por Omisión, de la pantalla Nombre de Host & IP del Administrador de Dominios. La macro ahora se utiliza en el script de la información por omisión de cuentas (NEWUSERHELP.DAT) para instalaciones nuevas.
$USERNAME$	Esta variable resuelve al nombre y apellido completos del propietario de la cuenta. Este campo es equivalente a "$USERFIRSTNAME$ $USERLASTNAME$"
$USERFIRSTNAME$	Esta variable resuelve al Nombre del propietario de la cuenta.
$USERFIRSTNAMELC$	Esta variable resuelve al Nombre del propietario de la cuenta, en minúsculas.
$USERLASTNAME$	Esta variable resuelve al Apellido del propietario de la cuenta.
$USERLASTNAMELC$	Esta variable resuelve el Apellido del propietario de la cuenta, en minúsculas.
$USERFIRSTINITIAL$	Esta variable resuelve a la inicial del nombre del propietario de la cuenta.
$USERFIRSTINITIALLC$	Esta variable resuelve a la inicial del Nombre del propietario de la cuenta, en minúsculas.
$USERLASTINITIAL$	Esta variable resuelve a la inicial del apellido del propietario de la cuenta.

$USERLASTINITIALLC$	Esta variable resuelve a la inicial del apellido del propietario de la cuenta, en minúsculas.
$MAILBOX$	Esta variable resuelve al nombre de buzón de la cuenta actual. Este valor también se utilizará como valor del comando USER que se transmite durante las sesiones de correo POP3.
$MAILBOXFIRSTCHARSn$	Donde "n" es un número entre 1 y 10. Se expandirá a los primeros "n" caracteres del nombre del buzón.

Ver:

Administrador de Plantillas 791
Administrador de Grupos 781

5.2.2.1.1 Servicios de Correo



Las opciones en esta pantalla de plantilla corresponden a las opciones localizadas en la pantalla Servicios de Correo[719] localizada en el Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla,[793] controlará las opciones de Servicios de Correo de todas las cuentas que pertenezcan a un Grupo[783] que utilice esa plantilla.

Servicios de Correo

Habilitar acceso POP (Post Office Protocol)
Cuando se selecciona esta casilla, las cuentas con parámetros controlados por esta plantilla pueden ser accesadas vía Post Office Protocol (POP). Virtualmente todos los clientes de correo soportan este protocolo. Deshabilite la casilla si no desea permitir acceso POP.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que las cuentas sean accesadas vía POP solo cuando el usuario se conecta desde una Dirección IP de la LAN[608].

Habilitar acceso IMAP (Internet Message Access Protocol)
Cuando está marcada esta casilla, las cuentas con parámetros controlados por esta plantilla pueden ser accesadas vía Internet Message Access Protocol (IMAP). IMAP es más versátil que POP, permitiendo que el correo sea administrado en el servidor y accesado utilizando múltiples clientes. La mayoría de los clientes de correo soportan este protocolo.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que las cuentas sean accesadas vía POP solo cuando el usuario se conecta desde una Dirección IP de la LAN[608].

...Habilitar acceso vía MDaemon Connector (requiere IMAP)
Esta opción solo está disponible en la plantilla de Cuentas Nuevas. Dé clic en la casilla si desea permitir que las cuentas nuevas compartan carpetas de Microsoft Outlook utilizando Outlook Connector para MDaemon[387]. **Nota:** esta opción solo estará disponible cuando Outlook Connector esté instalado en el servidor.

Restringir acceso SMTP solo a IPs de la LAN
Marque esta casilla si desea restringir el acceso SMTP a solo IPs de la LAN. Esto impedirá que las cuentas envíen correo a menos que se encuentren conectadas a su red. Si la cuenta intenta enviar correo desde una IP externa, la conexión se rehusará y será cerrada.

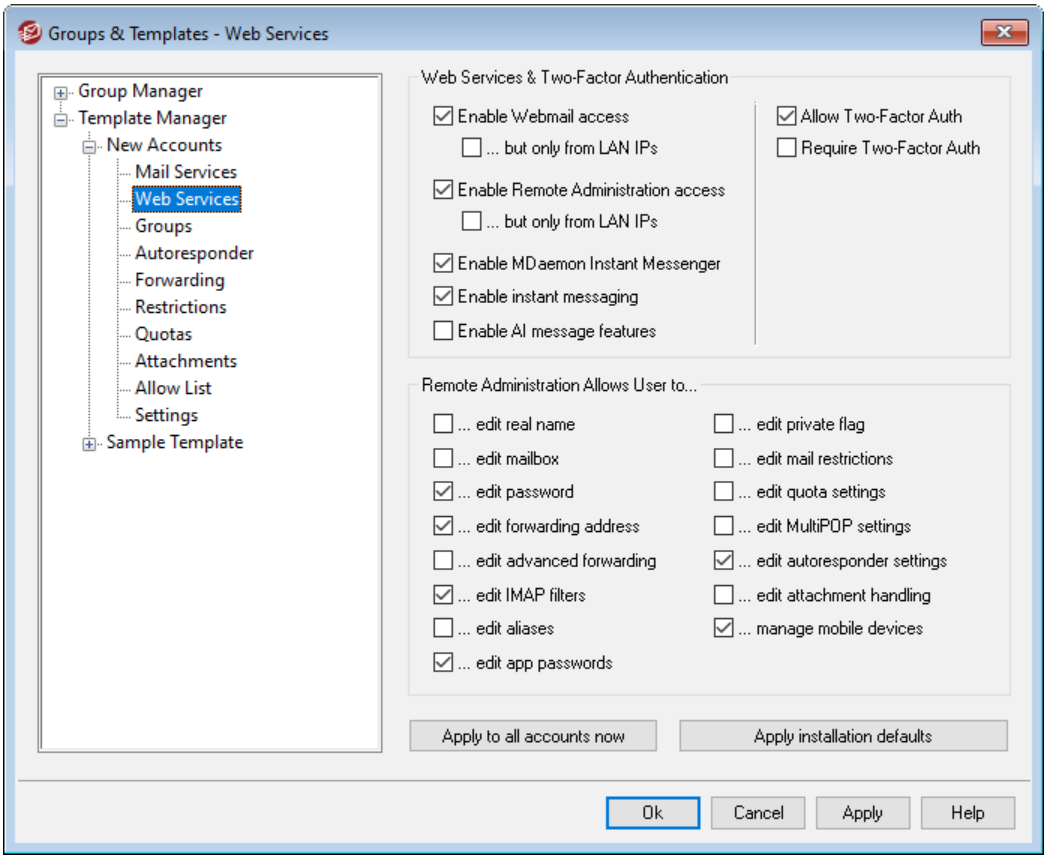
Habilitar acceso ActiveSync
Esta opción solo está disponible en la plantilla de Cuentas Nuevas. Seleccione la casilla si desea permitir que las cuentas nuevas utilicen ActiveSync en un dispositivo móvil para sincronizar correo, contactos, calendario y otros datos con MDaemon/Webmail. Este ajuste corresponde a la opción *Habilitar servicios ActiveSync para este usuario*, localizada en la pantalla ActiveSync para MDaemon[764] en el Editor de Cuentas.

Aplicar a todas las cuentas ahora
Esta opción solo está disponible en la plantilla de Cuentas Nuevas. Dé clic en este botón para aplicar inmediatamente los ajustes de la pantalla a las pantallas Servicios de Correo[719] y ActiveSync para MDaemon[764] de todas las cuentas existentes en MDaemon.

Ver:

Propiedades de Plantillas 793
Propiedades de Grupo 783
Plantilla de Cuentas Nuevas 792
Editor de Cuentas » Servicios de Correo 719

5.2.2.1.2 Servicios Web



Las opciones en esta pantalla de plantillas corresponden a las opciones localizadas en la pantalla Servicios Web 720 del Editor de Cuentas. Cuando una plantilla se define para controlar esta pantalla 793, controlará las opciones de Servicios Web para todas las cuentas que pertenezcan a un Grupo 783 que utiliza la plantilla.

Servicio Web y Autentificación de Dos Factores

Habilitar acceso vía Webmail
Habilite esta casilla si desea que las cuentas controladas por esta plantilla puedan tener acceso a Webmail 321, lo que permite a los usuarios accesar a su correo, calendarios y otras opciones utilizando un navegador.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que las cuentas sean accesadas vía POP solo cuando el usuario se conecta desde una Dirección IP de la LAN[608].

Habilitar acceso a la Administración Remota
Marque esta casilla si desea permitir que las cuentas controladas por esta plantilla modifiquen algunos de sus parámetros de cuenta vía MDaemon Administración Remota[354]. Las cuentas solo podrán editar aquellos parámetros que usted seleccione en la sección inferior.

Cuando se habilita esta funcionalidad y el servidor MDaemon Administración Remota está activo, el usuario podrá ingresar a MDaemon Administración Remota seleccionando en el navegador el dominio y puerto asignado a Administración Remota[356] (ej. `http://ejemplo.com:1000`) en MDaemon. Se le presentará una pantalla de inicio de sesión y luego una pantalla que contiene los parámetros para los que se tenga permisos de edición. Todo lo que debe hacer es editar los parámetros que desee y dé clic en el botón *Grabar cambios*. Puedo luego cerrar la sesión y el navegador. Si tiene acceso a Webmail entonces también puede ingresar a MDaemon Administración Remota desde el menú Opciones Avanzadas desde Webmail.

Si el usuario es Administrador Global o de Dominio (definido en la pantalla Roles Administrativos[757] del Editor de Cuentas) verá una pantalla diferente luego que ingrese a MDaemon Administración Remota.

...pero solo desde IPs de la LAN
Seleccione esta casilla si desea permitir que las cuentas tengan acceso a la Administración Remota solo cuando el usuario se conecte desde una Dirección IP de la LAN[608].

Habilitar MDaemon Mensajería Instantánea
Dé clic en esta caja si desea habilitar soporte MDIM[322] por omisión para las cuentas nuevas. Esta opción solo está disponible en la Plantilla de Cuentas Nuevas[792]. Existe una opción similar en Propiedades de Grupo[783] que se puede utilizar para controlar el acceso de miembros de grupos a MDIM.

Habilitar Mensajería Instantánea
Dé clic en esta opción si desea habilitar por omisión soporte para el sistema de Mensajería Instantánea de MDIM para las cuentas nuevas. Esta opción solo está disponible en la Plantilla de Cuentas Nuevas[792]. Existe una opción similar en Propiedades de Grupo[783] que se puede utilizar para controlar el acceso de miembros de grupos a la Mensajería Instantánea.

El usuario puede editar categorías
Marque esta casilla si desea permitir a los nuevos usuarios de Webmail editar categorías. Esto se encuentra deshabilitado por omisión para usuarios nuevos. **Nota:** Esta opción solo está disponible en la interface web de MDaemon Administración Remota.

Omitir la verificación de persistencia de IP para sesiones de Webmail
Cuando está habilitada la opción "Requerir persistencia de IP durante la sesión de Webmail" en Webmail[326], puede marcar esta casilla si desea exentar a los usuarios nuevos del requerimiento de persistencia de IP. **Nota:** Esta opción solo está disponible en la interface web de MDaemon Administración Remota.

Habilitar funcionalidades de IA en mensajes
Si está habilitada la opción *Funcionalidades de IA* en mensajes en el diálogo del dominio de una cuenta en Webmail 201, marque esta casilla si desea permitir que las cuentas controladas por esta plantilla utilicen esas funcionalidades en MDaemon Webmail; las funcionalidades solo estarán disponibles para el usuario cuando esté habilitada la opción a nivel dominio. **Ver:** "Funcionalidades IA en Mensajes en Webmail 802" abajo para obtener información importante y precauciones sobre el uso de esas funcionalidades.

Autentificación de Dos Factores

MDaemon soporta la Autentificación de Dos Factores (2FA) para usuarios que acceden a Webmail o a la Administración Remota de MDaemon vía su interface web. Las cuentas que ingresan a Webmail vía HTTPS pueden activar la Autentificación de dos factores en la pantalla **Opciones » Seguridad** en Webmail. Así, el usuario debe registrar un código de verificación al ingresar a Webmail o a Administración Remota. El código se obtiene de una app autentificadora instalada en el dispositivo móvil o tableta del usuario. Esta funcionalidad está diseñada para cualquier cliente que soporte Google Authenticator. Vea la Ayuda de Webmail para más información sobre como configurar 2FA para una cuenta.

Permitir Autentificación de Dos Factores
Por omisión, a las cuentas nuevas se les permite configurar y usar la Autentificación de Dos Factores (2FA) de Webmail. Deshabilite esta casilla si no desea permitir 2FA por omisión para las cuentas nuevas. Puede controlar este ajuste para cuentas específicas en la página de Servicios Web 720 de cada cuenta.

Requerir Autentificación de Dos Factores
Habilite esta opción si desea forzar a todas las cuentas nuevas a utilizar la Autentificación de dos Factores (2FA) al ingresar a la interface web de Webmail o de la Administración Remota. Cuando 2FA es requerida, cualquier cuenta que no haya sido configurada para utilizarla será redirigida a la página donde se configura, la siguiente ocasión en que intente ingresar a Webmail. Vea la Ayuda de Webmail para más información sobre como configurar 2FA para una cuenta.

Administración Remota permite a los usuarios...

...editar su nombre real
Al habilitar esta opción permitirá que las cuentas asociadas con esta plantilla modifiquen la información de su *Nombre y Apellido* 715.

...editar buzón
Al habilitar esta opción se permitirá a los usuarios modificar el *Nombre de su buzón* 715.

Dado que el *Nombre de Buzón* es parte de la dirección de correo de la cuenta, que es un identificador único y valor de ingreso a la sesión para la cuenta, modificarlo significa que el usuario estará cambiando su dirección de correo electrónico. Esto podría resultar en que mensajes futuros

dirigidos a la dirección anterior sean rechazados o eliminados.

...editar contraseña
Dé clic en esta casilla si desea permitir que las cuentas modifiquen la *Contraseña del buzón*. Para más información sobre requerimientos de contraseñas vea: Contraseñas 855.

...editar dirección de reenvío
Cuando se habilita esta opción, las cuentas asociadas con la plantilla podrán modificar la configuración de su dirección de reenvío 729.

...editar reenvío avanzado
Cuando se habilita esta opción, los usuarios pueden modificar sus *Ajustes Avanzadas de reenvío* 729.

...editar filtros IMAP
Use este control para permitir a cada usuario crear y administrar sus propios Filtros IMAP 737.

...editar alias
Habilite esta opción si desea permitir a los usuarios de cuenta utilizar la Administración Remota para editar los Alias 742 asociados con sus cuentas.

...editar contraseñas de apps
Por omisión, los usuarios pueden editar sus Contraseñas de Apps 751. Deshabilite esta casilla si no desea permitir a los usuarios editarlas.

...editar marca privada
Esta opción controla si se le permite al usuario utilizar la Administración Remota para editar la opción "*La Cuenta está oculta de listas "Everyone", calendarios compartidos y VRFY*"" localizada en la pantalla Ajustes 760 en el Editor de Cuentas.

...editar restricciones de correo
Esta casilla controla si la cuenta puede editar las restricciones de correo Entrante/Saliente, localizada en la pantalla Restricciones 731.

...editar parámetros de cuotas
Dé clic en esta casilla si desea permitir que los usuarios modifiquen los parámetros de sus Cuotas 733.

...editar la configuración MultiPOP
Dé clic en esta casilla si desea permitir que la cuenta agregue registros MultiPOP 739 y habiliten/deshabiliten la recolección MULTIPOP para esos registros.

...editar la configuración de la autorespuesta
Dé clic en esta casilla si desea dar permiso a los usuarios para agregar, editar o eliminar las Autorespuestas 726 para su cuenta.

...editar el manejo de adjuntos
Dé clic en esta casilla si desea permitir a los usuarios editar las opciones de manejo de archivos adjuntos localizadas en la pantalla Adjuntos 735.

...administrar dispositivo móvil
Dé clic en esta opción si desea permitir al usuario que utilice la Administración Remota para administrar parámetros específicos de su dispositivo, tales como ActiveSync.

Aplicar a todas las cuentas ahora

Esta opción solo está disponible en la Plantilla de Cuentas Nuevas 792. Dé clic para aplicar todas las configuraciones en esta pantalla a todas las cuentas existente en MDaemon que no son controladas específicamente por una Plantilla de Cuentas de Servicios Web.

Aplicar valores de instalación por omisión

Esta opción solo está disponible en la Plantilla de Cuentas Nuevas 792. Dé clic aquí para restablecer la Plantilla de Cuentas nuevas a los valores de instalación por omisión. Solo modificará la configuración de la plantilla, no modificará ninguna cuenta existente.

Cargar la configuración de la plantilla "Cuentas Nuevas"

Esta opción solo está disponible para plantillas personalizadas. Dé clic para establecer las opciones en esta pantalla a los valores por omisión definidos en la pantalla de Servicios Web en la Plantilla de Cuentas Nuevas 792.

Funcionalidades IA en Mensajes de Webmail

Al igual que MDaemon 23.5.0, el tema Pro en el cliente Webmail de MDaemon incluye varias funcionalidades de Inteligencia Artificial (IA para ayudar a sus usuarios a administrar su correo e incrementar la productividad. Estas funcionalidades son opcionales y están deshabilitadas por omisión, pero se pueden habilitar para cualquier usuario.

Con estas funcionalidades, en MDaemon Webmail puede utilizar IA :

- Generar un resumen de los contenidos de un mensaje de correo.
- Sugerir una respuesta al mensaje, de acuerdo a varios lineamientos que le puede indicar a la IA. También puede definir el *Tono* de la respuesta ya sea profesional respetuoso o casual. La *Posición*, o sentido de la respuesta puede definirse como interesado, no interesado, de acuerdo, en desacuerdo o escéptico. La respuesta con *Actitud* podrá definirse como confiado, emocionado, calmado o arrepentido. Por último, puede definir la *Longitud* de la respuesta, que puede ser desde muy breve a detallada.
- Puede ayudar a redactar un nuevo mensaje de correo, con base en algún texto que ya se haya incluido. Al igual que en la opción mencionada *Sugerir Respuesta*, también se puede definir el Tono, Posición, Actitud y Longitud como criterios a utilizar por la IA al redactar el mensaje.

La opción *Habilitar funcionalidades de IA en Mensajes* en la pantalla Ajustes de Webmail 345 controla si está o no habilitado el soporte a las funcionalidades de IA por omision para sus dominios. Existe una opción con el mismo nombre localizada en

el diálogo Webmail[201] del Administrador de Dominios, que se puede utilizar para ignorar el ajuste principal para dominios específicos. **Nota:** el habilitar el soporte a Funcionalidades IA en Mensajes no garantiza acceso a ellas para todos los usuarios del dominio. Se deberá activar la opción *Habilitar funcionalidades IA en mensajes* en la pantalla Servicios Web[720] del editor de cuentas para los usuarios a los que desee dar permiso. Alternativamente, puede utilizar las opciones de Plantillas de Cuentas[791] y Grupos[781] para asignar usuarios a un grupo que tenga acceso a funcionalidades IA en mensajes.

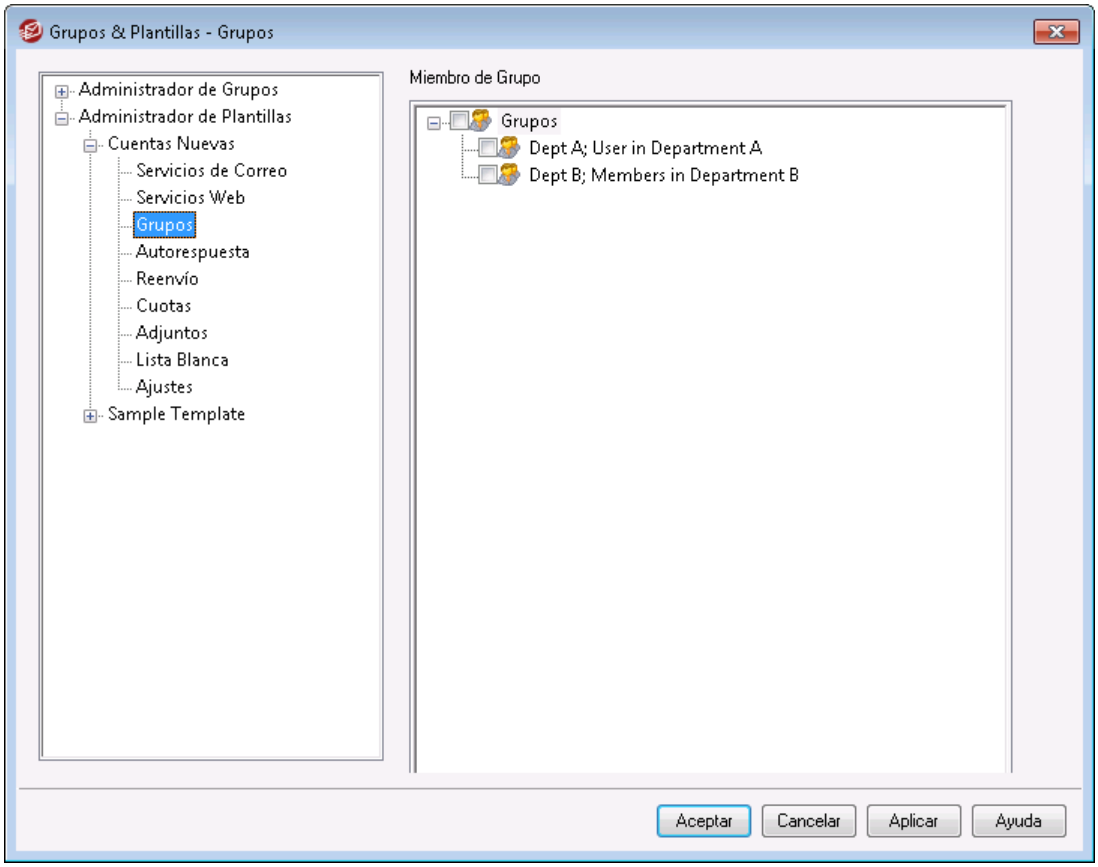
Cuando se habilitan en MDaemon las cuentas para utilizar las funcionalidades IA en mensajes se permite a los usuarios enviar y recibir información para y de servicios generativos IA de terceros, específicamente ChatGPT de OpenAI. Los Administradores y usuarios deberán estár conscientes de que esto introduce varios temas de privacidad debido a la habilidad de la funcionalidad de procesar datos personales y generar información potencialmente sensitiva. Para resolver los temas de privacidad, es vital que las organizaciones capaciten a sus empleados para usar IA con responsabilidad. **Nota:** Los datos enviados para/de Open AI no se almacenan en el servidor local o en nuestra red.

Puede encontrar la Política de Uso de MDaemon Technologies en la Página Artifical Intelligence (AI) Information. En esa misma página existe una liga a los Terminos de Uso de OpenAI.

Ver:

Propiedades de Plantillas[793]
Propiedades de Grupos[783]
Plantilla de Cuentas Nuevas[792]
Editor de Cuentas » Servicios Web[720]

5.2.2.1.3 Grupos



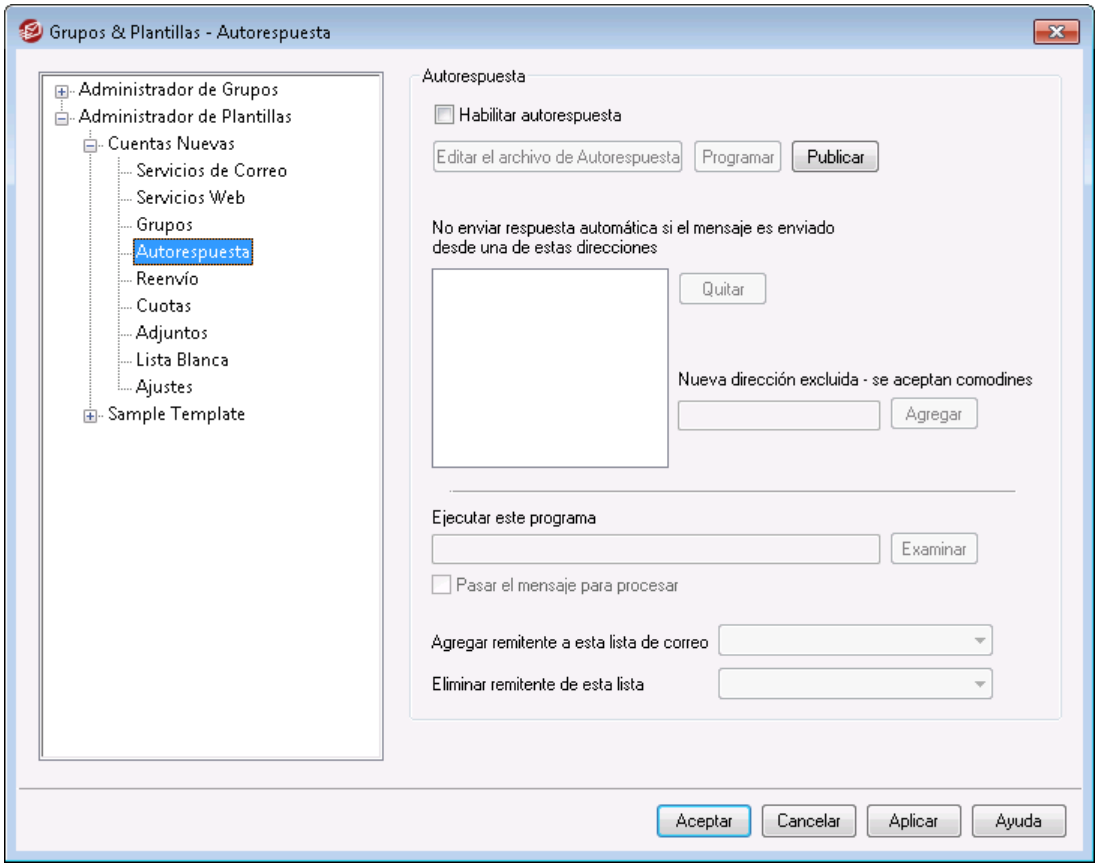
Membresía de Grupos

Esta pantalla solo está disponible en la Plantilla de Cuentas Nuevas[792] y corresponde a la sección Membresía de Grupo de la pantalla Carpeta de Correo & Grupos[718]. Cuando selecciona uno o más grupos en esta pantalla, las cuentas nuevas automáticamente se agregarán a ellos..

Ver:

Administrador de Grupos[781]
Propiedades de Grupo[783]

5.2.2.1.4 Autorespuestas



Las opciones en esta pantalla de plantillas corresponden a las opciones localizadas en la pantalla Autorespuestas 726 en el Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla 793, controlará las opciones de Autorespuesta de cualquier cuenta que pertenezca a un Grupo 783 que utilice la plantilla.

Las Autorespuestas son herramientas útiles para hacer que los mensajes de correo entrantes detonen ciertos eventos automáticamente, tales como correr un programa, agregar un remitente a una lista de correo, responder con un mensaje generado automáticamente y más. El uso más común de las autorespuestas es responder automáticamente a mensajes entrantes con un mensaje definido por el usuario mencionando que el destinatario está de vacaciones, no está disponible, responderá lo más pronto posible, etc. Los usuarios de MDaemon con acceso web 720 a Webmail 321 o a Administración Remota 354 pueden utilizar las opciones provistas para redactar ellos mismos mensajes de autorespuesta y programas las fechas en que serán utilizados. Finalmente, los mensajes de respuesta automática se basan en los contenidos del archivo `OOF.mrk`, que se encuentra en la carpeta raíz de cada usuario en `\data\`. Este archivo soporta un gran número de macros, que se pueden utilizar que buena parte del contenido del mensaje se genere de manera dinámica, haciendo las autorespuestas bastante versátiles.

Los eventos de autorespuesta siempre se respetan cuando el mensaje detonante proviene de una fuente remota. Sin embargo, para mensajes de origen del dominio del usuario, las autorespuestas solo se detonarán si se habilita la opción *Las autorespuestas se detonan por correo intra-dominio*, localizada en la pantalla Autorespuestas » Ajustes 842.

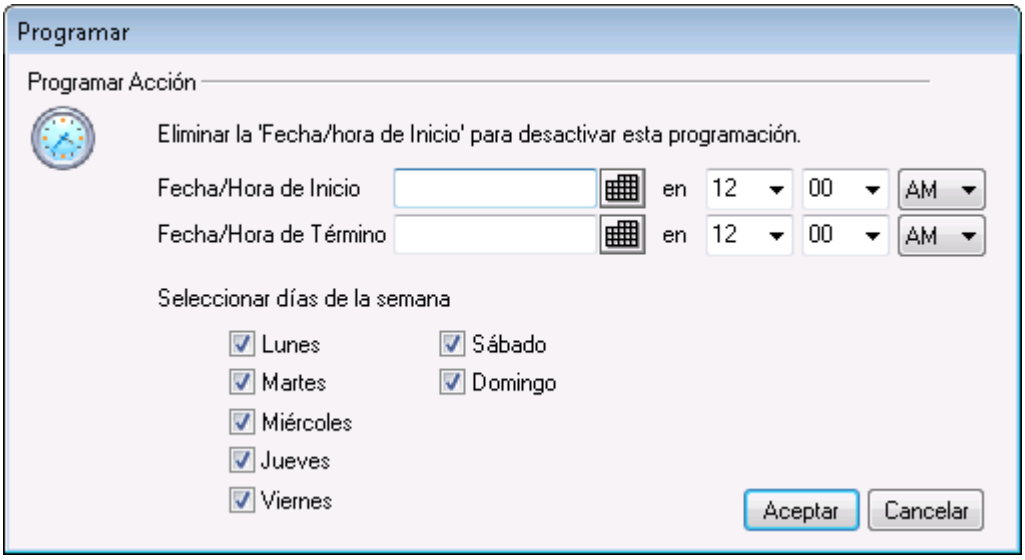
> También puede utilizar una opción en esa pantalla para limitar los mensajes de autorespuesta a una respuesta por remitente al día.

Autorespuesta

Habilitar autorespuesta
Habilite este control para activar una autorespuesta para todos los grupos controlados por esta plantilla. Para más información sobre autorespuestas vea: Autorespuestas 838.

Editar archivo de autorespuesta
Dé clic en este botón para editar el archivo de autorespuesta que se utilizará para aquellos asociados con esta plantilla.

Programación
Dé clic en este botón para abrir el diálogo de Programación en el que puede configurar una fecha y hora de inicio y terminación de la activación de la Autorespuesta. Deje el Programador en blanco si desea que la Autorespuesta se encuentre activa continuamente.



Publicar
Dé clic en este botón si desea copiar el archivo de autorespuesta de esta plantilla y los ajustes a una o más cuentas. Seleccione las cuentas a las que desea copiar la autorespuesta y dé clic en **OK**.

No enviar mensajes de autorespuesta si el mensaje proviene de una de estas direcciones
Aquí puede enlistar direcciones que desee sean excluidas de las respuestas iniciadas por esta autorespuesta.

> Ocasionalmente los mensajes de autorespuesta pueden enviarse a una dirección que devuelve también una autorespuesta. Esto puede generar un efecto "ping-pong"

haciendo que los mensajes se generen continuamente de idas y vuelta entre dos servidores. Si encuentra una de esas direcciones regístrela aquí para impedir que suceda eso. También hay una opción localizada en la pantalla Autorespuestas » Ajustes 842, que puede utilizarse para limitar el envío de mensajes de autorespuesta a uno por remitente al día.

Eliminar
Dé clic en este botón para eliminar cualesquiera registros seleccionados de la lista de direcciones excluidas.

Nuevas direcciones excluidas - se permiten comodines
Si desea agregar una dirección a la lista de direcciones excluidas regístrela aquí y dé clic en el botón *Agregar*.

Ejecutar un programa

Ejecutar este programa
Use este campo para especificar la ruta y nombre de archivo del programa que desee ejecutar cuando llegue un correo nuevo dirigido a un miembro del grupo controlado por esta plantilla. Se debe tener cuidado en asegurarse que este programa termina correctamente y puede correr sin ser atendido. Se pueden agregar comandos de línea opcionales, inmediatamente después de la ruta del ejecutable.

Pasar el mensaje a procesar
Seleccione esta opción y el proceso especificado en el campo *Ejecutar este Programa* será pasado al nombre del mensaje detonante como el primer parámetro de la línea de comandos. Cuando la autorespuesta está configurada para una cuenta que está reenviando correo a otra ubicación y no retiene una copia local en su propio buzón (ver Reenvío 729), esta función estará deshabilitada.

Por omisión, MDaemon colocará el nombre de archivo del mensaje como el último parámetro en la línea de comando. Puede omitir esta conducta utilizando la macro `$MESSAGE$`. Utilice esta macro en el lugar donde se debe colocar el nombre de archivo. Esto permite más flexibilidad en el uso de esta funcionalidad ya que es posible utilizar una línea de comandos compleja como:
`logmail /e /j /message=$MESSAGE$ /q`.

Listas de Distribución

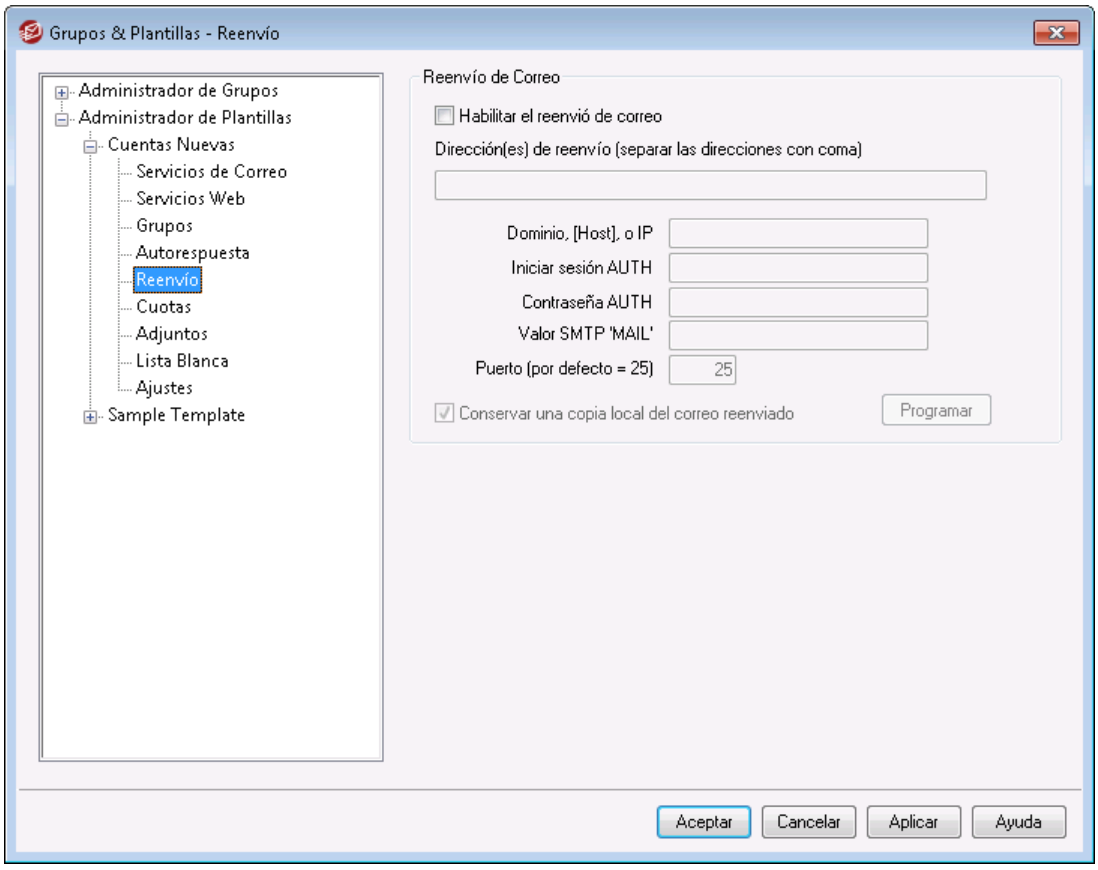
Agregar un remitente a esta lista de correo
Si se registra una lista de correo en este campo, el remitente del mensaje entrante será agregado automáticamente como miembro de esa lista. Esta es una opción muy útil para construir listas automáticamente.

Eliminar remitente de esta lista de correo
Si se registra una lista de correo en este campo, el remitente del mensaje entrante será eliminado automáticamente de la lista de correo especificada.

Ver:

Propiedades de Plantillas 793
Propiedades de Grupos 783
Plantillas de Cuentas Nuevas 792
Editor de Cuentas » Autorespuestas 726

5.2.2.1.5 Reenvío



Las opciones en esta pantalla de plantilla corresponden a las opciones localizadas en la pantalla Reenvío 729 del Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla 793, controlará las opciones de reenvió de cualquier cuenta que pertenezca al Grupo 783 que utilice la plantilla.

Reenvío de Correo

Habilitar el reenvío de correo
Marque esta casilla si desea reenviar los mensajes entrantes a las cuentas asociadas, a las direcciones especificadas en la opción *Direcciones de reenvío* registradas abajo. Los usuarios de MDaemon con acceso web 720 a Webmail 321 o a Administración Remota 354 pueden usar las opciones provistas para configurar las opciones de reenvío por sí mismos en lugar de requerir que lo haga el administrador.

Direcciones de reenvío (separe cada dirección con una coma)
Use este campo para definir las direcciones de correo a las que desea reenviar copias de los mensajes entrantes de las cuentas asociadas. Se generará en automático una copia de cada mensaje nuevo que llegue al servidor y será enviada a las direcciones especificadas en este campo, siempre y cuando se haya habilitado la opción *Habilitar reenvío de correo*. Cuando se reenvía correo a múltiples direcciones, deben separarse con una coma.

Dominios, [Host] o IP
Si desea enrutar los mensajes reenviados a través de otro servidor, tal como un servidor particular MX, especifique el dominio o IP aquí. Si desea enrutar los mensajes a un host específico, coloque el valor entre corchetes (ej. `[host1.example.com]`).

Inicio de Sesión/Contraseña AUTH
Registre aquí las credenciales de inicio de sesión para el servidor al que está reenviando el correo asociado al usuario.

Valor SMTP 'MAIL'
Si se especifica una dirección aquí, se utilizará en la sentencia "`MAIL From`" enviada durante la sesión SMTP hacia el host destino, en lugar de utilizar al remitente del mensaje. Si requiere una sentencia SMTP "`MAIL From`" vacía (ej. "`MAIL FROM <>`") entonces registro "[trash]" en esta opción.

Puerto (omisión = 25)
MDaemon enviará los mensajes reenviados utilizando el puerto TCP especificado aquí. El puerto SMTP por omisión es el 25.

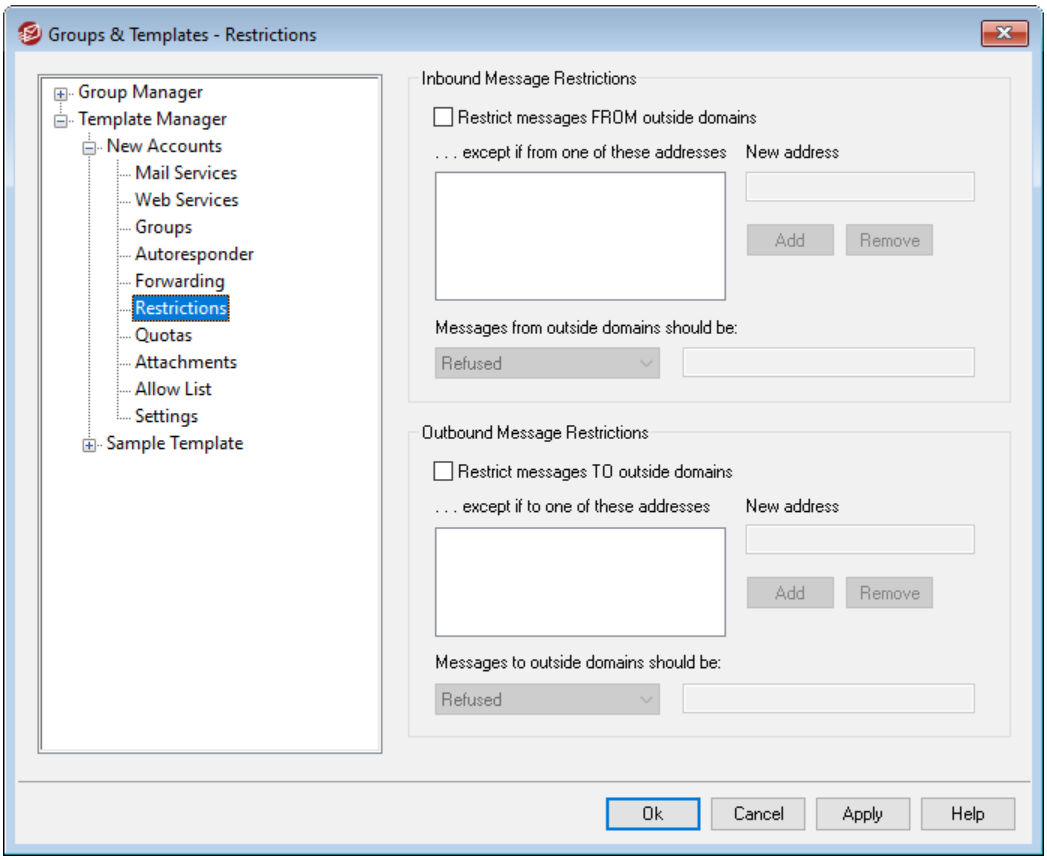
Retener una copia local del correo reenviado
Por omisión, se entrega normalmente una copia de cada mensaje reenviado, en el buzón del usuario local. Si deshabilita esta casilla no se retendrá una copia local.

Programar
Dé clic en este botón para crear una programación el reenvío del correo asociado a algunas cuentas. Puede configurar la fecha y hora de inicio, fecha y hora de término y especificar los días de la semana en que se reenviará correo.

Ver:

Propiedades de Plantillas 793
Propiedades de Grupos 783
Plantillas de Cuentas Nuevas 792
Editor de Cuentas » Autorespuestas 726

5.2.2.1.6 Restricciones



Las opciones en esta pantalla de plantillas corresponden a las opciones que se ubican en la pantalla Restricciones 731 en el Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla 793, controlará las opciones de Restricciones para cualquiera de las cuentas que pertenezcan a un Grupo 783 que utilice la plantilla.

Restricciones de Mensajes Entrantes

Restringir mensajes DE dominios externos
Haga clic en esta casilla si quiere impedir que esta cuenta reciba mensajes de

dominios no-locales.

...excepto si son enviados desde una de estas direcciones
Las direcciones especificadas en esta área son excepciones a las Restricciones de Mensajes Entrantes. Se permiten comodines. Así, si designa "*@altn.com" como excepción, todos los mensajes entrantes de cualquier dirección en altn.com serán aceptados y enviados a la cuenta.

Nuevas direcciones
Si desea añadir una dirección de excepción a la lista de Restricciones de Mensajes Entrantes regístrela aquí y luego haga clic en el botón *Agregar*.

Agregar
Después de introducir una dirección en la opción *Nuevas direcciones*, haga clic en este botón para agregarla a la lista de excepciones.

Quitar
Si desea quitar una dirección de la lista de restricciones, seleccione la dirección y luego haga clic en este botón.

Los mensajes de dominios externos deben...
Estas opciones en la lista desplegable gobiernan lo que hará MDaemon con los mensajes destinados a esta cuenta, pero originados de no locales. Puede escoger cualquiera de las siguientes opciones:

Rechazado – Los mensajes restringidos serán rechazados por MDaemon.

Devuelto al remitente – Los mensajes de dominios restringidos se devolverán al remitente.

Enviado al administrador de correo – Los mensajes restringidos serán aceptados pero enviados al postmaster en lugar de a esta cuenta.

Enviado a... - Los mensajes restringidos serán aceptados pero entregados a la dirección que especifique en la casilla de texto a la derecha.

Restricciones de Mensajes Salientes

Restringir mensajes A dominios externos
Haga clic en esta casilla si desea prevenir que la cuenta envíe mensajes a dominios no-locales.

...excepto si son enviados a una de estas direcciones
Las direcciones especificadas en esta área son excepciones a las Restricciones de Mensajes Salientes. Se permiten comodines. Así, si designa "*@altn.com" como excepción, todos los mensajes salientes dirigidos a cualquier dirección en altn.com serán entregados normalmente por MDaemon.

Nuevas direcciones
Si desea añadir una dirección de excepción a la lista de Restricciones de Mensajes Salientes tecléela aquí y luego haga clic en el botón agregar.

Agregar
Después de introducir una dirección en la opción *Nuevas direcciones*, haga clic en este botón para agregarla a la lista de excepciones.

Quitar
Si desea quitar una dirección de la lista de restricciones, seleccione la dirección y luego haga clic en este botón.

Los mensajes hacia dominios externos deben ser...
Estas opciones en la lista desplegable controlan lo que hará MDaemon con los mensajes originados por esta cuenta, pero destinados a un dominio no-local. Puede escoger cualquiera de las siguientes opciones:

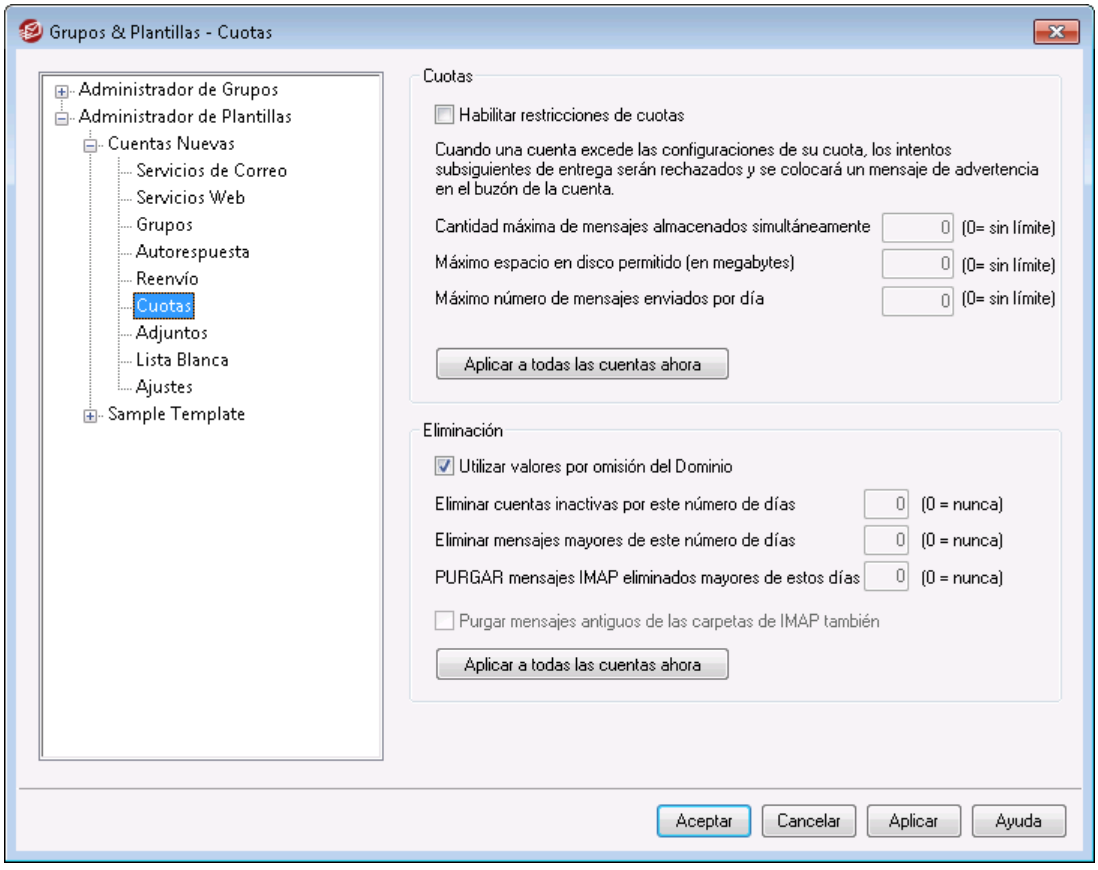
Rechazado – Los mensajes restringidos serán rechazados por MDaemon.

Devuelto al remitente – Los mensajes hacia dominios restringidos se devolverán al remitente.

Enviado al postmaster – Los mensajes restringidos serán aceptados pero enviados al postmaster en lugar de al destinatario.

Enviado a... - Los mensajes restringidos serán aceptados pero entregados a la dirección que especifique en la casilla de texto a la derecha.

5.2.2.1.7 Cuotas



Las opciones en esta pantalla de plantilla corresponden a las opciones localizadas en la pantalla Cuotas[733] del Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla[793], controlará las opciones de Cuotas para cualquier cuenta que pertenezca a un Grupo[783] que utilice la plantilla.

Cuotas

Habilitar restricciones de cuota
Marque esta casilla si desea especificar el número máximo de mensajes que pueden almacenar las cuentas controladas por esta plantilla, configurar el espacio máximo en disco que las cuentas pueden utilizar (incluyendo los archivos adjuntos en la carpeta Documentos de cada cuenta), o definir el número máximo de mensajes que pueden enviar las cuentas diariamente vía SMTP. Si se intenta una entrega de correo que exceda el máximo de mensajes o las limitaciones de espacio en disco, el mensaje será rechazado y se colocará un mensaje de aviso en el buzón del usuario. Si la recolección MultiPOP[739] excede los máximos de la cuenta, se emitirá una advertencia similar y los registros MultiPOP de la cuenta se deshabilitan en automático (pero no se eliminan de la base de datos).

Utilice la opción *Enviar correo al usuario con el porcentaje alcanzado de su cuota* en "Cuentas » Ajustes » Cuotas[812]" para hacer que se envíe un mensaje de advertencia cuando una cuenta se acerca a sus límites de cuota. Cuando la cuenta excede un porcentaje determinado, ya sea del *Número máximo de mensajes almacenados* o del *Máximo espacio en disco permitido*, se enviará un mensaje de advertencia a la cuenta, a medianoche. El mensaje enlistará el número de mensajes almacenados por la cuenta, el tamaño de su buzón y el porcentaje utilizado y remanente. Además, si se encuentra un mensaje previo de advertencia en el buzón, será reemplazado con el mensaje actualizado.

Cantidad máxima de mensajes almacenados simultáneamente
Utilice esta opción para definir el número máximo de mensajes que pueden almacenar las cuentas. Si utiliza "0" significa que no habrá límite al número de mensajes permitidos.

Máximo espacio en disco permitido (en megabytes)
Utilice esta opción para definir la cantidad máxima de espacio en disco que pueden utilizar las cuentas, incluyendo los archivos adjuntos que puedan estar almacenados en la carpeta de Documentos de cada cuenta. Si utiliza "0" significa que no habrá límite a la cantidad de espacio en disco que pueden utilizar las cuentas.

Máximo número de mensajes enviados por día
Utilice esta opción para definir el número máximo de mensajes que puede enviar diariamente cada cuenta vía SMTP. Si la cuenta alcanza este límite entonces los mensajes nuevos de la cuenta serán rechazados hasta que el contador se restablezca a media noche. Utilice "0" en la opción si no desea limitar el número de mensajes que puede enviar la cuenta.

Aplicar a todas las cuentas ahora

Dé clic en este botón para aplicar la configuración de esta pantalla a todas las cuentas existentes en MDaemon cuya configuración de Cuotas no esté controlada específicamente por una plantilla de cuentas. Esto restablecerá las cuentas a los valores por omisión de Cuotas. Esta opción solo está disponible en la Plantilla de Cuentas Nuevas 792.

Depuración

Las opciones en esta sección se utilizan para definir cuándo y si una cuenta controlada por esta plantilla será eliminada cuando esté inactiva. Puede definir también si los mensajes pertenecientes a la cuenta serán eliminados o no luego de cierta cantidad de tiempo. Todos los días a medianoche, MDaemon eliminará todos los mensajes que hayan excedido el límite de tiempo establecido o eliminará la cuenta por completo si ha alcanzado el tiempo límite de inactividad.

Utilizar los valores por omisión del dominio

Los valores por omisión para depuración se determinan por dominio y se localizan en la pantalla Opciones 219 del Administrador de Dominio. Si no desea tomar los valores por omisión del dominio para las cuentas controladas por plantillas, deshabilite la casilla y defina los valore deseados en las opciones siguientes.

Eliminar automáticamente la cuenta si permaneció inactiva por [XX] días (0 = nunca)
Especificar el número de días que desea permitir que la cuenta permanezca inactiva antes de ser eliminada. Un valor de "0" en este control significa que la cuenta nunca será eliminada por inactividad.

Eliminar mensajes mayores de [XX] días (0 = nunca)
Este es el número de días que cualquier mensaje dado puede residir en el buzón de la cuenta antes de ser eliminado automáticamente por MDaemon. Un valor de "0" significa que los mensajes nunca serán eliminados debido a su antigüedad. **Nota:** El ajuste de esta opción no aplica a mensajes contenidos en carpetas IMAP a menos que habilite también la opción siguiente "*Depurar también mensajes antiguos de las carpetas IMAP*"

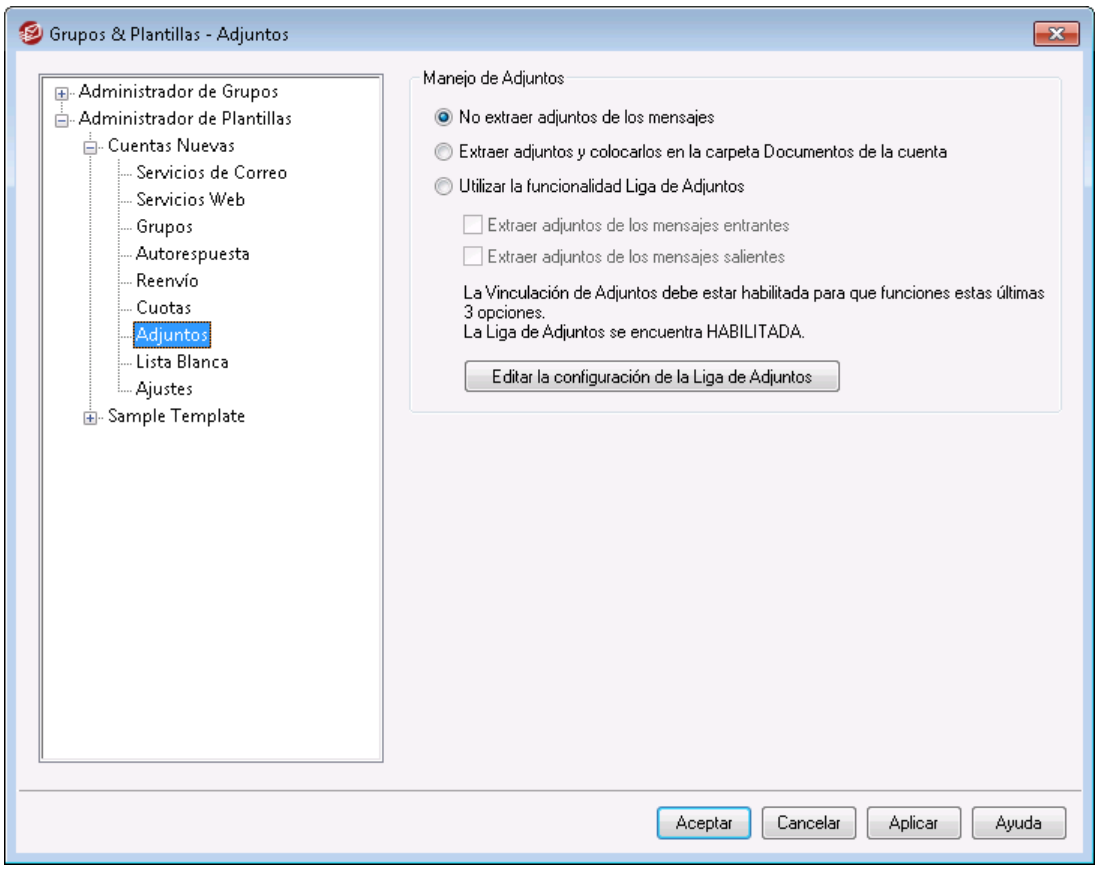
Depurar mensajes IMAP eliminados mayores de [XX] días (0 = nunca)
Utilice este control para especificar el número de días que desea permitir que mensajes IMAP marcados para ser eliminados permanezcan en las carpetas de los usuarios. Los mensajes marcados para eliminación por más de este número de días serán depurados. Un valor de "0" significa que los mensajes marcados para eliminación nunca serán depurados debido a su edad.

Depurar también mensajes antiguos de las carpetas IMAP
Dé clic en esta casilla si desea que la opción "*Eliminar mensajes mayores de ...*" se aplique también a los mensajes en carpetas IMAP. Cuando se deshabilita este control, los mensajes contenidos en carpetas IMAP no serán eliminados debido a su antigüedad.

Ver:

Propiedades de Plantillas 793
Propiedades de Grupos 783
Plantilla de Cuentas Nuevas 792
Editor de Cuentas » Cuotas 733
Opciones de Cuentas » Cuotas 860

5.2.2.1.8 Adjuntos



Las opciones en esta pantalla de plantilla corresponden a las opciones localizadas en la pantalla Adjuntos 735 en el Editor de Cuentas. Cuando se configura una plantilla para controlar esta pantalla 793, controlará las opciones de Adjuntos para cualquier cuenta que pertenezca a un Grupo 783 que utilice la plantilla.

Manejo de Adjuntos

No extraer adjuntos de los mensajes
Si se selecciona esta opción, los adjuntos no serán extraídos de los mensajes de las cuentas controladas por la plantilla. Los mensajes con adjuntos serán manejados normalmente, dejando los adjuntos intactos.

Extraer adjuntos y colocarlos en la carpeta Documentos de la cuenta
Si se selecciona, esta opción hace que MDaemon automáticamente extraiga cualquier archivo adjunto tipo Base64 MIME incluido en los mensajes entrantes para la cuenta. Los archivos extraídos se eliminan del mensaje entrante, se decodifican y se colocan en la carpeta Documentos de la cuenta. Luego se coloca una nota en el cuerpo del mensaje, conteniendo los nombres de los archivos que fueron extraídos. Esta opción no proporciona una liga a los adjuntos almacenados, pero los usuarios pueden utilizar Webmail 321 para accesar su carpeta Documentos.

Utilizar la funcionalidad Liga de Adjuntos
Seleccione esta opción si desea utilizar la funcionalidad de Liga de Adjuntos para los archivos adjuntos de los mensajes entrantes o salientes.

Si se selecciona esta opción, pero la funcionalidad está deshabilitada en la pantalla Liga de Adjuntos 366, entonces no serán los archivos adjuntos no serán extraídos.

Extraer adjuntos de los mensajes Entrantes

Cuando se habilita esta opción, los adjuntos son extraídos de los mensajes entrantes a la cuenta y se almacenan en la ubicación determinada en la pantalla Liga de Adjuntos 366. Luego se colocan ligas URL en el cuerpo del mensaje y el usuario puede dar clic en ellas para descargar los archivos. Por seguridad, estas ligas no contienen rutas directas, en lugar de esto contienen identificadores únicos (GUID) que el servidor utiliza para mapear el archivo a la ruta real. Este mapeo GUID se almacena en el archivo `AttachmentLinking.dat`.

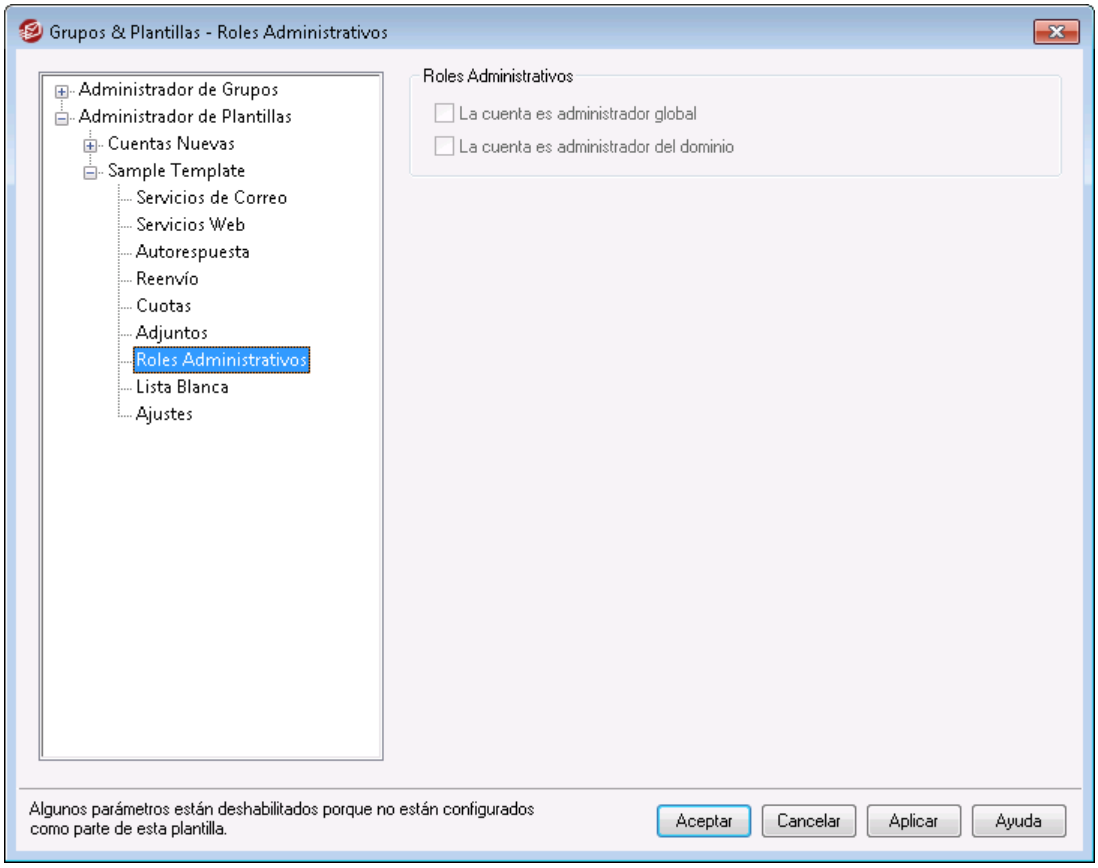
Extraer adjuntos de los mensajes salientes
Por omisión, la Liga de Adjuntos solo extraerá archivos de los mensajes entrantes. Marque esta casilla si desea también que se extraigan los adjuntos de los mensajes salientes de las cuentas. Cuando la cuenta envíe correo, la Liga de Adjuntos extraerá el archivo, lo almacenará y reemplazará con una URL para descargar el archivo.

Editar la configuración de Liga de Adjuntos
Dar clic en este botón para abrir el diálogo de la Liga de Adjuntos 366.

Ver:

Propiedades de Plantillas 793
Propiedades de Grupos 783
Plantilla de Cuentas Nuevas 792
Vinculación de Adjuntos 718
Editor de Cuentas » Adjuntos 735

5.2.2.1.9 Roles Administrativos



Roles Administrativos

La cuenta es Administrador Global
Habilite esa casilla si va a otorgar a este usuario acceso administrativo a nivel servidor. Los Administradores Globales pueden:

- Acceso completo a la configuración del servidor, todos los usuarios y todos los dominios vía Administración Remota.
- Acceso a todos los usuarios de MDaemon de todos los Dominios de MDaemon como contactos en la Mensajería Instantánea.
- La capacidad de postear a todas las listas de distribución, aun las que están marcadas como "Solo Lectura".
- La capacidad de postear a todas las listas de distribución aun cuando no sea miembro.

El usuario tendrá acceso completo a los archivos y opciones de MDaemon. Para información detallada sobre las opciones administrativas en la Administración Remota, vea Administración Remota 354.

La cuenta es Administrador del Dominio
Dé clic en esta casilla para asignar a los usuarios como Administradores de Dominio. Los Administradores de Dominio son similares a los administradores

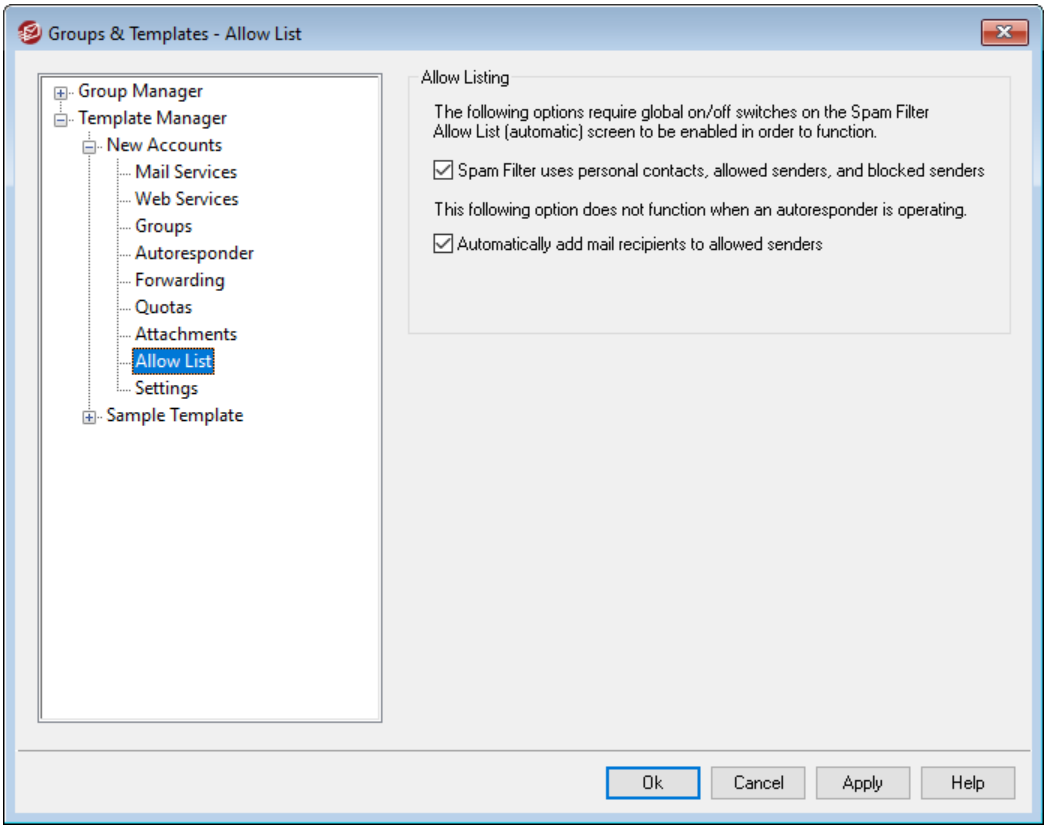
globales excepto que su acceso administrativo se limita a este dominio y a los permisos otorgados en la página Servicios Web[720].

Esta pantalla no está disponible en la Plantilla de Cuentas Nuevas[792]. El acceso administrativo no puede otorgarse automáticamente a cuentas nuevas. Para otorgar acceso administrativo a una cuenta, asocie la cuenta a una plantilla personalizada que use esta pantalla para otorgar ese acceso, o asigne manualmente la cuenta como administrador desde la pantalla Roles Administrativos[757] del Editor de Cuentas.

Ver:

Propiedades de Plantillas[793]
Propiedades de Grupo[783]
Plantilla de Cuentas Nuevas[792]
Editor de Cuentas » Roles Administrativos[757]

5.2.2.1.10 Lista de Permitidos



Las opciones en esta pantalla de plantillas corresponden a los ajustes localizados en la pantalla Lista de Permitidos[758] del Editor Cuentas. Cuando una plantilla está configurada para su control en esta pantalla[793], controlará los ajustes de Lista Blanca de cualquier cuenta que pertenezca al Grupo[783] que utiliza la plantilla.

Lista de Permitidos

El Filtro de Spam utiliza los archivos de contactos personales, lista de permitidos y lista de bloqueados
La pantalla Lista de Permitidos (automática) 688 contiene una opción global que se puede utilizar para hacer que el Filtro de Spam considere en lista blanca automáticamente a un mensaje cuando el remitente del mismo se encuentre en los contactos personales del destinatario local o en su carpeta de lista blanca. También considerará automáticamente en lista negra cualquier mensaje cuando el remitente se encuentre en la carpeta de lista negra del destinatario. Si ha habilitado la opción global del Filtro de Spam pero no quiere aplicarla a estas cuentas, deshabilite la casilla de verificación, para omitir la configuración global. Si la opción global se encuentra deshabilitada, entonces esta opción no estará disponible.

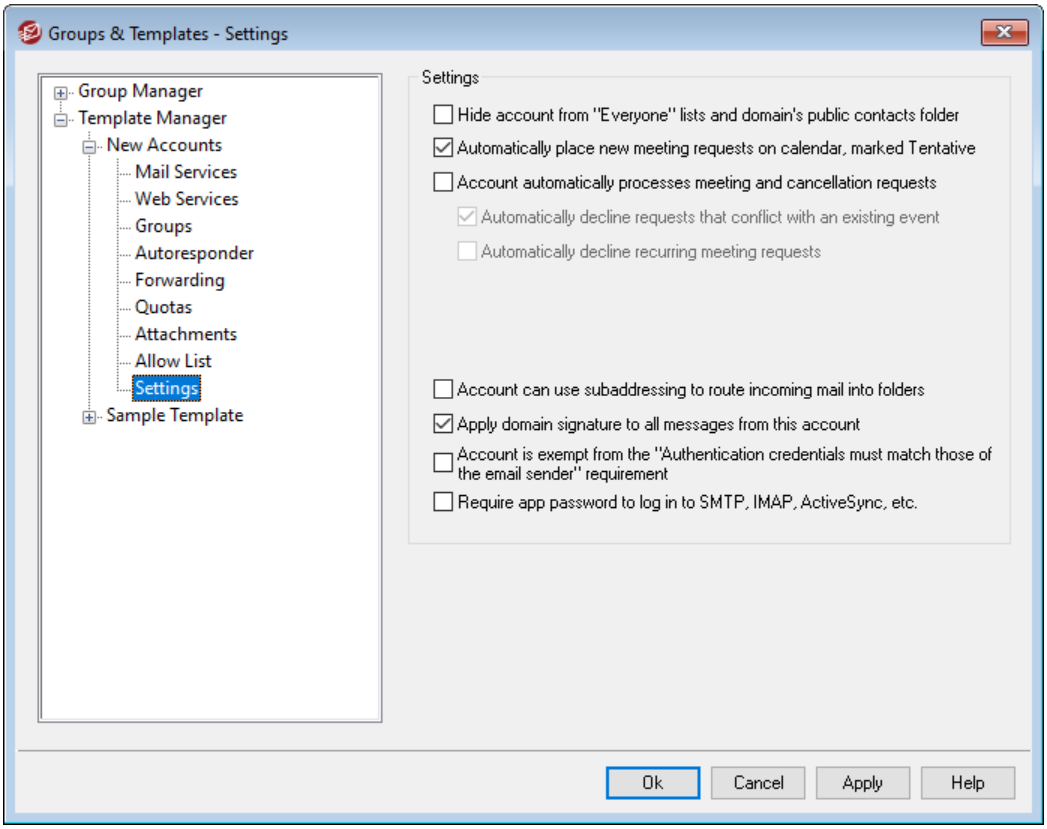
Agregar en automático destinatarios de correo a la lista de permitidos
Dé clic en esta opción si desea actualizarla carpeta de lista blanca de cada cuenta cada vez que envíe un mensaje saliente a direcciones de correo no-locales. Al utilizar esta opción junto con la opción anterior, *el Filtro de Spam utiliza los archivos de contactos personales, lista blanca y lista negra*, el número de falsos positivos del Filtro de Spam se puede reducir drásticamente. La opción *Actualizar automáticamente los contactos en lista blanca*, localizada en la pantalla Lista de Permitidos (automática) 688 debe estar habilitada antes de que pueda utilizar esta funcionalidad.

Esta opción se deshabilita cuando la cuenta está utilizando una autorespuesta.

Ver:

Propiedades de Plantilla 793
Propiedades de Grupos 783
Plantilla de Cuentas Nuevas 792
Editor de Cuentas » Lista de Permitidos 758

5.2.2.1.11 Ajustes



Los ajustes en esta pantalla de plantilla corresponden a los parámetros localizados en la pantalla Ajustes 760 del Editor de Cuentas. Cuando una plantilla se configura para controlar esta pantalla 793, controlará los parámetros de la pantalla Ajustes para cualquier cuenta que pertenezca a un Grupo 783 que utiliza esa plantilla.

Ajustes

La cuenta está oculta de listas "Everyone", calendarios compartidos y VRFY
MDaemon crea y mantiene en automático una lista de correo "everyone@" para cada dominio, que se puede utilizar para enviar un mensaje a todos los usuarios a la vez. Por omisión, MDaemon incluirá todas las cuentas cuando construye esta lista. Marque la casilla si desea excluir las cuentas controladas por esta plantilla, de esa lista. Esto también ocultará las cuentas de las carpetas compartidas y de los resultados del comando VRFY 100.

Colocar en automático peticiones de reuniones nuevas en el calendario, marcadas como Tentativas
Por omisión cuando una cuenta recibe una nueva petición de reunión, esta se coloca en el calendario del usuario y se marca como *Tentativa*. Deshabilite esta casilla si no desea que sea el ajuste por omisión para cuentas nuevas.

La cuenta procesa en automático peticiones de reuniones y cancelaciones
Dé clic en esta casilla si desea que se procesen en automático las peticiones de reuniones, cambios y cancelaciones, para cada cuenta, Cuando una cuenta recibe un mensaje que contiene una petición de reunión, el calendario de la cuenta se actualizará en automático. Esta opción está deshabilitada por omisión para todas las cuentas.

Declinar en automático peticiones que entran en conflicto con eventos existentes
Si está habilitado el procesamiento automático de reuniones y cancelaciones, las peticiones de junta serán declinadas en automático por omisión, cuando entren en conflicto con un evento existente. Deshabilite la casilla si desea permitir que se genere en el calendario el evento en conflicto.

Declinar en automático peticiones de reuniones recurrentes
Dé clic en esta casilla su se habilita el procesamiento automático de reuniones y cancelaciones, pero desea declinar aquellas peticiones si son para reuniones recurrentes.

La cuenta puede utilizar subdireccionamiento para enrutar el correo entrante en carpetas
Dé clic en esta casilla si desea permitir el subdireccionamiento 762 a las cuentas.

Aplicar la firma del dominio a todos los mensajes de esta cuenta
Cuando exista una Firma del Dominio 210 para el dominio al que pertenecen las cuentas controladas por esta plantilla, esta opción hace que se agregue a todos los mensajes enviados por esas cuentas.

La cuenta está exenta del requerimiento "Las credenciales de autentificación deben coincidir con las del remitente del correo"
Utilice esta opción si desea exentar a las cuentas controladas por esta plantilla de la opción global "*Las credenciales de autentificación deben coincidir con las del remitente del mensaje*" que se localiza en la pantalla Autentificación SMTP 523 .

Se requiere contraseña de app para iniciar sesión en SMTP, IMAP, ActiveSync, etc.
Marque esta casilla si desea requerir que las cuentas que utilizan esta plantilla debe utilizar Contraseñas de Apps 751 en clientes de correo, para iniciar sesión SMTP, IMAP, ActiveSync u otros protocolos de servicio de correo. La contraseña 855 regular de la cuenta, sin embargo, debe seguirse utilizando para iniciar sesión en Webmail o Administración Remota.

El requerir Contraseñas de Apps puede ayudar a proteger la contraseña de la cuenta de ataque de diccionario y fuerza bruta vía SMTP, IMAP, etc. Esto es más seguro porque aún si un ataque de este tipo adivinara la contraseña actual de la cuenta, no funcionaría y el atacante no lo sabría, dado que MDaemon solo aceptaría una Contraseña de App correcta. Adicionalmente, si sus cuentas en MDaemon utilizan autentificación de Active Directory y AD bloquea una cuenta luego de un número de intentos fallidos, esta opción puede ayudar a prevenir que las cuentas sean bloqueadas, dado que MDaemon solo verificará las Contraseñas de Apps, no intentará autentificar con Active Directory.

Ver:

Propiedades de Plantilla 793
Propiedades de Grupo 783
Plantilla de Cuentas Nuevas 792
Editor de Cuentas » Ajustes 760

5.3 Ajustes de Cuentas

5.3.1 Active Directory

Utilizando las opciones de Active Directory ubicadas en Cuentas » Ajustes de Cuenta » Active Directory, MDaemon puede ser configurado para monitorear el Active Directory y crear, editar y eliminar automáticamente y deshabilitar las cuentas de MDaemon cuando sus cuentas asociadas son alteradas en Active Directory. Más aun, también se puede configurar para mantener actualizados los registros de los contactos públicos con la información más reciente almacenada en el Active Directory. Los campos comunes como la dirección postal de una cuenta, los números de teléfono, la información de la empresa y más, pueden ser cargados en los registros públicos de contactos y actualizados cada vez que se modifiquen en el Active Directory.

Crear Cuentas

Cuando se establece el monitoreo del Active Directory, MDaemon consultará los cambios a un intervalo designado y luego creará una nueva cuenta de usuario de MDaemon siempre que encuentre que se ha agregado una nueva cuenta de Active Directory. Esta nueva cuenta de usuario de MDaemon se creará usando el nombre completo, acceso, buzón, descripción, y estado habilitado/deshabilitado encontrado en Active Directory.

Por defecto, las nuevas cuentas de MDaemon creadas como resultado del monitoreo del Active Directory se añadirán al Dominio por Defecto de MDaemon. Alternativamente, puede escoger tener dichas cuentas añadidas al dominio encontrado en el atributo de Active Directory "`UserPrincipalName`". Cuando se usa dicha opción, si una cuenta requiere un dominio que no existe dentro de MDaemon, se creará automáticamente un Dominio 190 nuevo.

Alternativamente, puede configurar su *Filtro de Búsqueda* 825 para monitorear un grupo en Active Directory, por lo que al agregar un usuario a un grupo o un grupo a un usuario se creará el usuario en MDaemon y eliminar un usuario de un grupo hará que la cuenta sea deshabilitada (no eliminada) de MDaemon.

Eliminar Cuentas

MDaemon puede ser configurado para tomar una de las siguientes acciones cuando una cuenta es eliminada del Active Directory: no hacer nada, eliminar la cuenta de MDaemon asociada, deshabilitar la cuenta de MDaemon asociada, o congelar la cuenta de MDaemon asociada (la cuenta podrá seguir recibiendo correo, pero el usuario no podrá recolectarlo o acceder a él).

Actualizar Cuentas

Cuando MDaemon detecta cambios en las cuentas de Active Directory, actualizará automáticamente las propiedades asociadas en la cuenta de MDaemon coincidente.

Sincronizando MDaemon con el Active Directory

Existe una opción "*Escanear ahora AD por completo*" está disponible para hacer que MDaemon consulte la base de datos del Active Directory y luego cree o modifique las cuentas de usuario de MDaemon según sea necesario. Cuando se encuentra una cuenta de Active Directory que coincide con una cuenta ya existente de MDaemon,

la cuenta de MDaemon se enlazará a esta. Luego, cualquier cambio futuro que se haga a las cuentas de Active Directory se propagará a las cuentas de MDaemon automáticamente.

Autentificación con Active Directory

Las cuentas creadas por la funcionalidad de Active Directory de MDaemon se establecerán con Autentificación de Active Directory (AD) por defecto. Con la Autentificación AD, MDaemon no tienen necesidad de almacenar la contraseña de la cuenta dentro de su propia base de datos de usuarios. En su lugar, el propietario de la cuenta usará sus credenciales de login/contraseña de Windows y MDaemon pasará dichas credenciales a Windows para la autentificación de la cuenta asociada.

Para usar la Autentificación AD, debe estar disponible un nombre de dominio de Windows en el espacio indicado en Monitoreo 828. Este es el dominio de Windows que MDaemon usará cuando intente autenticar las cuentas. En la mayoría de los casos MDaemon detectará este dominio de Windows automáticamente y lo llenará por usted. Sin embargo, puede usar un nombre de dominio alternativo en esta opción si desea, o puede usar "`NT_ANY`" si desea permitir la autenticación entre todos sus dominios de Windows en lugar de limitarla a uno específico. Si deja esta opción en blanco entonces MDaemon no usará la Autenticación Dinámica cuando se creen nuevas cuentas. En su lugar generará una contraseña aleatoria, que tendrá que editar manualmente antes de que los usuarios puedan acceder a sus cuentas de correo.

Monitoreo Persistente

El monitoreo del Active Directory continuará funcionando aun y cuando MDaemon esté apagado. Todos los cambios de Active Directory serán observados y luego MDaemon los procesará cuando se reinicie.

Seguridad de Archivos de Active Directory

No sirve de nada que las funcionalidades del Active Directory de MDaemon no alteren los archivos de esquema de Active Directory de ninguna manera — todo el monitoreo es unidireccional de Active Directory a MDaemon. MDaemon no alterará su directorio.

Plantilla de Active Directory

Siempre que MDaemon añade o realiza cambios a las cuentas debido al monitoreo y escaneo del Active Directory, usará una plantilla de Active Directory ("`/app/ActiveDS.dat`") para enlazar ciertos nombres de atributo a campos de la cuenta de MDaemon. Por ejemplo, MDaemon enlaza el atributo "`cn`" del Active Directory al campo de MDaemon "`FullName`" por defecto. Estos enlaces, sin embargo, no son definitivos. Puede editar de manera sencilla esta plantilla con el Bloc de Notas si lo desea y alterar cualquiera de los enlaces a campo por defecto. Por ejemplo, "`FullName=%givenName% %sn%`" podría usarse como reemplazo para la configuración por defecto: "FullName=%cn%". Vea `ActiveDS.dat` para más información.

Actualizar las Libretas Públicas de Contactos

El monitoreo del Active Directory se puede utilizar para mantener los registros públicos de contactos en MDaemon actualizados con la información más reciente. Campos comunes como la dirección postal de una cuenta, número de teléfono, información de contacto de negocios y más se pueden cargar a su registro público

de contacto y estos datos se actualizarán cada vez que se modifiquen en el Active Directory. Para habilitar esta funcionalidad, utilice la opción "*Monitorear el Active Directory y actualizar la libreta pública de direcciones*" localizada en: Active Directory » Monitoreo 828.

Se pueden monitorear una gran cantidad de campos de los registros de contactos utilizando esta funcionalidad. Para obtener una lista completa de cuales campos de los registros públicos de contactos se pueden mapear como atributos del Active Directory, vea el archivo `ActiveDS.dat`. Este archivo tiene varias plantillas nuevas para mapeo que le permitirán especificar uno o más atributos del Active Directory de los cuales podrá tomar un campo particular de los registros de contactos (por ejemplo, `%fullName%` para el campo de nombre completo, `%streetAddress%` para el campo de dirección postal, etc.).

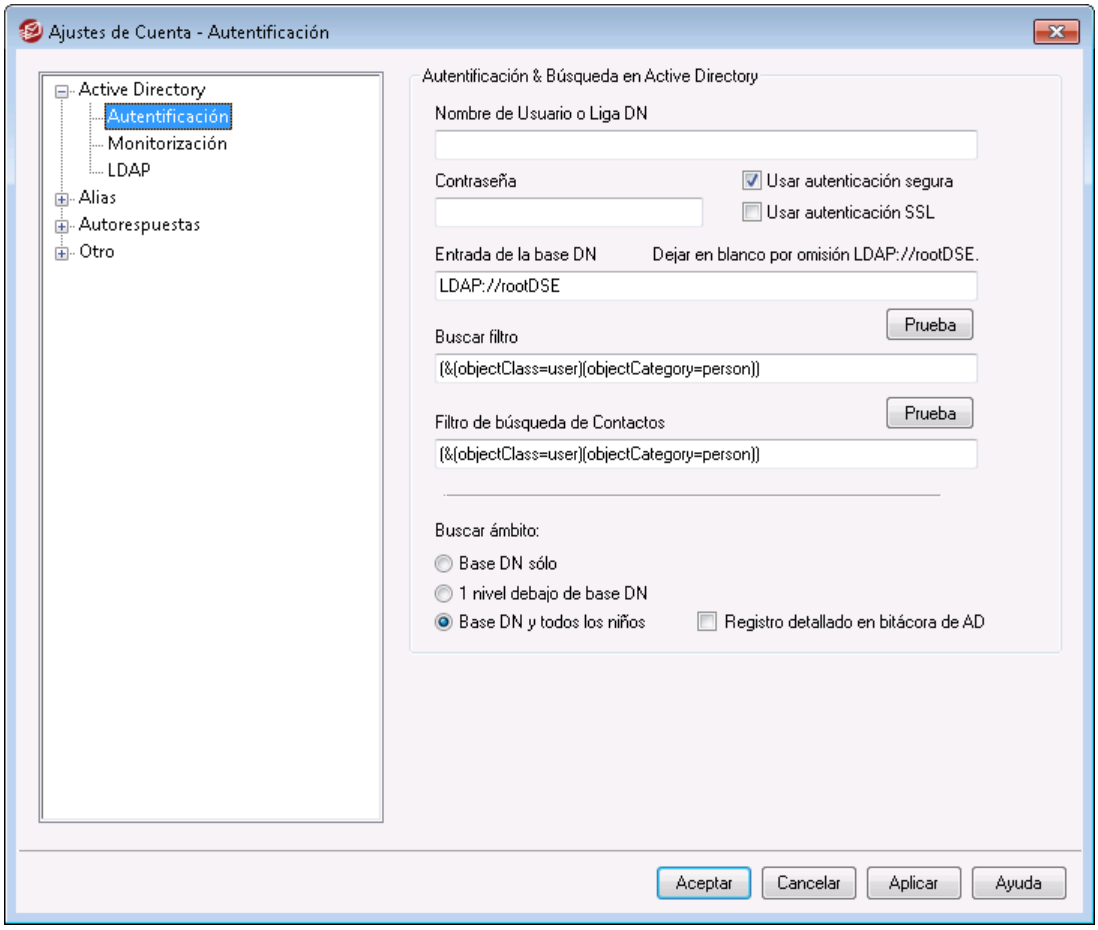
MDaemon debe ligar la dirección de correo de una cuenta a algún atributo dentro del Active Directory a fin de saber cuál registro de contacto debe actualizar. Si no puede encontrar esa coincidencia no hace nada. Por omisión MDaemon intentará construir una dirección de correo utilizando los datos tomados del atributo mapeado en la plantilla del Buzón (ver `ActiveDS.dat`) para lo que MDaemon internamente agregará el nombre del dominio por omisión 190, tal y como lo haría cuando crea y elimina cuentas basado en los datos del Active Directory. Sin embargo, puede quitar el comentario a la plantilla "abMappingEmail" dentro de `ActiveDS.dat` y ligarla a cualquier atributo del Active Directory que desee (como `%mail%`, por ejemplo). Sin embargo, por favor note que el valor de este atributo debe contener una dirección de correo que será reconocida como cuenta válida de usuario local.

Esta funcionalidad creará los registros de contactos en línea si no es que ya existen y actualizará los registros que ya existan. Más aun por favor note que sobrescribirá cualquier cambio que haga fuera del Active Directory. Los campos de registros de contactos que no sean mapeados quedarán sin alteración. Por esto cualquier dato preexistente que no sea sujeto a este proceso no será alterado o perdido. Finalmente, las cuentas de MDaemon configuradas como ocultas 760 no están sujetas a que sus registros de contactos sean creados o actualizados.

Ver:

Active Directory » Monitoreo 828
Active Directory » Autentificación 825

5.3.1.1 Autentificación



El acceso al Active Directory puede requerir que se configuren permisos especiales para que funcionen todas las opciones.

Autentificación y Consultas en Active Directory

Nombre de Usuario o Enlace DN
Este es el Inicio de sesión de Windows o DN que MDaemon utilizará al enlazarse al Active Directory utilizando LDAP. El Active Directory permite el uso de una cuenta de Windows o UPN al enlazarse.

Al utilizar un DN en esta opción en lugar de una cuenta de Windows, debe deshabilitar o dejar en blanco la opción siguiente "*Utilizar autentificación segura*".

Contraseña
Esta es la contraseña que corresponde al D N o cuenta de Windows utilizada en la opción *Enlazar DN* arriba.

Utilizar autentificación segura
Dé clic en esta casilla si desea utilizar autentificación segura al ejecutar sus búsquedas en el Active Directory. No puede usar esta opción cuando esté utilizando DN en lugar de una cuenta de Windows en la opción *Enlazar DN.*

Utilizar autentificación SSL
Dé clic en esta casilla si desea utilizar autentificación SSL al ejecutar sus búsquedas en el Active Directory.

Para usar esta opción se requiere un servidor SSL e infraestructura en su red de Windows y del Active Directory. Contacte a su departamento de sistemas si no está seguro sobre si su red está configurada de esta forma, para saber si debe habilitar esta opción.

Atributo de Dirección de Correo
Este atributo se utiliza para las listas de distribución de MDaemon y solo está disponible al accesar las opciones de Active Directory localizadas en el diálogo de las Listas de Distribución 305.

Búsqueda en el Active Directory

Registro DN Base
Este es el Nombre distinguido (Distinguished Name - DN) o punto de inicio en el Árbol de Información (Directory Information Tree - DIT) en el que MDaemon buscará en el Active Directory las cuentas y sus modificaciones. Por omisión, MDaemon iniciará la búsqueda en Root DSE, que es el registro más alto en la jerarquía del Active Directory. Si se define un punto de inicio más preciso y cercano a la ubicación de sus cuentas de usuario en su árbol particular del Active Directory, puede reducir la cantidad de tiempo requerido para buscar en el DIT las cuentas y sus modificaciones. Si deja el campo en blanco se regresará al valor por omisión `LDAP://rootDSE`

Filtro de Búsqueda
Este es el filtro de búsqueda LDAP que se utilizará al monitorear o consultar en su Active Directory las cuentas y sus modificaciones. Utilice este filtro para localizar con mayor precisión las cuentas de usuario que desea incluir en el monitoreo del Active Directory.

También puede configurar su filtro de búsqueda o monitor a un grupo en Active Directory, de manera que agregar un usuario al grupo o un grupo a un usuario hará que el usuario sea creado en MDaemon y eliminar un usuario de un grupo hará que la cuenta sea deshabilitada (no eliminada) en MDaemon. Por ejemplo, un filtro de búsqueda correcto para un grupo denominado 'MyGroup' se vería así:

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

Reemplace los bits 'ou=' y 'dc=' con algo adecuado para su red.

Filtro de búsqueda de Contactos
Utilice esta opción para especificar un filtro de búsqueda separado para consultar contactos. Si utiliza el mismo texto en este campo como en la opción *Filtro de*

Búsqueda descrito arriba, solo se utilizará una consulta para actualizar todos los datos. Cuando los filtros de búsqueda son diferentes, son necesarias dos consultas.

Probar
Utilice los botones *Probar* para probar los ajustes de sus filtros de búsqueda.

Ámbito de búsqueda:

Este es el ámbito o alcance de sus búsquedas en el Active Directory

Solo DN Base DN
Seleccione esta opción si desea limitar su búsqueda al DN base especificado arriba. La búsqueda no procederá bajo ese punto en su árbol (DIT).

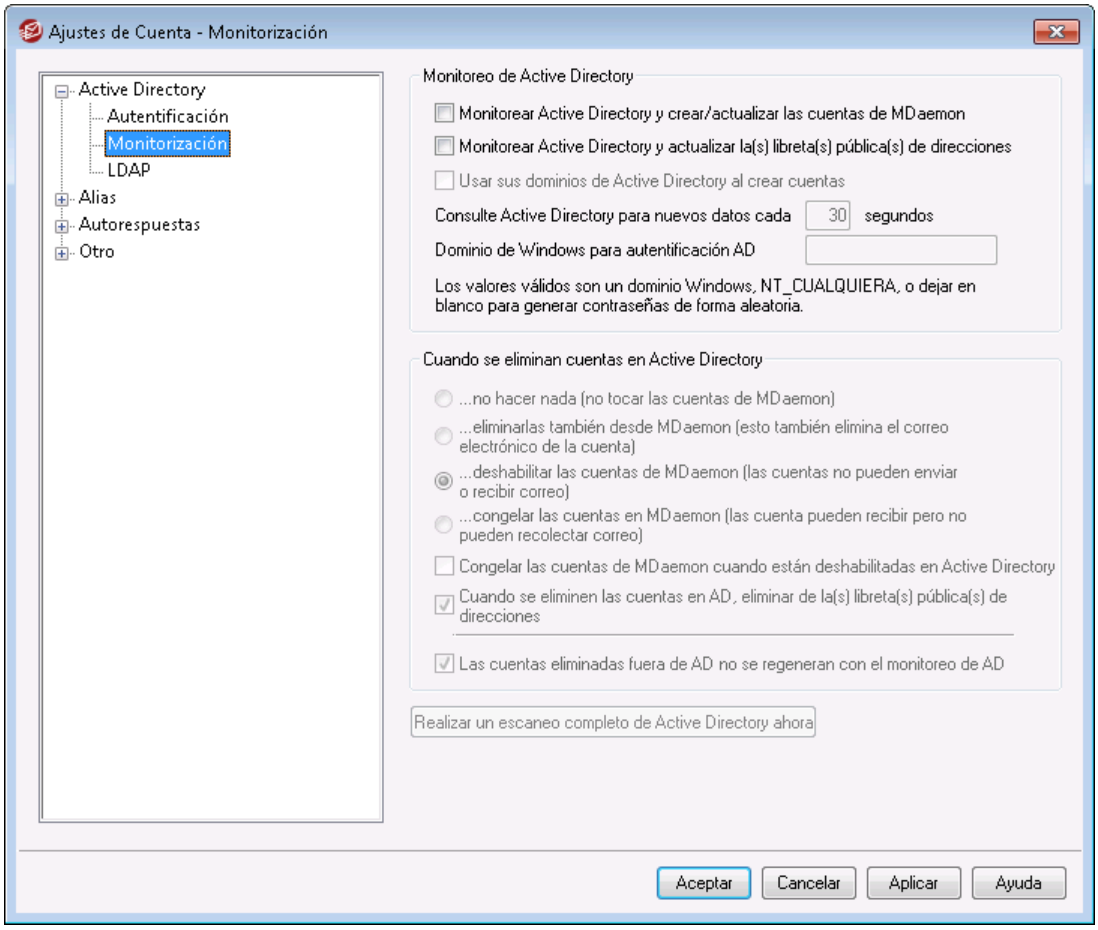
1 nivel bajo el DN base
Use esta opción si desea extender su búsqueda en el Active Directory solo un nivel bajo el DN establecido en su DIT.

DN Base DN y todos sus hijos
Esta opción ampliará el alcance de su búsqueda desde el DN proporcionado a todos sus hijos, hasta el nivel hijo más bajo registrado en el DIT. Esta es la opción seleccionada por omisión, que combinada con la configuración por omisión del DSE raíz establecido arriba, significa que el DIT completo, bajo el DSE raíz, será consultado.

Tamaño de página
Si los resultados de una consulta al Active Directory exceden un número específico de registros, entonces serán devueltos en "páginas" separadas a fin de obtener todos los registros resultantes. Esta configuración es el número máximo de registros que se incluirán por página.

Registro detallado en el Log de AD
Por omisión MDaemon utilizará el registro detallado para Active Directory. Deshabilite esta casilla si desea utilizar un registro menos extenso.

5.3.1.2 Monitoreo



Monitoreo de Active Directory

Monitorear Active Directory y crear/actualizar cuentas en MDaemon
Dé clic en esta opción para activar el monitoreo de Active Directory, lo que creará y actualizará las cuentas en MDaemon conforme se actualice Active Directory.

Monitorear Active Directory y actualizar las libretas públicas de direcciones
Habilite esta opción si desea utilizar el Active Directory para mantener todos los registros públicos de contactos actualizados con la información más reciente almacenada en el Active Directory. Los campos comunes como la dirección postal de una cuenta, números de teléfono, información de contacto de negocios y más, serán grabados en su registro público de contacto y estos datos se actualizarán cada vez que se modifiquen en el Active Directory. Numerosos campos de registros de contactos serán monitoreados de esta forma. Para obtener una lista completa de cuales campos se pueden mapear como atributos del Active Directory, vea el archivo `ActiveDS.dat`. Ver: Actualizando la Libreta Pública de Direcciones 823, para más información.

Usar dominios de Active Directory al crear cuentas
Use esta opción si quiere que las nuevas cuentas creadas como resultado del monitoreo del Active Directory sean añadidas al dominio encontrado en el atributo de Active Directory "`UserPrincipalName`". Cuando use esta opción, si una cuenta requiera un dominio que no existe dentro de MDaemon, se creará un

nuevo Dominio 190 automáticamente. Desmarque esta opción si desea que las nuevas cuentas se añadan al dominio de MDaemon por defecto.

Consultar Active Directory para nuevos datos cada [XX] segundos
Este es el intervalo al que MDaemon monitoreará el Active Directory para cambios.

Dominio de Windows para autentificación AD
Especifique un nombre de dominio de Windows si desea utilizar la Autentificación AD para cuentas creadas por el monitoreo del Active Directory. Si deja este campo en blanco las nuevas cuentas tendrán asignadas contraseñas aleatorias. Tendrá luego que editar dichas contraseñas manualmente para que las cuentas puedan ser accedidas.

Cuando una cuenta se borra del Active Directory...
La opción seleccionada a continuación determina la acción que MDaemon tomará cuando las cuentas de Active Directory asociadas a las de MDaemon sean eliminadas.

...no hacer nada
Escoja esta opción si no quiere que MDaemon haga ningún cambio a una cuenta de MDaemon cuando su cuenta asociada sea eliminada del Active Directory.

...eliminarlas también desde MDaemon
Si escoge esta opción hará que la cuenta de MDaemon sea eliminada cuando su cuenta asociada sea eliminada del Active Directory.

Esto hará que la cuenta de MDaemon asociada sea completamente eliminada. Todos los mensajes, carpetas de mensajes, libretas de direcciones, y demás de la cuenta serán eliminados.

...deshabilitar la cuenta en MDaemon
Cuando esta opción está seleccionada y una cuenta del Active Directory se elimina, su correspondiente cuenta de MDaemon será deshabilitada. Esto significa que la cuenta de MDaemon seguirá existiendo en el servidor, pero no podrá enviar o recibir correo o ser accedida por nadie.

...congelar la cuenta en MDaemon
Cuando esta opción es seleccionada MDaemon seguirá aceptando el correo entrante de la cuenta, pero lo "bloqueará" efectivamente para que no pueda ser accedido. En otras palabras, los mensajes entrantes para dicha cuenta no serán rechazados o eliminados por MDaemon, pero el propietario de la cuenta no podrá recolectar o acceder a dicho correo mientras esta cuenta esté inmovilizada.

Congelar cuentas de MDaemon deshabilitadas en Active Directory
Por defecto, cuando deshabilita una cuenta en el Active Directory, MDaemon también deshabilitará la cuenta asociada en MDaemon. Esto hace que la cuenta sea inaccesible y MDaemon no podrá ni aceptar ni enviar mensajes por ella. Sin embargo, si prefiere tener la cuenta asociada de MDaemon inmovilizada en lugar de deshabilitada, marque esta opción. MDaemon seguirá aceptando mensajes

para las cuentas inmovilizadas, pero los usuarios no podrán acceder a dichas cuentas para recolectar o enviar su correo.

Cuando se eliminan cuentas en AD, eliminarlas de la(s) libreta(s) pública(s) de direcciones
Por omisión, un contacto en carpeta pública se elimina siempre que su cuenta asociada es eliminada de Active Directory. Sin embargo, el contacto solo se elimina si originalmente fue creado con la funcionalidad de integración con Active Directory 823. Deshabilite la opción si no desea eliminar contactos cuando se eliminen las cuentas asociadas en Active Directory.

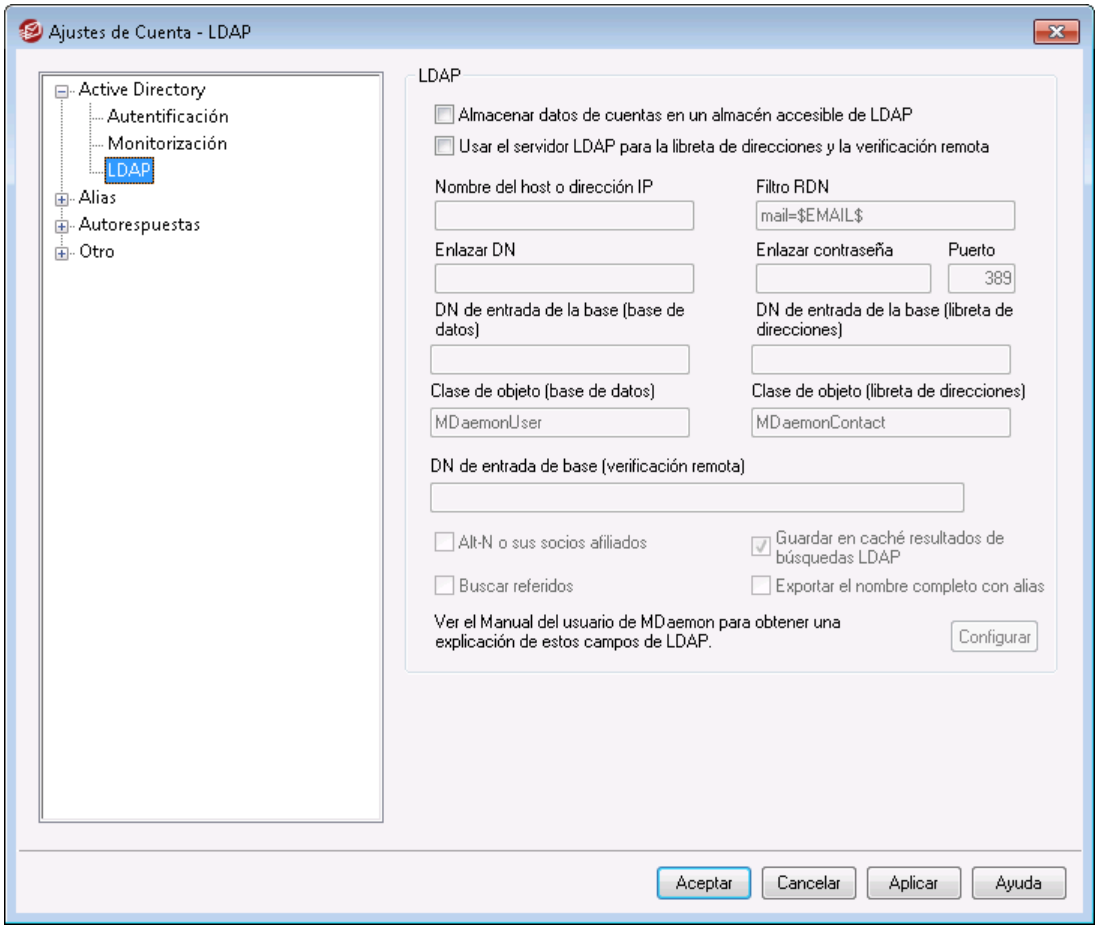
Las cuentas eliminadas fuera de AD no son creadas de nuevo por el monitoreo AD
Cuando elimine una cuenta en MDaemon fuera de Active Directory (por ejemplo, eliminándola manualmente desde la interface de MDaemon), por omisión la cuenta no será creada de nuevo por la funcionalidad de monitoreo de Active Directory. Deshabilite esta opción si desea que esas cuentas sean creadas de nuevo.

Realizar un escaneo completo de Active Directory ahora
Haga clic en este botón para hacer que MDaemon consulte a la base de datos de Active Directory y luego cree, edite, o elimine cuentas según sea necesario. Cuando una cuenta de Active Directory se encuentre que coincida con una cuenta de MDaemon existente, la cuenta de MDaemon quedará enlazada.

Ver:

Active Directory 822
Active Directory » Autentificación 825

5.3.1.3 LDAP



MDaemon soporta la funcionalidad LDAP (Lightweight Directory Access Protocol). Dé clic en "Cuentas » Ajustes de Cuentas » LDAP" para ingresar a la pantalla LDAP utilizada para configurar a MDaemon para mantener actualizadas las cuentas de usuario de su servidor LDAP. MDaemon puede mantener una base de datos de usuarios exacta y continuamente actualizada, comunicándose con su servidor LDAP cada vez que una cuenta de MDaemon se agrega o elimina. Esto permite a los usuarios con clientes de correo que soporta LDAP "compartir" una libreta de direcciones global que contendrá registros para todos sus usuarios de MDaemon, así como cualesquiera otros posibles contactos que usted incluya.

También puede utilizar su servidor LDAP como Base de Datos de Usuarios de MDaemon 849 en lugar de utilizar la tabla local del sistema `USERLIST.DAT` o una base de datos compatible con ODBC. También es posible utilizar este método para mantener su información de usuarios si cuenta con múltiples servidores MDaemon en diferentes ubicaciones, pero desea que compartir una única base de datos de usuarios. Cada servidor MDaemon se configurará para conectarse al mismo servidor LDAP a fin de compartir información de usuarios en lugar de almacenarla localmente.

LDAP

Almacenar datos de cuentas en un almacén accesible de LDAP
Haga clic en esta casilla si desea que MDaemon utilice su servidor LDAP como la base de datos de usuarios de MDaemon en lugar de ODBC o su sistema local `USERLIST.DAT`. Puede que quiera utilizar este método de mantener la información de usuarios si tiene múltiples servidores MDaemon en diferentes

ubicaciones y quiere que compartan una sola base de datos de usuario. Cada MDaemon deberá configurarse para conectarse al mismo servidor LDAP para poder compartir la información en lugar de almacenarla localmente.

Usar el servidor LDAP para la libreta de direcciones y la verificación remota
Si está utilizando ODBC o el método por defecto de `USERLIST.DAT` para mantenimiento de su base de datos de cuentas en lugar del método de servidor LDAP, puede aun así mantener el servidor LDAP actualizado con todos los nombres de usuarios, direcciones de correo, y alias utilizando esta casilla de verificación. Así pues, puede mantener el servidor LDAP actualizado para utilizarlo como sistema de libreta de direcciones global para usuarios de clientes de correo que tengan soporte para libretas de direcciones LDAP.

Esto mantendrá una base de datos de sus buzones, alias y listas de distribución que los servidores remotos pueden consultar para verificación remota de las direcciones de correo. Vea *DN de entrada de base (verificación remota)* a continuación para más información.

Propiedades del Servidor LDAP

Nombre del host o dirección IP
Introduzca el nombre de host o dirección IP de su servidor LDAP aquí.

Filtro RDN
Este control se usa para generar el RDN para cada entrada de usuario LDAP. El nombre distinguido relativo (relative distinguished name - RDN) es el componente ubicado más a la izquierda en cada entrada de nombre distinguido (DN). Para todas las entradas paritarias (aquellas que comparten entrada superior inmediata) el RDN debe ser único, así pues, se sugiere utilizar la cuenta de correo de cada usuario como su RDN para evitar posibles conflictos. Utilizando la macro $EMAIL$ como el valor de atributo de este control (correo=`$EMAIL$`) hará que se reemplace por la dirección de correo del usuario cuando se cree su entrada de LDAP. Así pues, la entrada DN del usuario estará compuesta por el RDN más la *Entrada de Base DN* siguiente.

Enlazar DN
Introduzca la DN de la entrada a la que desea conceder acceso administrativo a su servidor LDAP para que MDaemon pueda añadir y modificar sus entradas de usuario de MDaemon. Este es el DN usado para la operación de autenticación de enlace.

Enlazar contraseña
Esta contraseña será pasada al servidor LDAP juntamente con el valor de *Enlazar DN* para autenticación.

Puerto
Especifique el puerto que su servidor LDAP monitorea. MDaemon utilizará este puerto cuando envíe información de cuentas a éste.

DN de entrada de la base (base de datos)
Introduzca la entrada de base (raíz DN) que se usará en todas las entradas de usuario cuando utilice el servidor LDAP como su base de datos de usuario en lugar del archivo `USERLIST.DAT`. La entrada de Base DN está combinada con el RDN (ver *Filtro RDN* anterior) parar formar cada uno de los nombres distinguidos de usuario (DN).

DN de entrada de la base (libreta de direcciones)
Cuando monitoree información de cuentas a una libreta de direcciones LDAP, introduzca la entrada de base (raíz DN) que se usará en todas las entradas de la libreta de direcciones de MDaemon. La Entrada de Base DN se combina con el RDN (ver *Filtro RDN* anterior) para formar cada uno de los nombres distinguidos de usuario (DN).

Clase de objeto (base de datos)
Especifique la clase de objeto a la que cada entrada de la base de datos de usuario debe pertenecer. Cada entrada contendrá en el atributo `objectclass=` el valor aquí indicado.

Clase de objeto (libreta de direcciones)
Especifique la clase del objeto a la que cada entrada de usuario en la libreta de direcciones LDAP debe pertenecer. Cada entrada contendrá en el atributo `objectclass=` el valor aquí indicado.

DN de entrada de base (verificación remota)
Un problema común con las puertas de enlace y los servidores de respaldo remotos es que normalmente no tienen un método de determinar si el destinatario de un mensaje entrante es válido o no. Por ejemplo, si el mensaje viene al servidor de respaldo del dominio ejemplo.com dirigido a usuario01@ejemplo.com, entonces el servidor de respaldo no tiene manera de saber si existe o no el buzón, alias, o lista de correo en ejemplo.com para "usuario01". Así pues, el servidor de respaldo no tiene otra opción más que aceptar todos los mensajes. MDaemon contiene un método para verificar estas direcciones y resolver este problema. Especificando una entrada de base DN que se use para buzones, alias y listas de distribución, el servidor LDAP puede mantenerse actualizado con toda esa información. Así, el servidor de respaldo puede consultar de manera sencilla el servidor LDAP cada vez que un mensaje llega para el dominio y verificar si la dirección de destino es válida. Si no lo es entonces el mensaje será rechazado.

El protocolo del Servidor es versión 3
Dé clic en esta casilla si desea que MDaemon utilice la versión 3 del protocolo LDAP con su servidor.

Buscar referencias
En ocasiones el servidor LDAP no cuenta con un objeto, pero puede hacer una referencia cruzada a su ubicación, a la que puede referir al cliente. Si desea que MDaemon busque (i.e. siga) estas referencias, habilite esta opción. Se encuentra deshabilitada por omisión.

Conservar en Cache los resultados de consultas LDAP
Por omisión MDaemon graba en caché los resultados de las consultas LDAP. Deshabilite esta opción si no desea que se graben en caché.

Exportar nombre completo con alias
No-alias exportados a libretas de direcciones LDAP colocan el nombre completo de la cuenta en el campo CN. Los Alias, sin embargo, colocan en ese campo la dirección de correo (no el alias). Seleccione esta casilla si desea colocar ahí el nombre completo de la cuenta (si se conoce). Esta opción se encuentra deshabilitada por omisión.

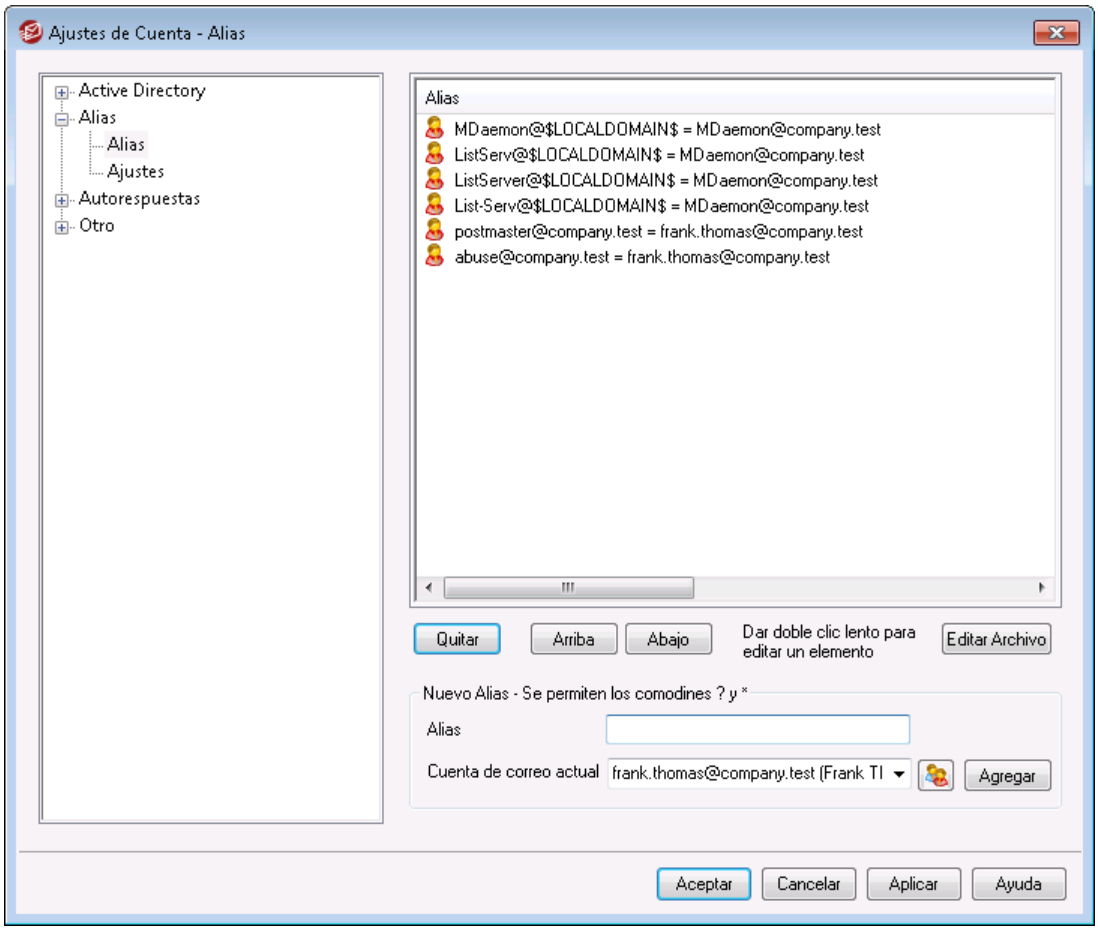
Configurar
Haga clic en este botón para abrir el archivo de configuración `LDAP.dat` en un editor de texto. Se usa para designar el nombre de atributo LDAP que correspondan con cada uno de los campos de las cuentas de MDaemon.

Ver:

Base de datos de las Cuentas 849

5.3.2 Alias

5.3.2.1 Alias



Los Alias le permiten crear nombres de buzón alternos para sus cuentas o listas de distribución, que son útiles cuando requiere de múltiples nombres de buzones para resolver una única cuenta de usuario o lista. Sin los alias tendría que crear cuentas de usuario separadas para cada dirección y luego reenviar los mensajes o usar reglas de filtrado complicadas para asociarlas con otras cuentas.

Por ejemplo, si `usuario1@ejemplo.com` maneja todas las consultas de facturación para su dominio, pero quiere decirle a todos que las envíen a `facturacion@ejemplo.com`, puede crear un alias para que los mensajes dirigidos a `facturacion@ejemplo.com` vayan a `usuario1@ejemplo.com`. O, si tiene diversos dominios y quiere que todos los mensajes dirigidos a Postmaster (independientemente del dominio) vayan a `usuario1@ejemplo.com`, puede usar un comodín para asociar el alias, `Postmaster@*`, con esta dirección.

Alias Actuales

Esta ventana contiene todos los alias actuales que haya creado.

Quitar
Haga clic en este botón para eliminar una entrada seleccionada de la lista actual de *Alias Actuales.*

Arriba
Los alias se procesan en el orden en que se enlistan. Puede mover un alias a una posición superior en la lista seleccionándolo y luego haciendo clic en este botón.

Abajo
Los alias se procesan en el orden en que se enlistan. Puede mover un alias a una posición inferior en la lista seleccionándolo y luego haciendo clic en este botón.

Editar Archivo
Dé clic en este botón si desea abrir el archivo `Alias.dat` en un editor de texto, para editarlo o hacer búsquedas manuales. Luego de hacer los cambios deseados, salga del editor de texto y entonces MDaemon volverá a cargar el archivo.

Alias
Introduzca la dirección de correo que desea que sea un alias de la dirección "*Buzón real*" a continuación. Los comodines "?" y "*" están permitidos, y puede usar "`@$LOCALDOMAIN$`" en el alias como comodín que coincidirá sólo con sus dominios locales. Por ejemplo "`usuario1@ejemplo.*`", "`*@$LOCALDOMAIN$`", y "`fran@$LOCALDOMAIN$`" son todos válidos para uso como alias.

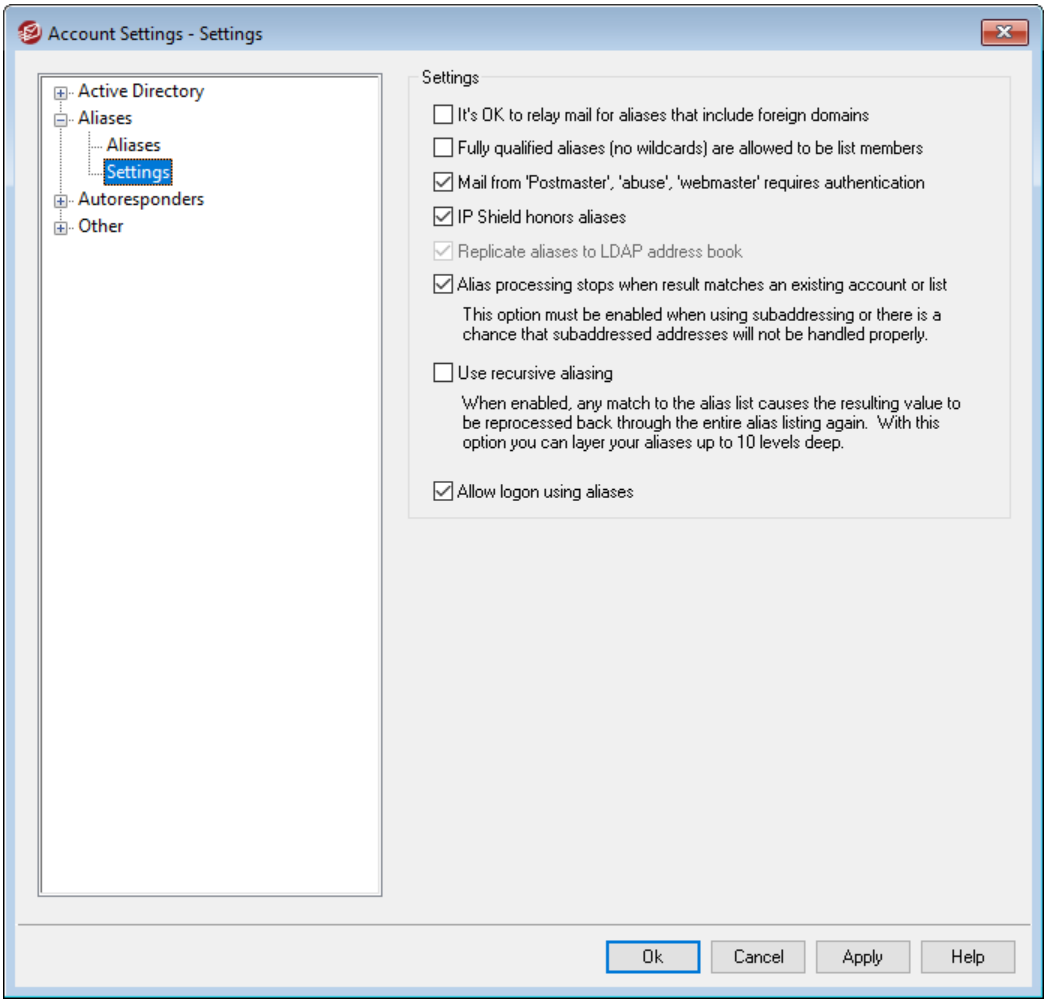
Buzón real
Seleccione la cuenta de la lista desplegable, use el icono de cuentas para navegar por una cuenta, o teclee una nueva dirección o lista de correo en este espacio. Esta es la dirección real que recibirá el mensaje cuando se direccione al alias correspondiente.

Agregar
Haga clic en el botón *Agregar* para añadir el alias a la lista. Los valores *Alias* y *Buzón real* se combinarán y colocarán en la ventana de *Alias Actuales*.

Ver:

Alias » Opciones 836
Editor de Cuentas » Alias 742

5.3.2.2 Ajustes



Ajustes

Está bien retransmitir correo para los alias que incluyen dominios externos
Haga clic en esta casilla si desea permitir a MDaemon que retransmita correo para alias que incluyan dominios no-locales. Esta opción sobrescribe la opción *No permitir retransmisión de mensajes* en el Control de retransmisión 512 para dichos alias.

Se permite que los alias completamente calificados (sin comodines) sean miembros de la lista
Haga clic en esta casilla si quiere permitir a los alias ser miembros de las listas de distribución de MDaemon. Sólo las cuentas reales pueden ser miembros si se habilita este control. **Nota:** los alias que contienen comodines no se les permite ser miembros de lista, aunque esta opción esté habilitada.

El correo desde el 'Postmaster', 'abuse' o 'webmaster' requiere autentificación
Cuando se habilita esta opción, MDaemon requerirá que los mensajes que digan ser de una de las cuentas o alias de "postmaster@...", "abuse@..." o "webmaster@..." o cuentas sean autenticados antes de que MDaemon los acepte. Los spammers y los hackers saben que dichas direcciones pueden existir y pueden, por lo tanto, intentar usarlas para enviar correo a través de su sistema. Esta opción les impide a ellos y a otros usuarios no autorizados poder

hacerlo. Para su comodidad esta opción también está disponible en la pantalla Autentificación SMTP[523], ubicada en: Seguridad » Ajustes de Seguridad. Cambiar la configuración aquí también la cambiará allá.

El protector de IP respeta los alias
Por defecto la Protección IP[521] respetará los alias cuando compruebe los mensajes entrantes para búsqueda de parejas dominio/IP válidas. La Protección IP traducirá un alias a la cuenta real a la que apunta y por lo tanto la respetará cuando pase por la protección. Si desmarca esta casilla la Protección IP tratará cada alias como si fuera una dirección independiente de la cuenta que representa. Así, si la dirección IP de un alias viola la protección IP el mensaje será rechazado. Esta opción está duplicada en la pantalla de Protección IP — si cambia la configuración aquí también cambiará allí.

Copiar alias a la libreta de direcciones LDAP
Haga clic en esta casilla si quiere que los alias se repliquen a la libreta de direcciones LDAP. La replicación de alias es necesaria para que la verificación remota de alias funcione correctamente, pero si no está usando dicha funcionalidad, entonces replicar los alias a la libreta de direcciones no es necesario. Si no usa la verificación remota puede deshabilitar con seguridad esta funcionalidad para ahorrar tiempo de proceso. Para más información acerca de la verificación remota LDAP vea LDAP[831]

El procesamiento de alias se detiene cuando un resultado coincide con una cuenta o lista existente
Cuando se habilita esta opción, el procesamiento de alias se detendrá cuando el destinatario del mensaje entrante coincida con una cuenta existente o lista de correo. Típicamente esto aplica a alias que incluyen un comodín. Por ejemplo, si tiene un alias establecido como "`*@ejemplo.com=usuario1@ejemplo.com`," entonces esta opción hará que dicho alias se aplique sólo a direcciones que no existen actualmente en su servidor. Así, si también tiene la cuenta "`usuario2@ejemplo.com`" los mensajes direccionados a usuario2 seguirían enviándose a él porque el alias no se aplicaría a dichos mensajes. Pero los mensajes direccionados a una dirección no existente o lista se enviarían a "`usuario1@ejemplo.com`" porque el alias con comodín aplicaría a esos mensajes. Esta opción está habilitada por defecto.

Esta opción debe estar habilitada cuando se usa Subdireccionamiento[762], para evitar problemas potenciales con la gestión de dichos mensajes.

Usar alias repetitivos
Haga clic en esta casilla si quiere procesar los alias de manera recursiva. Una coincidencia de alias causa que el resultado sea reprocesado de nuevo a través de la lista de alias—es posible anidar alias hasta 10 niveles de profundidad. Por ejemplo, podría establecer algo así:

```
usuario2@example.com = usuario1@example.com
usuario1@example.com = usuario5@example.net
usuario5@example.net = usuario9@example.org
```

Esto es lógicamente idéntico al alias único:

```
usuario2@ejemplo.com = usuario9@ejemplo.org
```

También significa que:

```
usuario1@ejemplo.com = usuario9@ejemplo.org
```

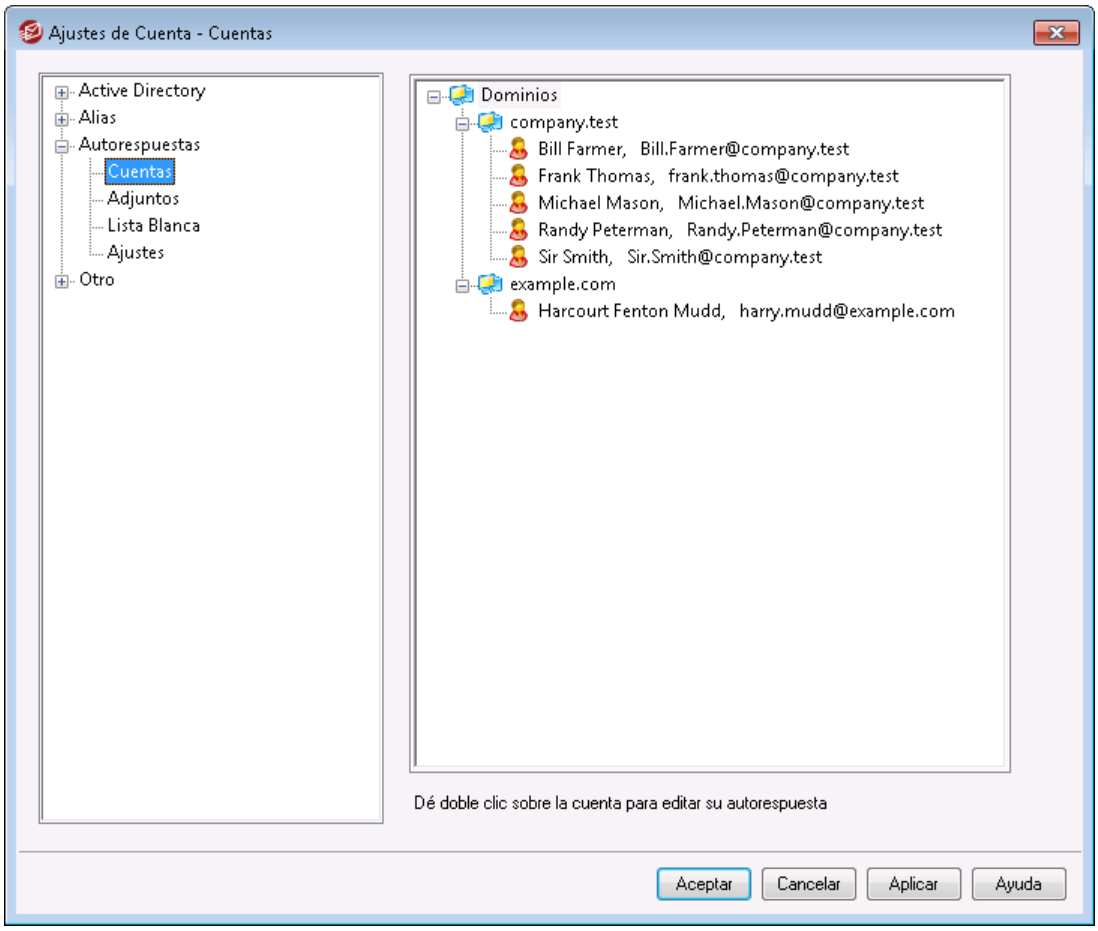
Permitir Inicio de Sesión usando Alias
Por omisión, a los usuarios se les permite iniciar sesión en sus cuentas utilizando uno de sus alias[834] en lugar del nombre real de su buzón. Deshabilite esta casilla si no desea permitir esto.

Ver:

Alias[834]

5.3.3 Autorespuestas

5.3.3.1 Cuentas



Las autorespuestas son herramientas útiles que hacen que los mensajes entrantes detonen algunos eventos automáticamente, tales como ejecutar un programa, añadir al remitente a una lista de correo, responder con un mensaje generado automáticamente, y más. El uso más común de las autorespuestas es responder a los mensajes entrantes automáticamente con un mensaje definido por el usuario indicando que el destinatario está de vacaciones, no está disponible, contestará lo antes posible, o similar. Los usuarios de MDaemon con Acceso Web[720] a

Webmail 321 o Administración Remota 354 pueden usar las opciones ofrecidas para redactar mensajes de autorespuesta por sí mismos y programar las fechas en que estarán en uso. Finalmente, los mensajes de respuesta automática se basan en el contenido del archivo `OOF.mrk`, que se encuentra en la carpeta raíz de cada usuario en `\data\`. Este archivo soporta un gran número de macros, que se pueden utilizar para hacer que gran parte del contenido del mensaje se genere dinámicamente, haciendo las autorespuestas bastante versátiles.

Los eventos de Autorespuesta son siempre autorizados cuando el mensaje que los detona es de una fuente remota. Sin embargo, para los mensajes originados en el mismo dominio del usuario, las auto respuestas sólo se activarán si se habilita la opción *Las respuestas automáticas son generadas por el correo del dominio interno*, ubicada en la pantalla Autorespuesta » Ajustes 842. Puede usar también una opción en dicha pantalla para limitar los mensajes de autorespuesta a uno por remitente por día.

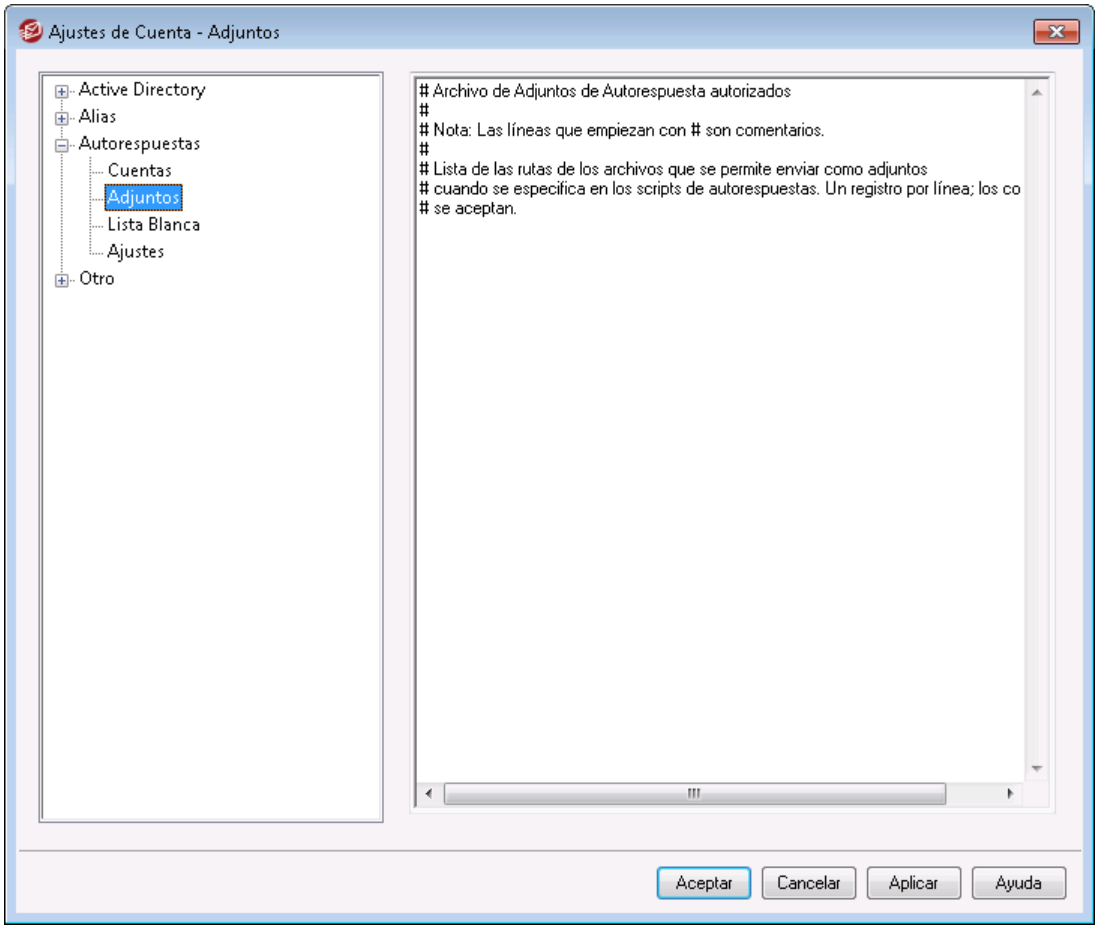
Lista de Cuentas

Esta área lista todos los buzones locales que tienen autorespuesta. Haga doble-clic en una cuenta en esta lista para abrir su correspondiente pantalla de Autorespuesta 726, que se usa para configurar una autorespuesta para dicha cuenta.

Ver:

Autorespuestas » Lista de Exentos 840
Autorespuestas » Ajustes 842
Crear Scripts de Autorespuestas 843
Editor de Cuentas » Autorespuestas 726

5.3.3.2 Adjuntos

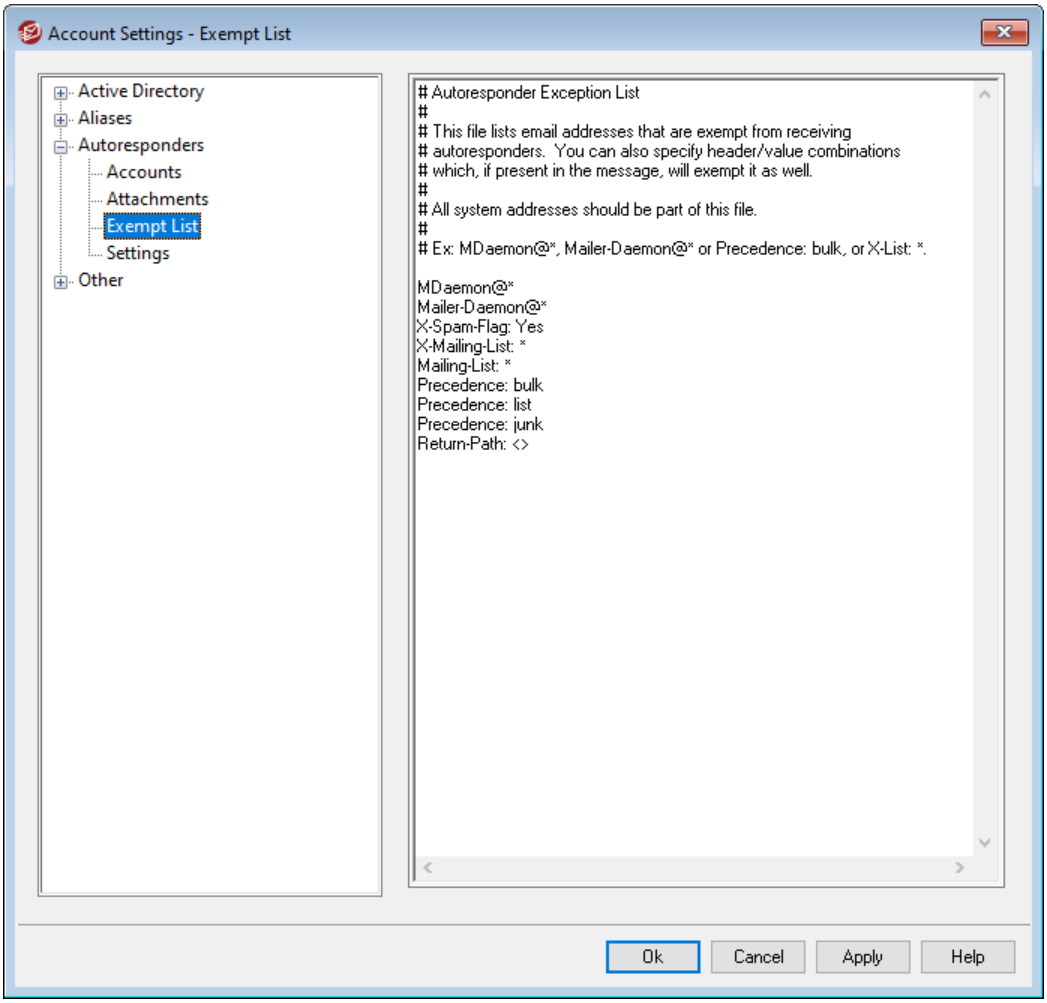


Proporcione las rutas completas aquí para los archivos que desee permitir se utilicen como adjuntos en los scripts de autorespuestas 843. En el script de autorespuesta, utilice la macro **%SetAttachment%** para adjuntar el archivo.

Ver:

Autorespuestas » Cuentas 838
Autorespuestas » Lista de Exentos 840
Autorespuestas » Ajustes 842
Creando Scripts de Autorespuestas 843
Editor de Cuentas » Autorespuestas 726

5.3.3.3 Lista de Exentos



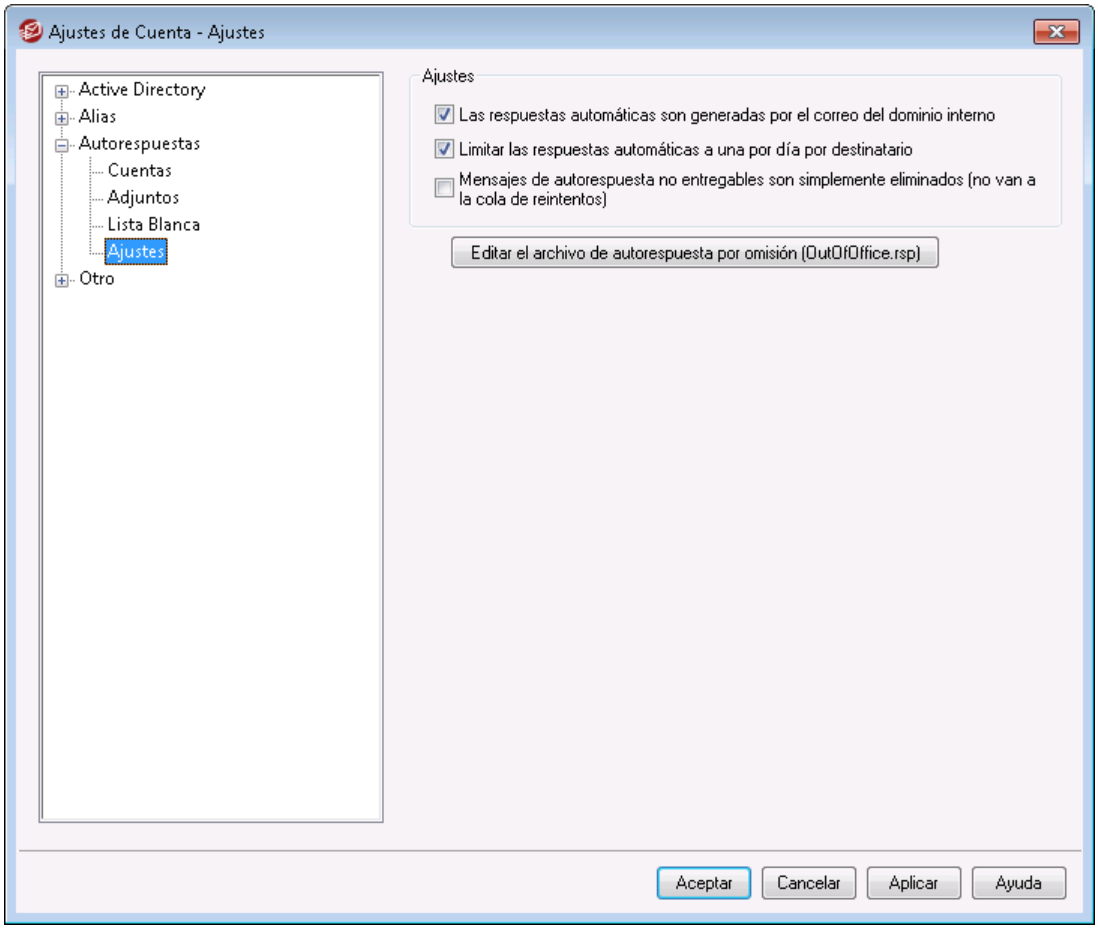
Use **Autorespuestas** » **Lista de Exentos** para configurar las excepciones globales a las Respuestas Automáticas. Los mensajes de entradas en esta lista no recibirán Respuestas Automáticas. Tanto las direcciones de correo como los parejas valor/encabezado pueden incluirse en la lista. Introduzca una dirección o pareja valor/encabezado por línea. Se permiten comodines.

Todos los sistemas de direcciones (p. ej. mdaemon@*, mailer-daemon@*, y demás) deberían ser listados para ayudar a prevenir ciclos de correo y otros problemas.

Ver:

Respuestas Automáticas » Cuentas 838
Respuestas Automáticas » Ajustes 842
Crear Scripts de Respuestas Automáticas 843
Editor de Cuentas » Respuestas Automáticas 726

5.3.3.4 Ajustes



Ajustes

Las respuestas automáticas son generadas por el correo del dominio interno
Por defecto, tanto el correo remoto como el local desencadenan las autorespuestas. Deshabilite esta casilla si no desea detonar autorespuestas cuando el mensaje entrante proviene del mismo dominio del usuario.

Limitar las respuestas automáticas a una por día por destinatario
Por defecto, las autorespuestas sólo generarán un mensaje de respuesta por día para una dirección dada. Esto evita que la gente reciba la misma respuesta redundante de usted una y otra vez el mismo día, cada vez que le envían un correo. Desmarque esta casilla si desea enviar mensajes de autorespuesta cada vez que alguien le envíe un mensaje, aunque ya hayan recibido uno ese día.

Esta opción también previene los ciclos de mensajes, que pueden ocurrir cuando un mensaje de autorespuesta es devuelto a una dirección que también tiene activa una autorespuesta. En lugar de permitir a ambas direcciones que envíen respuestas automáticas constantemente entre sí, esta opción permitirá sólo un mensaje por dirección por día.

Los mensajes de autorespuesta no entregables se eliminan (no van a la cola de reintentos)
Habilite esta opción si desea eliminar los mensajes de autorespuesta no entregables cuando expiran en la cola remota, en lugar de moverlos al sistema de la cola de reintentos[872].

Editar el archivo de autorespuesta por omisión (OutOfOffice.rsp)
Este es el archivo de respuesta por omisión. Los contenidos de este archivo se copiarán al archivo oof.mrk de la cuenta[726] si este no se encuentra o está vacío.

Ver:

Respuestas Automáticas » Cuentas[838]
Respuestas Automáticas » Lista de Exentos[840]
Crear Scripts de Respuestas Automáticas[843]
Editor de Cuenta » Respuestas Automáticas[726]

5.3.3.5 Crear Mensajes de Autorespuesta

Los archivos OOF.mrk son archivos ASCII de texto plano contenidos en la carpeta raíz `\data\` de cada usuario, que definen los mensajes que se devuelven como resultado de un evento de respuesta automática. Cuando se detona un mensaje de autorespuesta, el archivo se procesa y escanea buscando macros, que serán reemplazadas con los valores actuales para el mensaje entrante que detonó la respuesta. Las líneas que inician con el carácter "#" se ignoran y se utilizan para comentarios. Abajo se enlistan dos mensajes de muestra[847].

Macros de Autorespuesta

`$HEADERS$` Esta macro se reemplazará por todas las cabeceras del mensaje entrante. El texto que preceda inmediatamente a esta macro será duplicado al principio de cada línea expandida.

`$HEADER:XX$` Esta macro hará que el valor del encabezado especificado en lugar de "`xx`" sea expandido en el mensaje. Por ejemplo. Si el mensaje entrante tiene "`TO: juan@ejemplo.com`" entonces en la macro `$HEADER:TO$` expandirá "`juan@ejemplo.com`". Si el mensaje original tiene "`SUBJECT: Este es el asunto`" entonces la macro `$HEADER:SUBJECT$` sería reemplazada con el texto "`Este es el asunto`".

`$BODY$` Esta macro será reemplazada con el cuerpo del mensaje entero. En un intento de preservar el conjunto de caracteres para diferentes idiomas,

MDaemon leerá el mensaje como datos binarios en lugar de texto puro, permitiendo así una copia byte-a-byte del cuerpo del mensaje.

$BODY-AS-TEXT$	Como en la macro $BODY$, esta macro será reemplazada por el cuerpo entero del mensaje, pero como texto en lugar de binario. El texto que preceda a esta macro será duplicado al principio de cada línea expandida. Así pues, usando ">>$BODY-AS-TEXT$" en un script reemplazará cada línea del mensaje original en el mensaje generado, pero cada línea empezaría con ">>". El texto también se puede añadir a la derecha de esta macro.
$SENDER$	Esta macro resuelve la dirección completa contenida en la cabecera "From:" del mensaje entrante.
$SENDERMAILBOX$	Esta macro resuelve el buzón del remitente. El buzón es la porción de la dirección de correo a la izquierda del símbolo "@".
$SENDERDOMAIN$	Esta macro resuelve el dominio del remitente. Esta es la porción de la dirección de correo a la derecha del símbolo "@".
$RECIPIENT$	Esta macro resuelve la dirección completa del destinatario del mensaje.
$RECIPIENTMAILBOX$	Esta macro resuelve el buzón del destinatario del mensaje. El buzón es la porción de la dirección de correo a la izquierda del símbolo "@".
$RECIPIENTDOMAIN$	Esta macro resuelve el dominio del mensaje del destinatario. El dominio es la porción de la dirección de correo a la derecha del símbolo "@".
$SUBJECT$	Esta macro resuelve el valor del encabezado "Subject:".
$MESSAGEID$	Esta macro resuelve el valor del encabezado "Message-ID".
$CONTENTTYPE$	Esta macro resuelve el valor del encabezado "Content-Type".
$PARTBOUNDARY$	Esta macro resuelve el valor del valor MIME "Part-Boundary" encontrado en la cabecera "Content-Type" en los mensajes multiparte.
$DATESTAMP$	Esta macro expande la línea de fecha-hora a un estilo de RFC-2822

$ACTUALTO$	Algunos mensajes pueden contener un campo "ActualTo" que generalmente representa el buzón de destino y el host tal como fue entrado por el usuario original antes de reformatear o aplicar traducción de alias. Esta macro expande dicho valor.
$ACTUALFROM$	Algunos mensajes pueden contener un campo "ActualFrom" que generalmente representa el buzón y host de origen antes de reformatear o aplicar traducción de alias. Esta macro expande dicho valor.
$REPLYTO$	Esta macro resuelve el valor encontrado en la cabecera "ReplyTo".
$PRODUCTID$	Esta macro expande la cadena de información de versión de MDaemon.
AR_START	Devuelve la fecha/hora de inicio de la autorespuesta
AR_END	Devuelve la fecha/hora de término de la autorespuesta.

Macros de Reemplazo de Encabezados

Las macros listadas a continuación controlan los encabezados de mensajes de autorespuesta.

%SetSender%
ej: %SetSender%=buzon@ejemplo.org
Sólo para el mensaje de autorespuesta, esta macro restablece el remitente del mensaje original antes de construir las cabeceras del mensaje de autorespuesta. Así, esta macro controla la cabecera TO del mensaje de autorespuesta. Por ejemplo, si el remitente del mensaje original fuera "usuario2@ejemplo.org" y la respuesta automática del destinatario usara la macro %SetSender% para cambiarlo a "usuario1@ejemplo.com" entonces la cabecera TO del mensaje de autorespuesta se establecería como "usuario1@ejemplo.com."

%SetRecipient%
ej: %SetRecipient%=buzon@ejemplo.org
Sólo para el mensaje de autorespuesta, esta macro restablece el destinatario del mensaje original antes de construir las cabeceras del mensaje de autorespuesta. Así, esta macro controla la cabecera FROM del mensaje de autorespuesta. Por ejemplo, si el destinatario del mensaje original fuera "michael@ejemplo.com" y la cuenta de Michael tuviera una autorespuesta que usar la macro %SetRecipient% para cambiarlo a "michael.mason@ejemplo.com," entonces la cabecera FROM del mensaje de autorespuesta se establecería como "fran.vazquez@ejemplo.com."

%SetReplyTo%
ej: %SetReplyTo%=buzon@ejemplo.org
Controla el valor de la cabecera ReplyTo del mensaje de autorespuesta.

%SetSubject%
`ej: %SetSubject%=Texto del Asunto`
Reemplaza el valor del Asunto original del mensaje.

%SetMessageId%
`ej: %SetMessageId%=Cadena ID`
Cambia la cadena ID del mensaje.

%SetPartBoundary%
`ej: %SetPartBoundary%=Cadena Límite`
Cambia el límite de parte.

%SetContentType%
`ej: %SetContentType%=tipo MIME`
Cambia el tipo de contenido del mensaje al valor declarado.

%SetAttachment%
ej: `%SetAttachment%=rutaarchivo`
Forza a MDaemon a adjuntar el archivo específico al mensaje de autorespuesta recién generado . Solo los archivo especificados en la pantalla Adjuntos 840 pueden agregarse a las autorespuestas.

Ejemplos de Script de Autorespuesta

Un mensaje sencillo de autorespuesta contenido en el archivo oof.mrk utilizando varias macros de autorespuesta sería:

```
Estimado $SENDER$

  Su mensaje sobre el asunto '$SUBJECT$' no será leído por mí
  debido a que estoy de vacaciones. Hurra!!!

  Suyo sinceramente,

  $RECIPIENT$
```

También puede usar algunas de las macros de reemplazo de encabezados para expandir el contenido y controlar los encabezados que se generarán cuando el mensaje de autorespuesta se envíe de vuelta a `$SENDER$`:

```
  Estimado $SENDER$

  Su mensaje sobre el asunto '$SUBJECT$' no será leído por mi
  debido a que estoy de vacaciones. Hurra!!!

  Suyo sinceramente,

  $RECIPIENT$

  %SetSubject%=RE: $SUBJECT$
  %SetAttachment%=c:\photos\me_on_vaction.jpg
```

Usando este script de mensaje de autorespuesta, el mensaje tendrá el "`RE: `" añadido al principio del asunto y el archivo especificado adjunto.

La línea "`%SetSubject%=RE: $SUBJECT$`" se maneja de la siguiente manera:

1. La porción `$SUBJECT$` se expande y se reemplaza por el asunto del mensaje

original. Esto hace esta cadena equivalente a:

```
%SetSubject%=RE: Asunto del mensaje Original
```

2. MDaemon reemplaza el asunto original, que fue guardado en sus buffers internos, con el nuevamente calculado. Desde ese punto en adelante, cualquier uso de "$SUBJECT$" en el script devolverá el nuevo resultado.

Note la colocación de las nuevas macros - están listadas al final del script de respuesta. Es necesario para evitar los efectos colaterales. Por ejemplo, si la macro %SetSubject% estuviera colocada antes de la macro $SUBJECT$, que aparece en la segunda línea del script de respuesta, el texto del asunto ya habría sido cambiado para el momento en que la macro $SUBJECT$ fuera expandida. Así pues, en lugar de reemplazar $SUBJECT$ con el contenido de la cabecera "Subject:" original del mensaje, sería reemplazado con lo que fuera que hubiera establecido en el valor de %SetSubject%.

Ver:

Crear Mensajes de Autorespuesta 843
Respuestas Automáticas » Cuentas 838
Respuestas Automáticas » Lista de Exentos 840
Respuestas Automáticas » Ajustes 842
Editor de Cuentas » Autorespuestas 726

5.3.3.5.1 Ejemplos de Mensajes de Autorespuesta

Un mensaje sencillo de autorespuesta contenido en el archivo oof.mrk utilizando varias macros de autorespuesta sería:

```
Estimado $SENDER$

  Su mensaje sobre el asunto '$SUBJECT$' no será leído por mí
  debido a que estoy de vacaciones. Hurra!!!

  Suyo sinceramente,

  $RECIPIENT$
```

También puede usar algunas de las macros de reemplazo de encabezados para expandir el contenido y controlar los encabezados que se generarán cuando el mensaje de autorespuesta se envíe de vuelta a `$SENDER$`:

```
Estimado $SENDER$

Su mensaje sobre el asunto '$SUBJECT$' no será leído por mi
debido a que estoy de vacaciones. Hurra!!!

Suyo sinceramente,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

Usando este script de mensaje de autorespuesta, el mensaje tendrá el "`RE: `" añadido al principio del asunto y el archivo especificado adjunto.

La línea "`%SetSubject%=RE: $SUBJECT$`" se maneja de la siguiente manera:

1. La porción `$SUBJECT$` se expande y se reemplaza por el asunto del mensaje original. Esto hace esta cadena equivalente a:

   ```
   %SetSubject%=RE: Asunto del mensaje Original
   ```

2. MDaemon reemplaza el asunto original, que fue guardado en sus buffers internos, con el nuevamente calculado. Desde ese punto en adelante, cualquier uso de "`$SUBJECT$`" en el script devolverá el nuevo resultado.

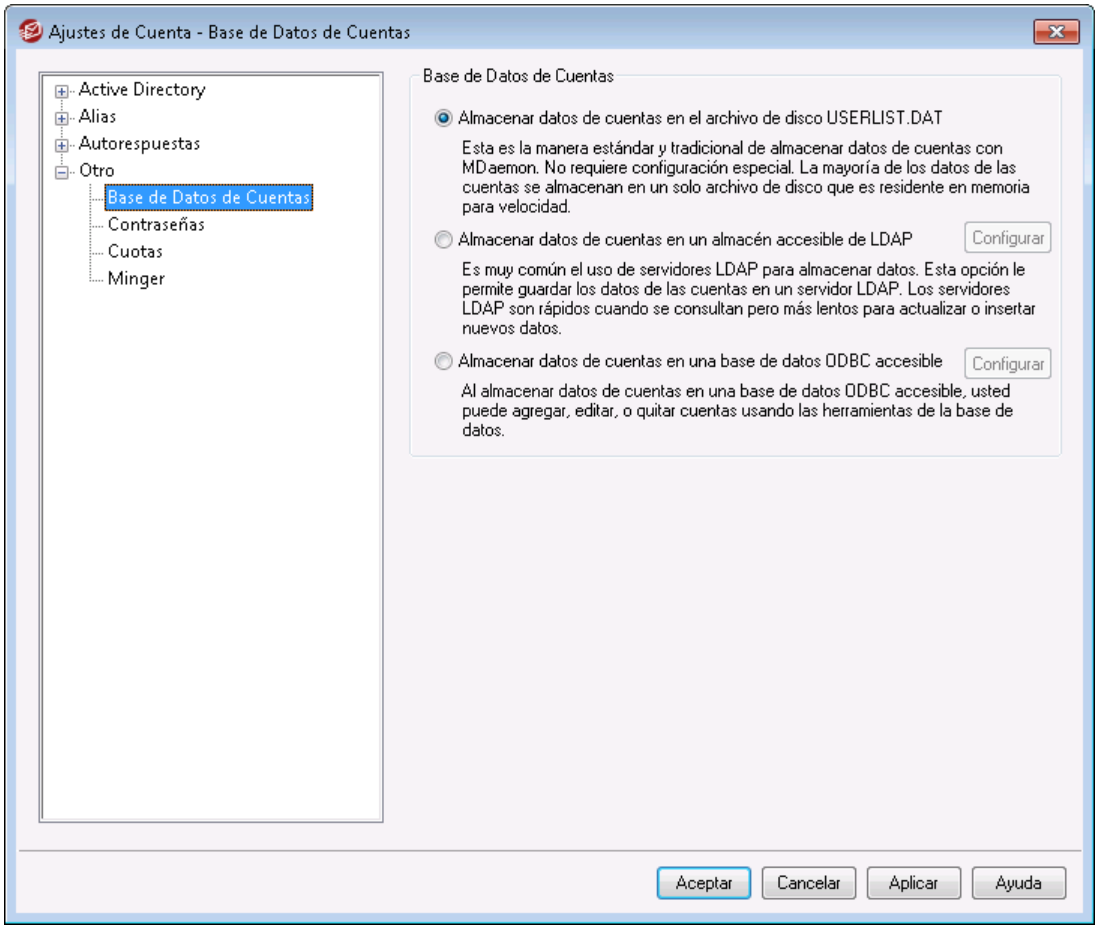
Note la colocación de las nuevas macros - están listadas al final del script de respuesta. Es necesario para evitar los efectos colaterales. Por ejemplo, si la macro `%SetSubject%` estuviera colocada antes de la macro `$SUBJECT$`, que aparece en la segunda línea del script de respuesta, el texto del asunto ya habría sido cambiado para el momento en que la macro `$SUBJECT$` fuera expandida. Así pues, en lugar de reemplazar `$SUBJECT$` con el contenido de la cabecera "`Subject:`" original del mensaje, sería reemplazado con lo que fuera que hubiera establecido en el valor de `%SetSubject%`.

Ver:

Crear Mensajes de Autorespuesta 843
Respuestas Automáticas » Cuentas 838
Respuestas Automáticas » Lista de Exentos 840
Respuestas Automáticas » Ajustes 842
Editor de Cuentas » Autorespuestas 726

5.3.4 Otros

5.3.4.1 Bases de datos de Cuentas



El diálogo de Base de Datos de las cuentas (ubicado bajo Cuentas » Ajustes de Cuenta) se usa para designar el método que quiere que MDaemon utilice para mantener sus cuentas de usuario: ODBC, LDAP, o el sistema local USERLIST.DAT.

Almacenar datos de cuentas en el archivo de disco USERLIST.DAT
Escoja esta opción si quiere que MDaemon use el archivo interno USERLIST.DAT como la base de datos de cuentas. Esta es la configuración por defecto de MDaemon y hace que toda la información de las cuentas de MDaemon se almacene localmente. La mayoría de la información se almacena en un único archivo, residente en memoria para incrementar la eficacia y la velocidad.

Almacenar datos de cuentas en un almacén accesible de LDAP
Escoja esta opción si quiere que MDaemon use un servidor LDAP como la base de datos de usuarios de MDaemon en lugar de ODBC o su sistema USERLIST.DAT local. Puede que quiera utilizar este método para mantener los datos de las cuentas de usuarios si tiene muchos servidores de MDaemon en diferentes ubicaciones, pero quiere que compartan una única base de datos de usuarios. Cada servidor MDaemon debería ser configurado para conectar al mismo servidor LDAP para poder compartir la información de usuario de MDaemon en lugar de almacenarla localmente. Los servidores LDAP responden normalmente de manera rápida y eficiente a las consultas, pero son más lentos a la hora de actualizar o insertar nuevos datos.

Configurar
Cuando se usa la opción de datos de cuenta LDAP, haga clic en este botón para abrir la pantalla LDAP[831] para establecer sus configuraciones de servidor LDAP.

Almacenar datos de cuentas en una base de datos ODBC accesible
Escoja esta opción si desea usar una base de datos ODBC como su base de datos de cuenta MDaemon.

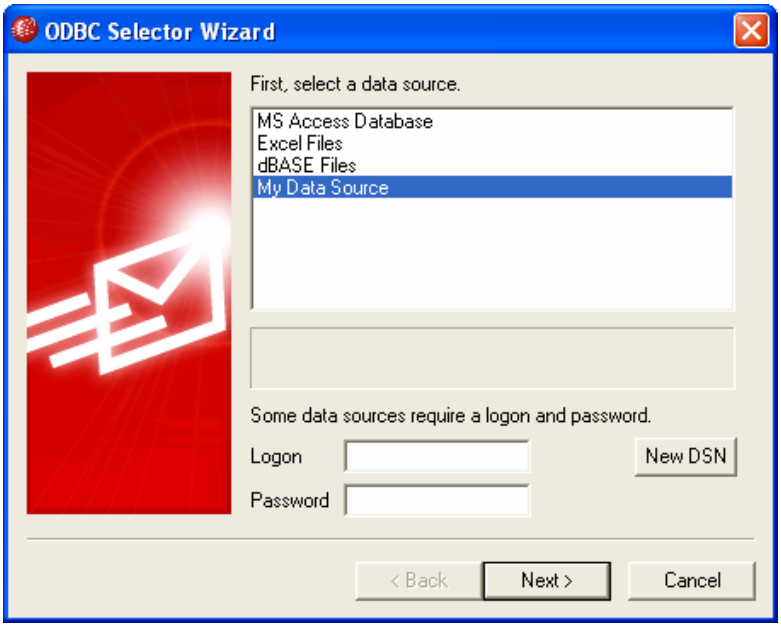
Configurar
Cuando se selecciona la opción de base de datos de cuentas ODBC, haga clic en este botón para abrir el Asistente para la selección de ODBC[850] para seleccionar y configurar su base de datos ODBC.

5.3.4.1.1 Asistente para la Selección de ODBC - Base de Datos de Cuentas

Utilice el asistente para la Selección de ODBC para seleccionar o configurar una fuente de datos ODBC para usar como su base de datos de cuentas de MDaemon.

Migrar su Base de Datos a un Almacén Accesible ODBC

1. En el diálogo de Base de datos de las cuentas (Cuentas » Ajustes de Cuentas » Base de datos de las Cuentas), haga clic en **Almacenar datos de cuentas en una base de datos ODBC accesible** y luego haga clic en **Configurar** para abrir el Asistente para la Selección ODBC.

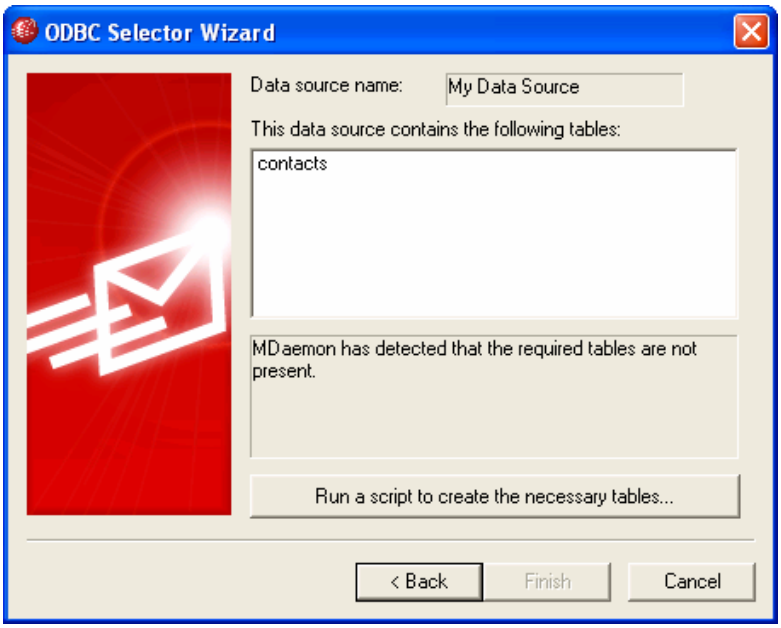


2. Seleccione la **fuente de datos** que desea usar para su base de datos de cuentas. Si no existe una fuente compatible, haga clic en **Nuevo DSN** y luego siga las instrucciones a continuación, listadas bajo, **Crear una nueva fuente de datos ODBC**[852].

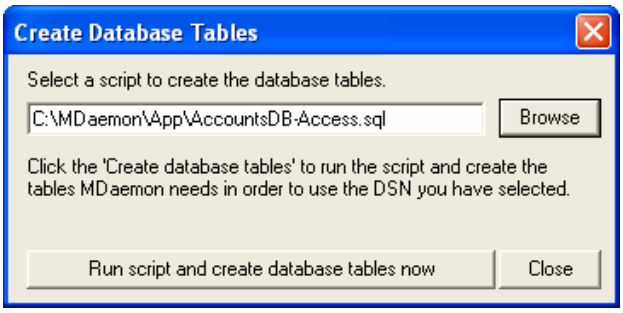
3. Si se requiere, introduzca **Registrarse** y **Contraseña**.

4. Haga clic en **Siguiente**.

5. Si la fuente de datos ya contiene las tablas requeridas por MDaemon, vaya al **Paso 8**. Si no, haga clic en **Ejecutar un archivo de comandos para crear las tablas necesarias...**



6. Teclee la ruta de archivo (o **Examinar**) al archivo de script que desea utilizar para crear las tablas para su aplicación de base de datos. La carpeta `\MDaemon\app\` contiene scripts para muchas de las más populares aplicaciones de base de datos.



7. Haga clic en **Ejecutar un archivo de comandos y crear tablas de base de datos ahora,** Haga clic en **OK**, u clic en **Cerrar**.

8. Haga clic en **Finalizar**, luego haga clic en **Aceptar** para cerrar el diálogo de Base de Datos de Cuentas.

9. Una herramienta de migración de base de datos migrará todas sus cuentas de usuario a la fuente de datos ODBC y luego cerrará MDaemon. Haga clic en **OK**, y luego reinicie MDaemon y empiece a usar la nueva base de datos de cuentas ODBC.

Ver:

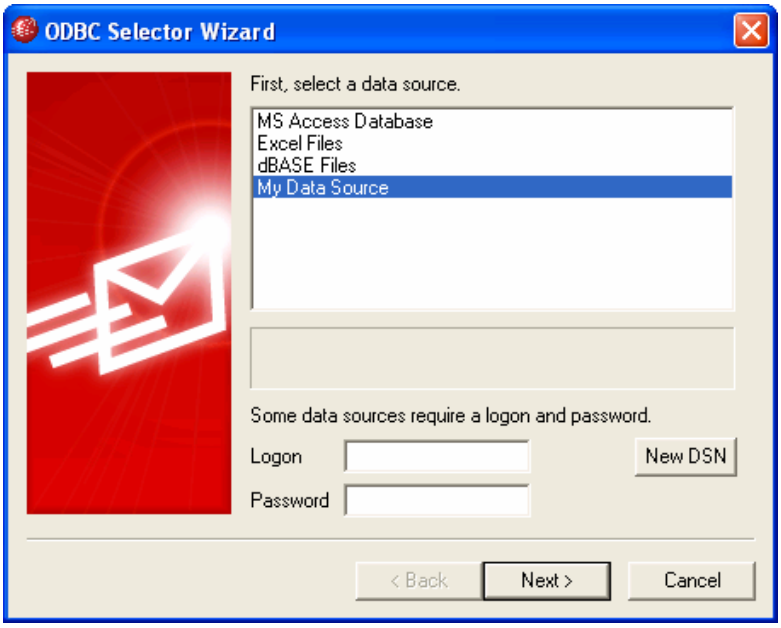
Base de datos de las Cuentas 849
Crear una nueva Fuente de datos ODBC 852

5.3.4.1.1.1 Crear una Nueva Fuente de Datos ODBC

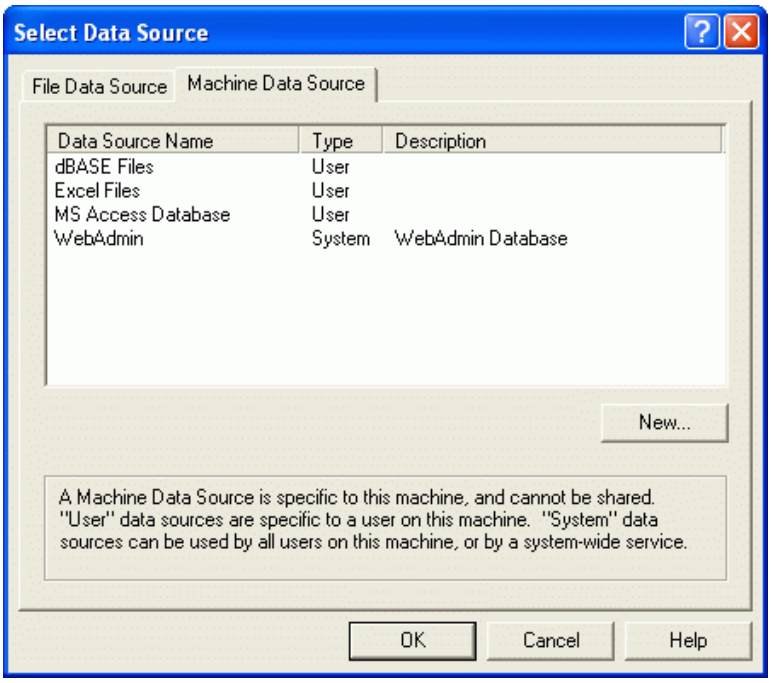
Para crear una nueva fuente de datos ODBC:

1. En el diálogo de Base de datos de Cuentas (Cuentas » Ajustes de Cuentas » Base de Datos de Cuentas), haga clic en **Almacenar datos de cuentas en una base de datos ODBC accesible**, y luego haga clic en **Configurar** para abrir el Asistente de Selector de ODBC.

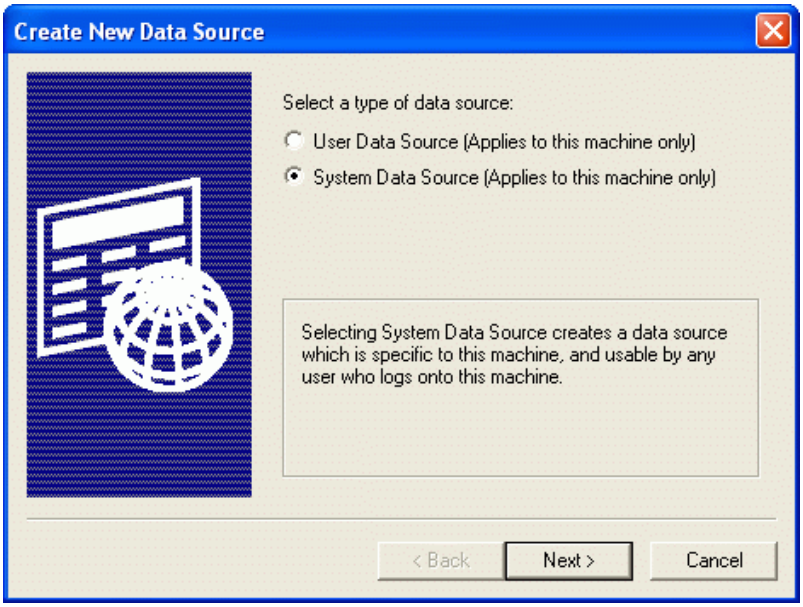
2. Haga clic en **Nuevo DSN** para abrir el diálogo de Seleccionar Fuente de Datos.



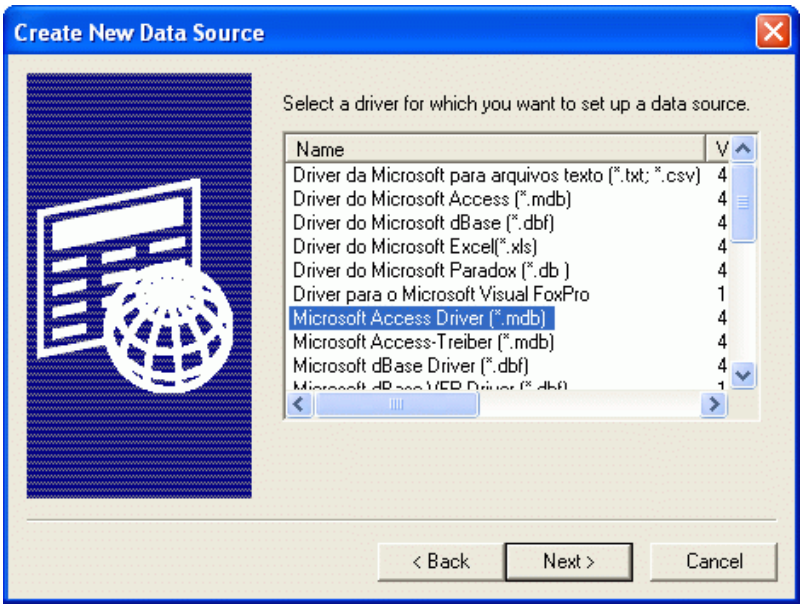
3. Cambie a la pestaña **Fuente de Datos de Máquina**, y haga clic en **Nuevo...** para abrir el diálogo de Crear Nueva Fuente de Datos.



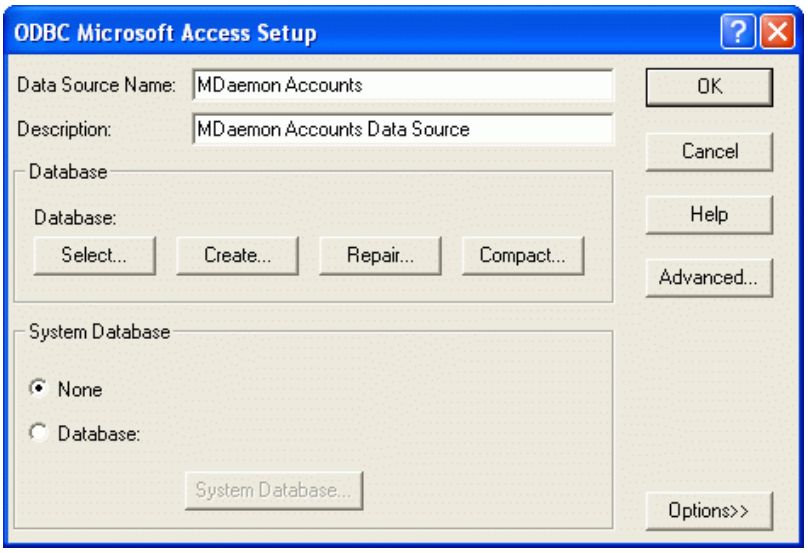
4. Seleccione **Fuente de Datos de Sistema**, y luego haga clic en **Siguiente**.



5. Seleccione el **manejador de base de datos** para el que desea configurar la fuente de datos y luego haga clic en **Siguiente**.



6. Haga clic en **Finalizar** para mostrar el diálogo de configuración específico de manejador. La apariencia de este diálogo estará basada en el manejador seleccionado (diálogo Microsoft Access Setup mostrado abajo).



7. Designe un **Nombre de Fuente de Datos** para su nueva fuente de datos y provea cualquier otra información requerida por el diálogo específico del manejador (tal como crear o especificar una base de datos, escoger un directorio o servidor, y demás).

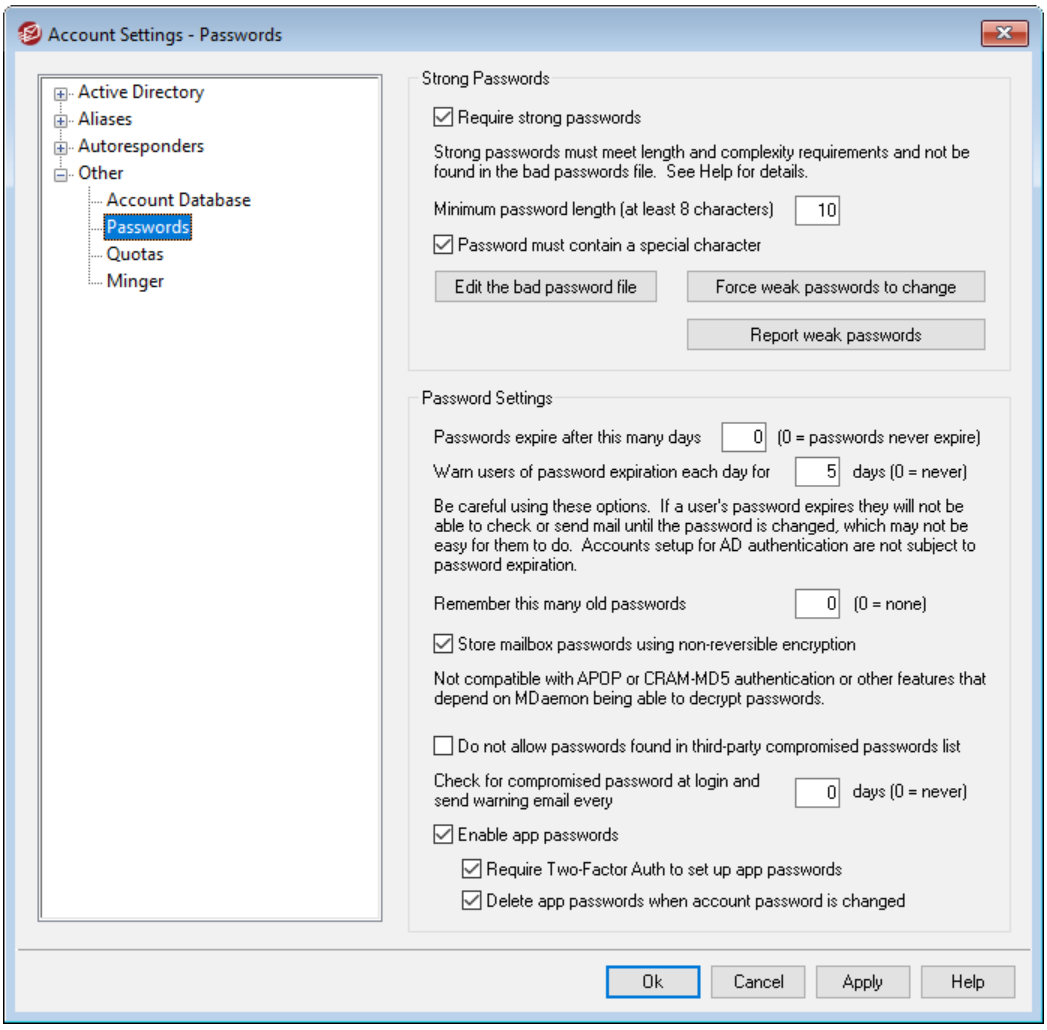
8. Haga clic en **Aceptar** para cerrar el diálogo específico del manejador.

9. Haga clic en **Aceptar** para cerrar el diálogo de Seleccionar Fuente de Datos.

Ver:

[Base de datos de Cuentas](#) 849
[Asistente de Selector de ODBC - Base de datos de Cuentas](#) 850

5.3.4.2 Contraseñas



Contraseñas fuertes

Requerir contraseñas fuertes
Por omisión, MDaemon requiere de contraseñas fuertes al crear cuentas nuevas o modificar contraseñas existentes. Deshabilite la casilla si desea eliminar este requerimiento.

Las contraseñas fuertes deben:
- Cumplir con la longitud mínima requerida
- Contener mayúsculas y minúsculas

- Contener letras y números.
- Contener un caracter especial (si se habilita la opción de caracteres especiales abajo)
- No contener el nombre del usuario o de su buzón
- No encontrarse en el archivo de contraseñas prohibidas

Longitud mínima de la contraseña (por lo menos 8 caracteres)
Utilice esta opción para definir la longitud mínima requerida para las contraseñas fuertes. Este se debe establecer en al menos 6 caracteres, pero se recomienda un valor mayor. El valor por omisión en instalaciones nuevas de MDaemon es de 10 caracteres. Si modifica esta opción no se detona automáticamente un requerimiento de cambio de contraseña para las contraseñas que no cumplan con el nuevo mínimo, pero cuando esos usuarios modifiquen su contraseña, se aplicará esta política.

Sin importar el mínimo establecido, las contraseñas pueden ser mayores de 72 caracteres cuando se habilita la opción "*Almacenar contraseñas de buzón utilizando encriptación no-reversible*". Si esa opción está deshabilitada, las contraseñas no podrán ser mayores de 15 caracteres.

Las contraseñas deben contener un caracter especial
Por omisión, para instalaciones nuevas de MDaemon, se requieren contraseñas fuertes conteniendo al menos uno de los siguientes caracteres especiales: !"#$% &'()*+,-./:;<=>?@[\]^_`{|}~. Deshabilite esta opción si no desea requerir caracteres especiales en las contraseñas fuertes.

Editar el archivo de contraseñas prohibidas
Dé clic en este botón para editar el archivo de contraseñas prohibidas. Los registros enlistados aquí son sensibles a mayúsculas/minúsculas y no se pueden utilizar como contraseñas. Si desea generar registros más complejos o versátiles, puede utilizar Expresiones Regulares 653 para hacerlo. Los registros que inician con "!" son tratados como Expresiones Regulares

Forzar el cambio de contraseñas débiles
Dé clic en este botón si desea forzar a todas las cuentas que tengan contraseñas débiles, a cambiarlas. Con esto se bloqueará a toda cuenta que tenga una contraseña débil hasta que la contraseña se modifique. La contraseña se puede modificar por el administrador vía la interface de MDaemon o un usuario bloqueado la puede modificar vía Webmail o la interface de administración remota. Cuando el usuario intente ingresar utilizando la contraseña anterior, se le requerirá crear una nueva antes de proceder. **Nota:** Esta opción no está disponible cuando se utiliza la opción de abajo "*Almacenar contraseñas de buzón utilizando encriptación no-reversible*".

Reportar contraseñas débiles
Dé clic en este botón para generar un reporte de todas las cuentas de MDaemon con contraseña débil. El reporte será enviado por correo a la dirección de correo que usted especifique luego de dar clic en OK. **Nota:** Esta opción no está disponible cuando se utiliza la opción de abajo "*Almacenar contraseñas de buzón utilizando encriptación no-reversible*".

Ajustes de Contraseña

Las contraseñas expiran luego de este número de días (0=las contraseñas nunca expiran)
Utilice esta opción si desea establecer un número máximo de días que una cuenta se puede utilizar antes de requerir que modifique su contraseña. El valor por omisión en esta opción es "0", lo que significa que las contraseñas nunca expiran. Pero si lo configura a, por ejemplo, 30 días, entonces el usuario tendrá 30 días para modificar su contraseña, **iniciando a partir de la última vez que se haya modificado la contraseña**. Por esto, cuando establezca inicialmente el valor de expiración, cualquier cuenta con contraseña que no haya sido modificada dentro del número de días especificado, tendrá su contraseña expirada de inmediato. Cuando expire la contraseña del usuario, no tendrá acceso vía POP, IMAP, SMTP, Webmail o Administración Remota. El usuario puede, sin embargo, conectarse a Webmail o a la Administración Remota donde se le requerirá que modifique la contraseña antes de proceder. Los clientes de correo tales como Outlook, Thunderbird y similares, no pueden utilizarse para modificar la contraseña. Más aun, muchos clientes ni siquiera mostrarán algún mensaje de ayuda a los usuarios, por lo que puede ser que requieran ayuda del administrador para saber por qué su contraseña está fallando.

Con el fin de que los usuarios puedan modificar sus contraseñas vía Webmail o Administración Remota, primero deben tener permisos en la opción "...editar contraseña" de la pantalla Servicios Web 798. Además, dado que modificar la contraseña puede no ser fácil o posible para algunos usuarios, deberá tener cuidado antes de utilizar esta opción.

Avisar a los usuarios sobre el vencimiento de su contraseña diariamente durante [xx] días (0 = nunca)
Las cuentas cuya contraseña está a punto de expirar, pueden recibir un recordatorio diario de que esto va a suceder y necesitan cambiarla. Utilice esta opción para definir el número de días previos a que expire la contraseña, que desea que MDaemon empiece a enviar estos mensajes.

Recordar este número de contraseñas anteriores (0=ninguna)
Utilice esta opción para especificar el número de contraseñas anteriores que quiera que MDaemon recuerde para cada usuario. Cuando os usuarios modifiquen sus contraseñas, no les permitirá utilizar las anteriores. Esta opción se encuentra deshabilitada por omisión con el valor "0".

Almacenar contraseñas de buzones utilizando encriptación no reversible
Marque esta casilla si desea que MDaemon almacene las contraseñas utilizando encriptación no-reversible. Esto impide que las contraseñas sean desencriptadas por MDaemon, el administrador o un posible atacante. Para hacer esto, MDaemon utiliza la función de hashing de contraseñas bcrypt, que permite manejar contraseñas más largas (hasta 72 caracteres) y permite que las contraseñas se preserven pero no sean reveladas al importar o exportar el catálogo de cuentas. Sin embargo, algunas funcionalidades no son compatibles con esta opción, tal como la detección de contraseñas débiles y la autentificación APOP & CRAM-MD5, porque dependen de que MDaemon pueda desencriptar las contraseñas. Las contraseñas no reversibles están habilitadas por omisión.

Contraseñas Comprometidas

MDaemon puede validar las contraseñas de usuario contra una lista de contraseñas comprometidas perteneciente a un servicio de terceros. Lo puede hacer sin transmitir la contraseña al servicio y si ésta se encuentra en la lista, esto no significa que la cuenta haya sido hackeada. Significa que alguien en algún lugar ha utilizado como contraseña la misma cadena de caracteres y esta ha aparecido en una brecha de datos. Las contraseñas publicadas pueden ser utilizadas por los hackers en ataques de diccionario, en cambio contraseñas únicas que nunca se han utilizado en otro lugar son más seguras. Ver Contraseñas para más información.

No permitir contraseñas que se encuentren en la lista de terceros de contraseñas comprometidas
Marque esta casilla si no desea permitir que se configure las contraseñas de las cuentas utilizando alguna que se encuentre en la lista de contraseñas comprometidas.

Verificar contraseñas comprometidas al inicio de sesión y envíe mensaje de advertencia cada [xx] días (0 = nunca)
Con esta opción, se puede verificar automáticamente la contraseña de cada usuario contra la lista de contraseñas comprometidas, cada cierto número específico de días, cuando el usuario inicia sesión. Si se está utilizando una contraseña comprometida, se enviará un mensaje de advertencia a la cuenta y al postmaster. Los mensajes de advertencia se pueden personalizar editando el archivo de plantilla de mensajes en la carpeta `\MDaemon\App`. Dado que las instrucciones para cambiar la contraseña pueden cambiar dependiendo de si la cuenta está utilizando una contraseña almacenada en MDaemon o con autentificación Active Directory 822, se cuenta con dos archivos de plantilla: `CompromisedPasswordMD.dat` y `CompromisedPasswordAD.dat`. Se pueden utilizar Macros para personalizar el mensaje, cambiar el asunto, cambiar los destinatarios y demás.

Contraseñas de Apps

Contraseñas de Apps 751 es una opción que se puede utilizar para hacer las cuentas más seguras creando contraseñas muy fuertes, generadas aleatoriamente para ser utilizadas solamente en clientes de correo y en apps de correo, dado que esas apps no pueden asegurarse con Autentificación de Dos Factores 720 (2FA). Ver: Contraseñas de Apps 751.

Habilitar contraseñas de apps
Todos los usuarios pueden crear por omisión Contraseñas de Apps para sus cuentas, al iniciar sesión en Webmail utilizando Autentificación de Dos Factores. Si desea deshabilitar el soporte a Contraseñas de Apps para un usuario en particular, lo puede hacer en la opción *...editar contraseñas de apps* 720 en la página de Servicios Web del usuario.

Requerir Autentificación de dos Factores para configurar contraseñas de apps
Por omisión, los usuarios deben iniciar sesión en Webmail utilizando Autentificación de Dos Factores 720 (2FA) con el fin de crear una nueva Contraseña de App. No se recomienda deshabilitar este requerimiento. Los Administradores Globales 757 están exentos de este requerimiento en MDRA, pero se recomienda que siempre utilicen 2FA al iniciar sesión en MRDA o en Webmail.

Eliminar contraseñas de apps cuando se modifica la contraseña de la cuenta
Por omisión, cuando se modifica la contraseña de una cuenta, todas las contraseñas de apps se eliminan y se requiere que el usuario genere nuevas si desea utilizarlas o se le requiere que las utilice si lo define el ajuste "*Requerir contraseñas de apps...*" (ver nota abajo).

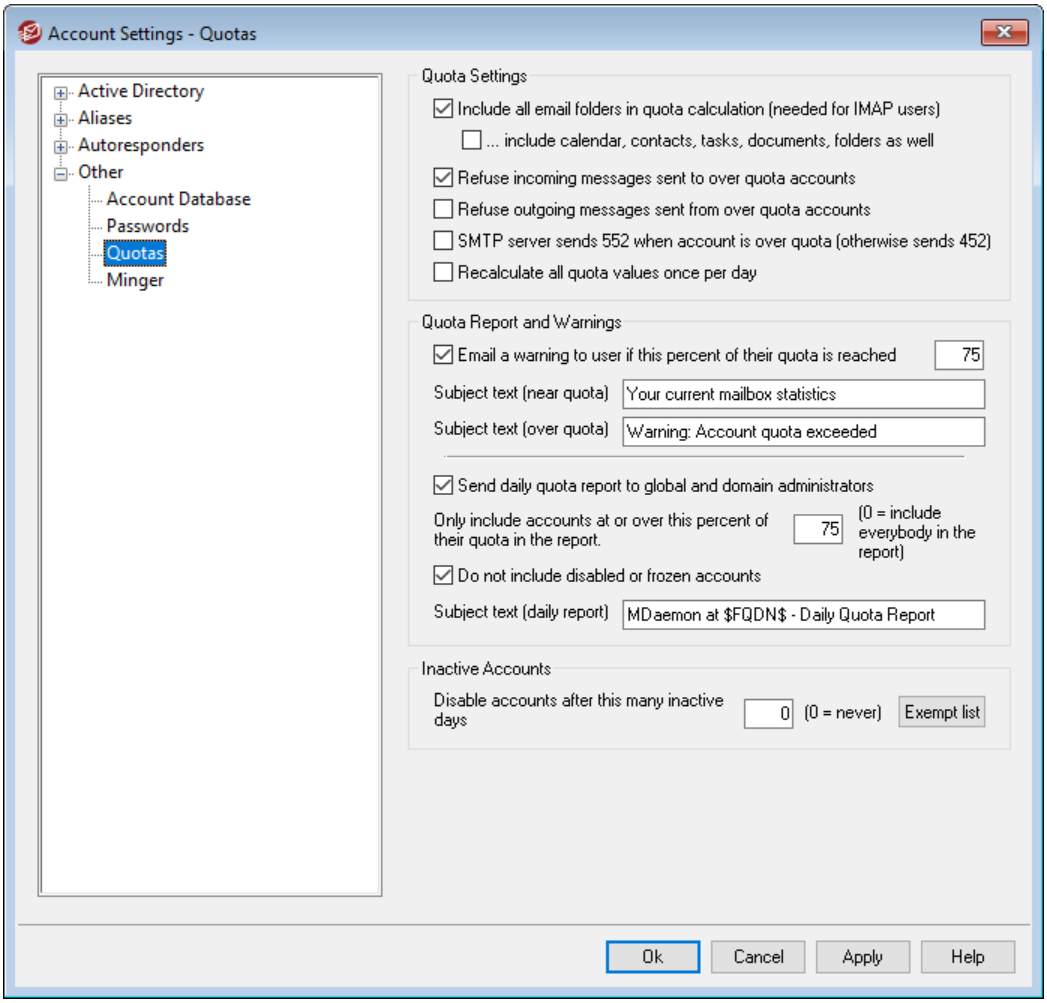
Existe una opción de cuenta en la página Ajustes del Editor de Cuentas 760 que puede utilizar para "*Requerir contraseña de app para iniciar sesión en SMTP, IMAP, ActiveSync, etc.*"

Requerir Contraseñas de Apps puede ayudar a proteger la contraseña de una cuenta de ataques de diccionario y fuerza bruta vía SMTP, IMAP, etc. Esto es más seguro porque aún si un ataque de este tipo adivinara la contraseña de la cuenta, no funcionaría y el atacante no lo sabría, dado que MDaemon solo aceptará la Contraseña de App correcta. Adicionalmente, si sus cuentas en MDaemon utilizan autentificación con Active Directory 822 y Active Directory bloquea las cuentas luego de un número de intentos fallidos, esta opción puede impedir que se bloqueen las cuentas, dado que MDaemon solo verificará las Contraseñas de apps y no intentará autentificar con Active Directory.

Ver:

Editor de Cuentas » Detalles de Cuentas 715
Editor de Cuentas » Servicios Web 720
Editor de Cuentas » Contraseñas de Apps 751
Expresiones Regulares 653

5.3.4.3 Cuotas



Ajustes de Cuotas

Incluir todas las carpetas de correo entrante en el cálculo de la cuota (se requiere para usuarios IMAP)

Cuando esta casilla está habilitada, todos los mensajes en todas las carpetas de correo en la cuenta del usuario se acumularán respecto a las limitaciones en número de mensajes o espacio en disco que tenga la cuenta. En otro caso, solamente los archivos de mensaje en la Bandeja de Entrada contarán para validación contra los límites. Esto generalmente solo se requiere para usuarios IMAP.

...incluir también las carpetas de Calendario, Documentos, Contactos, Tareas
Dé clic en esta caja si desea incluir todas las carpetas de calendario, contactos y tareas en el cálculo de la cuota.

Rechazar mensajes entrantes enviados a cuentas que han rebasado su cuota
Por omisión, cuando una cuenta tiene configurada una cuota del número de mensajes que puede recibir y este límite se ha alcanzado, MDaemon no aceptará ningún mensaje entrante dirigido a la cuenta hasta que el usuario elimine algo del correo almacenado en su buzón. Deshabilite esta casilla si no desea que se rechacen los mensajes entrantes dirigidos a cuentas que han rebasado su cuota.

Rechazar mensajes salientes enviados desde cuentas que han rebasado su cuota
Seleccione esta caja si desea que se rechacen los mensajes salientes enviados desde cualquier cuenta que ha alcanzado su cuota. Cuando una cuenta ha llegado al límite de su cuota, no podrá enviar correo hasta que se haya eliminado al menos una parte de sus mensajes almacenados. Esta opción esta deshabilitada por omisión.

El Servidor SMTP envía mensaje 552 cuando la cuenta sobrepasa la cuota (en otro caso envía un 452)
Por omisión, cuando la cuenta alcanza su cuota 733 MDaemon envía un error código 452 (i.e. "Requested action not taken: insufficient system storage") durante el proceso SMTP. Este código generalmente significa que el servidor podría reintentar más tarde. Verifique esta caja si desea enviar como alternativa el error de falla permanente código 552 ("Requested mail action aborted: exceeded storage allocation").

Recalcular todos los valores de cuotas una vez al día
Por omisión, los valores de cuotas en caché, solo se pueden restablecer cuando está habilitada y se envía la opción abajo "*Enviar el reporte diario de cuotas...*". Dé clic en esta casilla si usted prefiere que los valores de cuota se recalculen como parte de la rutina diaria de mantenimiento.

Avisos y Reportes de Cuotas

Enviar mensaje de advertencia al usuario si alcanza este porcentaje de su cuota
Si, durante el evento diario de mantenimiento y depuración 494, MDaemon determina que una cuenta excede el porcentaje ya sea del *Máximo número de mensajes almacenados* o *Máximo espacio en disco permitido* de acuerdo con la restricción de cuota definida en el Editor de Cuentas 733, se enviará un mensaje de advertencia a la cuenta. Utilice la opción que se describe abajo, *Texto del Asunto (cerca de cuota)* para definir el Asunto para este mensaje. El mensaje listará el número actual de mensajes almacenados, el tamaño del buzón, y el porcentaje usando y porcentaje restante. Además, si existe una alerta en el buzón de la cuenta, será reemplazada por un mensaje actualizado. Deshabilite esta opción si no desea enviar mensajes de aviso de cuotas a los usuarios. Siempre que se coloque un mensaje de advertencia en la Bandeja de Entrada de los usuarios, se crea una entrada en el registro del sistema para informarle esto. No se registra nada cuando el mensaje ya existe y solo se actualiza. Si se agrega una entrada una y otra vez, es indicación de que el usuario está eliminando el mensaje en su Bandeja de Entrada. Deshabilite esta opción si no desea enviar a los usuarios mensajes de advertencia de cuotas.

La Plantilla del Mensaje *Cerca de Cuota* (localizado en: MDaemon\app\NearQuota.dat) se utiliza para crear los mensajes de advertencia de que se está cerca de la cuota del usuario. Todas las macros relativas a cuentas de usuario (ej. $EMAIL$, $MAILBOX$, $DOMAIN$, etc.) se pueden utilizar en la plantilla.

Texto del Asunto (cerca de la cuota)
Este es el texto del Asunto del mensaje de advertencia enviado a los usuarios que exceden el porcentaje de cuota determinado arriba. Estos mensajes se

envían diariamente durante el evento diario de mantenimiento y depuración, lo que ocurre, por omisión, a media noche.

Texto del Asunto (sobre cuota)
Así como el mensaje de advertencia "cerca de la cuota", se enviará otro mensaje al usuario cuando su cuenta exceda la cuota. Este es el texto del Asunto del mensaje de advertencia "sobre cuota".

Enviar diariamente el reporte de cuotas a los administradores global y del dominio
Marque esta casilla y especifique un valor, si desea enviar diariamente un reporte de cuotas a los administradores global y del dominio. El reporte contendrá estadísticas de cuotas para todos los usuarios que se encuentran en y sobre el porcentaje determinado de uso sobre su cuota. Utilice "0" si desea que el reporte incluya estadísticas de todos los buzones.

N**o incluir cuentas deshabilitadas o congeladas**
Por omisión, los reportes de cuota no incluyen a las cuentas deshabilitadas o congeladas. Deshabilite esta casilla si desea incluirlas.

Texto del Asunto (reporte diario)
Utilice esta opción si desea personalizar el Asunto del reporte diario de Cuotas que envía MDaemon a los administradores. Vea `QuotaReport.dat` en la carpeta `MDaemon\APP` si desea personalizar el reporte mismo.

Cuentas Inactivas

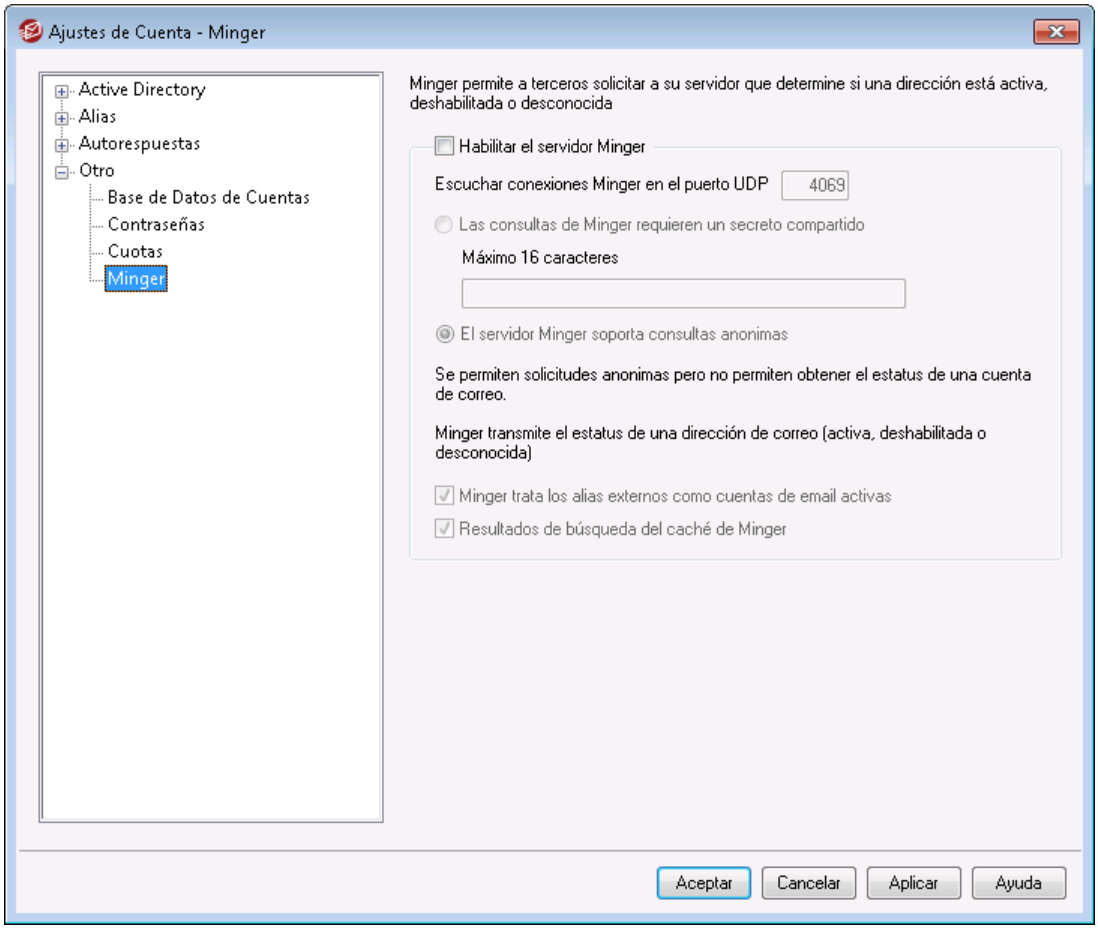
Deshabilitar cuentas después de XX días de inactividad (0=nunca)
Utilice esta opción si desea deshabilitar automáticamente las cuentas que han estado inactivas por más del número especificado de días. Una vez que se alcanza ese límite, la cuenta se deshabilita y se envía un mensaje al postmaster. Si se responde a ese correo la cuenta se puede rehabilitar. El procesamiento se realiza como parte del mantenimiento diario nocturno. El valor por omisión es 0 (deshabilitado).

Lista de Exentos
Las cuentas que se agregan a esta lista están exentas de la funcionalidad de deshabilitar cuentas inactivas.

Ver:

Editor de Cuentas » Cuotas 733
Valores por Omisión de Cuentas Nuevas » Cuotas 812

5.3.4.4 Minger



Ubicado bajo Cuentas » Ajustes de Cuenta, Minger es un protocolo de verificación de direcciones de correo creado por MDaemon Technologies. Originalmente basado principalmente en el protocolo Finger, Minger está creado principalmente para proveer de un mecanismo simple y eficiente de permitir a otros consultar su servidor para poder verificar si una dirección de correo es o no válida. Para mejor eficiencia Minger usa UDP en lugar de TCP, y para seguridad puede requerir autenticación—aunque soporta también las consultas anónimas. El diálogo de Minger se usa para habilitar/deshabilitar el servidor de Minger de MDaemon, designar el puerto que usará (por defecto 4069), y escoger si se debe o no requerir autenticación vía sistema de secreto compartido o permitir consultas anónimas.

MDaemon tiene también un cliente de Minger, que ha sido integrado en el sistema de Puertas de Enlace de Dominio (ver Verificación 264). Cada dominio para el que MDaemon está actuando de puerta de enlace o servidor de respaldo puede ser configurado para usar Minger para que MDaemon conecte al servidor remoto y verifique si los destinatarios de los mensajes entrantes para dichos dominios son o no válidos. Esto previene tener que asumir que todos los destinatarios son direcciones válidas.

Puede encontrar el último borrador del protocolo Minger en:

http://tools.ietf.org/html/draft-hathcock-minger-06

Servidor Minger

Habilitar el servidor Minger
Marque esta casilla para habilitar el servidor Minger de MDaemon.

Escuchar conexiones Minger en el puerto UDP
Este es el puerto en el que el servidor Minger escuchará las conexiones. La Internet Assigned Numbers Authority (IANA) ha reservado y asignado los puertos TCP y UDP 4069 para usar con los clientes y servidores Minger. No se recomienda cambiar este puerto puesto que ha sido reservado exclusivamente para uso de Minger.

Las consultas de Minger requieren un secreto compartido
Si desea requerir autenticación vía sistema de secreto compartido, escoja esta opción e introduzca una cadena de texto de al menos 16 caracteres. Cuando se escoge esta opción el servidor Minger rechazará consultas no autentificadas.

El servidor Minger soporta consultas anónimas
Escoja esta opción si desea soportar consultas de Minger anónimas—al cliente de conexión no se le requerirá autenticación antes de las consultas de verificación de direcciones. Esto es similar a lo que se puede conseguir ahora con fuentes que usan el comando `SMTP VRFY` o SMTP "call back" o "call forward", pero es mucho más eficiente y no da como resultado sesiones caídas de SMTP sobre TCP, registros log de SMTP llenos de sesiones caídas, y problemas similares inherentes a estos métodos.

Minger trata los alias externos como cuentas de correo activas
Cuando esta opción está marcada, Minger tratará los alias externos (alias que apuntan a direcciones externas) como si fueran direcciones activas conocidas. También, este comportamiento es forzado cuando una consulta viene de Security Gateway a MDaemon independientemente del estado de la configuración de esta opción.

Guardar en caché los resultados de búsquedas Minger

Por omisión MDaemon guardará en caché los resultados de las búsquedas Minger. Si no desea que se guarden, deshabilite esta opción.

5.4 Importar Cuentas

5.4.1 Importar Cuentas de un Archivo de Texto

Haga clic en la selección de menú Cuentas→Importando...→Importar cuentas desde un archivo de texto delimitado por comas... para acceder a esta funcionalidad de generación de cuentas. También puede llegar a ésta haciendo clic en el botón *Importar* del Administrador de Cuentas. Este es un método sencillo de importar y generar automáticamente cuentas de correo. MDaemon leerá un archivo de texto y generará nuevas cuentas de correo usando tan sólo el Nombre y Apellido del usuario. Si tiene cuidado de configurar correctamente sus cadenas de plantilla de cuentas (ver Plantillas de Cuentas Nuevas 792) puede generar cuentas únicas usando sólo el Nombre y Apellido, pero puede incluir también muchas otras opciones

específicas para configuraciones de usuario si quiere sobrescribir los valores predeterminados de la nueva cuenta. Todos los campos deben estar separados por comas.

Cada línea del archivo de texto delimitado por comas debe contener una sola entrada de usuario. La primera línea debe ser una línea base que de los nombres y secuencias de los campos en las líneas subsiguientes. Un archivo de ejemplo puede ser algo como esto:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"Michael", "Michael Mason", "C:\Mail\Michael\", N
```

Los nombres de campo en la línea de base son usados por MDaemon para determinar la secuencia de datos y para que puedan por lo tanto aparecer en cualquier orden. Cada uno de los nombres de campo debe estar entre comillas.

Todos los valores de "Cadena" deben estar entre comillas, y un valor de campo "boleano" será considerado falso a menos que el primer carácter sea: `y`, `Y`, `1`, `t`, o `T`.

Nombre, primer y segundo apellidos pueden ponerse en el nombre completo. Sin embargo, no se puede usar comas en ellos.

Después de usar el proceso de importación, MDaemon creará `TXIMPORT.LOG`, detallando los resultados de la importación y listando qué cuentas se han importado correctamente y cuáles han fallado. Las razones típicas de porqué una cuenta puede no haberse importado pueden incluir un conflicto con un buzón de cuenta existente, o información de directorio, un conflicto con un alias existente de una cuenta, o un conflicto con un nombre de lista de correo.

Vea la descripción de `MD_ImportUserInfo()` y `MD_ExportAllUsers()` dentro del archivo `MD-API.HTML` ubicado en su directorio `\API\`, para más información acerca de la asignación de campos.

Use los siguientes valores en la línea de base para asignar los campos de las cuentas de MDaemon:

Nombre del Campo	Tipo
MailBox	cadena
Domain	cadena
FullName	cadena
MailDir	cadena
Password	cadena
AutoDecode	booleano
IsForwarding	booleano

AllowAccess	booleano
AllowChangeViaEmail	booleano
KeepForwardedMail	booleano
HideFromEveryone	booleano
EncryptMail	booleano
ApplyQuotas	booleano
EnableMultiPOP	booleano
MaxMessageCount	entero
MaxDiskSpace	entero
FwdAddress	cadena
FwdHost	cadena
FwdSendAs	cadena
FwdPort	cadena
NTAccount	cadena
MailFormat	cadena
AutoRespScript	cadena
AutoRespProcess	cadena
AddToList	cadena
RemoveFromList	cadena
PassMessageToProcess	booleano
MaxUIDLCount	entero
MaxMessageSize	entero
RecurseIMAP	booleano
MaxInactive	entero
MaxMessageAge	entero
MaxDeletedIMAPMessageAge	entero
Comments	cadena
UserDefined	cadena

Ver:

Integración con Cuentas de Windows 866

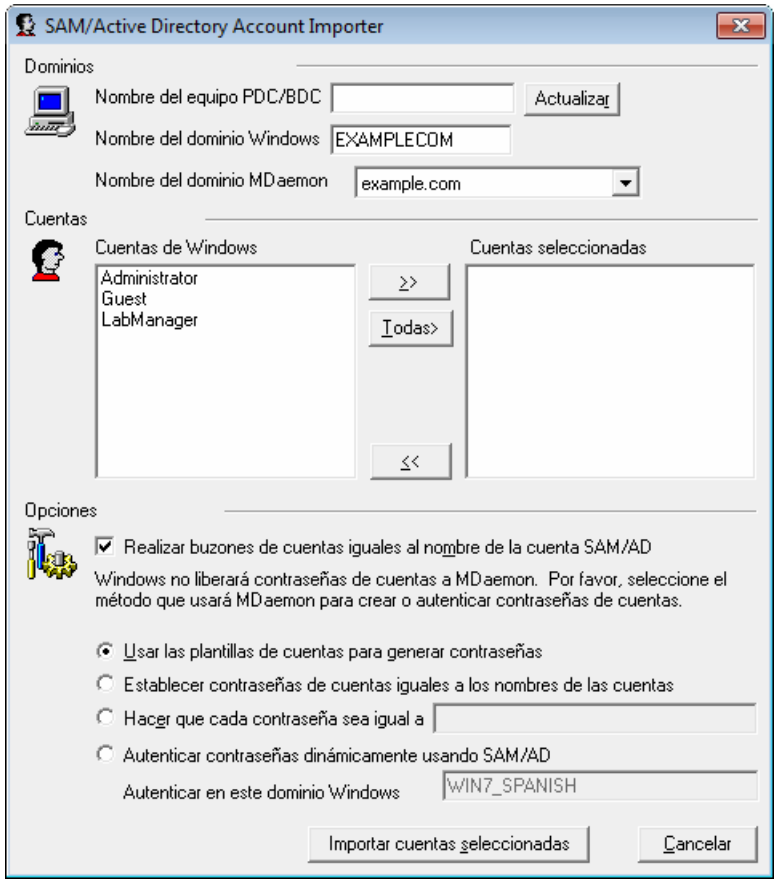
5.4.2 Integración con Cuentas de Windows

MDaemon soporta la integración con Cuentas de Windows. Este soporte consiste en un motor de importación SAM/Active Directory, al que puede llegarse desde el menú Cuentas de MDaemon (Cuentas→Importando...→Importar cuentas desde SAM/Active Directory...). Adicionalmente, el soporte para la autenticación de usuarios con Active Directory (AD), está integrado en el código de gestión de

usuarios de MDaemon. Es posible especificar un dominio de Windows en el campo de contraseña de la cuenta y luego MDaemon autentificará dinámicamente tales cuentas en tiempo real, usando el sistema de seguridad del dominio especificado de Windows. Bajo dicho esquema, si se cambia la contraseña de la cuenta en Windows la gestión de usuarios automáticamente actualizará MDaemon. Así pues, los usuarios sólo tendrán que recordar un conjunto de credenciales de autenticación. Esto también hace muy sencilla la configuración de cuentas para nuevas instalaciones.

El contexto de seguridad de la cuenta que ejecuta MDaemon debe tener el privilegio **SE_TCB_NAME** ("Actuar como parte del Sistema Operativo"). Si el proceso es un servicio que se ejecuta en una cuenta de *Sistema Local*, tendrá este privilegio por defecto. De otro modo, debe establecerse en la administración de usuarios de Windows para la cuenta bajo la que se esté ejecutando MDaemon.

Importación de Cuentas SAM/Active Directory



Dominios

Nombre del equipo PDC/BDC

Este campo le permite especificar el nombre de máquina desde el que MDaemon leerá la base de datos de cuentas de Windows. Puede especificar \\<DEFAULT> y MDaemon leerá los datos de la máquina local.

Actualizar

Haga clic en este botón para actualizar el listado de Cuentas de Windows.

Nombre del dominio Windows
Teclee el nombre de dominio de Windows desde el que desea importar cuentas.

Nombre del dominio de MDaemon
Escoja de la lista desplegable el dominio de MDaemon en el que las cuentas serán importadas.

Cuentas

Cuentas de Windows
Esta ventana contiene una lista de todos los nombres de cuenta recolectados de la base de datos de cuentas de Windows.

Cuentas seleccionadas
Esta ventana contiene todos los nombres de cuenta que ha seleccionado y que desea importar.

>>
Haga clic en este botón para mover los nombres de cuenta seleccionados desde la ventana "Cuentas de Windows" a la ventana "Cuentas seleccionadas".

<<
Haga clic en este botón para quitar las entradas marcadas de la ventana "Cuentas seleccionadas".

Opciones

Realizar buzones de cuentas iguales al nombre de cuenta SAM/AD
Haga clic en este interruptor para forzar que cada nombre de cuenta de usuario de Windows sea usado como valor de buzón. Con este método, no necesitará preocuparse de establecer las macros de Plantilla de Nueva Cuenta correctamente.

Usar las plantillas de cuentas para generar contraseñas
Esta opción hace que MDaemon genere contraseñas para las cuentas importadas usando las configuraciones de plantillas de las cuentas (Vea Valores Predeterminados).

Establecer contraseñas de cuentas iguales a los nombres de las cuentas
Esta opción hace que MDaemon use el nombre de cuenta como contraseña de cuenta.

Hacer que cada contraseña sea igual a...
Esta opción le permite especificar un valor de contraseña estática que será usado para todas las cuentas importadas.

Autenticar contraseñas dinámicamente usando SAM/AD
Esta opción permite la autenticación vía Active Directory (AD) de las cuentas importadas. En lugar de especificar una contraseña, MDaemon simplemente autentificará los valores de USER y PASS registrados en el cliente de correo usando la base de datos de NT en tiempo real.

Autenticar en este dominio Windows
Introduzca el nombre del dominio de Windows que MDaemon usará cuando autentifique conexiones dinámicamente. **Este no es el nombre de máquina del controlador de dominio. Es el nombre real del Dominio de Windows.**

Cuando las cuentas se configuran para autenticación AD, el nombre del dominio de Windows precedido de dos caracteres de barra invertida se usa en el campo `PASSWORD` de la cuenta y se almacena sin encriptar en el archivo `USERLIST.DAT`. Por ejemplo, si una cuenta se configura para autenticación AD en un dominio de Windows llamado `ALTN`, el campo de contraseña de la cuenta contendrá el valor `\\ALTN`. Los dos caracteres de barra invertida que preceden el nombre de dominio le indican a MDaemon que el campo de contraseña contiene el nombre del dominio de Windows y que MDaemon debería intentar autentificar los valores de USER y PASS proveídos por el cliente de correo usando la base de datos de cuentas de dicho dominio. Por dicha razón no debe empezar una contraseña con dos caracteres de barra invertida a menos que la cuenta esté configurada para autenticación AD según lo descrito anteriormente. En otras palabras, no puede tener contraseñas normales que empiecen por dos barras invertidas. Las contraseñas que empiezan con dos barras invertidas siempre se asume que provienen de un dominio de Windows y no de una contraseña.

Puede introducir la combinación de nombre de dominio de Windows y las dos barras invertidas en el campo de contraseña de cuenta en la pantalla Detalles de Cuenta 715 del Editor de Cuentas. No necesita restringirse a sí mismo a usar el importador para poder configurar las cuentas para autenticación dinámica.

Ver:

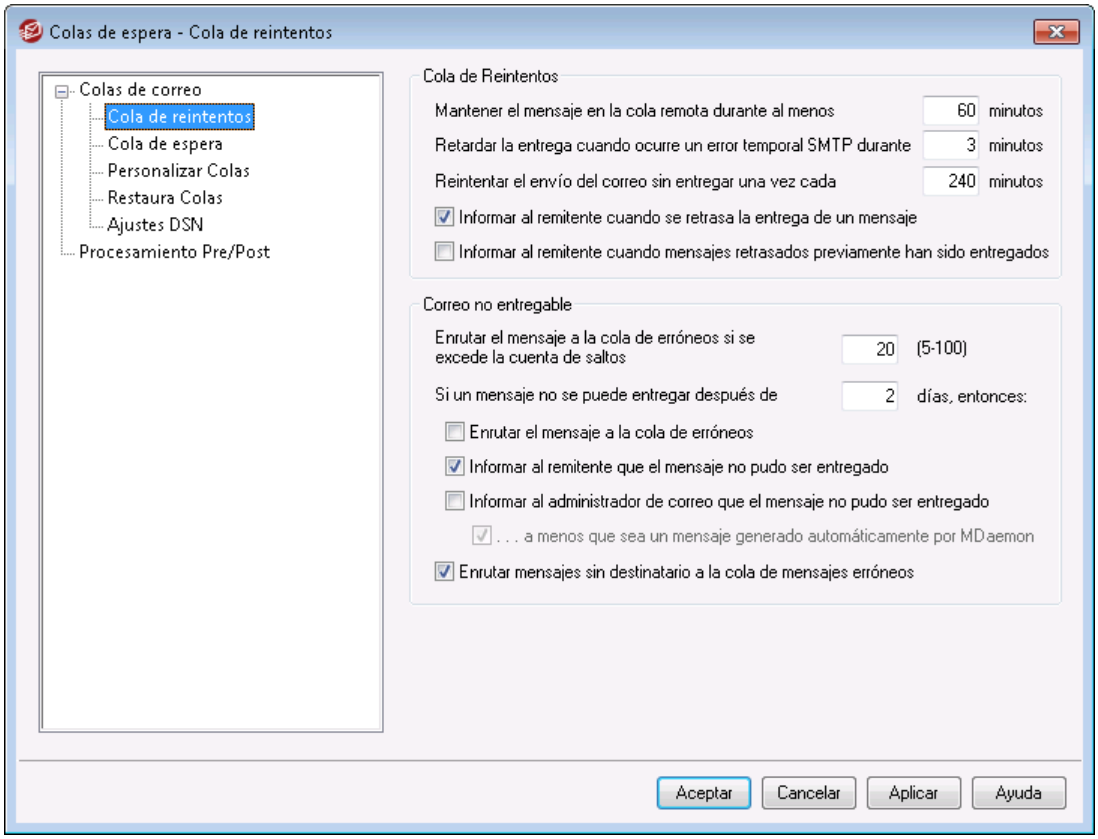
Importar Cuentas de un Archivo de Texto 864
Editor de Cuentas » Cuentas 715

Sección VI

6 Menú Colas

6.1 Colas de Correo

6.1.1 Cola de reintentos



El diálogo Cola de Reintentos, ubicado bajo Colas » Colas de Correo, se usa para determinar cómo manejará MDaemon los mensajes que no pueden ser enviados debido a algún error no-fatal, tal como cuando el servidor destino no está disponible temporalmente.

Cola de Reintentos

Mantener el mensaje en la cola remota durante al menos XX minutos
Esta configuración gobierna la longitud del tiempo que un mensaje permanecerá en la cola remota antes de ser eliminado y colocado en la cola de reintentos. La cola remota generalmente intentará enviar el mensaje con más frecuencia que la cola de reintentos.

Retardar la entrega luego de un error temp SMTP durante xx minutos
Cuando MDaemon se encuentra con un error temporal SMTP (4xx) al intentar entregar un mensaje, retardará los intentos subsecuentes para entregar el mensaje durante estos minutos. Esto ayuda a impedir que MDaemon intente entregar demasiado rápido el mensaje una y otra vez. Por omisión el retraso se configura en 3 minutos. Si desea deshabilitar el retardo, registro el valor en "0".

Reintentar el envío del correo sin entregar una vez cada XX minutos
Esta configuración determina con qué frecuencia se procesan los mensajes en la cola de reintentos.

Informar al remitente cuando se retrasa la entrega de un mensaje
Por omisión, MDaemon informará al remitente cuando un mensaje no pueda ser entregado debido a algún error temporal, que origine que el mensaje sea colocado en la cola de reintentos. Deshabilite esta casilla si no desea informar al remitente de este retraso.

Informar al remitente cuando son entregados mensajes retrasados previamente
Marque esta casilla si desea informar al remitente cuando un mensaje que se había retrasado haya sido entregado. Esta opción está deshabilitada por omisión.

Correo No Entregable

Enrutar mensaje a la Cola de Erróneos si el conteo de saltos excede (5-100)
Los estándares RFC establecen que un servidor de correo debe registrar en cada mensaje la hora en que es procesado. Estas marcas se pueden contar y utilizar como medida de control contra bucles recursivos de envío que en ocasiones pueden ser originados por configuraciones erróneas. Si no se detectan, estos ciclos de mensajes en reenvió consumirán muchos recursos. Al contar el número de veces que se han procesado los mensajes, pueden identificarse los que se encuentran en un bucle y colocarse en la cola de erróneos. Se asume que, si el mensaje no ha llegado a su destinatario luego de ser procesado por un número dado de servidores de correo, entonces existe probablemente un bucle de correo. Lo más probable es que la configuración por omisión de este control será suficiente para prevenir bucles de correo y no requerirá ser modificada.

Si un mensaje no se puede entregar después de xx días entonces:
Esta configuración determina el número de días que un mensaje puede permanecer en la cola de reintentos antes de ser eliminado. Si introduce "0" días en esta opción entonces el mensaje será rebotado de vuelta después del primer intento de reenvío. El parámetro por omisión es 2 días.

Enrutar el mensaje a la cola de mensajes erróneos
Cuando esta opción está habilitada, un mensaje será movido a la cola de mensajes erróneos una vez haya alcanzado el límite de tiempo establecido en la opción "*Si un mensaje no se puede entregar después de xx días entonces:*".

Informar al remitente que el mensaje no pudo ser entregado
Una vez que un mensaje ha alcanzado el límite de tiempo establecido en la opción "*Si un mensaje no se puede entregar después de xx días entonces:*", con esta opción se conseguirá que MDaemon envíe un mensaje DSN (Delivery Status Notification) 880 al remitente informándole que el mensaje ha sido permanentemente eliminado del servidor.

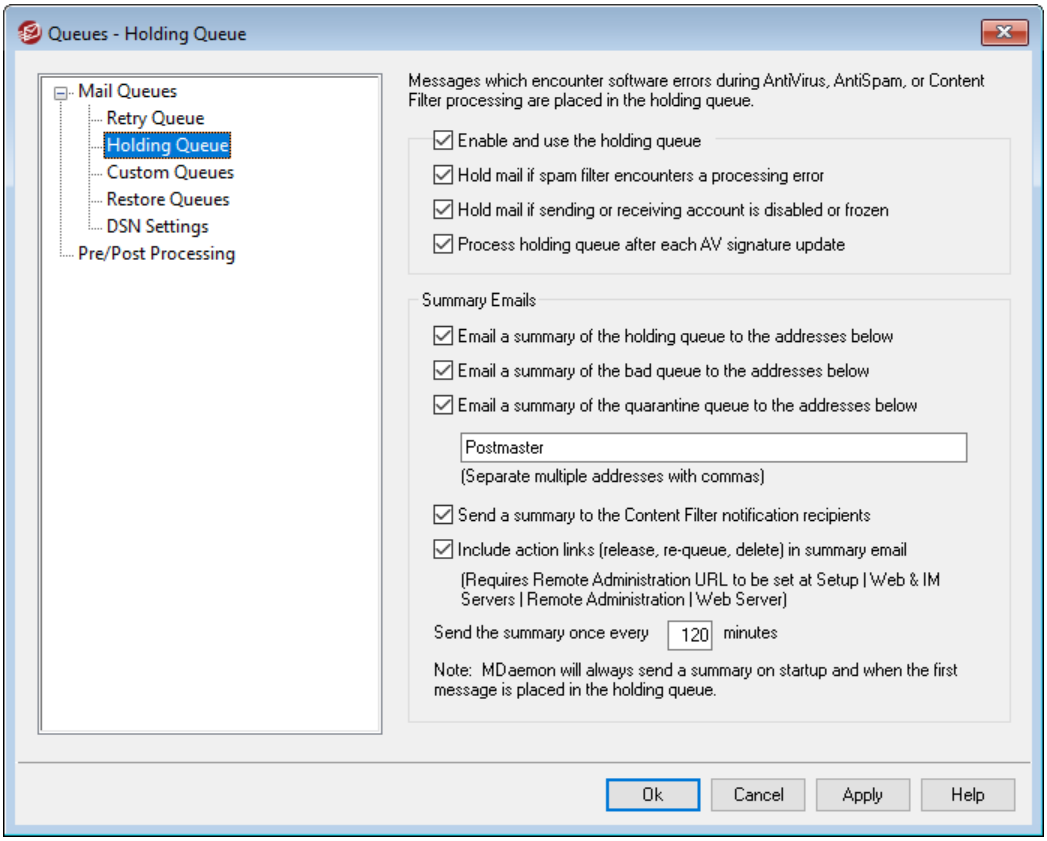
Informar al administrador de correo que el mensaje no pudo ser entregado
Si este control está habilitado, el postmaster será notificado cuando un mensaje haya sido eliminado permanentemente del sistema de reintentos.

. . . a menos que sea un mensaje generado automáticamente por MDaemon
Por defecto, el sistema de reintentos no informará al postmaster que un mensaje no pudo ser enviado cuando dicho mensaje sea autogenerado por MDaemon. Desmarque esta casilla si desea informar al postmaster acerca del fallo de dichos mensajes también. Ejemplos de mensajes autogenerados son notificaciones de recepción-devolución, mensajes generados por autorespuestas, resultados del procesamiento de cuentas, y demás.

...incluir el mensaje original al informar al remitente o al postmaster
Haga clic en esta opción para incluir el mensaje original como adjunto en los mensajes de fallo en el envío al remitente.

Enrutar mensajes sin destinatario a la cola de mensajes erróneos
Cuando está habilitada esta opción, los mensajes sin datos de destinatario serán movidos a la cola de mensajes erróneos. Al deshabilitarla, serán eliminados. Esta opción esta activa por omisión.

6.1.2 Cola de espera



La Cola de Espera, ubicada bajo Colas » Colas de Correo puede usarse para recibir mensajes que originen excepciones de software durante el proceso de Antivirus, AntiSpam o Filtro de Contenido. Si un error de software ocurre cuando se procesa un mensaje, éste será movido a la cola de espera y no será enviado.

Los mensajes colocados en la cola de espera se quedarán allí hasta que el administrador tome alguna acción para eliminarlos. Existe un botón de *Procesar Cola de Espera* en la barra de iconos de MDaemon y una opción idéntica en la barra de menú de Colas. Puede procesar también los mensajes haciendo clic-derecho en la cola de espera en la interfaz principal y luego seleccionando "Volver a poner en la cola" del menú de clic-derecho. Procesar la cola de espera moverá todos sus mensajes bien a la cola remota o local para el procesamiento normal de correo. Si el error que ha causado que el mensaje se colocara en la cola de espera sigue existiendo entonces dicho mensaje volverá otra vez a ella cuando el error vuelva a suceder. Si quiere intentar enviar los mensajes de la cola de espera independientemente de cualquier error que pudiera ocurrir, puede hacerlo haciendo clic-derecho en la cola de espera de la interfaz principal y seleccionando "Liberar" del menú de clic-derecho. Cuando se liberan los mensajes de la cola en espera, se abrirá un cuadro de confirmación para recordarle que los mensajes pueden contener virus o puede que no sea posible filtrarlos adecuadamente a través del Filtro de Contenido, AntiSpam y/o motor de Antivirus.

Cola de espera

Activar y usar cola de espera retenida
Haga clic en esta casilla para activar la cola en espera. Los mensajes que causen excepciones de software durante el proceso de Antivirus y Filtro de Contenidos serán movidos a esta cola siempre que ocurra un error.

Retener correo si el filtro de Spam encuentra un error de procesamiento
Haga clic en esta opción si desea mover a la Cola de espera los mensajes que causen errores durante el procesamiento de Filtro de Spam.

Retener correo si la cuenta que envía o recibe está deshabilitada o congelada
Cuando se habilita esta opción, MDaemon automáticamente retendrá los mensajes si la cuenta remitente o destino está deshabilitada o congelada.

Procesar la cola en espera después de cada actualización de firma AV
Cuando se habilite esta opción, la cola de espera será procesada automáticamente cada vez después de que las firmas de virus de Antivirus 645 se actualicen.

Mensajes Resumen

Enviar un resumen del contenido de la cola de espera a las direcciones siguientes
Si desea enviar a intervalos regulares un resumen de los mensajes contenidos en la cola de espera a una o más direcciones de correo, dé clic en esta opción y liste las direcciones en el espacio de texto indicado.

Enviar un resumen del contenido de la cola de erróneos a las direcciones siguientes
Si desea enviar un resumen de los mensajes contenidos en la cola de erróneos a una o más direcciones de correo a intervalos regulares, dé clic en esta opción y enliste las direcciones en el espacio de texto que se proporciona abajo.

Enviar por correo un resumen de la cola de cuarentena a las direcciones siguientes
Habilite esta opción si desea enviar un resumen de la cola de la cuarentena en el intervalo definido abajo.

Destinatarios de los mensajes de resumen
Utilice esta casilla para especificar las direcciones de correo a las que desea enviar Resúmenes del contenido de las colas seleccionadas en las dos opciones previas. Al listar direcciones múltiples, sepárelas con comas.

Los mensajes de notificación se envían al iniciar MDaemon, la primera vez que un mensaje se coloca en la cola de espera, y en el intervalo especificado en la opción siguiente *Enviar el resumen una vez cada XX minutos*.

Si un mensaje de notificación provoca un error de software puede que no sea enviado a los destinatarios remotos. Seguirá siendo, sin embargo, enviado a los destinatarios locales.

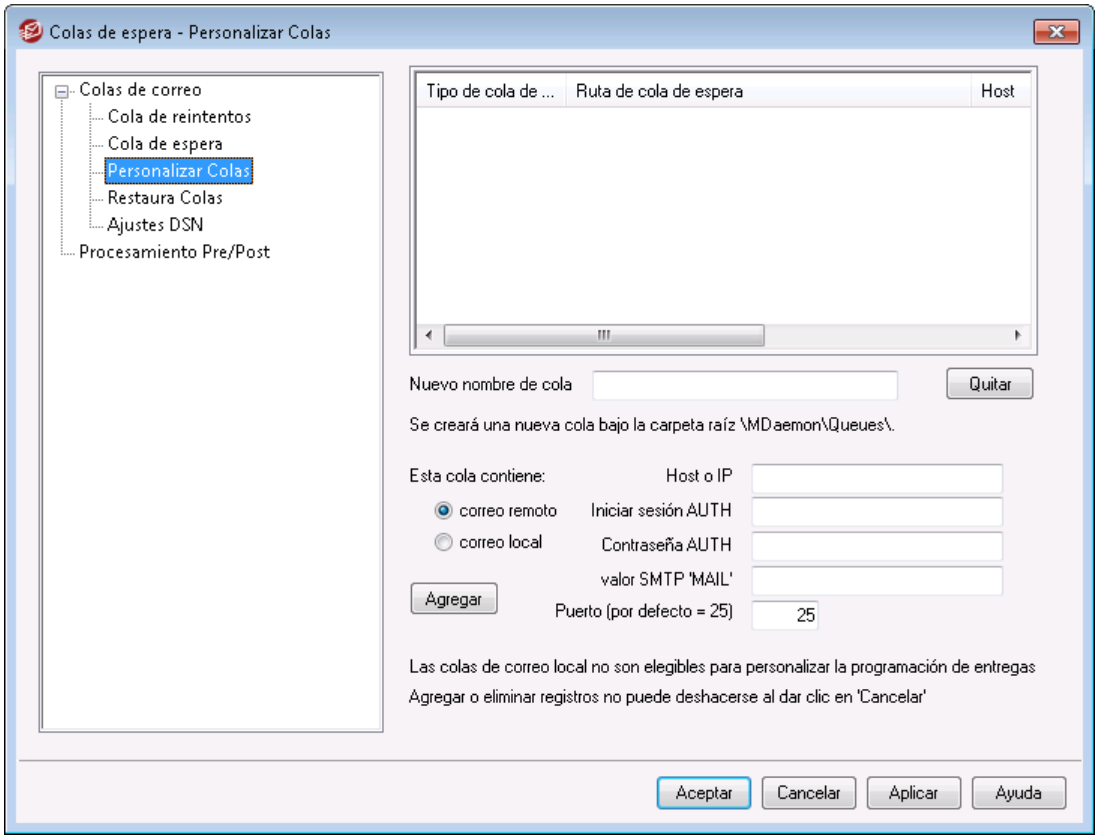
Enviar un resumen a los destinatarios de las notificaciones de Filtro de Contenidos
Haga clic en esta opción si quiere que una copia adicional de cada mensaje de notificación se envíe a los Destinatarios 665 designados del Filtro de contenido.

Incluir una liga de acción (liberar, re-encolar, eliminar) en el correo resumen
Por omisión, el correo resumen para las colas de espera, cuarentena y erróneos contiene ligas para liberar, re-encolar o eliminar cada mensaje. El correo resumen de la cola de erróneos contiene una liga adicional para eliminar todos los mensajes. Deshabilite esta opción si no desea incluir las ligas en los correos resumen.

A fin de que se generen las ligas, la URL de Administración Remota 356 debe estar configurada.

Enviar el resumen una vez cada XX minutos
Use esta opción para designar el número de minutos que pasará antes de que MDaemon envíe una notificación de mensaje en cola de espera a cada dirección especificada en los destinatarios de Filtro de Contenidos.

6.1.3 Personalizar Colas



Use el diálogo de Personalizar Colas bajo Colas » Colas de Correo para crear colas locales personalizadas y colas remotas de correo. El soporte a colas personalizadas hace posible que MDaemon monitoree diversas ubicaciones desde las cuales enviar correo. Puede crear nuevas colas y designarlas como locales o remotas, y puede luego usar las reglas de Filtro de Contenido para hacer que los mensajes sean automáticamente colocados en sus colas personalizadas, y para colas remotas puede usar el Programador de Eventos 380 para crear programaciones personalizadas para controlar con qué frecuencia se procesarán dichas colas.

Colas Personalizadas

Esta área muestra una entrada para cada cola personalizada, listando su ruta de archivo y si es local o remota.

Eliminar

Si desea eliminar una cola de la lista, seleccione su entrada y luego haga clic en el botón *Eliminar.*

> Cuando borra una cola personalizada, cualquier programador personalizado o regla de filtro de contenido asociada con ella también se eliminará.

Nuevo nombre de cola

Registre aquí el nombre de la nueva cola. La cola será creada en la carpeta `\MDaemon\Queues\` de MDaemon.

Esta cola contiene...

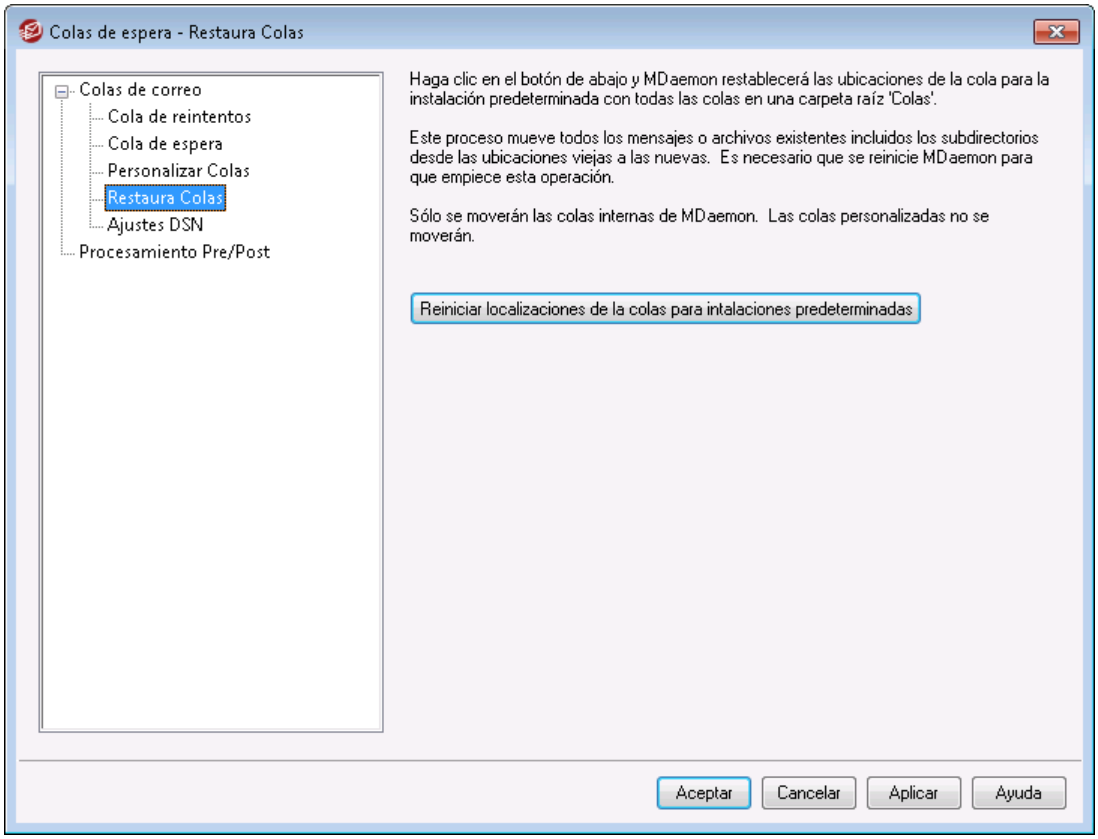
...correo remoto
Escoja esta opción si quiere que la cola de correo personalizada se use para el correo remoto.

Credenciales de la Cola
Puede especificar un *Host o IP*, *AUTH Logon/Contraseña*, valor *SMTP 'MAIL' y Port* para cualquier cola remota. Si se proporciona, todos los mensajes en la cola se entregan utilizando esos ajustes. Sin embargo, aun es posible en algunas circunstancias para mensajes individuales en la cola, que tengan sus propios valores de entrega únicos y si es así, esos datos tendrán prioridad sobre estos ajustes.El correo resumen de la cola de erróneos contiene una liga adicional para eliminar todos los mensajes. Deshabilite esta opción si no desea incluir las ligas en los correos resumen.

...correo local
Escoja esta opción si quiere que la cola de correo remoto se use para correo local. **Nota:** Las colas de correo local no son elegibles para programaciones personalizadas de entrega.

Agregar
Después de que haya escogido nombre y tipo para su cola, haga clic en el botón *Agregar* para añadirla a la lista de colas personalizadas.

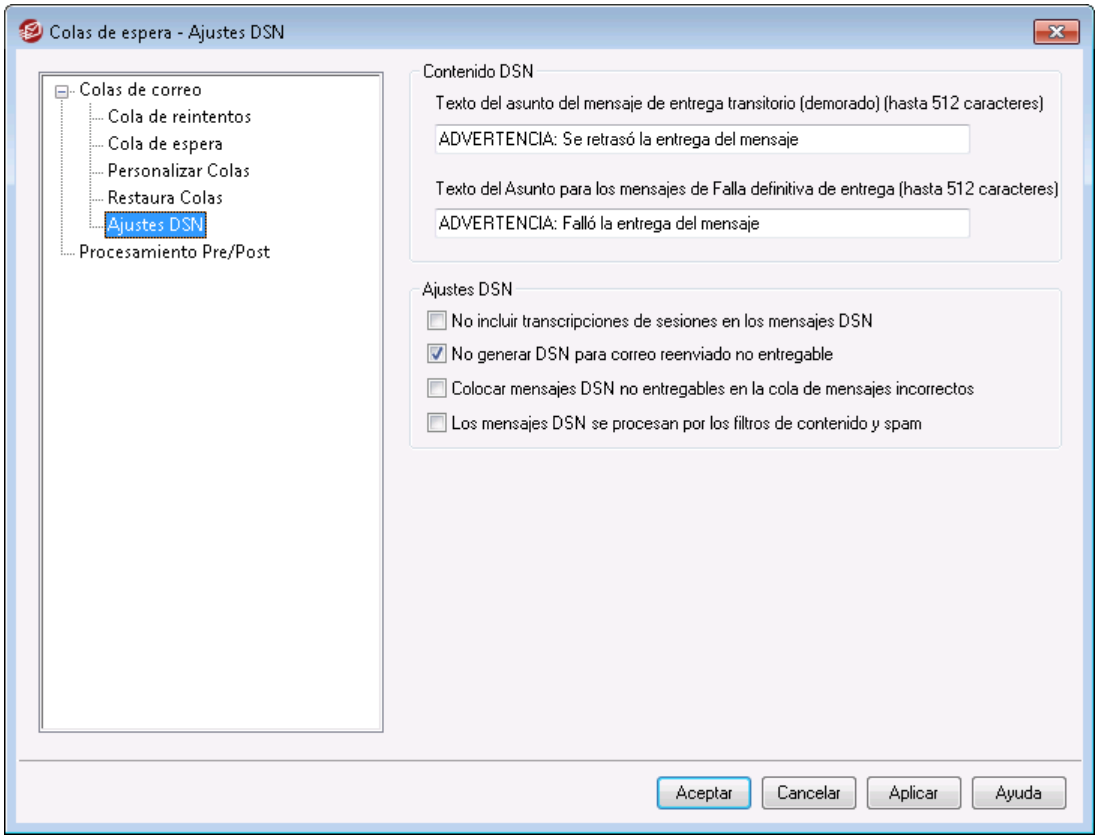
6.1.4 Restaurar Colas



Reiniciar ubicaciones de las colas para instalaciones predeterminadas
Por defecto, una nueva instalación de MDaemon almacena las colas de mensajes tales como Remota, Local, Raw y similares bajo la subcarpeta `\MDaemon\Queues\`. Las versiones previas de MDaemon almacenaban las colas en otras ubicaciones. Si su instalación de MDaemon utiliza las ubicaciones de carpeta antiguas y desearía mover sus colas a esta estructura más organizada haga clic en este botón y todas las colas y los archivos y mensajes que contengan serán movidos por usted. Después de hacer clic en este botón necesitará reiniciar MDaemon para que los cambios se apliquen.

Las Colas Personalizadas 877 no serán movidas por esta funcionalidad.

6.1.5 Ajustes DSN



Cuando MDaemon tiene problemas para entregar un mensaje, ya sea una falla temporal o permanente, se envía un Mensaje de Notificación de Estatus de envío (Delivery Status Notification: DSN) al remitente del mensaje. Esta pantalla contiene varias opciones relacionadas a esos mensajes DSN. Se localiza en Colas » Colas de Correo/DSN... » Ajustes DSN.

Contenido DSN

Texto del Asunto del mensaje de entrega transitoria (retrasada) (hasta 512 chars)
Este es el asunto del mensaje DSN que se enviará cuando se presente un problema transitorio que origine un retraso en la entrega del mensaje. Por ejemplo, si el servidor de correo del destinatario no está disponible cuando MDaemon intenta entregar el mensaje, MDaemon continuará intentando enviarlo en intervalos predeterminados y enviará este mensaje DSN informando al remitente del problema.

Texto del Asunto del mensaje de entrega fallida definitiva (hasta 512 chars)
Este es el asunto del mensaje DSN que se enviará cuando existe un problema que hace imposible que MDaemon entregue un mensaje. Por ejemplo, si el servidor de correo destino rechaza el mensaje porque la dirección del destinatario no existe, MDaemon dejará de intentar entregar el mensaje y enviará un mensaje DSN al remitente informando que no fue posible entregar su mensaje. Ver: Personalizar mensajes DSN 881.

Ajustes DSN

No incluir transcripciones de la sesión en los mensajes DSN
Dé clic en esta opción si no desea incluir la transcripción de la sesión SMTP con el error de entrega y los mensajes de advertencia. Esta opción esta deshabilitada por defecto.

No generar DSN para mensajes reenviados, no entregables.
Cuando esta opción se habilita, los mensajes reenviados que se encuentren con errores fatales, permanentes o que expiren en la Cola de Reintentos 872, se colocarán en la cola de mensajes erróneos, sin que se envíen mensaje DSN al remitente original. Esta opción está habilitada por omisión.

Colocar mensajes DSN no entregables en la Cola de Erróneos
Dé clic en esta casilla si desea colocar los mensajes de notificación DSN no entregables en la cola de mensajes erróneos en lugar de reintentar enviarlos.

Esto solo aplica a los mensajes DSN generados por MDaemon.

Los mensajes DSN se envían a través del filtro de spam y el filtro de contenido
Habilite esta opción si desea enviar mensajes DSN a través del filtro de contenido y el filtro de spam. Esta opción se encuentra deshabilitada por omisión.

Personalizar Mensajes DSN

La porción "legible para los humanos" de los mensajes DSN transitorios (retrasados) y permanentes (fallidos) se puede personalizar creando un archivo llamado `DSNDelay.dat` o `DSNFail.dat` respectivamente, en la carpeta `\MDaemon\App\`. Los puede crear con editor de texto tal como Bloc de Notas e ingrese el texto que desea utilizar. Se pueden utilizar las macros siguientes para personalizar el texto:

$SESSIONID$ - expande a la cadena del ID de la sesión de entrega

$QUEUEID$ - expande a la cadena del ID de la cola de correo del mensaje

$MESSAGEID$ - expande al valor del encabezado message-id

$RETRYDAYS$ - tiempo permitido en la cola (en días)

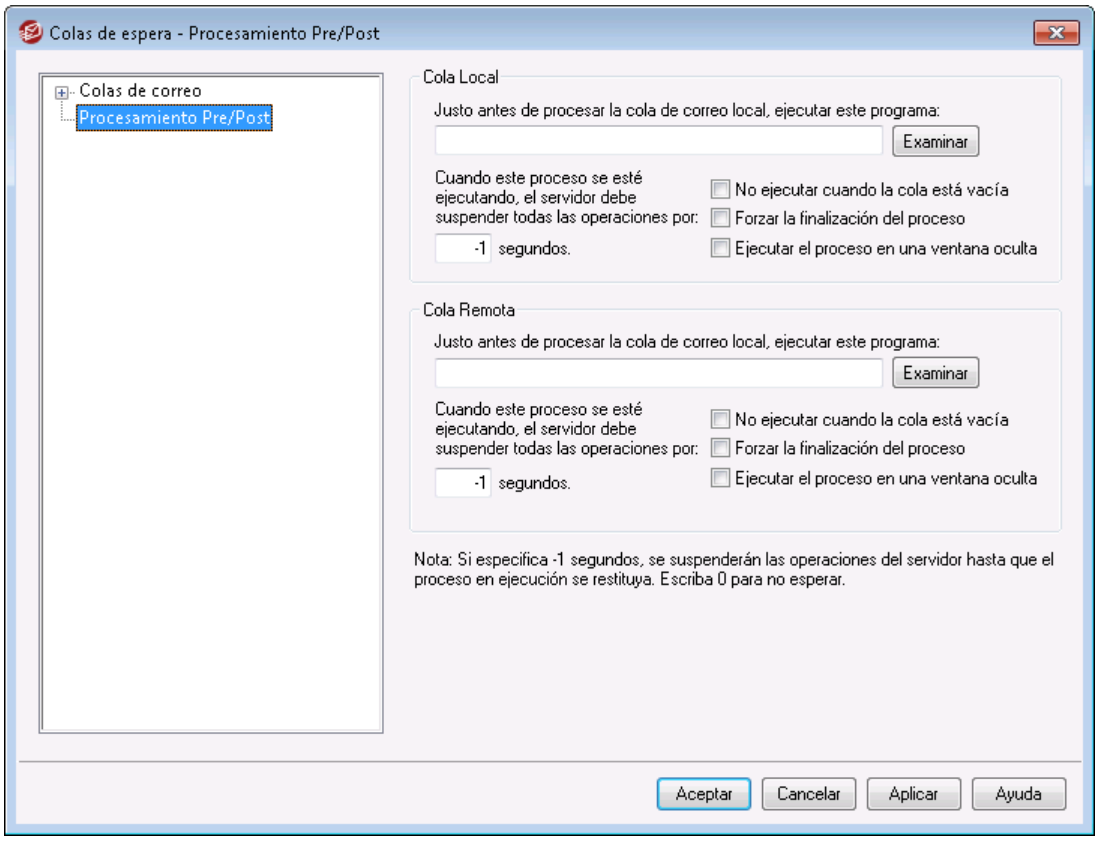
$RETRYHOURS$ - tiempo permitido en la cola (en horas)

MDaemon debe ser reiniciado antes de que se carguen las modificaciones a esos archivos.

Ver:

Cola de Reintentos 872

6.2 Procesamiento Pre/Post



Procesamiento Pre/Post de cola Local y Remota

Justo antes d procesar la cola de correo local, ejecutar este programa
Este campo especifica una ruta y nombre de programa que será ejecutado justo antes del proceso y envío de cualquier mensaje RFC-2822 que puedan estar en la cola local o remota. Si la información completa de ruta no se provee, MDaemon buscará primero ejecutables en el directorio de MDaemon, luego en el directorio de Sistema de Windows, luego en el directorio de Windows, y finalmente en los directorios listados en la variable de entorno PATH.

...suspender todas las operaciones por xx segundos
El valor introducido aquí determina cómo MDaemon se comportará mientras el programa especificado esté en progreso. MDaemon puede configurarse para parar su hijo de ejecución durante el número de segundos especificados mientras espera que el hilo de proceso regrese. Si el proceso regresa antes de que el número de segundos haya pasado, MDaemon seguirá su hilo de ejecución inmediatamente. Si introduce "0" en esta opción MDaemon no suspenderá sus operaciones en absoluto. Si entra "-1" hará que MDaemon espere hasta que el proceso regrese, no importa el tiempo que ello conlleve.

No ejecutar cuando la cola está vacía
Active esta opción si no quiere que el programa especificado se ejecute cuando la cola esté vacía.

Forzar la finalización del proceso
Algunas veces el proceso que necesita ejecutar puede que no termine por sí mismo. Este control hará que MDaemon force a la sesión a terminar cuando el

tiempo especificado en ...*Suspender todas las operaciones por xx segundos* haya pasado. Este control no funciona si el intervalo de tiempo está establecido en "-1".

Ejecutar el proceso en una ventana oculta
Haga clic en esta casilla si quiere que el proceso se ejecute en una ventana oculta.

6.3 Administrador de Colas y Estadísticas

El Administrador de Colas y Estadística de MDaemon está accesible desde dentro de MDaemon bajo la selección de menú Colas » Administrador de Colas y Estadísticas. El Administrador de Colas y Estadísticas está construido por un diálogo de cuatro páginas. Cada una de dichas páginas ha sido diseñada para servir a un propósito distinto y específico mientras que también mantienen un formato sencillo que las hace muy fácil de usar.

Página de cola 884

La pestaña por defecto es la *Página de cola*. Desde esta página puede gestionar fácilmente todas las colas de correo estándar de MDaemon, así como también las carpetas de buzón de Cuentas de Usuario. Simplemente haciendo clic en la cola o usuario de su elección, una lista de archivos de mensaje dentro de la cola especificada se mostrará juntamente con otras piezas clave de información pertinente sobre cada mensaje: el remitente, el destinatario, el contenido de la cabecera "Deliver-To" header, el asunto del mensaje, su tamaño, y durante cuánto tiempo ha estado en su ubicación actual. Adicionalmente, se provee de controles que hacen que resulte sencillo copiar o mover mensajes entre carpetas, o borrarlos completamente.

Página de usuario 887

La *Página de Usuario* muestra una lista de todos los usuarios de MDaemon. La lista incluye su nombre completo, nombre de buzón, número de mensajes en su buzón, la cantidad de espacio en disco que su cuenta está consumiendo, y la última fecha en la que comprobaron su correo. Esta lista también puede guardarse en disco como archivo de texto, o puede guardarse con formato delimitado por comas para uso con bases de datos.

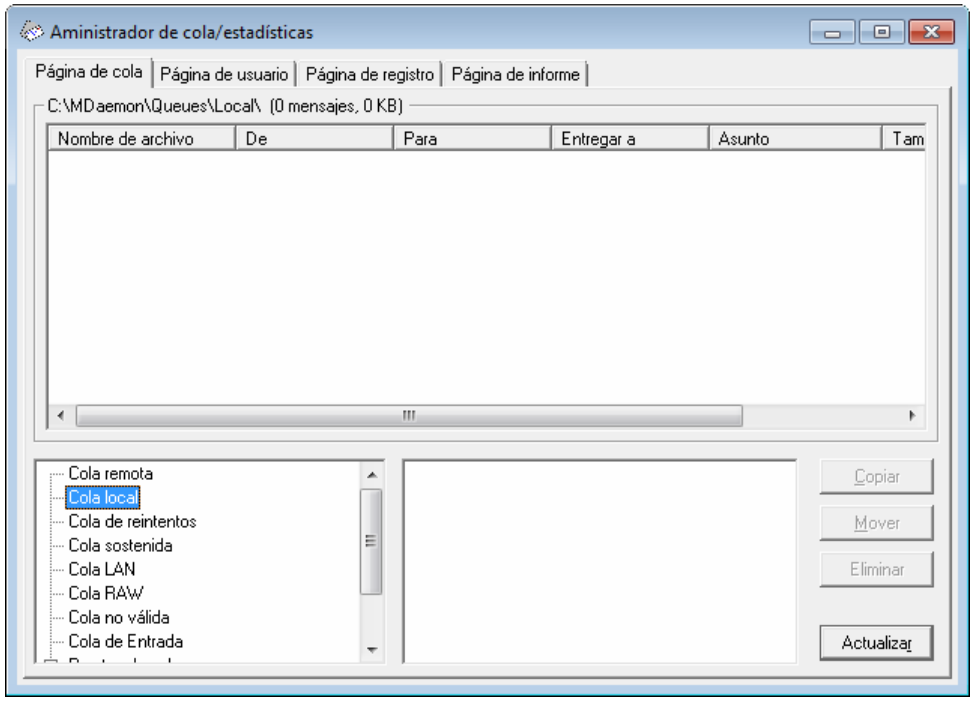
Página de registro 889

Con este diálogo puede mostrar los *Archivos de Registro* en un formato sencillo. Esta funcionalidad es muy útil para examinar rápidamente la historia de las transacciones de correo de MDaemon dado que condensa el *Archivo de Registro* seleccionado en una lista por columnas que contiene: el Tipo del mensaje (POP entrante, DomainPOP, RFC2822, y demás), el Host al que MDaemon se conectó durante la transacción, el remitente, el destinatario, el tamaño de mensaje, la fecha en la que cada mensaje fue procesado, y si la transacción fue o no correcta. También puede examinar la porción detallada de registro de cualquiera de las entradas en la lista haciendo doble-clic en la entrada deseada. Esto mostrará la porción del registro donde se hizo dicha transacción. Los registros mostrados en la *Página de Registro* pueden guardarse como archivo de texto o en formato delimitado por comas para uso con bases de datos.

Página de informe 891

La última pestaña es la *Página de Informe.* Con esta funcionalidad puede producir un informe que contiene todas las configuraciones de MDaemon, escritas en un formato legible de texto plano. Dado el gran número de configuraciones opcionales en MDaemon, esto puede acelerar notablemente el proceso de administrar cambios de configuración, así como también ayudar a diagnosticar posibles problemas de configuración. Adicionalmente este informe se muestra en un formato de texto editable que hace posible Copiar/Pegar la información que contiene (usando el menú de clic-derecho), o añadir anotaciones u otra información al archivo antes de guardarlo.

6.3.1 Página de colas



Cuadro de Lista de la Página de Cola

Cuando una cola o usuario es escogido del área de *Colas de mensajes* o el cuadro de lista de usuarios al lado de ésta, una lista de los archivos de mensaje contenidos en la cola seleccionada se mostrará en el cuadro de lista principal en esta página. Esta lista contiene cada nombre de archivo de mensaje, el remitente, el destinatario, el contenido de la cabecera "Deliver-To", el asunto del mensaje, su tamaño, y cuánto tiempo ha estado en su ubicación actual (listado por fecha y hora).

Encima de este cuadro se da la ruta de archivo al directorio mostrado actualmente, así como el número de mensajes mostrados y el tamaño del directorio.

Puede copiar, mover, o eliminar uno o más archivos seleccionándolos de la lista y luego haciendo clic en el botón apropiado bajo ésta.

El contenido de estos archivos puede ser también editado directamente desde el cuadro de lista *Página de Cola*. Simplemente haga doble-clic en el archivo que desea

editar (o escoja "Editar" del menú de clic-derecho) y el archivo se abrirá con el Bloc de Notas para edición.

Si quiere que el Administrador de Colas y Estadísticas abra un editor distinto a Bloc de Notas por defecto, entonces debe editar el archivo `mdstats.ini` ubicado en la carpeta `\MDaemon\app\`. Cambie la clave "`Editor=`" ubicada en la sección `[QueueOptions]` que apunte a `Editor=MyEditor.exe`. Si la ruta de archivo o el archivo `*.exe` no se encuentra en su ruta actual, entonces tendrá que incluir la ruta aquí como parte del nombre de archivo.

Este cuadro de lista puede navegarse usando las barras de desplazamiento horizontales, o puede hacer clic en cualquier lugar del cuadro de lista y usar las teclas de FLECHA para navegación. Puede ordenar la información contenida en el cuadro de lista *Página de Cola* por la columna que usted elija. Simplemente haga clic una vez en la columna deseada para ordenarla en orden ascendente (A-Z, 1-2), o haga clic dos veces para ordenarla en orden descendente (Z-A, 2-1). Las columnas también pueden redimensionarse posicionando el puntero encima de la línea entre cualquiera de las cabeceras de columna hasta que cambie su forma y luego arrastrando la columna a la anchura deseada.

Seleccionar Archivos

Para seleccionar archivos individualmente Haga clic en el archivo deseado.

Para seleccionar archivos contiguos Haga clic en el primer archivo de la lista de archivos contiguos que desea seleccionar, luego mientras pulsa la tecla SHIFT, haga clic en el último de los archivos contiguos en la lista deseada.

Alternativamente, puede usar las teclas FLECHAS, INICIO, FIN, RE PAG, Y AV PAG, mientras pulsa la tecla SHIFT, para seleccionar archivos en orden contiguo.

Para seleccionar archivos no-contiguos Haga clic en los archivos deseados en la columna **Nombre de Archivo** mientras mantiene presionada la tecla CTRL.

Colas de mensajes
Haga clic en el panel izquierdo inferior y una lista de los archivos contenidos en la cola especificada se mostrarán en el cuadro de lista *Página de Cola.* Si hace clic en la opción *Carpetas de Usuarios*, se mostrará una lista de todos los usuarios de MDaemon en el *Cuadro de Lista de Usuarios* a la derecha de la sección de *Colas de Mensajes.*

Cuadro de lista de usuarios
Este cuadro muestra una lista de todos los usuarios de MDaemon cuando se le dé clic a la opción *Carpetas de Usuario* en la sección de *Colas de Mensajes* (panel inferior izquierdo). Haga clic en un nombre de usuario para mostrar una lista de todos los archivos de mensaje contenidos actualmente en la carpeta de buzón del usuario.

Actualizar
Dado que las colas de correo son dinámicas mientras MDaemon esté activo - con archivos de mensaje constantemente siendo transferidos de y hacia ellas - debería hacer clic regularmente en este botón para actualizar cualquier lista de archivos que quiera tener mostrados.

Puede editar el archivo `MDstats.ini` para hacer que se refresquen automáticamente las listas mostradas. Para hacer esto simplemente abra el archivo `MDstats.ini` ubicado en el directorio de MDaemon `\app\` y edite la clave AutoRefresh bajo la cabecera `[QueueOptions]` para reflejar el número de segundos que desea dejar pasar entre actualizaciones. Si entra el valor "`0`" significa que no desea que la lista se refresque automáticamente. Ejemplo: `AutoRefresh=15` (la lista se refrescaría cada 15 segundos).

Copiar
Cuando uno o más archivos están seleccionados, haga clic en este botón para copiar los archivos seleccionados a otra cola o carpeta de buzón de usuario. Después de hacer clic en este botón se abrirá el diálogo de *Copiar Mensaje(s),* del que puede seleccionar la ubicación deseada a la que desea copiar los archivos seleccionados.

Mover
Cuando uno o más archivos están seleccionado, haga clic en este botón para copiar los archivos seleccionados a otra cola o carpeta de buzón de usuario. Después de hacer clic en este botón se abrirá el diálogo de *Mover Mensaje(s),* del que puede seleccionar la ubicación deseada a la que desea mover los archivos seleccionados.

Los archivos copiados o movidos a otras colas raramente retendrán los nombres de archivo originales. Para evitar sobrescribir archivos con el mismo nombre que puede que ya existan en la cola, MDaemon calcula siempre el siguiente nombre de archivo de destino basándose en el archivo `HIWATER.MRK` ubicado en la carpeta de destino.

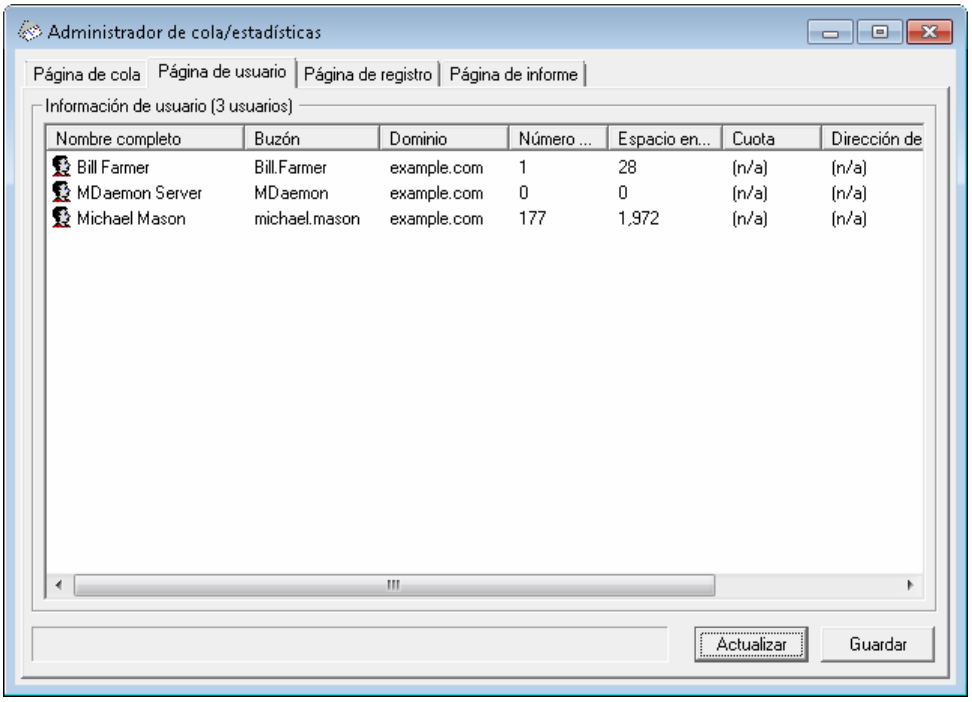
Eliminar
Cuando uno o más archivos están seleccionados en el *Cuadro de Lista de Estatus de Cola*, haga clic en este botón para eliminar el archivo seleccionado. Después de hacer clic en este botón aparecerá un cuadro de confirmación preguntando si desea realmente eliminar los archivos seleccionados.

Las colas de correo son dinámicas mientras MDaemon está activo, con los archivos de mensajes siendo constantemente transferidos de y hacia ellas. Por esta razón debería tener en cuenta que cuando copia, mueve, o eliminar archivos puede encontrarse a veces con un mensaje indicando que la acción que intenta realizar no se ha podido completar. Esto ocurre cuando el archivo de

mensaje con el que está intentando trabajar ya ha sido quitado por MDaemon antes de que la acción deseada empezara. Si hace clic en el botón *Actualizar*, puede actualizar la lista actual de archivos mostrados en el cuadro de lista.

Puede prevenir que los mensajes sean movidos fuera de su cola mientras los está editando cambiando el archivo `MDstats.ini`. Para hacerlo, simplemente abra el archivo `MDstats.ini` ubicado en el directorio de MDaemon `\app\` y cambie la clave `LockOnEdit=No` bajo la cabecera `[QueueOptions]` a `LockOnEdit=Yes`. Esto hará que se cree un archivo `LCK` siempre que esté editando un mensaje, lo que evitará que sea movido fuera de la cola hasta que haya acabado con él.

6.3.2 Página de usuario



Información de usuario
Cuando se escoge la *Página de usuario*, se cargará una lista de todas las cuentas de MDaemon en el cuadro de lista de *Información de usuario.* Esta lista contiene cada nombre complete de usuario, el nombre de su buzón, el dominio al que la cuenta pertenece, el número de mensajes que contiene, su formato de correo, la cantidad de espacio en disco (en kilobytes) que la cuenta está ocupando, su dirección de reenvío, y finalmente, la fecha en la que comprobaron por última vez el correo. Dado que la información en esta lista cambia constantemente, puede ser recargada de manera sencilla haciendo clic en el botón *Actualizar*.

Este cuadro de lista puede navegarse usando las barras de desplazamiento horizontal o vertical, o puede hacer clic en cualquier sitio de la lista y usar las teclas de FLECHA para la navegación. Puede ordenar la información contenida en la lista de *Información de usuario* por la columna que escoja. Simplemente haga clic una vez en la columna deseada para ordenarlo en orden ascendente (A-Z), o haga clic dos veces para ordenarlo en orden descendente (Z-A). Las columnas también pueden redimensionarse posicionando el puntero encima de la línea entre los encabezados de columna hasta que cambie su forma y luego arrastrando la columna al ancho deseado. Además, puede hacer doble-clic en cualquier entrada y MDStats cambiará a la *Página de Cola* con los contenidos de la carpeta del buzón mostrados.

Por defecto, la lista muestra la Cuenta de Mensajes no la de archivos, y el Espacio en disco usado *por mensajes* y no el espacio usado por todos los archivos en el directorio. Esta es la información de *Cuota* reportada por MDaemon. Alternativamente, puede mostrar el contador de *archivos* y el espacio en disco usado por todos los *archivos* en lugar de mensajes. Para cambiar esta configuración simplemente abra el archivo `MDstats.ini` ubicado en el directorio de MDaemon `\app\` y cambie la clave `ShowQuota=Yes` bajo la cabecera `[UserOptions]` para que apunte a `ShowQuota=No`.

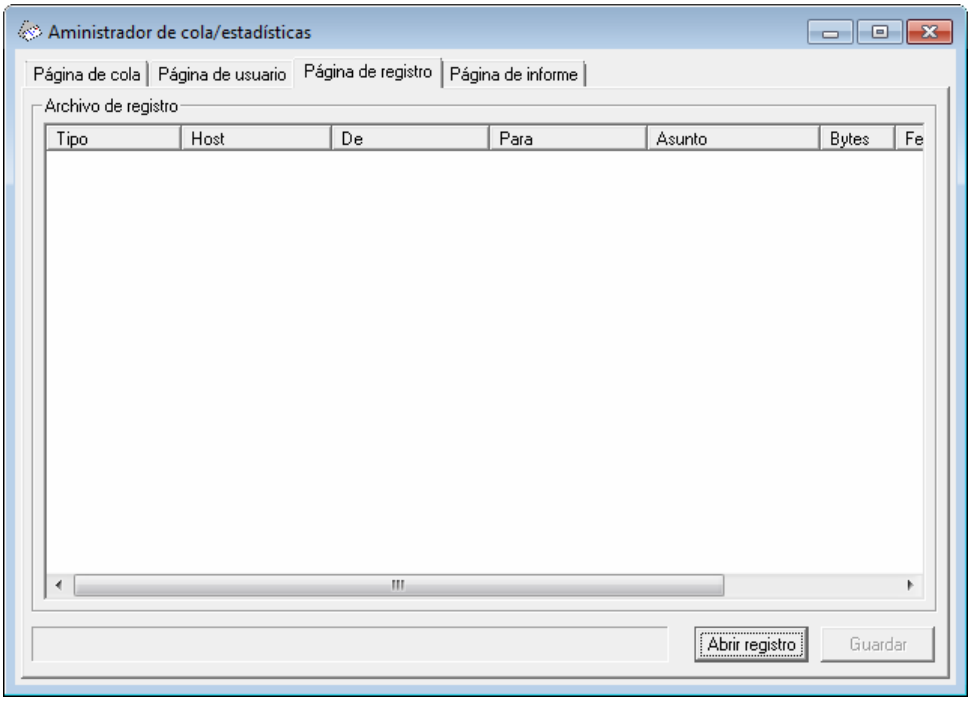
Las carpetas de usuario contienen un archivo llamado "`hiwater.mrk`" que se usa para determinar algo de la información de este usuario. Debería evitar eliminar este archivo innecesariamente puesto que prevendrá al Administrador de Cola y Estadística de poder obtener alguna de la información listada en el cuadro de lista *Información de Usuario.*

Actualizar
Las estadísticas de usuario tales como el número de mensajes contenidos en sus buzones, y la cantidad de espacio en disco que sus cuentas están usando, están cambiando constantemente. Puede actualizar fácilmente la información contenida en la lista de *Información de Usuario* haciendo clic en el botón *Actualizar*. Esto hará inmediatamente que toda la información mostrada sea la actual.

Indicador de progreso
Dado que las listas de *Información de Usuario* pueden a veces ser muy grandes, bajo la lista de *Información de Usuario* existe una barra de indicador de progresos que provee indicación visible de que el programa sigue operando cuando se están cargando archivos grandes.

Guardar
La información contenida en la lista de *Información de Usuario* puede guardarse como un archivo de formato delimitado por comas para uso con bases de datos, o como un archivo ASCII de texto plano haciendo clic en el botón *Guardar*. Después de escoger un nombre y una ubicación de archivo en el diálogo de Windows Guardar como, le será preguntado si quiere guardar el archivo en formato delimitado por comas o como un archivo de texto plano.

6.3.3 Página de registro



Página de registro
El cuadro de lista de *Informe de Registro* muestra los registros detallados de MDaemon que seleccione a través del botón *Abrir Registro* y el diálogo de Abrir de Windows que le sigue. La pantalla de *Informe de Registro* da una manera sencilla y fácil de revisar el historial de las transacciones de correo que MDaemon ha procesado sin tener que navegar a través de un gran volumen de información que algunas veces contienen los archivos de registro de MDaemon. Cuando un *Informe de Registro* se muestra en esta lista, el Administrador de Cola y Estadísticas lo reduce a un formato sencillo que contiene: el Tipo de mensaje (POP Entrante, DomainPOP, RFC2822, y demás), el Host al que MDaemon conectó durante la transacción, el remitente, el destinatario, el tamaño del mensaje, la fecha en la que se procesó cada mensaje, y si la transacción tuvo o no éxito.

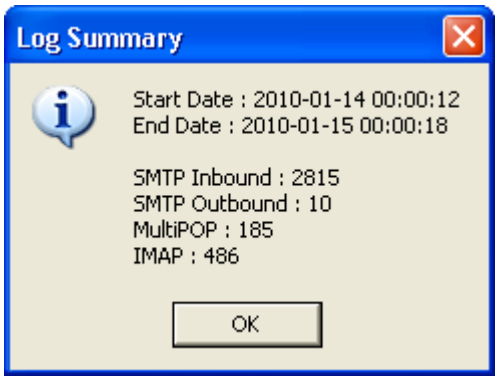
También puede examinar la porción detallada del registro acerca de cada una de las entradas de la lista haciendo doble-clic en la entrada deseada. Esto mostrará la porción del registro donde se realizó la transacción. Usando el menú de acceso directo de clic-derecho puede copiar/pegar esta porción detallada de registro en un editor de texto para guardarlo o editarlo si deseara hacerlo.

Este cuadro de lista puede navegarse usando las barras de desplazamiento horizontal y vertical, o puede hacer clic en cualquier sitio dentro del cuadro de lista y usar las teclas de FLECHA para navegar. Puede redimensionar las columnas del cuadro de lista posicionando el puntero encima de la línea entre dos encabezados de columna cualesquiera hasta que cambie su forma y luego arrastrar la columna al ancho deseado.

La *Página de Registro* mostrará los archivos de registro que han sido compilados usando la opción *Registrar las sesiones de correo detalladas* o la opción *Registrar las sesiones de correo resumidas* bajo Logueo » Modo de Registro. Sin embargo, recomendamos que use la opción *Registrar las sesiones de correo detalladas*. Cuando use la opción de formato *Registrar las sesiones de correo resumidas* encontrará que es muy poca la información mostrada en su *Informe de Registro*. Dado que la *Página de Registro* en si misma condensa el registro detallado en una vista resumida de la actividad de MDaemon, mientras que sigue proveyendo la habilidad de mirar en la vista detallada de cada transacción cuando sea necesario (haciendo doble-clic en la entrada), no es necesario hacer que MDaemon resuma el archivo de registro mientras lo compila.

Abrir Registro
Haga clic en este botón para abrir el diálogo de Abrir de Windows para escoger qué archivo de registro desea visualizar. Si hace clic en este botón cuando hay un *Archivo de Registro* ya mostrado en la lista de *Informe de Registro*, se le dará la opción de añadir el nuevo archivo al que ya está siendo mostrado.

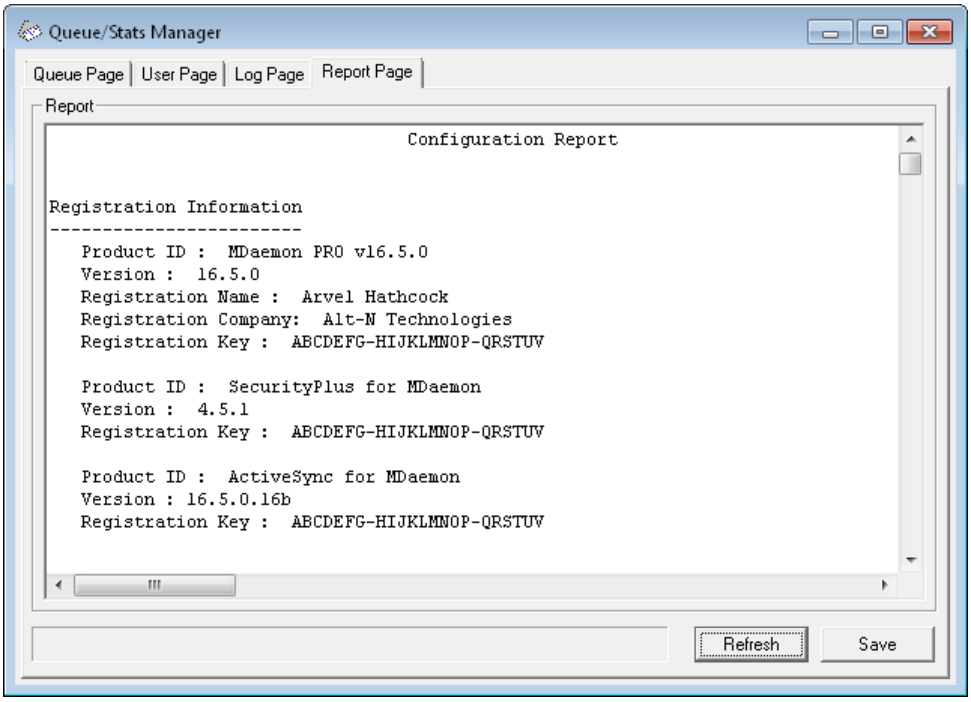
Después de que se muestre un registro, un cuadro de mensaje se abrirá conteniendo un resumen del registro seleccionado. Cuando guarde un Informe de Registro como archivo de texto, este resumen de registro se añadirá a él.



Indicador de Progreso
Dado que los *Archivos de Registro* pueden ser muy grandes, bajo la lista del *Informe de Registro* existe una barra de indicador de progreso que provee de una indicación visible de que el programa sigue operando cuando se están cargando o guardando archivos grandes.

Guardar
La información contenida en la lista de *Informe de Registro* puede guardarse como archivo en formato delimitado por comas para uso con bases de datos, o como archivo ASCII de texto plano haciendo clic en el botón *Guardar.* Después de escoger un nombre y ubicación para este archivo en el diálogo Guardar como de Windows, se le preguntará si desea guardar el archivo en formato delimitado por comas o como archivo de texto plano.

6.3.4 Página de informe



Informe
Cuando se hace clic en la *Página de Informe,* un informe a exhaustivo se producirá y listará todas las configuraciones de MDaemon en texto fácilmente legible. Esta funcionalidad reduce considerablemente el tiempo necesario para un administrador para comprobar las muchas configuraciones de MDaemon, y puede ayudar a resolver de manera rápida posibles problemas de configuración.

Puede navegar a través de este informe usando o bien las barras de desplazamiento o bien las teclas de CURSOR, y el *Informe* es también un editor de texto - haciendo posible insertar anotaciones o información adicional que puede querer en el informe antes de guardarlo en un archivo. Adicionalmente, puede usar el menú de acceso directo para Cortar, Copiar, y Pegar de y a esta pantalla haciendo clic-derecho en su ratón y realizando la selección deseada del menú que se abre.

Actualizar
Haga clic en este botón para actualizar el *Informe* mostrado actualmente de las configuraciones de MDaemon.

Indicador de Progreso
Al igual que en las otras pestañas del Administrador de colas y Estadísticas, la *Página de Informe* contiene una barra de indicador de progreso que sirve como indicador visible que el programa sigue operando mientras se guardan o cargan archivos grandes.

Guardar
Haga clic en este botón para guardar el *Informe* mostrado actualmente. Después de hacer clic en este botón se abrirá un diálogo estándar de Guardar como para que pueda designar un nombre de archivo y ubicación donde quiere guardarlo.

6.3.5 Personalizar el Administrador de Colas y Estadística

6.3.5.1 Archivo MDStats.INI

Personalizar el Administrador de Colas/Estadística

La siguiente es una lista de configuraciones que pueden ser modificadas en el archivo `MDstats.ini` ubicado en el directorio de MDaemon `\app\`.

[MDaemon]

AppDir=C:\MDaemon\app\	Ubicación del directorio \app\ de MDaemon.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor a usar cuando se realiza doble-clic en un mensaje, o cuando a un mensaje se le hace clic-derecho y luego se selecciona Editar.
LockOnEdit=No	Si se debe o no crear un archivo LCK cuando se edita un mensaje. Esto evitará que el mensaje de ser movido de una cola mientras está siendo editado.
AutoRefresh=Yes	Tiempo (en segundos) en que se refresca la lista de mensajes. 0 significa que no se refresca.
ShowDirectories=Yes	Muestra subdirectorios de las colas en el cuadro de lista además de los mensajes. Los directorios aparecerán como <NombreDirectorio>.

[UserOptions]

ShowQuota=Yes	Determinar si el listado de usuarios muestra la información de cuota (la cuenta de mensajes y espacio en disco tal cual MDaemon la calcula) o la información de archivos (número de archivos y espacio total en disco).

[LogOptions]

ShowUnknown=Yes	Muestra sesiones que MDStats no pudo determinar si fueron de entrada o de salida, SMTP, o POP.
ShowSmtpInbound=Yes	Muestra sesiones de SMTP entrantes.
ShowPopInbound=Yes	Muestra sesiones de POP entrantes (comprobaciones de correo).
ShowSmtpOutbound=Yes	Muestra sesiones de SMTP salientes.

ShowPopOutbound=Yes	Muestra sesiones de POP salientes (MultiPOP, DomainPOP).
ShowRFC822=Yes	Muestra envíos de correo locales RFC822.
ShowSmtpHelo=Yes	Para las sesiones de SMTP entrantes, muestra el dominio HELO en la columna de Host.
IgnoreEmptyPop=Yes	Ignora las comprobaciones de correo cuando no se ha enviado correo.
ShowImap=Yes	Muestra sesiones IMAP.
[Remap]	Remapea la letra de la unidad para ejecutar MDStats desde una máquina diferente de la que MDaemon está usando.
C:=\\server\c	Cuando se lea desde MDaemon.ini, reemplace "C:" con "\\server\c".
[Special]	
OnlyOneInstance=No	Permitir que se ejecute una sola instancia de MDStats. Intentar abrirlo nuevamente activará la instancia que ya se esté ejecutando.

Ver:

Parámetros de Línea de Comandos de MDStats 893

6.3.5.2 Parámetros de Línea de Comandos de MDStats

Nota: Todos los parámetros de línea de comandos no son sensibles a mayúsculas.

Números 1 al 8	Muestra una cola especificada en la Página de Colas. = Cola Remota = Cola Local = Cola de Reintentos = Cola LAN = Cola RAW = Cola errónea = Cola SmtpIn = Cola Guardar

/L[N] [InputFile] [OutputFile]	Produce un informe de registro. Especificando "N" después de "L" significa que no se guarda como archivo delimitado por coma.
/A	Si produce un archivo de registro, añade la nueva información en el archivo de salida en lugar de sobrescribirlo.

Sección

7 Funcionalidades Adicionales de MDaemon

7.1 MDaemon y Archivos de Texto

MDaemon usa un número de archivos de texto para almacenar algunos de sus datos, plantillas de mensaje generadas por el sistema, y configuraciones, que proveen una gran flexibilidad. Puede crear nuevos archivos de texto desde dentro de MDaemon usando la selección de menú Archivo » Nuevo. Esto puede ser útil para crear rápidamente archivos de datos para uso con Respuestas Automáticas u otras funcionalidades de MDaemon, tal como los archivos RAW.

Editar Archivos de MDaemon

Los diversos archivos de datos de MDaemon son archivos de texto plano y pueden editarse en el Bloc de Notas. Puede abrir fácilmente cualquiera de estos archivos desde dentro de MDaemon usando la selección de menú Archivo » Abrir » Archivo de Texto vacío. Por defecto esto busca en la carpeta de MDaemon `\app\` archivos `*.txt`. Cambie la lista desplegable *Files of Type:* a "All files" para ver el resto de archivos contenidos en dicha carpeta.

7.2 Control Remoto del Servidor via Correo

Muchas funciones de MDaemon pueden ser accesadas de manera remota utilizando el sistema mismo de transporte de correo, enviando un mensaje formateado especialmente a la cuenta de sistema MDaemon, "`MDaemon@<MDaemon's Domain>`". Los mensajes enviados al servidor se almacenan en el directorio de mensajes del servidor tal como si fuera cualquier otro usuario.

Algunos de estos mensajes de control requieren de una cuenta válida en el servidor. Para aquellos comandos que requieren una cuenta válida, el mensaje debe ser autentificado durante el procesamiento SMTP utilizando SMTP AUTH.

Se tienen dos categorías generales de comandos que pueden utilizarse en mensajes de correo electrónico: Listas de Distribución y 897 Correo General 899.

Ver:

Listas de Distribución 897
Controles Generales de Correo 899

7.2.1 Control de Listas de Distribución y Catálogos

Ninguno de estos comandos requiere de una cuenta en el servidor. Los parámetros contenidos en paréntesis cuadrados son opcionales. Por ejemplo: "nombre[dirección]" puede registrarse como "Michael" únicamente o con agregando el parámetro opcional usuario1@ejemplo.com". Los mensajes deberán ser enviados a "mdaemon[MDaemon domain]" con cada comando y parámetros asociados contenidos en una sola línea en el cuerpo del mensaje.

COMANDOS	PARÁMETROS	DESCRIPCIONES

SUBSCRIBE	nombre de lista [dirección] [{nombre real}] [(contraseña)]	El remitente es añadido a los miembros de la lista especificada si la lista existe y permite suscripciones. Si una dirección opcional se especifica después del nombre de la lista entonces la dirección se añadirá a los miembros de la lista en lugar de la dirección encontrada en el campo FROM: del mensaje de suscripción. Un nombre real puede añadirse para el suscriptor incluyéndolo entre llaves (p. ej.{Fran Vazquez}. Si la contraseña de la lista sigue a este comando (se requieren paréntesis alrededor) entonces el comando será respetado aun y cuando la suscripción a la lista esté desactivada.
		Ejemplos:
		`SUBSCRIBE list@example.com`
		`SUBSCRIBE list@example.com me@example.com {Bill F}`
		`SUBSCRIBE list@example.com you@example.org (PASS)`

UNSUBSCRIBE O SIGNOFF	nombre de lista [dirección] [(contraseña)]	El remitente es eliminado de los miembros de la lista especificada siempre que la lista exista y contenga al remitente como miembro actual. Si se especifica una dirección opcional después del nombre de la lista entonces esa será la dirección eliminada de la lista en lugar de la encontrada en el campo FROM: del mensaje de desuscripción. Si la contraseña de la lista acompaña a este comando (se requieren paréntesis alrededor) entonces el comando será respetado incluso si la función de desuscripción de la lista está apagada. Ejemplos:

		`UNSUBSCRIBE list@example.com (listPASS)` `SIGNOFF list@example.com me@example.com`

`DIGEST`	lista [dirección]	El remitente se establece para recibir correo de la lista en formato resumen. Si se especifica una dirección opcional después del nombre de la lista entonces dicha dirección se establecerá en modo resumen.
		Ejemplos:
		`DIGEST list@example.com`
		`DIGEST list@example.com user1@examp`

`NORMAL`	nombre de lista [dirección]	El remitente se establece para recibir correo de "list" en modo normal. Si se provee una dirección opcional después del nombre de la lista entonces dicha dirección se establecerá en formato normal en lugar del remitente.
		Ejemplos:
		`NORMAL list@example.com`
		`NORMAL list@example.com user1@altn.`

`NOMAIL`	nombre de lista [dirección]	Este comando establece 'dirección' en modo sin correo. Esta cuenta entrará en estado suspendido y no recibirá más tráfico de lista. Si no se especifica dirección entonces el remitente del mensaje será usado. Ejemplo: `NOMAIL list@example.com me@example.`

`MAIL`	nombre de lista [dirección]	Este comando devuelve 'address' al modo normal desde el modo sin correo. Si no se especifica dirección entonces se usará el remitente del mensaje.
		Ejemplos:
		`MAIL list@example.com`
		`MAIL list@example.com me@example.cor`

`REALNAME`	nombre de lista [dirección] {nombre real}	Este comando establece el valor de nombre real para la "dirección" que es un miembro de la lista "nombre de lista" al valor establecido. El nombre real debe estar entre los caracteres { y }. Ejemplo:

		REALNAME list@example.com {Bill Farr
LIST	[listname] [list password]	Proporciona información sobre una Lista de Correo. Si no registra el nombre de la lista, se genera un resumen de todas las listas. Si se incluye la contraseña de la lista, se genera información detallada sobre la misma. Ejemplo: LIST list@example.com Lz$12

Ver:

Control Remoto del Servidor vía Correo 896
Controles Generales de Correo 899

7.2.2 Controles Generales de Correo

Estos son los comandos generales de correo electrónico que pueden ser enviados a la cuenta del sistema vía mensajes de correo electrónico. Los mensajes deben ser enviados a "mdaemon@[MDaemon dominio]" con el comando y parámetros asociados contenidos en una sola línea en el cuerpo del mensaje.

COMANDOS	PARAMS	DESCRIPCIONES
HELP	ninguno	Una copia del archivo NEWUSERHELP.DAT se procesa y se envía de regreso al remitente del mensaje.
STATUS	ninguno	Se enviará un informe de estatus de las operaciones del servidor y sus condiciones actuales al remitente del mensaje. Puesto que la información contenida en este informe de estatus se considera privada el usuario solicitante debe estar autentificado como administrador. Ejemplo: STATUS

Ver:

Control Remoto del Servidor vía Correo 896
Control de Listas de Distribución 897

7.3 La especificación de mensajes RAW

7.3.1 Especificación de mensajes RAW

MDaemon cuenta con soporte inherente para un formato de mensaje de correo simple y potente conocido como correo RAW. El propósito del sistema de correo RAW es proveer de un formato simple y estándar que los sistemas de software como MDaemon puedan usar para crear mensajes compatibles con RFC-2822 mucho más complejos. El uso de agentes de transporte de correo tal como RAW permite a los clientes de correo descargar al servidor de todo el trabajo complicado de mantener la adherencia a los estándares de correo en Internet.

El correo RAW consiste en una serie de cabeceras de texto opcionales y requeridas seguidas por un cuerpo de mensaje. La mayoría de las cabeceras consisten en una señal seguida por un valor entre los símbolos <>. Cada línea de encabezado acaba con una combinación de caracteres <CRLF>. Las cabeceras están separadas del cuerpo del mensaje por una línea en blanco y son sensibles a mayúsculas, y las cabeceras *from* y *to* son las únicas que se requieren. Todo el texto, cabeceras y cuerpo, son texto llano ASCII y deben estar contenidos en un archivo de texto que acabe con la extensión "`.raw`" (por ejemplo "`mi-mensaje.raw`"). Luego, para poner en cola el mensaje para entrega, coloque el archivo `*.raw` en la cola RAW de MDaemon (normalmente ubicada en "`C:\MDaemon\Queues\Raw`").

Omitir el Filtro de Contenido

Por defecto, los mensajes RAW pasan a través del Filtro de Contenido como los mensajes normales. Si quiere que un mensaje RAW determinado omita el procesamiento del filtro, entonces empiece el nombre del archivo con "`p`" o "`P`". Por ejemplo, "`P_mi-mensaje.raw`" omitiría el filtro de contenido pero "`mi-mensaje.raw`" sería procesado a través de él normalmente.

Saltar el Filtro de Contenido evitará que los mensajes sean firmados por DKIM. Si ha configurado MDaemon para firmar todos los mensajes ello podría potencialmente causar algunos problemas de envío. Si quiere que MDaemon firme los mensajes RAW configurados para saltarse el Filtro de Contenidos puede hacerlo usando la opción `x-flag=sign` descrita a continuación.

Encabezados RAW

From <buzon@ejemplo.com>	Este campo contiene la dirección de correo del remitente.
To <buzon@ejemplo.com [, buzon@ejemplo.com]>	Este campo contiene la dirección(es) de correo del remitente(s). Múltiples remitentes pueden especificarse separando cada uno con un carácter de coma.
ReplyTo <buzon@ejemplo.com>	Una dirección de correo opcional donde se dirigirán las respuestas a este mensaje.
CC <buzon@ejemplo.com[, buzon@ejemplo.com]>	Una lista opcional de destinatarios de copia de este mensaje. Los destinatarios múltiples de copia pueden especificarse separando cada uno con un carácter de coma.
Subject <texto>	Un asunto opcional del mensaje.
Header <Cabecera: Valor>	Le permite colocar explícitamente una combinación de Cabecera/Valor en el mensaje. Esto hace posible que coloque cabeceras personalizadas o no-estándar en sus mensajes *.raw.

Campos Especiales Soportados por RAW

Codificar y Adjuntar Archivos

```
x-flag=attach <ruta, método> [-x]
```

Ejemplo: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

Este X-FLAG especifica el valor "ATTACH" juntamente con dos parámetros dentro de los caracteres <>. El primer parámetro es una ruta completa al archivo que debería ser adjuntado al mensaje. El segundo parámetros que está separado del primero por un carácter de coma especifica el método de codificación que se debe usar cuando se adjunte al mensaje. MDaemon soporta dos valores para este parámetro. El método MIME instruye al servidor para que use un método de codificación estándar Base64 de Internet. El método ASCII instruye al servidor para que simplemente importe el archivo al mensaje. Un parámetro opcional -X al final de la cadena instruye al servidor para eliminar el archivo del disco una vez se haya adjuntado.

Notificación de Estatus de Envío

```
x-flag=confirm_delivery
```

Cuando se convierte un mensaje RAW que contiene esta marca a correo RFC-2822, al cadena se transformará a la construcción "Return-Receipt-To: <remitente@ejemplo.com>".

Colocar Combinaciones Específicas de Cabecera/Valor en el Mensaje RFC-2822

```
header <cabecera: valor>
```

Si desea colocar la combinación específica de cabecera/valor en el mensaje RFC-2822 que se generará del archivo RAW, necesitará usar la macro HEADER listada en la sección anterior de cabeceras RAW. Por ejemplo, si quiere que la cabecera "Delivered-By: servidor-correo@ejemplo.com" sea colocada en el mensaje RFC-2822 colocaría esto: "header <Delivered-By: servidor-correo@ejemplo.com>" en el mensaje RAW. Note que la macro "header" requiere tanto el campo como el valor. Puede colocar tantas macro "header" como necesita en su mensaje RAW.

Mensajes RAW con firma DKIM

```
x-flag=sign
```

El incluir este comando especial en un archivo `*.raw` hará que el mensaje RAW sea firmado por DKIM. Esto sólo debería usarse en mensajes RAW que tenga configurados para saltarse el Filtro de Contenido (empezando sus nombres de archivo con "`p`" o "`P`"). No debe usar este comando en los Mensajes RAW normales que se procesan a través del filtro. Dichos mensajes deben firmarse normalmente.

Todos los mensajes RAW que son generados por el Filtro de Contenido usarán el comando `x-flag=sign` automáticamente.

Mensajes de correo RAW de ejemplo

Ejemplo 1:

```
from <mdaemon@altn.com>
to <user01@example.com>

Hola John!
```

Ejemplo 2:

```
from <user01@example.com>
to <user09@example.net>
subject <Archivos Solicitados>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X


Aquí están todos los archivos que solicitó.
```

7.4 Archivos Semáforo

MDaemon está equipado con soporte para Archivos Semáforo, los cuales pueden usarse con una variedad de propósitos, incluyendo hacer que MDaemon ejecute acciones específicas. Periódicamente MDaemon escaneará la subcarpeta `\APP\`

buscando la existencia de dichos archivos. Si encuentra uno, el comportamiento asociado se desencadena y el archivo semáforo se elimina. Esto provee de un mecanismo sencillo que permite a los administradores y desarrolladores manipular MDaemon sin tener que interactuar con la interfaz. La siguiente es una lista de los semáforos y sus funciones:

NOMBRE DE ARCHIVO	ACCIÓN
ACLFIX.SEM	Ejecuta la rutina de mantenimiento de ACLs.
ADDUSER.SEM	Este semáforo crea nuevas cuentas de usuario. Se usa para forzar a MDaemon a adjuntar nuevos registros al final del archivo USERLIST.DAT sin causar una reconstrucción completa que consume bastantes recursos de la base de datos de usuarios. Cada línea en este archivo debe ser un registro de cuenta completo en la forma especificada en la sección de Funciones de la Gestión de Cuentas de la API de MDaemon (vea MD-API.html en la subcarpeta de MDaemon \docs\API\). Múltiples nuevas cuentas pueden ser especificadas – un registro de cuenta por línea. MDaemon procesará el archivo línea a línea y añadirá cada nueva cuenta. Puede crear ADDUSER.LCK para bloquear el archivo mientras lo está actualizando y MDaemon no tocará ADDUSER.SEM hasta que ADDUSER.LCK sea borrado. Para ver un ejemplo de archivo ADDUSER.SEM abra ADDUSER.SMP en su directorio de aplicaciones con un editor de texto.
ALERT.SEM	Muestra en una ventana de pop-up los contenidos del archivo de semáforo a todos los usuarios de Webmail que tengan sesión iniciada cuando el archivo se crea. No se muestra, sin embargo, inmediatamente a todos los usuarios — se muestra a cada usuario individualmente la siguiente vez que su navegador haga una petición al servidor de Webmail. **Nota:** A diferencia de otros archivos de semáforo, este archivo es específico de Webmail. En lugar de colocarlo en el directorio \app\ debe colocarse en el directorio \MDaemon\WorldClient\.
ALIAS.SEM	Recarga el archivo(s) de alias.
AUTORESPEXCEPT.SEM	Recarga el archivo(s) de excepciones de autorespuesta.

BATV.SEM	Recarga el archivo(s) de Backscatter Protection (BATV).
BAYESLEARN.SEM	Este SEM inicia manualmente el proceso de aprendizaje Bayesiano. Equivale a hacer clic en el botón Aprender de la pestaña Bayesiano del Filtro de Spam. Nota: esto iniciará el procedimiento de aprendizaje Bayesiano, aunque éste haya sido deshabilitado.
BLOCKLIST.SEM	Recarga el archivo(s) de lista de bloqueados.
CFILTER.SEM	Vuelve a cargar las reglas de Filtrado de Contenido, borra los datos de caché del Filtrado de Contenido y vuelve a cargar el archivo de la Lista de Permitidos (no filtrar) 692 del Filtro de spam.
CLEARQUOTACOUNTS.SEM	Los resultados de las comprobaciones de cuota de usuario se mantienen en el archivo `quotacounts.dat`. Si desea vaciar los valores de cuota en caché para un usuario, añada la dirección de correo del usuario a este archivo de semáforo y colóquelo en la carpeta `\app\`. Si se encuentra un asterisco (*) en una línea por sí mismo, el archivo entero se borrará y por lo tanto invalidará todos los valores de cuota en caché.
CREDSMATCHEXEMPTLIST.SEM	Vuelve a cargar la Lista de Exentos de Coincidencia de Credenciales 525.
DELUSER.SEM	Puede usar este archivo de semáforo para eliminar una o más cuentas de usuarios. Cree un archivo de texto que contenga las direcciones de cada cuenta que quiere que sea borrada (una dirección por línea), nombre al archivo `DELUSER.SEM` y luego muévalo al directorio de MDaemon `\app\`. MDaemon eliminará las cuentas y luego borrará el archivo `DELUSER.SEM`. Si desea eliminar una cuenta, pero no eliminar su carpeta de correo, agregue "^" a la dirección (ej. `frank@example.com^`).
DMARCEXEMPTLIST.SEM	Vuelve a cargar la Lista de Exentos DMARC 545.
DNS.SEM	Vuelve a cargar los Servidores DNS de Windows 113 y la configuración de DNS del filtro de Spam.

DOMAINSHARING.SEM	Recarga los datos del archivo de compartición de dominios.
EDITUSER.SEM	Este semáforo se usa para actualizar registros específicos dentro del archivo USERLIST.DAT sin una reconstrucción que podría potencialmente consumir mucho tiempo. Para actualizar registros de un usuario en específico con USERLIST.DAT, genere un archivo denominado EDITUSER.SEM que incluya un registro completo de reemplazo, un registro por línea, para los registros de usuario que desee editar. Cada registro debe construirse de acuerdo con el formato del archivo USERLIST.DAT descrito en el artículo de la base de conocimiento Formato de Archivo Userlist , pero debe empezar con la dirección de correo original, seguida de una coma. MDaemon procesará el archivo EDITUSER.SEM una línea a la vez. Puede crear el archivo EDITUSER.LCK para bloquear el archivo mientras lo actualiza y MDaemon no tocará EDITUSER.SEM hasta que EDITUSER.LCK sea eliminado. Para ver un ejemplo del archivo EDITUSER.SEM, abra EDITUSER.SMP en su directorio \APP\ con un editor de texto.
EXCPTION.SEM	Forza a MDaemon a recargar el archivo EXCPTION.DAT.
EXITNOW.SEM	Apaga MDaemon.
GATEWAYS.SEM	Para rendimiento óptimo, MDaemon mantiene una lista de las puertas de enlace en memoria. Cree GATEWAYS.SEM en el directorio APP de MDaemon para recargar el archivo gateways.dat.
GREYLIST.SEM	Recarga el archivo(s) de Lista Gris.
GROUPS.SEM	Recarga el archivo(s) de grupos de cuentas.
GRPLIST.SEM	Recarga la caché interna de los nombres de Lista de Correo.
HANGUPG.SEM	Fuera un corte condicional del dispositivo RAS. MDaemon esperará cualquier sesión pendiente de correo para que se cierre y luego cortará la sesión RAS.

HANGUPR.SEM	Fuerza un corte incondicional del dispositivo RAS. Este es un corte inmediato e incondicional sin tener en cuenta las sesiones de correo que puedan estar en progreso en la conexión.
HOSTSCREEN.SEM	Recarga el archivo(s) de Monitorización de Hosts.
IPSCREEN.SEM	Recarga el archivo(s) de Monitorización de IPs.
IPSHIELD.SEM	El archivo `IPShield.dat` se guarda en memoria caché para incrementar la velocidad de acceso. Utilice `IPSHIELD.SEM` para volver a cargarlo en memoria.
LDAPCACHE.SEM	Recarga los archivos de datos de usuario de LDAP y puertas de enlace.
LOCKSEMS.SEM	Previene que todos los semáforos se procesen hasta que el usuario lo borra.
LOGSETTINGS.SEM	Recarga las configuraciones de los archivos de registro.
MDSPAMD.SEM	Recarga la lista de permitidos del Filtro de Spam y MDSPAMD, lo que le forza a reinicializar todos sus datos de configuración.
MINGER.SEM	Detiene y reinicia el servidor Minger 863.
MXCACHE.SEM	Recarga todos los archivos de datos de Caché MX.
NODNSBL.SEM	Recarga el archivo de lista de permitidos de DNSBL.
NOPRIORITY.SEM	Forza a MDaemon a volver a cargar el archivo `NoPriority.dat`.
ONLINE.SEM	MDaemon creará este archivo de semáforo una vez haya realizado una conexión con éxito usando RAS para el ISP. MD quitará el semáforo cuando la conexión haya terminado. Esto es útil si quiere saber cuándo MD está usando el sub-sistema RAS.
POSTDIAL.SEM	MDaemon creará este archivo inmediatamente después de que una conexión hecha por MDaemon se cierre.

PREDIAL.SEM	MDaemon creará este archivo justo antes de intentar usar RAS/DUN. Esto permitirá a otro software detectar cuándo debe dejar libre el puerto de marcación para que MDaemon pueda usarlo.
PRIORITY.SEM	Recarga el archivo(s) de Correo Prioritario.
PROCBAD.SEM	Inicia el envío del contenido de la Cola Errónea.
PROCDIG.SEM	Inicia la construcción y envío de Resúmenes de la lista de correo.
PROCHOLDING.SEM	Inicia el envío del contenido de la Cola Retenida.
PROCNOW.SEM	Inicia una comprobación para el correo remoto y el envío del correo remoto en cola.
PROCREM.SEM	MDaemon irá inmediatamente a procesar el correo y realizará transacciones para todo el correo remoto.
PROCRETR.SEM	Inicia el envío del contenido de la cola de reintentos.
PRUNE.SEM	Recarga las configuraciones de auto-eliminación.
PUBLICSUFFIX.SEM	Vuele a cargar el archivo de Sufijos Públicos 552.
QUEUE.SEM	Este archivo semáforo se utiliza para habilitar/deshabilitar las colas de correo. El archivo puede contener cualquier cantidad de líneas, pero cada una puede contener solo las siguientes cadenas (una por línea): ENABLE INBOUND, ENABLE REMOTE, ENABLE LOCAL, o DISABLE INBOUND, DISABLE REMOTE, DISABLE LOCAL.
RCPTBLOCKLIST.SEM	Vuelve a cargar la Lista de Destinatarios Bloqueados 561.
RESTART.SEM	Para y luego inicia MDaemon.
RESTARTCF.SEM	Para y reinicia `CFEngine.exe` (el ejecutable del Filtro de Contenido).
RESTARTWC.SEM	Detiene y reinicia MDaemon Webmail. Solamente funciona cuando Webmail está utilizando su propio

servidor web integrado 326.

RELOADCACHE.SEM	Recarga todas las configuraciones de datos de caché y archivos excepto las configuraciones y archivos del Filtro de Contenidos.
REVERSEEXCEPT.SEM	Recarga el archivo de excepciones de búsquedas invertidas.
SCHEDULE.SEM	Recarga el archivo(s) de programación.
SENDERBLOCKLIST.SEM	Vuelve a cargar la Lista de Remitentes Bloqueados 559.
SPAMHONEYPOTS.SEM	Recarga los datos del archivo(s) de Honeypot de spam.
SPF.SEM	Recarga los archivo(s) de SPF, DKIM y VBR.
SUPPRESS.SEM	Recarga las configuraciones de lista de bloqueados y elimina del caché las configuraciones de dominio.
TARPIT.SEM	Recarga el archivo(s) de la monitorización dinámica y tarpit.
TRANSLAT.SEM	Recarga los archivos de traducción de encabezados.
TRAY.SEM	Redibuja el icono de MDaemon de la bandeja de sistema.
TRUST.SEM	Los dominios confiables y direcciones IP se guardan residentes en memoria para rendimiento óptimo. Si necesita recargar estas configuraciones manualmente puede crear TRUST.SEM para hacerlo.
UPDATEAV.SEM	Inicia la actualización de definiciones de antivirus.
UPDATESA.SEM	Inicia la actualización de las definiciones de antivirus de Security Plus para MDaemon.
USERLIST.SEM	Recarga el archivo USERLIST.DAT. Use esto cuando haga modificaciones en USERLIST.DAT y necesite que MDaemon lo recargue.

WATCHDOG.SEM	MDaemon comprobará y eliminará este semáforo del directorio APP en aproximadamente intervalos de 10-20 segundos. Este archivo puede usarse para aplicaciones externas para comprobar que MDaemon se esté ejecutando. Si este archivo permanece en el directorio APP durante más de 20 segundos, es un buen indicativo de que MDaemon ya no se está ejecutando.

7.5 Ruta de Distribución

Un archivo de mensaje esperando en una cola contiene típicamente dentro de sus encabezados toda la información que se necesita para que el mensaje sea enviado a la ubicación correcta. Estos encabezados están guardados dentro del archivo (tal como el encabezado X-MDaemon-Deliver-To) que proveen a MDaemon con instrucciones de cómo y a quién debe enviarse el mensaje. Algunas veces sin embargo es necesario o útil sobrescribir esta información y proveer alternativas específicas para ver a dónde y quien debe enviarse un mensaje. Las Rutas de Distribución (Route Slips) permiten tal mecanismo. Una ruta de distribución es un archivo que provee a MDaemon con instrucciones muy específicas sobre dónde y a quién debe enviarse el mensaje. Si se encuentra una ruta de distribución para un mensaje en particular entonces las configuraciones dentro del archivo de ruta y no las que se encuentran dentro del archivo .MSG en sí mismo, controlan dónde y a quién se envía el mensaje.

Los archivos de ruta de distribución acaban con la extensión `.RTE`. Por ejemplo, si un mensaje esperando a ser enviado se llama "`MD0000.MSG`," entonces el archivo de ruta de distribución correspondiente se llamará `MD0000.RTE` y deberá estar ubicado en la misma carpeta (cola de correo) que el archivo de mensaje.

El formato de un archivo de ruta de distribución es el siguiente:

```
[RemoteHost]
DeliverTo=ejemplo.net
```

Esta sección de una ruta de distribución provee a MDaemon con el servidor al cual debe enviarse el archivo `.MSG` correspondiente. MDaemon siempre intentará una conexión directa a este host enrutando el mensaje en el menor tiempo posible. Sólo puede especificarse un host.

```
[Port]
Port=xxx
```

Este control especifica el puerto a donde la conexión TCP/IP y el intento de envío se deberían hacer. El puerto 25 es el puerto por defecto para el correo SMTP.

```
[LocalRcpts]
Rcpt0=direccion@ejemplo.com
Rcpt1=otra-direccion@ejemplo.com
Rcpt2=aun-otra-direccion@ejemplo.com

[RemoteRcpts]
Rcpt0=direccion@ejemplo.net
Rcpt1=otra-direccion@ejemplo.net
Rcpt2=aun-otra-direccion@ejemplo.net
```

Estas secciones del archivo de ruta de distribución le permiten especificar cualquier número de destinatarios locales y remotos que deberían recibir una copia del archivo `.MSG` asociado. Las direcciones de destino local y remota deben estar separadas y colocarse en sus correspondientes secciones `[LocalRcpts]` y `[RemoteRcpts]`.

Los archivos de ruta de distribución proveen de un buen mecanismo de envío o redirección de correo, pero no son generalmente necesarios. Un uso que MDaemon hace de ellos es en el caso de correo "enrutado" de listas de distribución. Cuando se tiene una lista de correo establecida para enrutar una sola copia del mensaje de lista a un host remoto, se utiliza una ruta de distribución para conseguirlo. Es un método muy eficaz de envío de correo cuando tiene direcciones masivas a las que enviar correo puesto que sólo se requiere una copia del mensaje mientras que pueden especificarse cualquier número de destinatarios. Sin embargo, no todos los hosts remotos permiten este tipo de enrutado. Puesto que en última instancia son ellos los que tienen que recibir una copia del archivo de mensaje a cada dirección, algunos hosts establecen un límite en el número de destinatarios que permiten que se especifique.

Sección VII

8 Crear y Usar Certificados SSL

Al utilizar el diálogo SSL & TLS para crear certificados, MDaemon genera certificados autofirmados. En otras palabras, el emisor del certificado, o la Autoridad de Certificación (CA), es la misma que el propietario del certificado. Esto es perfectamente válido y permitido, pero dado que los CA no estarán listados en las listas de CAs de confianza de los usuarios, siempre que conecten a las URL HTTPS de Webmail o Administración Remota, se les preguntará si desean o no proceder al sitio y/o instalar el certificado. Una vez accedan a instalar el certificado y confiar en su dominio de Webmail como CA válida, no necesitarán ver más el mensaje de alerta de seguridad cuando conecten con Webmail o Administración Remota.

Cuando conecte a MDaemon vía un cliente de correo tal como Microsoft Outlook, sin embargo, no se les dará la opción de instalar el certificado. Se les permitirá escoger si desean o no continuar usando el certificado temporalmente, aun y cuando éste no esté validado. Cada vez que inicien su cliente de correo y conecten con el servidor, tendrán que escoger antes de continuar usando el certificado no-validado. Para evitar esto puede ya sea obtener un certificado de una Autoridad de Certificación (CA), tal como Let's Encrypt 594,, o puede exportar su certificado autofirmado y distribuirlo entre sus usuarios vía correo o por algún otro medio. Luego, puede instalar manualmente su certificado para evitar mensajes de advertencia en el futuro.

Crear un Certificado

Para crear un certificado desde dentro de MDaemon:

1. Vaya al diálogo SSL & TLS dentro de MDaemon (haga clic en Seguridad » Ajustes de Seguridad » SSL & TLS » MDaemon).
2. Marque la casilla etiquetada, "*Habilitar SSL, STARTTLS, y STLS*".
3. Dé clic en **Crear Certificado**.
4. En la casilla denominada **Nombre de Host**, registre el dominio para el que se generará el certificado (*por ejemplo "mail.example.com"*)
5. Teclee el nombre de la organización o empresa propietaria del certificado en la casilla etiquetada, "*Nombre de la organización/empresa*".
6. En "*Nombre de host alternativos.....*", teclee todos los otros nombres de dominio que los usuarios usarán para acceder a su servidor (por ejemplo, "`*.ejemplo.com`", "`ejemplo.com`", "`mail.altn.com`", y demás).
7. Escoja una longitud para la clave de encriptación del cuadro de lista desplegable.
8. Escoja el País/región en el que reside su servidor.
9. Haga clic en **OK.**

Usar Certificados Expedidos por un CA de Terceros

Si ha comprado o generado de otra manera un certificado de algún origen distinto a MDaemon, puede usar dicho certificado usando la Consola de Administración de Microsoft para importarlo en el almacén de Certificados que utiliza MDaemon. Para hacerlo en Windows XP:

1. En su barra de tareas de Windows, haga clic en **Inicio » Ejecutar...** y teclee "**mmc /a**" en el cuadro de texto.
2. Haga clic en **Aceptar**.
3. En la Consola de Administración de Microsoft, haga clic en **Archivo » Agregar o quitar complemento...** en la barra de menú (o pulse **Ctrl+M** en su teclado).
4. En la pestaña Independiente, haga clic en **Agregar...**
5. En el diálogo de *Agregar un complemento independiente*, haga clic en **Certificados,** y luego haga clic en **Agregar**.
6. En el diálogo de *Complemento de certificados,* escoja **Cuenta de equipo,** y luego haga clic en **Siguiente**.
7. En el diálogo *Seleccionar equipo*, escoja **Equipo local**, y luego haga clic en **Finalizar**.
8. Haga clic en **Cerrar**, y clic en **Aceptar**.
9. Bajo *Certificados (Equipo Local)* en el panel izquierdo, si el certificado que está importando es autofirmado, haga clic en **Entidades emisoras raíz de confianza** y luego **Certificados**. Si es autofirmado haga clic en **Personal**.
10. En la barra de menú, haga clic en **Acción » Todas las Tareas » Importar...**, y luego haga clic en **Siguiente**.
11. Introduzca la ruta de archivo al certificado que desea importar (usando el botón Explorar si es necesario), y luego haga clic en **Siguiente**.
12. Haga clic en **Siguiente**, y clic en **Finalizar**.

MDaemon sólo mostrará certificados que tienen claves privadas que usan el formato Personal Information Exchange format (PKCS #12). Si su certificado importado no aparece en la lista puede que necesite importar un archivo `*.PEM`, que contiene tanto un certificado de clave como una clave privada. Importando este archivo usando el mismo proceso descrito anteriormente lo convertirá a formato PKCS #12.

Utilizar Let's Encrypt para Administrar su Certificado

Let's Encrypt es una autoridad de Certificación (Certificate Authority - CA) que proporciona certificados gratuitos vía un proceso automatizado diseñado para eliminar los procesos completos de creación, validación, firma y renovación manuales de certificados para sitios web seguros.

Para soportar el uso del proceso automatizado de Let's Encrypt para administrar un certificado, se cuenta con la pantalla Let's Encrypt[594] para ayudarle a configurar y ejecutar fácilmente el script de PowerShell incluido en la carpeta "`MDaemon\LetsEncrypt`". Al ejecutar el script se configurará todo lo necesario para Let's Encrypt, incluyendo la colocación de los archivos necesarios en la carpeta HTTP de Webmail para completar la validación http-01. Utiliza el Nombre de host SMTP[192] del dominio por omisión[190] como dominio para el certificado, incluye cualesquiera *Nombres de host Alternos* que haya especificado, recupera el certificado, lo importa a Windows y configura MDaemon para utilizar el certificado para MDaemon, Webmail y Administración Remota. Más aun, el script crea un archivo de registro en la carpeta "`MDaemon\Logs\`" , denominado `LetsEncrypt.log`. Este archivo se elimina y vuelve a crear cada vez que se ejecuta el script e incluye la fecha y hora del inicio de ejecución del script. También, se envían mensajes de notificación de la ocurrencia de errores, si se especifica una *Cuenta de correo de Admin para notificaciones*. Vea el tema Let's Encrypt[594] para más información.

Ver:

SSL & TLS[575]

Sección

9 Glosario

ACL—Sus siglas vienen de **A**ccess **C**ontrol **L**ists (Lista de Control de Acceso). ACL es una extensión del Internet Message Access Protocol (IMAP4) que hace posible crear una lista de acceso para cada una de sus carpetas de mensaje, así pues concediendo acceso a sus carpetas a los usuarios que también tienen cuentas en su servidor de correo. Además, puede establecer permisos que gobiernan hasta qué punto cada usuario tiene control sobre dichas carpetas. Por ejemplo, puede designar si un usuario tiene o no permiso para borrar mensaje, marcarlos como leídos o no leídos, copiar mensajes a carpetas, crear nuevas subcarpetas, y demás. Sólo los clientes de correo con soporte para ACL pueden usarse para compartir este acceso y establecer permisos. Sin embargo, si su cliente de correo no tiene soporte para ACL puede aun así establecer permisos desde la interfaz de MDaemon.

ACL se discute por completo en RFC 2086, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII—Pronunciado "as-key" en inglés, ASCII es el acrónimo de "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". Es el código estándar mundial para la representación de letras mayúsculas y minúsculas del alfabeto Latino, así como números y puntuaciones en formato de número binario de 7 dígitos, con cada carácter asignado un número de 0 a 127 (0000000 a 1111111). Por ejemplo, el código ASCII para la M mayúscula es 77. La mayoría de los ordenadores usan código ASCII para representar texto, lo que hace posible transferir datos a otros ordenadores. La mayoría de los editores de texto y procesadores de texto pueden almacenar archivos en formato ASCII (algunas veces llamados archivos ASCII). Sin embargo, la mayor parte de archivos de datos—particularmente aquellos que contienen datos numéricos—no se almacenan en formato ASCII.

Muchos conjuntos de caracteres grandes tienen 128 caracteres adicionales porque usan 8 bits en lugar de 7. Estos caracteres extra se usan para representar símbolos y caracteres no-ingleses. El sistema operativo DOS usa un superconjunto de ASCII llamado ASCII extendido o ASCII superior. Un estándar más cercano al universal, sin embargo, es el ISO Latin 1, que es usado por muchos sistemas operativos y navegadores web.

ATRN—Vea las entradas ETRN y ODMR posteriores.

Adjunto—Un archivo adjunto a un mensaje de correo. La mayoría de los sistemas de correo sólo soportan el envío de archivos de texto como correo, así pues, si el adjunto es un archivo binario o archivo de texto formateado (p. ej. un documento del procesador word), primero debe ser codificado como texto antes de que sea enviado y decodificado una vez se recibe. Existen una serie de esquemas de codificación—dos de los más prevalentes son Multipurpose Internet Mail Extensions (MIME) y Unix-to-Unix encode (Uuencode). Para los mensajes entrantes, MDaemon puede ser configurado para dejar el proceso de decodificación al destinatario de correo o decodificar automáticamente los adjuntos y almacenarlos en una ubicación específica antes de enviar el mensaje al usuario local.

Backbone—Una serie lineal de conexiones que forman la ruta principal de una red. Este término es relativo puesto que las líneas no-backbone de una red grande pueden ser mayores que el backbone de una red pequeña.

Ancho de Banda—La cantidad de datos a ser transmitidos en una cantidad fija de tiempo a través de una conexión de red o de módem, usualmente se mide en bits-por-segundo (bps). Una página completa de texto en inglés tiene unos 16.000 bits, lo que en un módem rápido se podría transferir en 1 o 2 segundos. Un vídeo en movimiento a pantalla completa puede requerir unos 10.000.000 de bits-por-segundo, dependiendo de la compresión.

Una buena manera de ilustrar el ancho de banda es una autopista. La autopista representa la conexión mientras que los coches que viajan en ella representan los datos de ordenador. Como más ancha sea la autopista (como más ancho sea el ancho de banda) más coches podrán viajar en ella.

Baudio—El ratio de baudios es una medida de con qué frecuencia la señal portadora cambia el valor en una línea de teléfono. Es una referencia a la velocidad a la que un módem transmite datos. Normalmente, los modems más lentos se describen en términos de ratio de Baudios mientras que los modems de alta velocidad se describen en bits por segundo. "Ratio de Baudios" y "bits por segundo" no son necesariamente términos sinónimos puesto que cada señal puede codificar más un bit en conexiones de alta velocidad.

Bit—Un único Dígito **Bi**nario. Es la unidad más pequeña de datos de ordenador; un único dígito en base-2 (0 o 1). Normalmente se abrevia con la minúscula "b" como en "bps" (bits por segundo). Una página de texto completa son aproximadamente 16.000 bits.

Mapa de bits (Bitmap)—La mayoría de las imágenes que ve en su ordenador, incluyendo las que encuentra en Internet, son mapas de bits. Un mapa de bits es solamente un mapa de puntos (o bits) que parece una fotografía mientras no esté demasiado pegado a la pantalla, o tenga el mapa de bits demasiado aumentado, para ver la forma que hacen. Los tipos de archivo de mapa de bits más comunes incluyen BMP, JPEG, GIF, PICT, PCX, y TIFF. Dado que las imágenes de mapa de bits están hechas de un puñado de puntos, si realiza demasiado zoom en un mapa de bits parecerán bloques en lugar de una imagen suave. Los gráficos de vector (creados normalmente en formatos CorelDraw, PostScript, o CAD) se escalan mucho mejor porque están hechos de formas generadas matemáticamente en lugar de simplemente por puntos aparentemente "al azar".

Bps—"**B**its **P**or **S**egundo" es una medida de cuán rápido los datos de un ordenador pueden moverse de un lugar a otro. Por ejemplo, un módem de 33,6 kbps puede transferir 33.600 bits por segundo. Kilobits (1000 bits) por segundo y megabits (1.000.000 bits) por segundo se abrevian como "Kbps" y "Mbps" respectivamente.

Navegador—Versión corta para "Navegador Web", es una aplicación usada para mostrar páginas web. Interpreta código HTML, texto, enlaces de hipertexto, imágenes, JavaScript, y demás. Los navegadores más distribuidos son Internet Explorer y Netscape Communicator.

Byte—Un conjunto de bits (normalmente ocho) que representa un sólo carácter. Existen 8 bits en un byte, algunas veces más, dependiendo de cómo se realice la medida. "Byte" se abrevia con una "B" mayúscula.

Caché—En inglés, pronunciado como "cash". Existen diversos tipos de caches, pero todas se usan para almacenar información recientemente utilizada para que pueda ser accedida con rapidez posteriormente. Por ejemplo, un navegador web usa una caché para almacenar página, imágenes, URLs, y otros elementos de los sitios web que se han visitado recientemente. Cuando se regresa a una página

web en caché, el navegador no tendrá que descargar nuevamente dichos elementos. Dado que acceder a la caché de su disco duro es mucho más rápido que acceder a Internet, eso acelera considerablemente la navegación.

La caché de IP de MDaemon almacena las direcciones IP de los dominios a los cuales ha enviado recientemente mensajes. Esto previene a MDaemon de tener que buscar de nuevo dichas direcciones cuando envía mensajes adicionales a los mismos dominios. Esto puede acelerar notablemente el proceso de envío.

CGI—Common **G**ateway **I**nterface es un conjunto de reglas que describe como un Servidor Web se comunica con otra pieza de software de la misma máquina, y cómo la otra pieza de software (el "programa CGI") habla con el servidor web. Cualquier pieza de software puede ser un programa CGI si gestiona las entradas y salidas de acuerdo con el estándar CGI. aun así, un programa CGI es normalmente un programa pequeño que recoge datos de un servidor web y hace algo con ellos, tal como poner el contenido de un formulario en un correo electrónico, o hacer algo más con dichos datos. Los programas CGI normalmente se almacenan en el directorio "cgi-bin" del sitio web y por lo tanto aparecen en la URL que accede a ellos, pero no siempre.

cgi-bin—El nombre más común del directorio de un servidor web en el que se almacenan los programas CGI. La parte "bin" de "cgi-bin" es el nombre corto de "binario" dado que la mayoría de programas usados se les define como "binarios". En realidad, la mayoría de los programas cgi-bin son archivos de texto; scripts ejecutados por programas ubicados en otros lugares.

CIDR—"**C**lassless **I**nter-**D**omain **R**outing" es un nuevo sistema de direccionamiento IP que reemplaza el sistema antiguo, que se basaba en las clases A, B y C. La dirección IP CIDR parece una dirección IP normal seguida con una barra y un número, llamado prefijo IP. Por ejemplo:

123.123.0.0/12

El prefijo IP define cuántas direcciones cubre la dirección CIDR, con un menor número cubriendo más direcciones. En el ejemplo anterior, el prefijo IP de "/12" puede usarse para direccionar 4.096 direcciones de las antiguas Clase C.

Las direcciones CIDR reducen el tamaño de las tablas de enrutamiento y hacen que haya más direcciones IP disponibles dentro de las organizaciones.

CIDR está descrito en los RFCs 1517-1519, que pueden visualizarse en:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Cliente—Un programa de software que se usa para contactar y obtener datos de o a un programa de software *servidor*. El servidor está normalmente ubicado en otro ordenador, bien en su red local o en otra ubicación. Cada programa *cliente* está diseñado para trabajar con uno o más programas *servidor* de tipo específico, y cada servidor requiere un tipo específico de cliente. Un *navegador* web es un tipo específico de cliente que comunica con *servidores* web.

Common Gateway Interface—Vea la entrada anterior CGI.

Cookie—En terminología de ordenador, una *cookie* son datos enviados por un servidor web a su navegador web, que son guardados y utilizados posteriormente

para diversos propósitos cuando vuelve al mismo sitio o va a otra ubicación en él. Cuando un servidor web recibe una solicitud de un navegador web que incluye una cookie, es capaz de usar la información que la cookie contiene para el propósito para el que ésta esté diseñada, tal como personalizar lo que se le muestra al usuario, o guardar un registro de las peticiones del usuario. Típicamente las cookies se usan para almacenar contraseñas, nombres de usuario, preferencias, información de carros de compra, y cosas similares relacionadas con el sitio con el que se corresponden para que el sitio pueda parecer que "recuerda" quien es y que se ha hecho allí.

Dependiendo de las configuraciones de su navegador, puede aceptar o no aceptar las cookies, y guardarlas durante una cantidad determinada de tiempo. Normalmente las cookies expiran después del tiempo predeterminado y se guardan en memoria hasta que el software del navegador se cierra, momento en el que se guardan en disco.

Las cookies **no pueden** leer su disco duro. Pueden, sin embargo, usarse para recopilar información sobre usted relacionada con el uso particular de sus sitios web, lo que sería imposible sin ellas.

Marcación de Red—Un componente de Windows que le permite conectar su ordenador a la red vía módem. A menos que su ordenador esté conectado a una Red de Area Local (LAN) con acceso a Internet, necesitará configurar la Marcación de Red (DUN) para marcar un Punto de Presencia (POP) y acceder a su Proveedor de Servicios de Internet (ISP) antes de tener acceso a Internet. Su ISP puede que necesite ser proveído con cierta información tal como la dirección de la puerta de enlace y la dirección IP de su ordenador.

DUN es accesible a través del icono de Mi PC. Un perfil diferente de marcación puede configurarse para cada servicio online que use. Una vez configurado, puede copiar un acceso directo de perfil a su escritorio para que todo lo que necesite hacer para realizar una conexión sea hacer doble-clic en el icono de conexión.

Defecto—Es el término usado para referirse al valor predeterminado para opciones en los programas de ordenador. Las configuraciones por defecto son aquellas que se usan cuando no ha sido designada configuración específica por el usuario. Por ejemplo, la configuración de fuente por defecto en Netscape Communicator es "Times". Esta configuración seguirá siendo "Times" a menos que lo cambie a algo más. Las configuraciones por defecto son normalmente el valor que la mayoría de gente escoge.

Frecuentemente el término *poner por defecto* se usa también como verbo. Si una configuración personalizada no funciona o el programa está falto de algunos trozos de datos para completar una tarea, normalmente se "pondrá por defecto" para una configuración o acción específica.

DHCP—Acrónimo para "**D**ynamic **H**ost **C**ontrol **P**rotocol". Los servidores de red usan este protocolo para asignar dinámicamente las direcciones IP a los ordenadores de red. Un servidor DHCP espera que un ordenador se conecte a él y le asigne una dirección IP de una lista guardada.

DHCP está descrito en RFC-2131, que puede ser visualizado en:

http://www.rfc-editor.org/rfc/rfc2131.txt

Puerta de Enlace de Dominio—Vea la entrada posterior Puerta de Enlace.

Nombre de Dominio—Este es el nombre único que identifica un sitio web de Internet. Por ejemplo, "mdaemon.com" es el nombre de dominio de MDaemon Technologies. Cada nombre de dominio contiene dos o más partes separadas por puntos; la parte de más a la izquierda es más específica mientras que la de más a la derecha es la más genérica. Cada nombre de dominio también apunta a la dirección IP de un sólo servidor, pero un solo servidor puede tener más de un nombre de dominio. Por ejemplo, "mail.mdaemon.com", "mdaemon.com" y "ejemplo.com" podrían apuntar todos al mismo servidor que "mdaemon.com", pero "mdaemon.com" no puede apuntar a dos servidores diferentes. Existen, sin embargo, métodos para designar servidores alternativos a los que los clientes serán redireccionados si el servidor principal se cae o se vuelve no disponible.

También es común que un nombre de dominio esté registrado, pero no esté conectado a ninguna máquina. La razón más común es que el propietario del dominio no ha creado un sitio web todavía, o para que puedan tener direcciones de correo electrónico en un dominio concreto sin tener que mantener un sitio web. En el último caso, debe existir una máquina real en Internet que gestione el correo del nombre de dominio listado.

Finalmente, es común ver el término "nombre de dominio" acortado y referido simplemente como "dominio". La palabra "dominio" tiene otros significados y puede referirse a otras cosas, tal como los dominios en Windows NT o un tipo de valores, así que debería tener en cuenta la distinción para evitar confusiones.

Domain Names están explicados en los RFCs 1034-1035, que pueden ser visualizados en:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP—Desarrollado por MDaemon Technologies para formar parte del servidor MDaemon, DomainPOP hace posible proveer servicios de correo para una red local entera o grupo de trabajo desde un único buzón POP de ISP. En el pasado, a menos que el servidor de correo electrónico de la empresa tuviera conexión "en vivo" a Internet, la única manera de proveer servicios de correo Internet a un grupo de trabajo para cada persona era tener su propio buzón en el ISP de la empresa del que recolectaran su correo. Con DomainPOP sólo se requiere un único buzón. El ISP recoge todo el correo para el dominio de la empresa en el buzón del cual se recolecta periódicamente DomainPOP. Luego, DomainPOP analiza los mensajes para determinar los supuestos destinatarios de cada uno y los distribuye al buzón del usuario local apropiado. Así pues, se provee correo para una red entera de una sola cuenta de marcación ISP.

Descarga—El proceso por el cual su ordenador obtiene información de otro ordenador. Por ejemplo, la información se obtiene de Internet *descargándolo* de otros ordenadores. El contrario es *subir*. Si desea enviar información a otro ordenador entonces estará *subiendo* información a éste.

Driver—Un pequeño programa que se comunica con ciertos dispositivos de hardware. Los drivers contienen información necesitada por el ordenador y otros programas para controlar y reconocer el dispositivo. Los ordenadores basados en Windows tienen con frecuencia drivers empaquetados como archivos de librería dinámica (DLL). La mayoría de los dispositivos de hardware que se usan en Macs no necesitan drivers, pero cuando se necesita un normalmente vendrá en forma de Extensión de Sistema.

DUN—Vea la entrada anterior Marcación de Red.

Email (correo electrónico)—Este término también se encuentra en las formas: "Correo","E-mail", "e-mail", y "email"; todos tienen el mismo significado. La transmisión de Email es la transmisión de mensajes de texto sobre redes de comunicación. La mayoría de las redes tienen alguna forma de sistema de correo (email) están confinados a una sola red de ordenadores, pero otros tienen puertas de enlace a otras redes (lo que les permite comunicar con múltiples ubicaciones), o con Internet (lo que permite enviar correo a cualquier sitio en el mundo).

La mayoría de los sistemas de correo incluyen alguna forma de *cliente de correo* (también referido como *cliente mail* o simplemente *cliente*) que contiene un editor de texto y otras herramientas para redactar mensajes, y uno o más *servidores* que reciben el correo de los clientes y lo envían a la *dirección de correo* (o direcciones) especificadas en el mensaje, y luego son enrutados por el servidor hacia otro servidor que es responsable de almacenar los mensajes destinados a dicha dirección. Si el destino del mensaje es una dirección local para la que el servidor original es responsable entonces puede almacenarse en el servidor original en lugar de ser enrutado a otro. Por último, el destinatario del mensaje conectará con su servidor y recogerá el mensaje usando su cliente de correo. Este proceso entero de transferir un mensaje de correo de su cliente a su servidor de destino normalmente sólo toma unos cuantos segundos o minutos.

Además de contener texto simple, los mensajes de correo también pueden incluir archivos *adjuntos*. Estos adjuntos pueden ser cualquier tipo de archivo que desee: fotografías, archivos de texto, archivos de programa, otros mensajes de correo, y demás. sin embargo, puesto que la mayoría de sistemas de correo sólo soporta el envío de archivos de texto, los adjuntos deben ser primero codificados (convertidos a formato texto) antes de poder ser enviados, y luego decodificados cuando llegan a su destino final. Este proceso lo hacen normalmente de manera automática los clientes de correo de recepción y envío.

Todos los Proveedores de Servicios de Internet (ISPs) ofrecen correo. La mayoría también soportan puertas de enlace para que pueda intercambiar correo con usuarios de otros sistemas de correo. A pesar de que hay muchos protocolos diferentes que se usan para procesar correo por muchos sistemas de correo distintos, diversos estándares comunes hacen posible para los usuarios intercambiar mensajes en virtualmente todos los sistemas.

Dirección de Email (Dirección de Correo)—Un nombre o cadena de caracteres que identifica un buzón electrónico al que se puede mandar correo. Las direcciones de correo son las ubicaciones de y desde donde los mensajes de correo se mandan. Los servidores de correo necesitan las direcciones de correo para poder enrutar los mensajes a sus destinos correctos. Diferentes tipos de redes tienen diferentes formatos de dirección de correo, pero en Internet todas las direcciones de correo tienen la forma: "buzon@ejemplo.com".

Por ejemplo,

```
Michael.Mason@altn.com
```

Cliente de Correo—También llamado *cliente de mail o correo* (o sólo *cliente*), un *cliente de correo* es una aplicación de software que le permite enviar, recibir, y organizar correo. Está basada en arquitectura cliente-servidor; un cliente se usa para redactar el correo y luego mandarlo al servidor, que luego lo enruta al servidor del destinatario desde el que será recuperado por el cliente del destinatario. Normalmente, los clientes de correo son aplicaciones de software instaladas en la máquina del usuario, pero productos tal como MDaemon contiene un cliente

incorporado que "sirve" a los navegadores web de los usuarios. Así, su navegador se usa como cliente en lugar de necesitar instalar uno en su máquina. Esto aumenta enormemente la portabilidad y utilidad del correo.

Encriptación—Una medida de seguridad, *encriptación* es codificar o mezclar la información en un archivo para que sólo sea inteligible cuando haya sido decodificada o desencriptada. La encriptación se usa de manera habitual en el correo electrónico para que se un tercero intercepta el correo no pueda leerlo. El mensaje se encripta cuando se envía y se desencripta cuando llega a su destino final.

Ethernet—El tipo más común de conexión usado en Redes de Area Local (LAN). Dos de las formas más ampliamente usadas de Ethernet son 10BaseT y 100BaseT. Un Ethernet 10BaseT puede transferir datos a velocidades de hasta 10 mbps (megabits por segundo) a través de conexión inalámbrica o por cable. Una Ethernet 100BaseT transfiere datas a velocidades de hasta 100 mbps. Una Gigabit Ethernet puede transferir datos a velocidades de hasta 1000 mbps y la usan algunos ordenadores Apple.

ETRN—Acrónimo que significa **E**xtended **TURN**. Es una extensión de SMTP que permite a un servidor SMTP enviar una solicitud a otro servidor SMTP para enviar, o "desencolar", correo que está siendo retenido por éste. Dado que SMTP por sí mismo no puede solicitar correo (el correo normalmente se recolecta a través de protocolos POP o IMAP), esto hace posible para el servidor SMTP que hace la petición ETRN que el servidor remoto empiece una sesión SMTP y empiece a enviar el correo almacenado al host especificado en la petición.

El comando `TURN` usado para este propósito suponía un riesgo de seguridad puesto que hacía que la sesión SMTP hiciera una dirección inversa y empezar a enviar el correo almacenado de manera inmediata sin ningún tipo de verificación o autenticación de que el servidor solicitante fuera realmente quien decía ser. `ETRN` empieza una nueva sesión de SMTP en lugar de invertir la dirección. Así si el servidor que realiza la petición es un host "suplantado", el servidor de envío seguirá intentando enviarlo al servidor de correo real en su lugar. Actualmente existe una propuesta de estándar que introduce el Authenticated TURN (`ATRN`), que, al igual que `TURN`, invierte la dirección de la sesión SMTP, pero requiere autenticación antes de hacerlo. Este nuevo estándar es On-Demand Mail Relay (ODMR).MDaemon ofrece soporte tanto para ETRN como para ATRN de ODMR.

ETRN se detalla en el RFC 1985, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMR se detalla en el RFC 2645, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ—En inglés pronunciado junto como "fac" o como las letras separadas "F-A-Q", FAQ significa "**F**requently **A**sked **Q**uestions" (Preguntas más frecuentes). Las FAQs son documentos que proveen contestaciones a las preguntas más frecuentes de un asunto en concreto. Normalmente aparecen en algún formato tipo lista con cada cuestión listada y seguida de la respuesta. En FAQs grandes, a veces todas las preguntas se listan al principio del documento con sus referencias (o hiperenlaces si son FAQs online) a la ubicación de la pregunta y respuesta en el documento. Las FAQs se usan frecuentemente como punto inicial para soporte técnico e instrucciones—se puede ahorrar una gran cantidad de

tiempo y esfuerzo si tiene acceso a FAQ que contesten a su preguntan en lugar de estar forzado a contactar con el soporte técnico.

File Transfer Protocol—Ve la entrada FTP posterior.

Firewall—En terminología de ordenadores, un *firewall* existe cuando toma medidas de seguridad, bien a través de software o hardware, para separar una red de ordenadores en una o más partes, o de otro modo limitar el acceso a ella a usuarios concretos. Por ejemplo, puede querer dejar ver a todos la página inicial del sitio web alojado en su red, pero permitir sólo a algunos empleados que accedan a un área de "sólo empleados". Independientemente del método que use para conseguirlo—requerir una contraseña, permitir conexiones sólo de ciertas direcciones IP, o similares—el área de empleado se dirá que está detrás de un firewall.

FTP—Acrónimo para "**F**ile **T**ransfer **P**rotocol" (Protocolo de Transferencia de Archivos). Es un método común y eficaz de transferir archivos a través de Internet de un ordenador a otro. Existen aplicaciones cliente/servidor específicas diseñadas para este propósito llamadas "servidores FTP" y "clientes FTP"—Filezilla, por ejemplo, es uno de los clientes más comunes. Normalmente los clientes FTP pueden ejecutar bastantes otras funciones además de simplemente transferir archivos y son por lo tanto productos muy potentes. Algunos navegadores web también contienen soporte para FTP, aunque a veces sólo para descarga. Adicionalmente, la mayoría de los servidores FTP son "FTP anónimos", lo que significa que cualquiera puede acceder a ellos para descargar archivos—normalmente especificando "anonymous" como nombre de usuario y su dirección de correo como contraseña. Muchas veces puede descargar archivos desde sitios de FTP anónimos sin tener que identificarse en absoluto—pueden obtenerse simplemente haciendo clic en un enlace. Para los navegadores que soportan FTP, habitualmente todo lo que se necesita hacer es conectar al sitio FTP usando "ftp://..." en su URL en lugar de "http://..."

FTP se detalla en RFC-959, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc959.txt

Puerta de Enlace (Gateway)—Hardware o software de ordenador que traduce datos entre dos aplicaciones o redes con protocolos que no son similares. "Puerta de Enlace" también se usa para describir cualquier manera de proveer acceso de un sistema a otro. Por ejemplo, su ISP es una puerta de enlace a Internet.

El Servidor de Mensajería MDaemon puede funcionar como puerta de enlace de correo para otros dominios a través de la funcionalidad de Puertas de Enlace de Dominio. Actúa como intermediario, o Puerta de Enlace, recolectando el correo del dominio y luego reteniéndolo hasta que el dominio lo recolecta. Esto es útil tanto para dominios que no mantienen una conexión continua a Internet como para dominios que requieren de un servidor de respaldo en caso de que su servidor no esté disponible.

GIF—"**G**raphics **I**nterchange **F**ormat" es un formato popular para archivos de imagen y es el formato más común de imagen encontrado en Internet. GIF usa colores indexados o una paleta de un cierto número de colores, lo que reduce considerablemente el tamaño—especialmente cuando la imagen contiene grandes áreas del mismo color. Su reducido tamaño le permite transferirse con rapidez entre sistemas y cuentas para popularizarlos. La fórmula de compresión GIF fue originalmente desarrollada por CompuServe y por lo tanto verá a veces referencias a éste como CompuServe GIF.

Graphical User Interface—Vea la entrada GUI posterior.

GUI—Pronunciado en inglés "gooey", es el acrónimo de "**G**raphical **U**ser **I**nterface" (Interfaz Gráfica de Usuario) El GUI hace que sea posible interactuar con su ordenador o aplicación usando un dispositivo de puntero para hacer clic en elementos gráficos de la pantalla en lugar de teclear texto en una línea de comando. Los sistemas operativos de Microsoft Windows y Apple Mac son ambos basados en GUI, pero—aunque fue primero introducida por Apple—la idea de una interfaz gráfica de usuario fue originada realmente en Xerox.

Host—Cualquier ordenador en una red que actúe como servidor para otros ordenadores de la misma red. La máquina host puede estar ejecutando un servidor web, servidor de correo, u otros servicios, y es común que provea de distintos servicios a la vez. También se usa habitualmente el verbo "hospedar". Por ejemplo, una máquina que ejecuta un servidor de correo estará "hospedando" el correo.

En las redes peer-to-peer es común que las máquinas sean ambas clientes y hosts al mismo tiempo. Por ejemplo, su máquina puede hospedar la impresora de la red, pero puede ser usada también por usted como cliente para recolectar y descargar correo y archivos de otro host.

HTML—Acrónimo para "**H**yper**t**ext **M**arkup **L**anguage" (Lenguaje de Marcas de Hipertexto). Es el lenguaje de codificación usado para crear documentos de Hipertexto usados en el World Wide Web. Para ponerlo de manera sencilla, un documento HTML es un documento de texto llano que contiene códigos de formato y etiquetas que el navegador web del usuario interpreta y presenta como una página web completa con texto y colores formateados. Por ejemplo, un navegador que reciba un documento HTML que contenga el texto "<B>Texto</B>" presentaría la palabra "Texto" en negrita. Dado que los archivos de texto plano son muy pequeños, ello hace posible que sean transferidos rápidamente a través de Internet.

HTTP—Hyper**t**ext **T**ransfer **P**rotocol (HTTP - Protocolo de Transferencia de Hipertexto) es el protocolo que se usa para transferir archivos de hipertexto entre ordenadores en Internet. HTTP requiere un programa cliente en un extremo (normalmente un navegadores web) y un servidor HTTP en el otro.

HTTP se detalla en el RFC-2616, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc2616.txt

Hypertext—Cualquier texto que contenga un hipertexto o salto a otro documento o lugar dentro del mismo documento se llama hipertexto. Algunas veces el texto también es llamado enlace de hipertexto o simplemente enlace. El hipertexto puede ser bien una frase o palabra y tiene el enlace incrustado en él para que al hacer clic le desplace a la ubicación "marcada" o haga que el documento enlazado se muestre. Normalmente los enlaces de hipertexto son evidentes dado que el texto se subraya con un color distinto, pero no es un requisito. Algunas veces el hipertexto se mostrará igual que el texto normal, pero caso siempre será indicado por algún tipo de cambio gráfico de su cursor cuando el puntero del ratón se pause encima de él.

Hypertext Markup Language—Vea la entrada HTML anterior.

IMAP—Desarrollado por la Universidad de Stanford, **I**nternet **M**essage **A**ccess **P**rotocol (IMAP) es un protocolo usado para gestionar y recopilar mensajes de correo. La última versión es IMAP4 y es similar a POP3 pero con un número de

funcionalidades adicionales. IMAP4 es conocido como un protocolo usado para gestionar los mensajes de correo en el servidor en lugar de en la máquina local del usuario—los mensajes pueden ser buscados por palabras claves, organizados en carpetas, especialmente seleccionados para descarga, y otras funcionalidades, todo mientras siguen estando en el servidor. Así pues IMAP exige menos demanda de la máquina del usuario y centraliza el correo para que pueda ser accedido desde múltiples ubicaciones.

IMAP se detalla en RFC-2060, que puede ser visualizado en:

http://www.rfc-editor.org/rfc/rfc2060.txt

Extensión ACL de IMAP4—Vea la entrada ACL anterior.

Internet—Internet fue creado en 1969 por los militares de los Estados Unidos, originalmente para ser una red de comunicación que no pudiera ser destruida durante una guerra nuclear. Ahora consiste en millones de ordenadores y redes alrededor del mundo. Por diseño, Internet es descentralizado—no está controlado por ninguna empresa, organización o país. Cada host (o máquina) en Internet es independiente de los otros y puede proveer cualquier servicio de información que sus operadores deseen hacer disponibles. No obstante, la mayoría de la información que se transfiere a Internet en algún punto pasa a través de "backbones", que son conexiones de ancha banda extremadamente rápidas controladas por las organizaciones y los Proveedores de Servicios de Internet más grandes. La mayoría de la gente accede a Internet a través de un servicio online tal como AOL o a través de un Proveedor de Servicios de Internet (ISP) que mantiene o está conectado a uno de estos backbones.

Mucha gente cree que la *World Wide Web* (WWW) e Internet son la misma cosa, pero no es el caso. La WWW es sólo una parte de Internet y no Internet en sí mismo. Es la parte más popular, visible, y más utilizada comercialmente, pero sigue siendo sólo una parte.

Intranet—Para ponerlo de manera sencilla, una intranet es una red pequeña o privada de Internet usada estrictamente dentro de la red de la empresa u organización. Aunque las intranets varían considerablemente desde una organización a otra, pueden contener cualquier funcionalidad disponible en Internet. Pueden tener sus propios sistemas de correo, directorios de archivos, páginas web para navegar, artículos para leer, y demás. La diferencia principal entre una intranet e Internet es relativamente pequeña y está confinada a una organización o grupo.

IP—Acrónimo para "**I**nternet **P**rotocol" (Protocolo de Internet, como en TCP/IP). Los protocolos de Internet hacen posible que los datos sean transferidos entre sistemas a través de Internet. Sin importar la plataforma o sistema operativo de cada máquina, si se usa el mismo Protocolo de Internet en cada máquina podrán transferir datos a cada una. El término "IP" también se utiliza de manera común como abreviación a "Dirección IP". El estándar actual del Protocolo de Internet es IP versión 4 (IPv4).

El Protocolo de Internet se detalla en el RFC-791, que puede ser visualizarse en:

http://www.rfc-editor.org/rfc/rfc791.txt

Dirección IP—Ocasionalmente llamado Número IP, la Dirección IP significa Dirección de Protocolo de Internet y se usa para identificar una red particular de TCP/IP y los hosts o máquina de dicha red. Es una dirección numérica de 32-bits que contiene cuatro números entre 0 y 255 separados por puntos (p.ej.

"127.0.0.1"). Dentro de una red aislada, cada ordenador debe tener una dirección IP única, que puede ser asignada aleatoriamente. Pero, cada ordenador en Internet debe tener una IP registrada para evitar la duplicación. Cada dirección IP de Internet puede ser bien estática o dinámica. Las direcciones estáticas no cambian y siempre representan la misma ubicación o máquina en Internet. Las direcciones IP dinámicas cambian y son normalmente asignadas por un ISP a los ordenadores que están solamente en Internet de manera temporal—tal como cuando un usuario realiza una conexión a Internet por marcación. Sin embargo, aun así es posible tener una dirección IP estática en una cuenta por marcación.

Los ISPs y las grandes empresas normalmente intentan adquirir un rango o conjunto de direcciones IP del Servicio de Registro de InterNIC para que todos los clientes de su red o que utilicen sus servicio tengan direcciones similares. Estos conjuntos se dividen en tres clases: Clase A, B, y C. Los conjuntos de Clase A y B son usados por organizaciones muy grandes y soportan 16 millones y 65.000 hosts respectivamente. Los conjuntos de Clase C son para redes más pequeñas y soportan 255 hosts. Los conjuntos de Clase A y Clase B son ahora muy difíciles de conseguir debido a las pocas direcciones disponibles; consecuentemente la mayoría de empresas tienen que conformarse en su lugar con conjuntos de Clase C en su lugar. Debido a la falta de direcciones IP, existe un nuevo protocolo de direcciones IP llamado Classless Inter-domain Routing (CIDR) que gradualmente está reemplazando el sistema antiguo.

El actual estándar de Protocolo de Internet, IPv4, se detalla en el RFC-791, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc791.txt

IP versión 6 (IPv6) se detalla en el RFC-2460 en:

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDR se detalla en los RFCs 1517-1519 en:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Número IP—Vea la entrada superior *Dirección IP.*

ISP—Un **I**nternet **S**ervice **P**rovider (ISP o Proveedor de Servicios de Internet) es una empresa que provee acceso Internet y servicios al usuario final. La mayoría de ISPs proveen de múltiples servicios de Internet a sus clientes, tal como: acceso WWW, correo, acceso a grupos de noticias y servidores de noticias, y demás. Típicamente, los usuarios conectarán a sus ISP a través de marcación, o alguna otra forma de conexión, y luego el ISP les conectará a un router, que les enrutará al backbone de Internet.

Java—Desarrollado por Sun Microsystems, Java es un lenguaje de programación orientado a red con una sintaxis parecida a C/C++ pero que se estructura alrededor de clases en lugar de funciones. En las aplicaciones de Internet se usa comúnmente para programar applets, que son pequeños programas incrustados en páginas web. Estos programas pueden ser automáticamente descargados y ejecutados por el navegador de un usuario para proveer de un gran número de funciones que no harían que fuera normalmente posible sólo con HTML u otros lenguajes de script, y sin miedo de virus que dañen su ordenador. Dado que Java

es tanto eficiente como fácil de usar, se está haciendo popular entre muchos desarrolladores de software y hardware.

JavaScript—No debe confundirse con Java, JavaScript fue desarrollado por Netscape como un lenguaje de script diseñado para extender las capacidades de HTML y crear páginas web interactivas. Es un lenguaje de programación sencillo y fácil de usar, que lo hace mucho más sencillo que Java y otros lenguajes pero también tiene límites hasta cierto punto. aun y con sus limitaciones es muy potente para agregar un número de elementos interactivos en las páginas web. Por ejemplo, JavaScript es útil cuando quiere que los datos sean preprocesados antes de que sean enviados al servidor, o cuando quiere que sus páginas respondan a la interacción de usuario con enlaces o elementos de formulario. También puede usarse para controlar plugins y applets basados en las selecciones del usuario, y para conseguir un gran número de otras funciones. JavaScript se incluye dentro del texto de los documentos HTML y es interpretado por los navegadores para ejecutar sus funciones.

JPEG—Un formato de archivos gráfico muy eficiente en comprimir imágenes de muchos-colores y fotografías—mucho más que el formato GIF. Mientras que GIF es la mejor opción para imágenes que contienen formas regulares y grandes áreas de patrones repetitivos de color, JPEG es mucho más adecuado para imágenes con patrones irregulares y un gran número de colores. JPEG es el formato más común para imágenes de mucho colorido y fotografías en Internet. El acrónimo JPEG proviene de "**J**oint **P**hotographic **E**xperts **G**roup"—el grupo que desarrolló el formato.

Kbps—Comúnmente usado cuando se habla de velocidades de módem (p.ej. 56 Kbps), este acrónimo significa "**K**ilo**b**its **Po**r **S**egundo". Es el número de kilobits (1000 bits) de datos que son movidos o procesados cada segundo. Note que es kilo*bits* y no kilo*bytes*—un kilobyte es ocho veces más datos que un kilobit.

Kilobyte—Un kilobyte (K o KB) es mil bytes de datos de ordenador. Técnicamente es 1024 bytes (2^10 = 1024) pero en usos normales se suele redondear a 1000 por simplicidad.

LAN—Una **L**ocal **A**rea **N**etwork (LAN-Red de Area Local) es una red de ordenadores limitada a un único edificio o área, normalmente teniendo todos sus nodos (ordenadores o estaciones de trabajo) conectados juntos con alguna configuración de cables u otros tipos de medios. La mayoría de las grandes empresas tienen una LAN, lo que simplifica enormemente la gestión y compartición de la información entre los empleados y oficinas. La mayoría de LANs utilizan algún tipo de sistema de correo o chat, y comparten dispositivos tales como impresoras para evitar tener que tener un dispositivo separado para cada estación. Cuando los nodos de la red se conectan vía líneas de teléfono, ondas de radio, o enlaces de satélite se las llama Wide Area Network (WAN) en lugar de LAN.

Latencia—El tiempo que tarda un paquete de datos en desplazarse en una conexión de red. Mientras se está enviando un paquete de datos, existe un tiempo "latente" durante el que el ordenador remitente espera confirmación de que se ha recibido el paquete. Además del ancho de banda, la latencia es uno de los factores que determinan la velocidad de su conexión.

LDAP—Lightweight **D**irectory **A**ccess **P**rotocol (LDAP-Protocolo ligero de acceso a directorio) es un servicio de protocolo de directorio online que simplifica el Protocolo de Acceso a Directorio (DAP). El sistema de directorio en una estructura jerárquica consiste de los siguientes niveles: La "raíz" o el inicio del

directorio, país, organización, unidad organizativa, e individuales dentro de dicha unidad. Cada entrada LDAP es una colección de atributos con un identificador único, llamado nombre distinguido (DN). Dado que es un protocolo abierto, es eficiente, y tiene la habilidad de ser distribuido entre muchos servidores. LDAP puede hacer eventualmente posible para virtualmente cualquier aplicación de cualquier plataforma acceder a información de directorio para localizar direcciones de correo, empresas, archivos, y demás a nivel mundial.

LDAP se detalla en el RFC-2251, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc2251.txt

Enlace—Vea la entrada *Hyperenlace.*

Servidor de Listas—Una aplicación de servidor que se usa para distribuir mensajes de correo a múltiples destinatarios simplemente direccionando el mensaje a una única dirección. Para ponerlo de manera sencilla, cuando un mensaje de correo va destinado a una *lista de correo* mantenida por el servidor de listas el servidor lo enviará automáticamente a todos los miembros de la lista. Las listas de distribución tienen normalmente una única dirección de correo normal (por ejemplo, lista@ejemplo.com) pero dicha dirección hace referencia a una lista completa de destinatarios en lugar de a una persona específica o buzón. Cuando alguien se *suscribe* a una lista de correo, el servidor de lista añadirá automáticamente la dirección a la lista y distribuirá futuros correos destinados a la lista a dicha dirección, o miembro, y a todos los otros miembros. Cuando alguien se desuscribe, el servidor de lista simplemente eliminará la dirección para que no reciba más mensajes de lista.

Frecuentemente el término listserv se usa de manera genérica para referirse a cualquier servidor de lista. Sin embargo, Listserv® es una marca registrada de L-Soft international, Inc. y es un programa especial desarrollado por Eric Thomas para BITNET en 1986. A parte de otros servidores de lista, MDaemon está equipado con un conjunto de funciones y funcionalidades de servidor de lista o servidor de distribución.

Logon—Un código o serie de caracteres usados para obtener acceso o para identificarse a sí mismo en un servidor o máquina. En la mayoría de los casos debe ir acompañado de una contraseña para obtener acceso.

Existen muchos términos usados como sinónimos de "logon", tales como *login*, *acceso*, *nombre de usuario*, *username*, *D de usuario*, *sign-in*, y otros. Frecuentemente "logon" también se usa como verbo. Por ejemplo, "Voy a hacer *logon* al servidor de correo". En dicho contexto, sin embargo, el uso más común (y probablemente más apropiado) es "Voy a acceder al servidor de correo".

Buzón—Un área en la memoria o en un dispositivo de almacenaje que está asignada a una dirección de correo específica donde se almacenan los mensajes de correo. En un sistema de correo, cada usuario tiene un buzón privado en el que los mensajes se almacenan cuando el usuario de dicho servidor de correo los recibe. También es común que se use el término "buzón" cuando se refiere a la porción más a la izquierda de una dirección de correo. Por ejemplo, "usuario01" en "usuario01@ejemplo.com" es el buzón mientras que "ejemplo.com" es el nombre de dominio.

Lista de Correo—También llamado grupos de correo, una lista de correo es un grupo de direcciones de correo identificadas por una única dirección de correo. Por ejemplo, "lista@ejemplo.com". Típicamente cuando un servidor de listas

recibe un mensaje de correo dirigido a una de sus listas el mensaje se distribuirá automáticamente a todos los miembros de la lista (todas las direcciones incluidas en la lista). MDaemon está equipado con un extenso juego de funcionalidades de lista de correo que le permiten hacer listas públicas o privadas (cualquiera puede publicar o acceder, o sólo los miembros pueden publicar o acceder), enviar mensajes en formato resumen o mensajes individuales, y se pude usar en una gran variedad de otras maneras.

Megabyte—Aunque son técnicamente 1.048.576 bytes (o 1024 kilobytes), un megabyte se redondea comúnmente y se usa para referirse a un millón de bytes. Megabyte se abrevia como: "MB", como en "20 MB".

MIME—Definido en 1992 por la Internet Engineering Task Force (IETF), **M**ultipurpose **I**nternet **M**ail **E**xtensions (MIME - Extensiones de Correo de Internet Multipropósito) es el método de codificación estándar para adjuntar archivos que no son de texto a mensajes de correo de Internet estándar. Dado que típicamente sólo se pueden transferir archivos de texto vía correo, los archivos que no lo son deben ser primero codificados a un formato de texto llano y luego decodificados después de que llegan a su destino. Así pues, un programa de correo dice ser Compatible con MIME si puede tanto enviar como recibir archivos usando el estándar MIME. Cuando un adjunto de mensaje codificado MIME es enviado, normalmente tanto el tipo de archivo que se envía como el método que debe usarse para volverlo a su original están especificados como parte del mensaje. Existen muchos tipos predefinidos de contenido MIME, tal como "image/jpeg" y "text/plain" Sin embargo, también es posible definir su propios tipos MIME.

El estándar MIME también es usado por los servidores para identificar los archivos que se envían a los navegadores web. Dado que los navegadores soportan varios tipos de MIME, esto permite al navegador mostrar archivos que no están en formato HTML. Además, actualizando la lista de Tipos-MIME del navegador y el software que se usa para gestionar cada tipo, pueden ofrecer soporte rápidamente para nuevos formatos.

MIME se detalla en los RFCs 2045-2049, que pueden ser visualizados en:

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—Un servidor (normalmente un servidor FTP) que tiene una copia de los mismos archivos que están en otro servidor. Su propósito es generalmente proveer de una ubicación alternativa desde donde descargar los archivos de mirror si el servidor principal está sobrecargado o caído. El término "mirror" puede también referirse a la configuración donde la información se escribe en más de un disco duro de manera simultánea. Esto se usa como medida de redundancia para que si un disco falla el ordenador pueda continuar operando sin perder ningún dato vital.

Módem—Acrónimo derivado de **mo**dulador-**dem**odulador. Un módem es un dispositivo conectado a un ordenador que permite la transferencia de datos a otros ordenadores a través de líneas telefónicas. El módem convierte los datos

digitales del ordenador a formato analógico (los modula) y luego los transmite a otro módem donde se invierte el proceso (demodula). Para ponerlo de manera sencilla, un módem es un convertidor analógico-a-digital y digital-a-analógico. La velocidad a la que los datos son transferidos se expresa o bien en ratio de baudios (p.ej. 9600 baudios) o kilobits por segundo (p.ej. 28.8 kbps).

MultiPOP—Componente de MDaemon que puede ser configurado para recolectar correo, vía el protocolo POP3, simultáneamente desde varios servidores de correo para los usuarios de MDaemon. Esto hace posible para los propietarios de cuentas de MDaemon que tengan cuentas en otros lugares u otros servidores de correo que sean recolectadas y procesadas con su cuenta de correo de MDaemon. Así pues almacenan todo su correo en un sólo buzón.

NAT—Vea la entrada posterior Network Address Translation - Traducción de Direcciones de Red.

Red—Dos o más ordenadores conectados juntos de algún modo. El propósito de una red es permitir la compartición de recursos y de información entre múltiples sistemas. Algunos ejemplos comunes son: múltiples ordenadores compartiendo impresoras, unidades de DVD-ROM, discos duros, archivos individuales y demás.

Existen muchos tipos de redes, pero los tipos más ampliamente definidos son las Redes de Area Local (LANs) y las Redes de Area Amplia (WANs). En una LAN, los ordenadores individuales (o nodos) están geográficamente cerca—normalmente en el mismo edificio. También se conectan normalmente de manera directa con cables, aunque las conexiones inalámbricas también se están volviendo muy comunes. Los nodos en una WAN están normalmente separados (en otro edificio o ciudad) y se conectan a través de líneas de teléfono, conexiones de satélite, u otras formas de conexión.

Internet en sí mismo es una red. Se suele describir como la Red de Redes.

Network Address Translation-Traducción de Direcciones de Red—Network address translation (NAT) es un sistema donde dos conjuntos de Direcciones de Protocolo de Internet (direcciones IP) son usadas por una sola red—una para el tráfico externo y otra para el tráfico interno. Esto se usa principalmente como medida de firewall para ayudar a asegurar la red. Su ordenador parecerá tener una dirección IP determinada fuera de su LAN mientras que su IP real es radicalmente distinta. El hardware y software colocado "entre" su red e Internet ejecuta la traducción entre las dos direcciones. Usando este método, es común que varios ordenadores de una LAN "compartan" una dirección IP de la empresa. Así pues no existe manera para alguien desde el exterior de saber su dirección real y conectar directamente con su ordenador sin estar primero identificado o autenticado durante la traducción.

Network Interface Card-Tarjeta de Interfaz de Red—Una network interface card (NIC) es una placa de circuitos de ordenador que permite al ordenador conectarse a una red. Las NICs ofrecen conexión permanente a la red mientras que un módem (usado por algunos ordenadores caseros para acceder a la red vía línea de teléfono) normalmente provee sólo de una conexión temporal. La mayoría de las NICs están diseñadas para tipos específicos de redes y de protocolos, tal como Ethernet o token ring y TCP/IP.

Network News Transfer Protocol-Protocolo de Transferencia de Noticias en Red—Vea la entrada posterior NNTP.

NIC—Vea la entrada anterior Network Interface Card.

NNTP—Network **N**ews **T**ransfer **P**rotocol - Protocolo de Transferencia de Noticias en Red (NNTP) es el protocolo usado para transferir y distribuir mensajes a grupos de noticias USENET. Los navegadores más comunes y clientes de correo tiene clientes de NNTP integrados.

NNTP se detalla en el RFC-977, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc977.txt

Nodo—Cualquier ordenador por sí mismo conectado a una red.

ODMR—On-**D**emand **M**ail **R**elay (Transmisión de Correo bajo demanda) es un nuevo protocolo designado para habilitar a los servidores de correo con sólo una conexión intermitente a proveedores de servicios, y que no tienen una dirección IP estática, para recibir correo de manera similar a aquellos servidores que sí que disponen de ella y que usan el comando `ETRN`. Si el sistema tiene una dirección IP estática, el comando ESMTP ETRN puede usarse. Sin embargo, los sistemas con direcciones IP dinámicas no tienen de una opción implementada ampliamente. ODMR resuelve este problema. Juntamente con otras cosas, ODMR introduce el comando Authenticated TURN (`ATRN`) que hace que el flujo de una sesión de SMTP sea invertido (como el antiguo comando TURN) pero con la seguridad añadida de requerir que el servidor esté autenticado. Esto hace posible que un servidor SMTP con dirección IP dinámica conecte a su ISP y tenga el correo de uno o más hosts enviado a él vía SMTP en lugar de recolectarlo vía POP o IMAP. Esto ayuda a cubrir la demanda de una solución de bajo coste para aquellas empresas que necesitan su propio servidor de correo, pero no se pueden permitir una dirección IP estática o una presencia online dedicada.

ODMR se detalla en el RFC 2645, que puede ser visualizado en:

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM—Original **E**quipment **M**anufacturer (OEM) es normalmente un término que lleva a confusión. Una empresa OEM es una empresa que usa equipamiento de otras empresas o productos en su propio producto que se empaqueta o vende bajo una marca o empresa distinta. Por ejemplo, HyperMegaGlobalCom, Inc. es un OEM porque compra componentes de ordenador de una o más empresas diferentes, los pone todos juntos en un único producto personalizado, y luego lo vende con "HyperMegaGlobalCom" estampado en ellos. La empresa que le vendió a HyperMegaGlobalCom los componentes puede que también sea OEM si también adquirieron sus componentes de alguien más. "OEM" es nombre desafortunado puesto que los OEMs no son realmente los fabricante reales; son los "empaquetadores" o "personalizadores". A pesar de esto, mucha gente sigue usando a menudo el término "OEM" cuando se refiere a los fabricantes de hardware en lugar de a aquellos que lo empaquetan—y es comprensible.

Al vuelo—El término "al vuelo" se usa habitualmente de dos maneras distintas. Primero, se usa de manera habitual para denotar algo que pude hacerse "de manera rápida" o de manera sencilla mientras se está "en mitad" de hacer otra tarea. Por ejemplo, un producto de gestión de libros puede tener soporte para la creación de cuentas "al vuelo" mientras que está en medio de una entrada de ventas—"Simplemente pare de introducir los datos, haga clic en el botón X, introduzca un nombre, y luego continúe introduciendo las cifras". La otra forma en la que se usa "al vuelo" es cuando se refiere a algo que puede generarse dinámicamente en lugar de manualmente o de manera estática. Por ejemplo, usando la información almacenada en una "cookie" una página personalizada puede generarse "al vuelo" cuando un usuario vuelve al sitio web. En lugar de

requerir que alguien cree manualmente una página personalizada al gusto del usuario, puede generarse dinámicamente basándose en las acciones pasadas de esa persona durante su navegación.

Original Equipment Manufacturer—Vea la entrada anterior OEM.

Packet—Una unidad de datos de ordenador enviada sobre una red. Siempre que recibe datos de un ordenador a otro sobre la LAN o sobre Internet llega a su ordenador en forma de paquetes. El mensaje o archivo original se divide en estos paquetes, se transmite, y luego se recombina en destino. Cada paquete contiene su origen y destino, un bloque de datos de contenido, un código de comprobación de errores. También están "numerados" para que puedan ser conectados a los paquetes relacionados que se están enviando. El proceso de enviar y recibir paquetes se conoce como "intercambio de paquetes". Los paquetes también son comúnmente llamados "datagramas".

Intercambio de Paquetes—El proceso de envío de enviar y recibir paquetes sobre una red o Internet. En contraste al intercambio de circuitos (tal como en un teléfono análogo), que envía datos en un hilo continuo sobre una única ruta o circuito, el intercambio de paquetes transmite los datos en "paquetes", que puede que no tomen necesariamente la misma ruta para llegar a su destino. Además, dado que los datos están en unidades separadas, los usuarios múltiples pueden enviar diferentes archivos simultáneamente sobre la misma ruta.

Parámetro—Un parámetro es una característica o valor. En computación, es cualquier valor pasado a un programa por un usuario u otro programa. Su nombre y contraseña, una configuración de preferencias, tamaño de fuente, y demás, son todos parámetros. En programación, un parámetro es un valor pasado a una subrutina o función para procesamiento.

PDF—Portable **D**ocument **F**ormat (PDF) es un formato de archivo altamente comprimido y multi plataforma desarrollado por Adobe Systems Incorporated que captura el formato de documento, texto, e imágenes de una variedad de aplicaciones. Esto hace posible que el documento parezca el mismo y se imprima con precisión en distintos ordenadores y plataformas (a diferencia de muchos procesadores de texto). Para ver un archivo PDF se requiere Adobe Acrobat Reader, una aplicación gratuita distribuida por Adobe Systems. También existe un plug-in para ver archivos PDF con su navegador web. Esto hace posible ver los archivos PDF publicados en un sitio web directamente en lugar de tener que descargarlos antes y luego visualizarlos con un programa separado.

Parse (Procesar)—En lingüística, es dividir el lenguaje en sus componentes gramaticales para poder ser analizados. Por ejemplo, dividir una frase en verbos, adjetivos, nombres, y demás.

En ordenadores, parse (procesar) es dividir una instrucción en lenguaje de computador en partes que puedan ser de utilidad al ordenador. Un parser en un compilador es lo que coge la instrucción de programa que ha escrito un desarrollador y lo divide en parte que pueden ser usadas para desarrollar otras acciones o para crear las instrucciones que forman un programa ejecutable.

MDaemon y otros productos con frecuencia procesan los mensajes de correo para determinar su destino o los procesan a través de filtros y otras herramientas.

Ping—Un acrónimo para **P**acket **In**ternet **G**roper. Es un programa básico de Internet usado para determinar si una dirección IP específica es alcanzable y

acepta solicitudes. Lo hace enviando una solicitud de Echo de Mensaje de Protocolo de Control de Internet (ICMP) y esperando una respuesta. "Hacer Ping" se usa comúnmente como verbo cuando se refiere a este proceso. Por ejemplo, "Voy a hacer ping al servidor para ver si está online". "Hacer ping" a una dirección IP es normalmente tan simple como teclear "ping" seguido por la dirección IP o el dominio en el símbolo de sistema de DOS. Por ejemplo "Ping 192.0.2.0".

ICMP se detalla en RFC-792 y el protocolo Echo se detalla en RFC-862. Estos pueden verse en:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP—Significa **P**ost **O**ffice **P**rotocol. POP (también aparece comúnmente como POP3) es el protocolo de correo más común para solicitar correo de un servidor de correo. La mayoría de clientes usan el protocolo POP a pesar de que algunos también soportan el protocolo IMAP, más nuevo. POP2 se convirtió en un estándar a mediados de los 80 y requería SMTP para enviar mensajes. Se reemplazó con la nueva versión, POP3, que puede usarse con o sin SMTP. En inglés, POP se usa a veces como un verbo para recolectar correo de un servidor. Por ejemplo, "I'm going to POP my mailbox to get my mail." (Voy a recolectar mi correo).

POP3 se detalla en el RFC-1939, que puede verse en:

http://www.rfc-editor.org/rfc/rfc1939.txt

Port—En las redes TCP/IP y UDP e Internet, un puerto es el punto final de una conexión lógica y se identifica con un número del 0 a 65536. Los puertos del 0 al 1024 están reservados para su uso por ciertos protocolos y servicios con ciertos privilegios. Por ejemplo, los servidores web se listan típicamente en el puerto 80, los servidores SMTP normalmente se comunican en el puerto 25, y los servidores POP envían y reciben correo en el 110. Generalmente, sólo un programa a la vez puede usar o "enlazar", a cualquier puerto en una máquina dada. Cuando se navega por Internet, muchas veces algunos servidores se ejecutarán en puertos no por defecto, que requieren que se especifique el puerto después de la URL con dos puntos. Por ejemplo, "www.ejemplo.com:3000".

Los puertos también pueden usarse para referirse a los sockets de un ordenador usados para conectar dispositivos periféricos y hardware a él. Por ejemplo, los puertos de serie, puertos paralelos, puertos USB, y demás.

Finalmente, el puerto se usa generalmente para describir el proceso de hacer que un programa diseñado para una plataforma específica o máquina funcione en otra plataforma. Por ejemplo, "portar una aplicación Windows a UNIX" o "crear un puerto UNIX para una aplicación".

Publicar-Publicación—En mensajería de Internet, tal como el correo o los grupos de noticias, es cuando se envía un mensaje a un sistema de comunicación en red para que otros lo vean. Por ejemplo, un mensaje mostrado en un grupo de noticias, lista de correo, o tablón de discusión es una publicación. También puede usarse en el modo "publicar un mensaje a la lista de correo o grupo de noticias".

PPP—Significa "Point to Point Protocol" (Protocolo punto a punto). Es el estándar de Internet para conexiones por marcación. PPP es un conjunto de reglas que define cómo su conexión de módem intercambia paquetes de datos con otros sistemas en Internet.

PPP se detalla en el RFC-1661, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocolo—En computación, un protocolo es un conjunto de guías o estándares por los cuales servidores y aplicaciones se comunican. Existen muchos protocolos diferentes usados con diferentes propósitos, por ejemplo, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, y demás.

Registro—Una base de datos usado por Microsoft Windows para almacenar información de configuración sobre software instalado en el ordenador. Esto incluye cosas como configuraciones de usuario, asociaciones de extensión de archivo, fondos de escritorio, esquemas de colores, y muchas otras. Tiene las siguientes seis partes:

HKEY_User—Almacena la información de usuario para cada usuario del sistema.

HKEY_Current_User—Las preferencias para el usuario actual.

HKEY_Current_Configuration—Almacena las configuraciones para la visualización e impresoras.

HKEY_Classes_Root—Asociaciones de Archivo e información OLE.

HKEY_Local_Machine—Configuraciones de Hardware, sistema operativo, y aplicaciones instaladas.

HKEY_Dyn_Data—Datos de Rendimiento.

Cuando los programas están instalados en su ordenador el instalador normalmente escribe alguna información al registro automáticamente. Puede editar manualmente el registro, sin embargo, usando el programa regedit.exe integrado en Windows. Pero, debe ejercitar extrema precaución cuando lo haga porque si altera la configuración errónea hará que su ordenador no funcione correctamente, o no funcione en absoluto.

RFC—Request **F**or **C**omments es el nombre del resultado y el proceso de crear un estándar en Internet. Cada nuevo estándar y protocolo se propone y publica en Internet como un "Request For Comments." La Internet Engineering Task Force (IETF) facilita la discusión para nuevos estándares y eventualmente lo establece. A pesar del hecho de que el estándar se establezca y no se "soliciten" más "comentario", el estándar se seguirá usando el acrónimo de "Request for Comment" juntamente con su número identificador. Por ejemplo el RFC-822 (ahora superseído por el RFC-2822) es el estándar oficial, o "RFC," para correo. Sin embargo, algunos protocolos que se adoptan oficialmente como "estándares" no tiene un número oficial de estándar asociado con ellos que esté listado en el documento de Estándares Oficiales de Protocolo de Internet (que se nombra a si mismo STD-1 y actualmente RFC-3700). Puede encontrar RFCs en Internet en muchas ubicaciones, pero la fuente autoritativa es el Editor RFC, ubicado en http://www.rfc-editor.org/.

El documento de Estándares Oficiales de Protocolo de Internet está ubicado en:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF—Rich **T**ext **F**ormat (Formato de texto enriquecido) es un formato de archivo universal desarrollado por Microsoft y soportado por casi todos los procesadores de texto. En contraste al formato de texto plano, RTF le permite mantener el formato, información de fuente, color del texto, y demás. El tamaño de archivo de los archivos RTF puede ser muy grande cuando se compara a otros formatos de archivo tal como formato de documento de Word 2000 (*.doc) y Adobe PDF.

Server—Un ordenador, o programa que provee de un tipo específico de servicio a un cliente de software que se ejecuta en otros ordenadores. El término puede referirse a una pieza particular de software, tal como un servidor SMTP, o una máquina en la que dicho software se esté ejecutando. Una sola *máquina* servidor puede tener diferentes *programas* servidor ejecutándose de manera concurrente. Por ejemplo, su servidor de red puede que esté ejecutando un servidor web, servidor de correo, servidor FTP, servidor de fax, y otros, todos a la vez.

SMTP—Acrónimo para **S**imple **M**ail **T**ransfer **P**rotocol. Es el protocolo primario usado para enviar correo en Internet de un servidor a otro o de un cliente a un servidor. El SMTP consiste de un conjunto de reglas de cómo un programa que envía correo y un programa que recibe correo deben interactuar. Una vez el servidor ha recibido correo vía SMTP normalmente lo almacena y luego puede ser recuperado por el cliente vía POP, IMAP u otro protocolo.

El protocolo SMTP se detalla en el RFC-2821, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam—Correo basura en Internet. "Spam" se usa más comúnmente para referirse a correo masivo no solicitado, aunque se usa también con frecuencia para referirse a cualquier tipo de correo no deseado en general. Un "spammer" obtendrá cientos, miles o incluso cientos de miles de direcciones de correo de diversas fuente y luego enviará "spam" a la lista con mensajes o solicitudes. El "spam" puede, sin embargo, usarse para referir a un grupo de noticias o discusión también, cuando la publicación es algún anuncio no deseado o no relacionado con el producto o sitio web.

Spam se está convirtiendo rápidamente en un serio problema en Internet, consumiendo una gran cantidad de tiempo y recursos de servidor. Y dado que los spammers usan normalmente diversas técnicas para intentar enmascarar el origen del mensaje—tal como "suplantar" sus direcciones para que parezca que son alguien distinto o intentar retransmitir spam de manera encubierta a través de múltiples servidores—prevenirlo puede convertirse en un reto. El servidor MDaemon de Alt-N Technologies está equipado con un número de funcionalidades diseñadas específicamente para ayudar a combatir el spam, tal como: Listas DNS de Bloqueados (DNS-BL), Protección IP, Monitorización de IP, Control de Retransmisión, y otras.

El origen del uso del término "Spam" para referirse a correo basura es ampliamente debatido, pero se acepta de manera general que viene de un sketch popular de Monty Python en el que la palabra "spam" se repite constante y periódicamente acompañada por vikingos cantando, "Spam spam spam spam, spam spam spam spam..." Sin embargo, puede que sea simplemente una comparación con la marca registrada de un producto cárnico de Hormel del mismo nombre—todo el mundo lo prueba en un momento u otro, pero hay alguien que realmente lo pide o le guste?

TCP/IP—Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) ha sido descrito como la fundación de Internet. Es el paquete básico de protocolos de comunicación usado en Internet para conectar hosts. Es el protocolo más usado también para las Redes de Área Local. También es un sistema de dos capas, siendo la superior TCP, que maneja la fragmentación y defragmentación de archivos en paquetes para la transmisión por la red. IP, que es la capa inferior, gestiona el direccionamiento de los paquetes para que lleguen a sus destinos correctos. TCP se detalla en el siguiente RFC-793. IP se detalla en el RFC-791. Estos RFCs pueden encontrase en:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet—Un comando y programa usado para acceder a sitios de Internet que soportan acceso Telnet. El comando Telnet le lleva al símbolo de sistema del servidor Telnet. Si tiene una cuenta en dicho servidor, podrá acceder a los recursos permitidos tal como archivos, correo y demás. El inconveniente de Telnet es que es un programa de línea de comandos que usa comandos Unix.

El protocolo TELNET se detalla en los RFCs 854-855, que pueden visualizarse en:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminal—Un dispositivo que permite enviar comandos a un ordenador remoto. Un terminal es un teclado, pantalla de visualización, y algún circuito sencillo. Muchas veces, sin embargo, los ordenadores personales se usan para "emular" terminales.

Tiff—Acrónimo para **T**agged **I**mage **F**ile **F**ormat. Es un formato gráfico de archivo creado para ser un traductor universal de gráficos para múltiples plataformas. TIFF puede gestionar profundidades de color de entre 1-bit a 24-bits.

UDP—User **D**atagram **P**rotocol (UDP) es uno de los protocolos que forma parte del juego de protocolos que TCP/IP usa para transmisiones de datos. UDP es conocido por ser un protocolo sin estados dado que no informa de si los paquetes que están siendo enviados han sido recibidos.

UDP se detalla en el RFC-768, que puede visualizarse en:

http://www.rfc-editor.org/rfc/rfc768.txt

Unix—Unix, o UNIX, es un sistema operativo creado por los Laboratorios Bell en los años 60. Diseñado para ser usado por muchos usuarios al mismo tiempo, es el sistema de servidores más popular en Internet. Existen muchos sistemas operativos distintos basados en UNIX tal como Linux, GNU, Ultrix, XENIX, y otros.

URL—Cada archivo o servidor en Internet tiene una **U**niform **R**esource **L**ocator (URL). Es la dirección que se introduce en el navegador para llegar a dicho servidor o archivo. Las URLs no pueden tener espacios y siempre usan el carácter de barra normal. Existen dos partes separadas por "://". La primera parte es el protocolo que se está usando o recurso al que se dirige (por ejemplo, http, telnet, ftp, y demás) y la segunda parte es la dirección de Internet del servidor de archivo (por ejemplo, www.altn.com o 127.0.0.1).

Uuencode—Un conjunto de algoritmos para convertir archivos a series de caracteres de 7-bits ASCII para su transmisión en Internet. A pesar de que significa Unix-to-Unix encode (codificación Unix-a-Unix), ya no es exclusivo de UNIX. Se ha convertido en un protocolo universal usado para transferir archivos entre diferentes plataformas. Es un método de codificación comúnmente usado en el correo.

WAN—Una WAN, o **W**ide **A**rea **N**etwork, es similar a la Red de Area Local (LAN) pero normalmente ocupa múltiples edificios, o incluso ciudades. Las WANs se

componen a veces de redes LAN más pequeñas interconectadas. Internet podría describirse como la mayor WAN en el mundo.

Zip—Se refiere a archivos comprimidos o "zipeados", normalmente con la extensión de archivo ".zip". "Zipear" es comprimir uno o más archivos en un único archivo de almacén para poder ahorrar espacio o para facilitar una transferencia más rápida a otro ordenador. Para usar un archivo zip, sin embargo, necesitará descomprimirlo primero con el programa apropiado tal como PKZIP o WinZip. Existen múltiples utilidades de compresión/descompresión disponibles—ambas shareware y freeware—desde muchos sitios en Internet. Afortunadamente no tendrá que descomprimir la utilidad antes de poder instalarla.

Índice

- 2 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- V -

- W -

- X -