This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.

Copyright © 1996-2023 MDaemon Technologies, Ltd.
MDaemon® and related trademarks are the property of MDaemon Technologies, Ltd. and are registered and/or used in the U.S. and countries around the world. All trademarks are property of their respective owners.

User Manual

23.5

MDaemon Messaging Server
User Manual

Copyright © 1996-2023 MDaemon Technologies. Alt-N®, MDaemon®, and RelayFax® are trademarks of MDaemon Technologies.

Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

v23.5.0 - September 2023

Table of Contents

Section I MDaemon Messaging Server 23.5 11

1 MDaemon Features ... 12
2 System Requirements ... 14
3 New in MDaemon 23.5 ... 15
4 Upgrading to MDaemon 23.5.0 ... 59
5 Getting Help ... 64

Section II MDaemon's Main Display 67

1 Stats ... 68
AutoDiscovery Service ... 73
2 Event Tracking and Logging ... 77
Event Tracking Window's Shortcut Menu ... 79
3 Composite Log View ... 79
4 Tray Icon ... 80
Shortcut Menu ... 81
Locking/Unlocking MDaemon's Main Interface ... 82
5 Session Window ... 82
6 MDaemon's SMTP Work Flow ... 83

Section III Setup Menu 85

1 Server Settings ... 86
Servers & Delivery ... 86
Servers ... 86
Delivery ... 89
Sessions ... 92
Timeouts ... 95
Unknown Mail ... 97
DNS & IPs ... 99
DNS ... 99
Ports ... 101
IPv6 ... 104
Binding ... 105
IP Cache ... 106
Domain Sharing ... 108
Public & Shared Folders ... 110
Public & Shared Folders ... 113
Message Recall ... 115
Host Authentication ... 118
Priority Mail ... 119
Header Translation ... 121
Header Translation Exceptions ... 122
Archiving ... 123
Pruning ... 126
Signatures ... 127

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Default Signatures ... 127
Default Client Signatures ... 132
MultiPOP ... 137
DomainPOP ... 142
Host & Settings ... 144
Parsing ... 146
Processing ... 148
Routing ... 149
Foreign Mail ... 151
Name Matching ... 152
Archive ... 154
RAS ... 155
RAS ... 155
Logon ... 157
Processing ... 158
Logging ... 159
Log Mode ... 159
Composite Log ... 161
Statistics Log ... 163
Windows Event Log ... 165
Maintenance ... 166
Settings ... 168
More Settings ... 171
2 Domain Manager ... 174
Host Name & IP ... 177
Smart Host ... 179
Accounts ... 181
MDIM ... 183
Calendar ... 185
Webmail ... 187
Dequeuing ... 193
On-Demand Mail Relay (ODMR) ... 194
Signatures ... 195
Client Signatures ... 200
Settings ... 205
ActiveSync ... 207
Client Settings ... 208
Policy Manager ... 214
Assigned Policy ... 222
Accounts ... 223
Clients ... 232
3 Gateway Manager ... 239
Global Gateway Settings ... 243
Automatic Gateway Creation ... 245
Gateway Editor ... 247
Domain ... 247
Verification ... 248
Configuring Multiple LDAP Verification Queries ... 251
Forwarding ... 252
Dequeuing ... 253
Quotas ... 256
Settings ... 258
4 Mailing List Manager ... 259

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailing List Settings ... **262**
Mailing List Editor ... **265**
Members ... 265
Settings ... 268
Enhanced List Pruning ... 270
Headers ... 271
Subscription ... 274
Subscribing to Mailing Lists ... 276
Reminders ... 278
Digest ... 279
Notifications ... 281
Moderation ... 283
Routing ... 285
Support Files ... 287
Public Folder ... 289
Active Directory ... 290
ODBC ... 292
Configuring an ODBC Data Source ... 293
Creating a New ODBC Data Source ... 296
5 Public Folder Manager ... **300**
Access Control List ... **302**
6 Web & IM Services ... **308**
Webmail ... **308**
Overview ... 308
Calendar & Scheduling System ... 309
MDaemon Instant Messenger ... 309
Instant Messaging ... 310
Dropbox Integration ... 311
Using Webmail ... 312
Web Server ... 313
SSL & HTTPS ... 316
MDIM ... 320
Calendar ... 322
Free/Busy Options ... 322
RelayFax ... 324
Dropbox ... 325
Google Drive ... 328
Categories ... 332
Settings ... 333
Branding ... 341
Remote Administration ... **341**
Web Server ... 343
SSL & HTTPS ... 348
Running Remote Administration under IIS ... 352
Terms of Use ... **356**
Attachment Linking ... **357**
CalDAV & CardDAV ... **360**
XMPP ... **365**
7 Event Scheduling ... **369**
AntiVirus Scheduling ... **369**
AntiVirus Updates ... 369
Schedule ... 370
Mail Scheduling ... **372**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mail Sending & Collecting ... 372
MultiPOP Collection ... 375
Mail Schedule ... 377
8 MDaemon Connector ... 379
MC Server Settings ... 380
Settings ... 380
Accounts ... 381
MC Client Settings ... 382
General ... 384
Advanced ... 388
Folders ... 390
Send/Receive ... 391
Miscellaneous ... 393
Database ... 395
Signature ... 397
Add-ins ... 398
9 Cluster Service ... 399
Options/Customize ... 402
Shared Network Paths ... 404
Diagnostics ... 406
10 ActiveSync ... 408
System ... 408
Tuning ... 410
Client Settings ... 413
Security ... 420
Diagnostics ... 422
Protocol Restrictions ... 424
Domains ... 426
Policy Manager ... 434
Accounts ... 442
Clients ... 451
Groups ... 460
Client Types ... 466
11 Message Indexing ... 473
Options/Customize ... 473
Diagnostics ... 475
12 Preferences ... 477
Preferences ... 477
UI ... 477
System ... 480
Disk ... 482
Fixes ... 484
Headers ... 485
Updates ... 487
Miscellaneous ... 489
Windows Service ... 491
Section IV Security Menu 493
1 Health Check ... 496
2 Security Manager ... 498
Security Settings ... 498

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Relay Control ... 498
Reverse Lookup ... 500
POP Before SMTP ... 504
Trusted Hosts ... 505
Trusted IPs ... 506
Sender Authentication ... 507
IP Shield ... 507
SMTP Authentication ... 509
SPF Verification ... 512
DomainKeys Identified Mail ... 514
DKIM Verification ... 516
DKIM Signing ... 518
DKIM Settings ... 521
DMARC ... 523
DMARC Verification ... 530
DMARC Reporting ... 533
DMARC Settings ... 537
Message Certification ... 538
VBR Certification ... 541
Approved List ... 544
Screening ... 545
Sender Block List ... 545
Recipient Block List ... 547
IP Screen ... 548
Host Screen ... 550
SMTP Screen ... 552
Hijack Detection ... 554
Spambot Detection ... 556
Location Screening ... 558
From Header Screening ... 560
SSL & TLS ... 561
MDaemon ... 563
Webmail ... 566
Remote Administration ... 570
No STARTTLS List ... 574
STARTTLS List ... 575
SMTP Extensions ... 576
DNSSEC ... 579
Let's Encrypt ... 580
Other ... 582
Backscatter Protection - Overview ... 582
Backscatter Protection ... 583
Bandwidth Throttling - Overview ... 585
Bandwidth Throttling ... 586
Tarpitting ... 588
Greylisting ... 590
LAN Domains ... 593
LAN IPs ... 594
Site Policy ... 595
3 Dynamic Screening ... 596
Options/Customize ... 596
Auth Failure Tracking ... 600
Protocols ... 603
Notifications ... 604

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Diagnostics ... **607**
Dynamic Allow List ... **609**
Dynamic Block List ... **611**
Domain NAT Exemptions ... **613**
4 MDPGP ... **614**
5 Outbreak Protection ... **624**
6 Content Filter and AntiVirus ... **630**
Content Filter Editor ... **631**
Rules ... 631
Creating a New Content Filter Rule ... 633
Modifying an Existing Content Filter Rule ... 638
Using Regular Expressions in Your Filter Rules ... 638
Attachments ... 643
Notifications ... 645
Message Macros ... 646
Recipients ... 649
Compression ... 650
AntiVirus ... **653**
Virus Scanning ... 653
AV Updater ... 657
Updater Configuration Dialog ... 659
7 Spam Filter ... **660**
Spam Filter ... **660**
Spam Filter ... 661
Bayesian Classification ... 664
Bayesian Auto-learning ... 668
Spam Daemon (MDSpamD) ... 670
Allow List (automatic) ... 672
Allow List (no filtering) ... 675
Allow List (by recipient) ... 676
Allow List (by sender) ... 677
Block List (by sender) ... 678
Updates ... 679
Reporting ... 680
Settings ... 681
DNS Block Lists (DNS-BL) ... **683**
Hosts ... 684
Allow List ... 686
Settings ... 687
Auto-generating a Spam Folder and Filter ... 689
Spam Honeypots ... **690**

Section V Accounts Menu 693

1 Account Manager ... **694**
Account Editor ... **697**
Account Details ... 697
Mail Folder & Groups ... 700
Mail Services ... 701
Web Services ... 703
Autoresponder ... 708
Forwarding ... 711
Restrictions ... 713

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Quotas ... 715
Attachments ... 718
IMAP Filters ... 720
MultiPOP ... 723
Aliases ... 725
Shared Folders ... 726
Access Control List ... 728
App Passwords ... 734
Signature ... 737
Administrative Roles ... 741
Allow List ... 742
Settings ... 744
ActiveSync for MDaemon ... 747
Client Settings ... 748
Assigned Policy ... 754
Clients ... 755

2 Groups & Templates ... 764

Group Manager ... 764
Group Properties ... 766
Client Signature ... 769
Template Manager ... 774
Template Properties ... 776
Mail Services ... 780
Web Services ... 782
Groups ... 787
Autoresponder ... 788
Forwarding ... 792
Restrictions ... 794
Quotas ... 796
Attachments ... 799
Administrative Roles ... 801
Allow List ... 802
Settings ... 804

3 Account Settings ... 806

Active Directory ... 806
Authentication ... 809
Monitoring ... 812
LDAP ... 815
Aliases ... 818
Aliases ... 818
Settings ... 820
Autoresponders ... 823
Accounts ... 823
Attachments ... 825
Exempt List ... 826
Settings ... 827
Creating Auto Response Messages ... 828
Auto Response Message Samples ... 831
Other ... 833
Account Database ... 833
ODBC Selector Wizard ... 834
Creating a New Data Source ... 836
Passwords ... 840

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Quotas ... 844
Minger ... 847
4 Importing Accounts ... 849
Importing Accounts from a Text File ... 849
Windows Account Integration ... 851

Section VI Queues Menu 855
1 Mail Queues ... 856
Retry Queue ... 856
Holding Queue ... 858
Custom Queues ... 861
Restore Queues ... 863
DSN Settings ... 864
2 Pre/Post Processing ... 866
3 Queue and Statistics Manager ... 867
Queue Page ... 868
User Page ... 871
Log Page ... 873
Report Page ... 875
Customizing the Queue and Statistic Manager ... 876
MDstats.ini File ... 876
MDStats Command Line Parameters ... 877

Section VII Additional MDaemon Features 879
1 MDaemon and Text Files ... 880
2 Remote Server Control via Email ... 880
Mailing List and Catalog Control ... 880
General Email Controls ... 883
3 The RAW Message Specification ... 883
The RAW Message Specification ... 883
Bypassing the Content Filter ... 883
RAW Headers ... 884
Special fields supported by RAW ... 884
Sample RAW mail messages ... 885
4 Semaphore Files ... 886
5 Route Slips ... 891

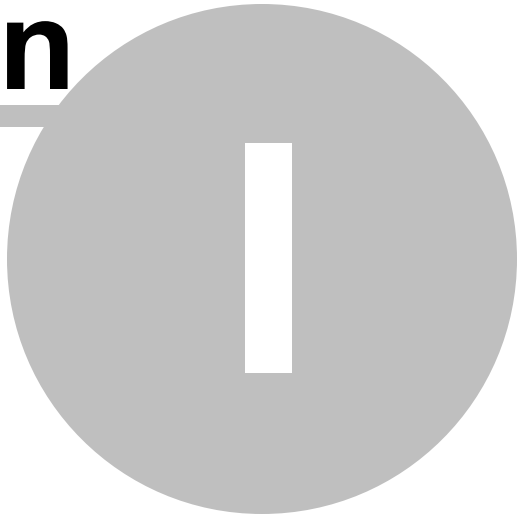
Section VIII Creating and Using SSL Certificates 895
1 Creating a Certificate ... 896
2 Using Certificates Issued by a 3rd party ... 896

Section IX Glossary 899

Index 921

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section



1 MDaemon Messaging Server 23.5

Introduction

MDaemon Technologies' MDaemon Messaging Server is a standards-based SMTP/POP3/IMAP mail server that supports Windows 7, Server 2008 R2, or newer and offers a full range of mail server functionality. MDaemon is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. MDaemon offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP and Active Directory support, an integrated browser-based email client, content filtering, spam filters, extensive security features, and more.

MDaemon Features

MDaemon is equipped with many features besides SMTP, POP3, and IMAP4 email processing. The following is a list of just some of those features.

- Complete support for virus scanning and protection is available as an add-on to your MDaemon or MDaemon Private Cloud license. This provides access to real-time Outbreak Protection 624, and MDaemon AntiVirus 653. Messages can then be scanned for viruses and cleaned or deleted automatically before ever reaching the intended recipients. Further, you can configure MDaemon to send a message to the administrator, sender, and recipient of the infected message notifying them of the virus.
- MDaemon features a complete suite of Mailing List or email group management functions allowing for the formation of an unlimited number of distinct distribution lists that can contain local and/or remote members. Lists can be set to allow or refuse subscription requests, be public or private, post replies to either the list or the originator of the message, be sent in digest format, and be configured using numerous other features.
- An integrated component of MDaemon is Webmail 308. This feature makes it possible for your users to access their email using their favorite web browser rather than from a workstation dependent email client. This tool is perfect for mobile staff and users who do not have a dedicated machine from which to access their email.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- MDaemon Webmail is equipped with a complete suite of email client features. You can: send and receive email, spell check messages, manage your email in multiple personal folders, display the interface in any of 18 languages, schedule meetings and appointments and share calendars and tasks with other users, manage your MDaemon account settings (when used in conjunction with Remote Administration 341), manage contacts, and more. Webmail is also equipped with MDaemon Instant Messenger (MDIM) 309, a small utility that can be downloaded and installed on a user's local computer. This provides easy access to your email and folders and checks for new messages without having to open your web browser. It also includes a complete Instant Messaging system that can be used to quickly "chat" with other MDaemon users who are also using MDIM or another XMPP 365 client.
- MDaemon is equipped with many features designed to help you make your email system secure. The Spam Filter and DNS Block Lists features will help you put an end to most "spam" email messages that "spammers" try to route through or to your domain. IP and Host Screening and the Address Block Lists provide the capability to screen and prevent certain addresses and domains from connecting to or sending mail through your system. They also make it possible to connect to specific IP addresses while screening all others.
- Equipped with support for Lightweight Directory Access Protocol (LDAP), MDaemon can keep your LDAP server up to date on all of its user accounts. This makes it possible for you to keep an LDAP address book up to date so that users with email clients that support LDAP can access it. You can also choose to use Active Directory or your LDAP server as the MDaemon account database instead of an ODBC compliant database or the local `USERLIST.DAT` system. Thus, you can configure multiple MDaemon's at different locations to share the same account database.
- MDaemon's extensive parsing features make it possible to provide email for an entire LAN with as little as a single dial-up ISP POP3 mailbox. This makes it possible to provide email to an entire network for a fraction of the normally associated cost.
- Address Aliases provides the ability to route email messages addressed to "fictitious" mailboxes to a valid account or mailing list. This makes it possible for individual accounts and lists to have multiple email addresses at one or more domains.
- The Domain Gateways feature provides the option of setting up separate domains for various departments or groups that may be local to your network or located somewhere else on the Internet. Using this feature, all mail addressed to a domain for which MDaemon is acting as a gateway will be placed in that domain's mailbox by MDaemon. It can then be collected by that domain's MDaemon server or email client and distributed to the domain's users. This feature can also be used to enable MDaemon to act as a backup mail server for other domains.
- Integrated web-based remote administration. MDaemon's Remote Administration 341 component is integrated with MDaemon and Webmail and enables your users to review and edit their account settings via their web-browser. You can designate which settings that your users may edit, and assign access permissions on a per account basis. Remote Administration can also be used by the Administrator (and whomever else you wish to allow) to review or

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

edit any of MDaemon's settings and any other files that you wish to make available to the Remote Administration system for reviewing.

- An internal message transport system known as RAW mail provides a simple method for placing messages into the mail stream and greatly simplifies custom mail software development. Using RAW, a complete mail system can be devised using a simple text editor and a couple of batch files.
- A highly versatile Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and more.

MDaemon Private Cloud

MDaemon Private Cloud (MDPC) is a special edition of the MDaemon Messaging Server that was developed specifically for resellers and IT Service providers who wish to use MDaemon software to provide hosted email services to their customers. Unlike MDaemon, which is sold for on-premise use, MDPC was built on a new licensing and code foundation specifically designed for use in a hosted environment. MDaemon Private Cloud includes all MDaemon features and the following additional features:

- New licensing and billing (per-user/per-month)
- Outlook support
- Improved multi-domain control
- Per-domain branding (white label)
- Per-domain reporting
- Non-billable user test accounts (counts will not be included in total billing counts)
- Outbreak Protection, MDaemon Antivirus, and the ClamAV antivirus engine (optional with additional cost)
- ActiveSync for MDaemon (optional with additional cost)

System Requirements

For the most up to date information on MDaemon's system requirements and recommendations, visit the System Requirements page at mdaemon.com.

Trademarks

Copyright © 1996-2023 MDaemon Technologies. Alt-N®, MDaemon®, and RelayFax® are trademarks of MDaemon Technologies.

Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

See:

New in MDaemon 23.5 15
Upgrading to MDaemon 23.5.0 59
MDaemon's Main Display 68
Getting Help 64

1.3 New in MDaemon 23.5

Changes and New Features

Webmail

WebAuthn Support 333

MDaemon supports the Web Authentication API (also known as WebAuthn), which Webmail users can utilize to have a secure, passwordless sign-in experience, by allowing them to use biometrics, USB security keys, Bluetooth, and more for authentication. WebAuthn can also be used for Two-factor Authentication 333 (2FA), although if you are using both passwordless authentication and two-factor authentication then you can't use the same authentication method for both. You can find the WebAuthn settings on the Webmail Settings 333 page.

Visit: webauthn.guide, for more information on WebAuthn and how it works.

AI Message Features 339

As of MDaemon 23.5.0, the Pro theme in MDaemon's Webmail client includes various Artificial Intelligence (AI) features to help assist your users in managing their email and increasing productivity. With these features, in MDaemon Webmail you can use AI (specifically ChatGPT by OpenAI) to get a summary of the contents of an email message, suggest a reply to a message based on criteria you choose, and help you compose a new message based on some of your own text and other criteria.

Webmail's AI message features are disabled by default for all domains. They can be enabled by using the "*Enable AI message features*" option on the Webmail Settings 333 page or the Domain Manager's Webmail 187 page. Webmail's AI message features are also disabled per user by default. You can enable them per user on the Account Editor's Web Services 703 page, or as part of a Group 764 controlled by an Account Templates 774. When the Domain setting is disabled, that takes precedence over the user setting. Therefore, none of that domain's users will be able to use the AI message features regardless of their user setting.

See: Webmail's AI Message Features 339, for more information and cautions about using these features. Further, you can find MDaemon Technologies' AI Usage Policy at our Artifical Intelligence (AI) Information Page. On that same page there is also a link to OpenAI's Terms of Use.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Theme Improvements

- Pro and WorldClient: There is now an option to delete all attachments from a given message.
- Pro and WorldClient: Added a Description column to the Documents view.
- Pro: The Compose view contact picker now has a dialog for adding a contact with three fields (Name, Email, Mobile Phone).
- Pro: There are new Style options at: Settings | Personalize.
- Pro: Multiple event reminders are now supported.

Other Webmail Improvements

- Added a Public Schedule option, so that users can allow others to schedule a meeting.
- Separated the setup process for Two Factor Authentication email verification from the setup process for authenticator app verification.
- The Password Recovery feature now sends an email without revealing to the user where the email was sent. Two Factor Auth occurs after clicking the recovery link in the email.
- Changed how Webmail authenticates to MDaemon's SMTP server so the user's password is not needed.
- Added an option to "Mark deleted messages as read" at: Settings | Personalize.
- There is now an All Documents toggle button in the Documents view.

Remote Administration (MDRA)

Health Check 496

There is now a Health Check page in MDRA at: Security | Health Check. This page provides a convenient list of important security settings consolidated onto a single page, and it displays each setting's current value and its default value. Where those values differ, the setting is highlighted so that Global Administrators can quickly review those particular settings and then restore any of them to their default values if desired. Each group of settings also has a shortcut icon next to it, so that you can jump to the page on which those settings are located. In addition, you can also view a list of all Health Check changes made during the current browser session, and undo any of those listed changes if necessary.

Other MDRA Improvements

- Added editor GUIs for all direct edit files.
- There is now an "**X**" icon that you can click to hide any given chart in the Traffic and Mailboxes summary report pages. To restore a hidden report, click your account name in the upper right corner of the page and then click the box next to the report you wish to restore.
- Added a **Delete All** button to the Mailing List Members 265 page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- As with Webmail, support for WebAuthn was added to MDRA, which gives users a secure, passwordless authentication method, and it can also be used as a Two Factor Authentication method. The WebAuthn options in MDRA are located on the Remote Admin Settings 343 page. See: WebAuthn Support 15 in the Webmail section above.
- The Public Folder Editor 300 and Shared Folder Editor 726 now has a **Nest under** option to choose the parent folder under which the selected public or shared folder will nest.
- Added some text to the Account Editor's Mailing Lists page to explain that a user might show up as a member of a mailing list due to membership in a Group 764.
- In the Message Search and Queues, added the ability to view the email message, in addition to being able to view its source. RAW messages are still only in text/plain.
- Added links to the Queues on the Status page.
- Added the ability to include multiple addresses (separated by commas) when adding new Access Rights to a Public Folder's Access Control 302 page. You cannot add addresses when editing existing rights.

Security

- Added HTTPS support for Outbreak Protection 624.
- Updated ClamAV to 1.0.3.
- LetsEncrypt - Added support for TLS 1.3
- Updated SpamAssassin to 4.0.0.

XMLAPI

MDaemon 23.5.0 includes many additions and improvements to the XMLAPI. See the Release Notes for a complete list of these improvements.

Other

- Added an App Passwords 840 option to delete an account's app passwords when the account's password is changed. The new option is on by default.
- Added a Restrictions 794 page to the Account Templates. When an account is removed from a group with an account template that controls restrictions, the account's restrictions revert to their previous values, or possibly to another group's account template if the account is a member of multiple groups.
- The Location Screening 558 option "SMTP connections are accepted but authentication is blocked" is now per country instead of global. Blocking SMTP connections prevents your server from receiving mail from a country. Allowing SMTP connections with authentication disabled lets your server receive mail from a country while blocking brute force / dictionary attacks from them. Protocols other than SMTP are not affected.
- Removed obsolete "Compose in new browser window" Webmail option from the UI.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- LetsEncrypt - Added support for TLS 1.3.

MDaemon Server Release Notes

For a comprehensive list of these and all other additions, changes and fixes included in MDaemon 23.5.0, see the Release Notes.

Changes and New Features

MDaemon Server

- (23.0.2) Added a MultiPOP 137 option to send a notification email after multiple failures when checking a MultiPOP account. Since temporary failures are not uncommon, there is an option for how many consecutive failures it takes to trigger the notification. There is also an option for how many days to wait between notifications, to avoid sending too many of them. The content and recipients of the notification emails can be customized by editing \MDaemon\App\MPOPFailureNotice.dat. By default the notifications are sent after 5 failures, no more than once every 7 days, to the MultiPOP account owner.
- There is a new MultiPOP 137 page under Server Settings. From this page you can enable/disable MDaemon's MultiPOP server, and use the "*MultiPOP always deletes mail...*" option (formerly located on the MultiPOP Collection 375 page) to override the *Leave a copy of message on POP server* 723 option for all users. This new page also contains OAuth 2.0 support options for MultiPOP mail collection from Gmail and Office 365.

  MultiPOP OAuth 2.0 support for collecting mail from Gmail and Office 365 138 — OAuth 2.0 is modern authentication, which these services are now requiring as they disable support for legacy/basic authentication. In order for MDaemon's MultiPOP feature to use OAuth 2.0 to collect mail from Gmail or Office365 on behalf of your users, you must register your MDaemon server with Google or Microsoft, respectively, creating an OAuth 2.0 application using the Google API Console or Microsoft's Azure Active Directory. This is similar to the procedure required for using MDaemon's Dropbox Integration 325 for your Webmail users. See the MultiPOP 138 help topic for more information on configuring OAuth 2.0 support.
- MDaemon's IMAP server now supports keyword flags. This allows email clients such as Mozilla Thunderbird to store Message Tags on the server, which lets you see tags in one instance of a client that were set in another instance of the client.
- Improved the IMAP server's performance when opening large mail folders.

Security

- (23.0.2) Added support for Spamhaus Data Query Service (DQS) to the Spam Filter 660. For more information on Spamhaus DQS, visit: https://info.spamhaus.com/getting-started-with-dqs

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- There is a new *Block Logon Policy Violations* option on Dynamic Screening 596, that you can use if you wish to block any IP address that attempts to logon without using the full email address. This option is off by default. See the Systems 480 page for more information on the corresponding option, "*Servers require full email address for authentication*".
- An *Only for valid accounts option* was added to expand the *Ignore authentication attempts using identical passwords* option on the Auth Failure Tracking 600 page. Activate this option if you only wish to ignore the duplicate password authentication attempts when they are attempting to sign in to a valid account. This means that if, for example, a user updates his password in one client but another client is still running with the old password, that old client's sign-in attempts will still be ignored, since it will have the correct sign-in name. A bot trying random sign-in names with a similar password will not have that same benefit, and will be blocked as soon as it surpasses the auth failure threshold. This will help to defeat bots much quicker. The XML API DynamicScreen operation has also been updated to reflect these new features.
- A Content Filter » Attachments 643 option was added to: "*Add warning to top of message body if attachment is removed*". When MDaemon removes an attachment from a message, for example because a virus was detected, it will add a warning message to the top of the message body. There is also a **Warning** button to use if you wish to review or modify that message's template. This option is enabled by default.
- Added the option to *Exclude Trusted IPs from AntiVirus scanning* 653.
- MDaemon sends a warning email to admins when SSL certificates 561 configured for use by MDaemon 563, Webmail 566, or Remote Administration 570 are about to expire.
- MTA-STS 576 now has an exempt list, so problem domains can be made exempt instead of MTA-STS needing to be turned off when failures affect deliverability.
- The ClamAV AntiVirus component was updated to version 0.105.2 (in MDaemon 23.0.1).

Webmail

- Google Drive Integration 328 — Webmail can now be linked to your users' Google accounts to allow them to save message attachments directly to their Google Drive, and to edit and work with documents stored there. In order to enable this, an **API Key**, **Client ID**, and **Client Secret** are required. All are obtained directly from Google by creating an App using the Google API Console and registering your MDaemon with their service. An OAuth 2.0 authentication component is part of this app, which allows your Webmail users to sign-in to Webmail and then authorize access to their Google Drive account through MDaemon. Once authorized, users can view their folders and files that are in Google Drive. Further, they can upload, download, move, copy, rename, and delete files, as well as copy/move files to and from the local document folders. If the user wants to edit a document, clicking the option to view the file in Google Drive will allow the user to make edits to it in accordance with their permissions set in Google Drive. The Google Drive setup process is similar to MDaemon's Dropbox Integration 325 and MultiPOP OAuth Integration 137 features. See Google Drive Integration 328 for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Added an option in all themes except Lite to "*Enable Drag and Drop to move folders*". The new option is located in Webmail on the **Folders** page under the Options menu, and it is enabled by default.
- Made the session cookie secure over HTTPS.
- Category changes notification now sent to MDaemon
- WorldClient no longer modifies the robots.txt file on startup.
- The built-in web server prevents the download of .dll files from the HTML directory.
- Added one to the maxlength of the new password input, so that the "Maximum of 15 characters" unmet requirement will show.
- Added reporting for sign-in attempts without a full email address, to support the new Dynamic Screening option to Block Logon Policy Violations 596.
- (23.0.2) Made the unsnooze option more visible with an orange highlight.

Pro Theme

- Added read receipts support.
- Added an option to disable the HTML editor context menu.
- Added the ability to resize the folder list.

Remote Administration (MDRA)

23.0.2

- Added AntiVirus 653 option to *"Exclude trusted IPs from AntiVirus scanning*".
- Added the "*Do not allow authentication on the SMTP port*" option to SMTP Authentication 509.
- Added a Public Folder Manager 300 option to specify an ActiveSync Display Name.
- Added four more filter options to the Account Manager 694: Admins Only, Non-Admins Only, Global Admins Only, and Domain Admins Only
- Added a page for the Spamhaus Data Query Service (DQS) to the Spam Filter 660. For more information on Spamhaus DQS, visit: https://info.spamhaus.com/getting-started-with-dqs

23.0.0

- In the Domain Manager, there is now a Webmail Setting 333 to "*Allow users to receive Two Factor Authentication verification codes over email*", so that users can receive their verification code via an alternate email address rather than using the Google Authenticator app. This setting is enabled by default.
- Changed the default permissions when adding a new ACL entry to Lookup and Read.
- The **Test** buttons at: Spam Filter » DNS-BL » Hosts 684 and Setup » Active Directory » Authentication 809 are now disabled while the process is ongoing.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- The built-in web server prevents the execution and download of .dll files in the Templates directory.
- Users can now customize the appearance of the Remote Administration web-interface by clicking their user name (e.g. frank.thomas) in the top right corner of the window. There are options to switch the interface to Dark Mode, set the Font Size, and choose the preferred Language.
- Changed the account delete confirmation to use the custom confirmation feature.
- Added Dynamic Screening reporting for sign-in attempts without a full email address.

ActiveSync

- Added a Client Settings option to *Block Sender when moving mail into Junk-Email folder* 413. When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.
- You can now disable the Full Wipe button 451 for ActiveSync clients if you choose, so that you can't do a remote Full Wipe on an ActiveSync device without first disabling the new Disallow Factory Reset Wipes 413 option.
- Made BodyPreferences data human readable to make troubleshooting sync issues easier.
- Improve shutdown performance when clients are syncing huge mailboxes.
- Added the ability to define a custom display name for mailbox and public folders.
- Improved shutdown performance.
- ActiveSync clients can now send to Personal Distribution Lists in Contact folders.
- Changed layout of Client Settings Dialog in the GUI to add room for new settings.

Other

- (23.0.2) Content Filter - $LIST_ATTACHMENTS_REMOVED$ 646 can be used in rule actions (e.g. "send note", "add warning...")
- In the MDaemon GUI, changed the default permissions when adding a new ACL entry to Lookup and Read.
- in the MDaemon GUI, added a warning pop-up if you attempt to set the Webmail, Remote Administration, or XMPP BOSH Server ports to have conflicting values.
- XMLAPI - Added Editor operation which can be used to edit MDaemon's various INI files
- Changed several plug-ins to allow newer versions to run so customers can test possible hotfix/patch versions.
- LetsEncrypt - Updated script to check orders that are ready or valid.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon Server Release Notes

For a comprehensive list of additions, changes and fixes included in MDaemon 23.0.2, see the Release Notes.

New in MDaemon 22.0

Changes and New Features

Webmail

Pro Theme

- While viewing a message, you can hover over the sender's name to open a pop-up, which contains options for adding the sender to your Contacts and Allowed or Blocked Senders folders.
- Compose, Message, Event, Contact, Task, and Note views can now open in a new window.
- You can now open the next unread message from the message preview pane and message view.
- Added message snippets to the message list when in multi-line mode.
- You can now make available an *Edit Alias Display Names* option for Pro theme users, located under Settings » Compose. This allows users to edit the display name of any alias associated with their account. Use the new "*Allow users to edit their alias display names*" Webmail Settings 333 if you wish to allow this. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.
- Options and links that used to say "whitelist" or "blacklist" sender, now say "allow" or "block" sender. Additionally, the White List and Black List folders are now called "Allowed Senders" and "Blocked Senders".
- The Message List can be sorted by the Flag column.
- In the Tasks list, overdue tasks will now appear in red.
- Upgraded the XMPP client to version 4.4.0.

Other

- When strong passwords are required, there is now a list of password requirements that displays green and checked off as the user meets the requirements. Also added more descriptive error messages for what is wrong with an invalid password on submission.
- Compose Options now contains options for selecting the default "From:" address that will be used when composing, replying to, or forwarding a message.
- A "1 minute" setting was added to the List Refresh Time option, located on the Options » Personalize page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Added support for CSRFTokens on the Webmail Sign-in page. This is enabled when the "*Use Cross-Site-Request-Forgery tokens*" option is enabled on the Webmail Settings » Web Server 313 page. If you are using custom templates for Webmail, add a hidden input to the Login form as follows: `<input type="hidden" name="LOGINTOKEN" value=<$LOGINTOKEN$> />`
- Public Calendar - Modified the List view to start on the current day and show the next 30 days.
- Added automatic conversion of URLs to hyperlinks in the message view.
- The names of default folders (Drafts, Sent Items, etc.) are translated into the Webmail user's language no matter which language of MDaemon is installed (previously only the English MDaemon did this).
- There is now an option to send Two Factor Authentication verification codes to a secondary email address.
- LookOut and WorldClient themes - Changed all list category display behavior to match.
- The Allowed Senders and Blocked Senders folders now have different icons to indicate that they are special folders.

Remote Administration (MDRA)

- Added a Two Factor Auth Exception IPs page in MDRA, located under the Main menu. This allows users to sign in to Remote Admin or Webmail without requiring 2FA, when connecting from one of the specified IP addresses.
- There is a new "*Allow users to edit their alias display names*" Webmail Settings 333 option in MDRA. Activate this option if you wish to allow users to edit the display name of any alias associated with their account. They can do this by using the *Edit Alias Display Names* option, located in Webmail's Pro Theme.
- Changed autocomplete="off" to autocomplete="new-password" on password fields to stop Firefox from auto-completing passwords outside of the login page.
- Added the Notification Message Editor to the Content Filter's Notifications 645 page.
- Added support for CSRFTokens on the Sign-in page. This is enabled when the "*Use Cross-Site-Request-Forgery tokens*" option is enabled on the Remote Administration Settings page in MDRA.
- Any remote or local Custom Queues 861 you have created can be managed under the Messages and Queues section in MDRA.

Security

- MDaemon now supports TLS 1.3 on newer versions of Windows. Windows Server 2022 and Windows 11 have TLS 1.3 enabled by default. Windows 10 versions 2004 (OS Build 19041) and newer have experimental TLS 1.3 support that can be enabled for inbound connections by setting the following in the registry:

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

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- MDaemon logs the cipher suite (e.g., TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) used by SSL/TLS connections.
- Added a Passwords 840 option for strong passwords to require a special character. It is enabled by default for new installs and disabled by default for existing installs.
- AV Mailbox Scanner - When an infected message is found during mailbox scan MDaemon's infected counter will be incremented.
- AntiVirus - Updated ClamAV to version 0.104.3.

ActiveSync

- Improved FolderSync performance.
- The ActiveSync Connection Monitoring Dialog has a new right-click menu command to terminate a session and block a client.
- Added an option to the Client Settings 451 dialog to allow Outlook to send mail using an alias. If Reply-To is set to a valid alias for the sending account, the message will be sent via that alias.
- Added support for EAS 16.1 Find command. Removed the protocol restriction 424 preventing iOS from using EAS 16.1

Other

- Content Filter - Added support for $CONTACT...$ macros in the "Append a corporate signature 633" action. These macros can be used to personalize the signature with information from the sender's contact in their public contacts folder. See: Signature Macros 128 for a full list of supported macros.
- Content Filter - Added an action to extract attachment 633 and add attachment linking 357 into the message.
- Summary Emails 858 for the holding, quarantine, and bad queue may now have links to release, re-queue, or delete each message. This new "*Include action link*" option is enabled by default. Note: The Remote Administration URL 343 must be set for the links to be generated.
- LetsEncrypt 580 - Updated the script to work with PS 7.
- Added a Deferred Delivery Message Recall 115 option to replace the 'Date:' header with the current date and time when a message is released from the Deferred Queue. It is disabled by default.
- MDaemon Connector 379 has been updated to version 7.0.7.
- XMLAPI - Added support for forwarding scheduling.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon Server Release Notes

For a comprehensive list of additions, changes and fixes included in MDaemon 22.0, see the Release Notes.

New in MDaemon 21.5

Major New Features

App Passwords 734

App Passwords are very strong, randomly-generated passwords for use in email clients and apps, to help make your email apps more secure since they can't be protected by Two-Factor Authentication 703 (2FA). 2FA is a secure way for a user to sign in to Webmail or MDaemon Remote Administration (MDRA), but an email app can't use it, because the app must be able to access your email in the background without you having to enter a code from your authenticator app. The App Passwords feature allows you to create strong, secure passwords for use in your apps, while still keeping your account password secured by 2FA. App Passwords can only be used in email apps, they cannot be used to sign in to Webmail or MDRA. This means that even if an App Password were somehow compromised, the unauthorized user still wouldn't be able to get into your account to change your password or other settings, but you, however, would still be able to sign in to your account with your account password and 2FA, to delete the compromised App Password and create a new one if needed.

App Password requirements and recommendations

- In order to create App Passwords, 2FA must be enabled for the account (although you can turn off this requirement 840 if you choose).
- App Passwords can only be used in email apps—they cannot be used to sign in to Webmail or MDRA.
- Each App Password is displayed only once, when it is created. There is no way to retrieve it later, so users should be ready to enter it into their app when it is created.
- Users should use a different App Password for each email app, and they should revoke (delete) its password whenever they stop using an app or when a device is lost or stolen.
- Each App Password lists when it was created, when it was last used, and the IP address from which it last accessed the account's email. If a user finds something suspicious about the Last Used or Last IP data, the user should revoke that App Password and create a new one for his or her app.
- When an account password is changed, all App Passwords are automatically deleted—a user cannot continue using old App Passwords.

Requiring App Passwords for SMTP, IMAP, ActiveSync, and more

There is an account option on the Account Editor's Settings 744 page that you can use to "*Require app password to log in to SMTP, IMAP, ActiveSync, etc.*"

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Requiring App Passwords can help protect an account's password from dictionary and brute force attacks via SMTP, IMAP, etc. This is more secure because even if an attack of this sort were to guess an account's actual password, it wouldn't work and the attacker wouldn't know, because MDaemon would only accept a correct App Password. Additionally, if your accounts in MDaemon are using Active Directory 806 authentication and Active Directory is set to lock an account after a number of failed attempts, this option can help prevent accounts from being locked out, because MDaemon will only check the App Passwords, not try to authenticate to Active Directory.

Other New Features and Improvements

Pro Theme

- The Mobile theme is now called the **Pro** theme. It was expanded and improved to be responsive and adaptable for use on different kinds of devices and screen sizes, without sacrificing features.
- Added Cross-Site-Request-Forgery tokens for more secure transactions. The feature is disabled by default. To enable it through MDRA go to Main | Webmail Settings | Web Server 313 and check "Use Cross-Site-Request-Forgery tokens".
- Added an option at Settings | Personalize to enable Dark mode, to display the Pro theme with a dark background.
- Added a link to "Track my package" in opened messages.
  - Carrier tracking numbers being watched by default are: USPS, UPS, OnTrac, FedEx, and DHL.
  - The default configuration file is at: `\MDaemon\WorldClient\package_tracking.json`
  - Admins can add more carriers by creating the file: `\MDaemon\WorldClient\package_tracking.custom.json`, using the same format as the default `package_tracking.json` file. At least one service name, a tracking URL, and at least one valid regular expression is required. Include service names that may appear in a message to reduce the chances of false positive matches.
- Added the Message List Layout dialog to the smaller browser size. Only the Message List Density setting is displayed.
- Added a password strength meter.
- Added the image slideshow feature for the Message View.
- Added a card view for the Contacts list.
- Moved the "New item" button from the toolbar to the space above the folder list for desktop sizes.
- Added a plus icon next to "Personal" to create a new calendar in the calendar view.
- Added an event tooltip with Edit options and Send an Email to an Attendee option.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Made the search bar always visible for browser window widths of 1200px or greater.
- Added a dialog to allow users to remove a contact from the the BlackList when adding them to the WhiteList and vice-versa.
- Added an error message when there is an error creating or renaming a folder.
- Added support for HTML notes in Events, Contacts, Tasks, and Notes.
- Replaced the current HTML editor (CKEditor) with Jodit.
- Changed the basic header view to show the From email address.
- Added the Voice Recorder.

Other Webmail Improvements

- Added an Unsubscribe link next to the From address when the List-Unsubscribe header exists in a message. This can be disabled in Webmail at Settings | Personalize.
- Added ability to import email into the current message list.
- Updated the Dropbox integration to use the refresh_token provided by Dropbox to reconnect users without interaction with the OAuth dialog. When the access_token expires, Webmail will attempt to use the refresh_token to get a new access_token. No longer necessary settings have been removed from the Cloud Apps page. The admin does NOT need to make any changes to the Dropbox app at Dropbox.com.
- Search All / Subfolders requests no longer search unsubscribed folders when unsubscribed folders are hidden.
- Added a checkbox named "Skip Search" to exclude specific folders from Search All / Subfolders requests.
- Added a setting in Remote Admin that allows the Two-Factor Authentication Remember Me checkbox to be hidden.
- Added a blur effect for the background when the user session is expired.
- Added an Automatic CC and BCC feature at Settings | Compose.
- Added an option to: `WorldClient\Domains.ini [Default:Settings] PreventComposeWithAlias`, to prevent composing messages with an alias. The setting is off by default.
- Lite theme - Added auto-save draft message to the Compose view.
- Added an option in the Options | Folders view to allow users to skip contact folders in auto-complete searches. Added the option in the right click menu as well.
- Added a Webmail log entry for the User-Agent when a user logs in.
- Added a notification in the Compose view if a local recipient has their autoresponder enabled.
- WorldClient theme - Added a paperclip icon to event tiles that have attachments.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Maximum attachment size is set to 25 MB for new installs.
- Changed the "Delete All" folder action to "Empty Folder"
- WorldClient theme - Added "Change Password" and "Change Recovery Email" buttons to the Security page

Remote Administration (MDRA)

- Added the ability to drag and drop content filter rules. The copy, edit, and delete buttons are now on each respective rule.
- Added Cross-Site-Request-Forgery tokens for more secure transactions. The feature is enabled by default. To disable it go to: Main | Remote Admin Settings | Settings and uncheck "Use Cross-Site-Request-Forgery tokens".
- Added a password strength meter to some password fields.
- Added the option: "Enable Two-Factor Authentication Remember Me," to Setup | Domain Manager | Edit | Webmail Settings 187 and Main | Webmail Settings | Settings 333.
- Added Blocked IPs and Refused IPs reports for Dynamic Screening.
- Added the Groups 460 and Client Types 466 views under ActiveSync.
- Updated the ActiveSync Diagnostics 422 and Tuning 410 pages.
- Added a browser usage by OS chart and table at Reports | Traffic | Webmail Login Statistics.
- Added buttons to open a Browse Users and Browse Groups pop-up, to add them to mailing lists, at: Main | Mailing Lists | Edit | New 265. Only Domain or Global Admins 741 have access to the buttons.
- Added Account Only Wipe options at Main | My Account | ActiveSync Clients and at ActiveSync | Client Management 451.
- Change logging has been added. It will log every change that is made via Remote Administration.
- Updated Message Recall 115 to match the MDaemon GUI.
- Added the "Extract attachments from winmail.dat" option at Security | Content Filter | Compression 650.
- Added Slovenian language to MDaemon Remote Administration.

Other MDaemon Improvements

- Added support for SMTP Command Pipelining (RFC 2920). MDaemon will send MAIL, RCPT, and DATA commands in batches instead of individually, which improves performance over high latency network links. SMTP pipelining is always enabled for inbound connections. It is enabled by default for outbound connections, but can be disabled at Setup | Server Settings | Servers & Delivery | Servers 86.
- Added support for SMTP CHUNKING (RFC 3030). CHUNKING allows non-line-oriented messages to be transferred. It is enabled by default for inbound connections, but disabled by default for outbound. Bare line feeds in received

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

messages are converted to carriage return line feeds by default. These defaults can be changed by setting `[Special] SMTPChunkingInbound=Yes/No`, `SMTPChunkingOutbound=Yes/No`, and `SMTPChunkingAllowBareLF=Yes/No` in `\MDaemon\App\MDaemon.ini`.

- Content Filter - Updated the default restricted attachments 643 list.
- Content Filter - Added rule action to add attachment to message 633.
- ActiveSync Server start/stop entries are written to MDaemon's System log.
- Clustering - Added support for synchronizing reminders from secondary nodes.
- Dynamic Screening - Added option to Log Locations using ISO-3166 Codes 596 instead of names.
- XMLAPI - Added support for ActiveSync AlwaysSendMeetingUpdates setting.
- XMLAPI - Added support for semaphore file creation.
- XMLAPI - Added Support to report/modify settings from Setup/Server Settings/Logging.
- MDaemon Instant Messenger - Improved group chat feature by adding ability to multi-select chat buddies for group chat. Also added an option to auto-accept chat room requests.
- Location Screening 558 has a new option to control whether or not the `X-MDOrigin-Country` header is added to messages. It is enabled by default.
- There is now an Accounts setting for whether to allow users to sign in using aliases, located at: Accounts | Account Settings | Aliases | Settings 820. It is enabled by default.
- MDaemon Connector has been updated to version 7.5.0.
- The default delivery confirmation message text (in \MDaemon\App\Receipt.dat) has been changed to use the $HEADER:X-RCPT-TO$ macro instead of $RECIPIENT$ to avoid disclosing the actual email address an alias resolves to.

MDaemon Server Release Notes

For a comprehensive list of additions, changes and fixes included in MDaemon 21.5, see the Release Notes.

New in MDaemon 21.0

Major New Features

Persistent Chat Rooms 367

MDaemon's XMPP server now supports persistent chat rooms, which do not need to be recreated every time all users leave the room. Configure them at: Setup | Web & IM Services | XMPP.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Virus/Spam Misclassification Reporting

When on the Quarantine, Bad, or Spam Trap queue screens in the MDaemon GUI, a right-click popup menu option was added to report messages to MDaemon.com as false positives or false negatives. Similar options have also been added to MDaemon Remote Administration. The messages will be analyzed and passed along to third-party vendors for corrective action.

ActiveSync Migration Client (ASMC) GUI

A GUI has been created to assist in running ASMC (`ASMCUI.exe` in MDaemon's `\app\` folder). It allows you to store your options and recall them at a later time. ASMC supports migrating mail, calendars, tasks, notes, and contacts from ActiveSync servers that support protocol version 14.1. Documentation for it can be found in MDaemon's Docs folder, at: `\MDaemon\Docs\ActiveSync Migration Client.html`.

Webmail Mobile Theme Improvements

Greatly expanded and improved the Mobile Theme for Webmail users. See `RelNotes.html` located in MDaemon's `\Docs\` folder for a complete list of the many features that have been added.

Clustering Improvements

A significant number of improvements have been made to MDaemon's Cluster Service:

- Added a Multi-Node Mail Routing option, where mail queues are shared between the cluster nodes. Having multiple machines process and deliver the messages allows them to split the work more evenly and prevents messages from being stuck in the queues of any machines that are down.
- SSL certificates are now replicated from the primary to secondary nodes.
- Queues on secondary nodes are frozen during the initial data replication, which improves responsiveness during startup.
- Replication is paused as soon as MDaemon shutdown starts, eliminating clustering-related shutdown delays.
- Cluster nodes may be added using IP address or DNS name.
- The shared network paths can now be managed more easily from the new Shared Network Paths screen.
- Logging and diagnostics tools are provided on the new Diagnostics screen.

Other New Features and Changes

Remote Administration (MDRA)

Dozens of options have been added to MDaemon's Remote Administration interface. For a complete list of these options and other changes to MDRA, see `RelNotes.html` located in MDaemon's `\Docs\` folder.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Content Filter

Added ability to search for restricted files[643] inside 7-Zip compressed files.

Autoresponders[823]

Autoresponders now support Unicode (UTF-8), allowing the text to be in any language.

IMAP Filters[720]

IMAP filtering rules can now search the message body for particular text.

Webmail

- You can now attach an event to a new email by right-clicking the event and choosing the "Send" option in the LookOut and WorldClient themes, and from the event preview in Mobile theme.
- All New Account Creation features have been removed.
- When you publish a calender (share a Public Access link to it), new options allow you set its default calendar view (e.g. month/week/day) and publish a Free/Busy calendar link.
- Added an option to skip the IP persistence check on a per user basis. In MDRA edit a user account, go to Web Services and check "Skip IP persistence check for Webmail sessions".
- Added ability to search the CC field in advanced search.
- Added Maximum Messages sent per day[715] to the displayed quotas.

User Interface

- Setup | Mobile Device Management has been removed and replaced by the ActiveSync Management dialog at Setup | ActiveSync.
- The ActiveSync Client Settings screen has been removed. Customize client settings on the Tuning, Domains, Groups, Accounts, and Clients screens.
- The ActiveSync Client Type screen has menu commands to whitelist and blacklist client types.
- Added screens at Setup | Message Indexing for the configuration of real-time and nightly maintenance of the search indexes used by Webmail, ActiveSync, and Remote Administration.
- Several plugins now share a common Diagnostics configuration screen.
- The MDRA and Webmail browser-based help systems have been updated with a new responsive theme, to make them more useable across different types of devices.

XML API

- The appearance of the XML API documentation portal can be customized globally and by domain. See the "Changes and development notes" in the help

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

portal (ie. http[s]://ServerName[:MDRAPort]/MdMgmtWS) or view the file \MDaemon\Docs\API\XML API\Help_Readme.xml on disk using Internet Explorer for more information. A sample company.mail directory is provided at \MDaemon\Docs\API\XML API\Samples\Branding.

- Added Alias operation to simplify Alias management, resolve and report aliases.
- Added FolderOperation Search action to search messages.
- Added support for the Cluster Service to QueryServiceState and ControlServiceState.

Archiving

- When a message is sent between local accounts, both "in" and "out" archive copies will be created if both "Archive inbound mail" and "Archive outbound mail" are enabled.
- The option to archive spam messages, which was removed in version 20.0, is back.
- Spam messages released from the Spam Trap are archived.

Component Updates

- MDaemon Connector has been updated to version 7.0.0.
- Spam Filter: updated to SpamAssassin 3.4.4. and removed deprecated settings in local.cf.
- AntiVirus: ClamAV updated to version 0.103.0, and Cyren AV engine updated to version 6.3.0.2.
- XMPP Server: Updated database backend to version SQLite 3.33.0.

MDaemon Server Release Notes

For a comprehensive list of additions, changes and fixes included in MDaemon 21.0, see the Release Notes.

New in MDaemon 20.0

MDaemon Cluster Service

MDaemon's new Cluster Service is designed to share your configuration between two or more MDaemon servers on your network. This makes it possible for you to use load balancing hardware or software to distribute your email load across multiple MDaemon servers, which can improve speed and efficiency by reducing network congestion and overload and by maximizing your email resources. It also helps to ensure redundancy in your email systems should one of your servers suffer a hardware or software failure. See: Cluster Service, for more information on setting up an MDaemon server cluster on your network.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New SMTP Extensions

RequireTLS (RFC 8689) 576

The RequireTLS effort in IETF is finally finished, and support for this has been implemented. RequireTLS allows you to flag messages that **must** be sent using TLS. If TLS is not possible (or if the parameters of the TLS certificate exchange are unacceptable) messages will be bounced rather than delivered insecurely. RequireTLS is enabled by default, but the only messages that will be subject to the RequireTLS process are messages specifically flagged by a Content Filter rule using the new Content Filter action 633, "*Flag message for REQUIRETLS...*", or messages sent to `<local-part>+requiretls@domain.tld` (for example, `arvel+requiretls@mdaemon.com`). All other messages are treated as if the service is disabled. Additionally, several requirements must be met in order for a message to be sent using RequireTLS. If any of them fail, the message will bounce back rather than be sent in the clear. For more information about these requirements and how to set up RequireTLS, see: SMTP Extensions 576. For a complete description of RequireTLS, see: RFC 8689: SMTP Require TLS Option.

SMTP MTA-STS (RFC 8461) - Strict Transport Security 577

The MTA-STS effort in the IETF has finished, and support for this has been implemented. SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate. MTA-STS support is enabled by default. See: SMTP Extensions 576 for more information on setting this up, and MTA-STS is fully described in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP TLS Reporting (RFC 8460) 577

TLS Reporting allows domains using MTA-STS to be notified about any failures to retrieve the MTA-STS policy or negotiate a secure channel using STARTTLS. When enabled, MDaemon will send a report daily to each STS-enabled domain that it has sent (or attempted to send) mail to that day. There are several options provided for configuring the information that your reports will contain. TLS Reporting is disabled by default and discussed in RFC 8460: SMTP TLS Reporting.

Domain/Company-wide MDPGP Encryption with a Single Key

MDPGP 614 now supports encrypting messages between domains using a single encryption key for all users. For example, suppose 'Domain-a' and 'Domain-b' wish to encrypt all emails sent between them but do not wish to setup and police individual encryption keys for every user account within the domain. This can now be done as follows:

'Domain-a' and 'Domain-b' each provide the other with a public encryption key via any method they like. For example, they can email the keys to one another by right-clicking on an existing public key in the MDPGP UI and selecting 'Export & Email Key.' If they wish to create new keys dedicated for this purpose they can click the 'Create keys for a specific user' button and choose the '_Domain Key (domain.tld)_ <anybody@domain.tld>' item which has been put there for this purpose (although any key will work). Once each side has received the other's key they click the 'Import Domain's Key' button on the MDPGP UI and enter the domain name to which all emails

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

will be encrypted using the provided key. The system does not create a key in the dropdown list for every one of your domains. You can use the key that is provided for all your domains or you can create domain specific keys yourself if you wish.

If either side already has a public key they wish to use and it is already on the key-ring they can right-click on the key in the MDPGP UI and select 'Set as a Domain's Key'. However, do not use a key for which you also have the corresponding private key. If you do, MDPGP will encrypt a message and then immediately see that the decryption key is known and promptly decrypt that very same message.

At this point MDPGP creates a Content Filter rule called 'Encrypt all mail to <domain>' which will invoke the encryption operation on every email sent to that domain. Using the Content Filter means that you can control this process by enabling or disabling the Content Filter rule. You can also tweak the rule to fine-tune the criteria you wish to employ before messages are encrypted (for example, maybe you want to do this same thing but for two domains or for only certain recipients within the domain). The Content Filter provides the flexibility to achieve this.

Encrypting Outbound Mail Based on the Receiving IP Address

MDPGP 614 has a new checkbox and setup button where you can map IP addresses to specific encryption keys. Any outbound SMTP session delivering a message to one of these IPs will first encrypt the message using the associated key just prior to transmission. If the message is already encrypted by some other key no work is done. This is useful (for example) in situations where you want to make sure all messages sent to certain key partners, suppliers, affiliates, etc are always encrypted.

Macros for Mailing List Messages

The Mailing List Editor » Routing 285 screen has some new options which will allow for macros to be used within the message body of list posts. This will allow you (for example) to personalize each list message. Macros have been supported for a long time in list mail header and footer files, but they have never been supported in the message body. Since the macros are related to individual list members, this option is only compatible with lists that are configured to "*Deliver list mail to each member individually*." Additionally, for security purposes you can set this option to require that the list's password be provided in order to use macros in the message body. If you choose not to require a password, then any list member who is allowed to post to the list will be allowed to use them. See the Mailing List Routing 285 screen for more information, and for the list of macros that can be used.

Improved Hijack Detection System

Hijack Detection 554 has some new options to help prevent accounts from being used to blast out spam due to their passwords being stolen. One common characteristic of spam email is that the messages are often sent to a large number of invalid recipients, due to the spammer attempting to send them to old email addresses or otherwise guess new ones. Therefore if an MDaemon account begins sending messages to a notable number of invalid recipients in a short amount of time, that is a good indication that the account has been hijacked and is being used to send spam. To prevent this, MDaemon can now track the number of times that an authenticated user tries to send an email to an invalid recipient. If this happens too many times within too short of a time frame, you can have MDaemon freeze the account (the postmaster will get an email about this

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

and they can respond to re-enable the account). This can help to stop a hijacked account automatically, before it does too much damage. **Note:** As part of this work, the From Header Modification options were moved to their own From Header Screening 560 page, to make room for the new Hijack Detection options.

Deferred Message Queue and Improved Message Recall 115

To help improve the efficiency of the Message Recall system and Deferred-Delivery header support, MDaemon now has a dedicated queue for deferred messages. Previously, the Inbound queue could become clogged with deferred messages, which could slow down the delivery of non-deferred mail. The new, Deferred queue helps to solve that problem. Messages in the Deferred queue are placed there by the system and have the date they are set to leave the queue encoded into the file name. MDaemon checks the queue once per minute and when it's time for messages to leave the queue they are moved to the Inbound queue and subject to normal message processing/delivery.

Additionally, MDaemon now tracks the Message-IDs of the most recent email sent by each authenticated local user, which means users can now recall the last message they sent (but only the last message they sent) simply by putting RECALL (alone by itself) as the Subject in a message sent to the mdaemon@ system account. There is no need to find and paste the Message-ID of the message you want to recall when it was the last message sent. Recalling any other message still requires the Message-ID be included in the Subject text or the original message from the users SENT folder attached to the recall request.

In addition to remembering the most recent email sent by each authenticated user, MDaemon also remembers the locations and Message-IDs of the last 1000 emails sent by all authenticated users. Consequently, this makes it possible to recall messages right out of user mailboxes even after they've been delivered. So, messages will disappear from user mail clients and phones if they are recalled. **Note:** this is of course only possible for messages sent to other local users; once MDaemon has delivered a message to some other server it is no longer under MDaemon's control and therefore cannot be recalled.

Authentication Failure Log

There is a new Authentication Failures log file that contains a single line with details for every SMTP, IMAP, and POP logon attempt that fails. The information includes the Protocol used, the SessionID so you can search other logs, the IP of the offender, the raw Logon value they tried to use (sometimes this is an alias), and the Account that matches the logon (or 'none' if no account matches).

Authentication When Forwarding/Routing Mail

There are several forwarding options in MDaemon where you can now add authentication credentials. This means that several files in the \APP\ folder (e.g. `forward.dat`, `gateways.dat`, `MDaemon.ini`, and all Mailing List `.grp` files) that now have the potential to contain obfuscated logon and password data in a weakly encrypted state. As always, you should therefore use the operating system tools at your command, as well as any other measures you choose, to secure the MDaemon machine and directory structure from unauthorized access. Authentication credential

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

options were added to: Unknown Mail 97, Mailing List Routing 285, Gateway Editor » Forwarding 252, Gateway Editor » Dequeuing 253, and Account Editor » Forwarding 711.

Host Authentication 118

Host Authentication is a new screen where you can configure port, logon, and password values for any host. When MDaemon sends SMTP mail to that host the associated credentials found here will be used. Please note that these credentials are a fallback and are only used when other more task-specific credentials are unavailable. For example, if you configure an Auth logon/password using the new Account Editor » Forwarding 711 or Gateway Manager » Dequeuing 253 options, then those credentials are used and they supersede what is configured here. This feature works with host names only (not IP addresses).

Improved Custom Queues and Message Routing 861

You can now specify a host, logon, password, SMTP return-path, and port for any remote queue. If provided, all messages in the queue are delivered using these new settings. However, by design it still remains possible for individual messages within the queue to have their own unique delivery data, which will take priority over these new settings. Additionally, you can now set up as many remote queues as you want, filter mail into them using the Content Filter based on whatever criteria you choose, give to each queue its own delivery schedule, and have completely different routing take place based on your wishes.

Improved Domain Sharing 108

For some time Domain Sharing has performed lookups on SMTP MAIL sender values as needed. However, messages were often refused with 'Authentication Required' and yet there is no way authentication can be performed when the sender account resides on a different server. This has been addressed and MDaemon can accept mail without requiring authentication from accounts that are found to exist on other servers. This can be disabled with a new Security Manager option at: Sender Authentication » SMTP Authentication 509. If you would rather not perform Domain Sharing lookups on the SMTP MAIL sender at all you can completely disable that with a Domain Sharing option.

Domain Sharing also has a new option that enables sharing of mailing lists. When a message arrives for a mailing list a copy is created for each Domain Sharing host that also keeps a version of that list (a query is made to check). When these hosts receive their copies they will make delivery to all the members of that list which they serve. In this way mailing lists can be split across multiple servers with no loss in functionality. For this to work each Domain Sharing host must include the other hosts' IP addresses in their Trusted IPs 506 configuration.

Finally, Domain Sharing has an Advanced button that opens a file where you can configure domain names that are allowed to use Domain Sharing. When nothing is in this file (the default condition) then all your domains can use Domain Sharing. See the instructions at the top of the file for more information.

Improved Control Over Message Forwarding

Preferences » Miscellaneous 489 has a new option that allows administrators to prevent account mail forwarding from sending emails outside the domain. If a user configures mail forwarding for their account to send to a foreign domain the message will be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

moved to the Bad Message queue. This setting only applies to messages that are forwarded using the mail forwarding options for the account.

Account Editor » Forwarding 711 has a new *Schedule* button that will let accounts configure a schedule for when forwarding starts and stops. This is also included on the corresponding Account Templates 792 screen. These settings configure the date and time forwarding starts and the date and time that it stops, but forwarding will only happen on the days of the week you select.

The Forwarding Address field in the New Accounts Template 775 now works with account macros. The only macros with data at the point of new account creation however are those related to the account user's full name, domain, mailbox, and password values. So (for example) if you want every new account to forward to the same email address but at a different domain you can put this in the Forwarding Address field: `$MAILBOX$@example.com`. Macros also work in the *Send As*, *AUTH Logon*, and *AUTH Password* fields.

Forwarding a message now updates the forwarding account's last access time. This means that accounts which do nothing else but forward mail are no longer potentially deleted for inactivity. **Note:** The forwarding must actually occur and not be defeated by other configuration options such as restrictions on where the forwarder can send mail or being 'off-schedule'. Just having a forwarding address configured will not automatically flag the account as active.

Improved SMTP Authentication

Sender Authentication » SMTP Authentication 509 has two new options. First, the "*Do not allow authentication on the SMTP port*" option will completely disable AUTH support over the SMTP port. AUTH will not be offered in the EHLO response and will be treated as an unknown command if provided by the SMTP client. The other option is to "*...add their IP to the Dynamic Screen if they attempt it anyway*." This option will add to the Dynamic Screen 611 the IP address of any client that attempts to authenticate when AUTH is disabled. The connection will also be immediately terminated. These settings are useful in configurations where all legitimate accounts are using the MSA (or other) port to submit authenticated mail. In such configurations the assumption is that any attempt to authenticate on the SMTP port must be from an attacker.

Improved Account Management

The Account Manager's filtering options have been expanded. You can now also choose to display accounts based on whether or not they are Enabled, are using MultiPOP, are near quota (70%), are near quota (90%), or are not forwarding. You can also search the account description field for any text you want and select accounts based on that. Further, the shortcut/right-click menu has new options to add or remove all the selected accounts from or to mailing lists and groups. It also has an option to Copy an existing account in order to create a new one. All settings of the existing account are copied to the new account except Full Name, Mailbox, Password, and Mail Folder. Finally, the Account Editor's IMAP Filters 720 screen has a new button called Publish for adding a new rule to the account being edited and to every other account in that account's domain. This can save some time when a new rule is needed for everyone.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable "Do Not Disturb"for Entire Domain

The Domain Manager's Host Name & IP screen has a new setting that lets you enable "Do Not Disturb" for a domain. When active, the domain will refuse all connections from all users for all services, but it will still accept incoming messages from the outside world. Further, you can schedule when 'Do Not Disturb' starts and stops. For example, if you configure May 1, 2020 to June 30, 2020 from 5:00pm to 7:00am, Monday thru Friday, then that means no mail services will be available for that domain's users on those days of the week beginning at 5:00pm and resuming at 7:01am, so long as the current date falls between May 1 and June 30, 2020. Erasing the scheduled start date deactivates the schedule and has the effect of **putting the domain on 'Do Not Disturb' forever**.

Improved Archiving

MDaemon's simple message archiving system has been changed to be more efficient and consistent. Archiving now work as follows: When a message is delivered from the Local Queue(s) to a user's mail folder an archive copy will be created at that time (in the 'IN' folder of the recipient, if so configured). When a message is picked up from the Remote Queue(s) for SMTP delivery (whether delivery succeeds or not) an archive copy will be created at that time (in the 'OUT' folder of the sender, if so configured). You will see lines like "ARCHIVE message: pgp5001000000172.msg" in the Routing log or you might see lines like "* Archived: (archives) \company.test\in\frank@company.test\arc5001000000023.msg" in the Routing log when Local and Remote mail is processed. Further, a 'ToArchive' queue now exists as a system queue (not exposed in the UI). This queue is checked at regular intervals for messages which have been dropped there (manually, or by a plugin, or otherwise). When messages are found there they are immediately archived and deleted. If messages are found which are not eligible for archiving then they are simply deleted. The name of the queue is \MDaemon\Queues\ToArchive\. The Routing screen/log will show details whenever a message is successfully archived. Also, Archiving of encrypted messages is now handled more consistently. By default unencrypted copies of encrypted messages are stored in the archive. If a message can't be decrypted, the encrypted form will be stored instead. If you would rather have encrypted versions stored, then there is an option to allow you to do so. Additionally, there is now an option to archive messages sent to public folder submission addresses, which is enabled by default. Finally, the following types of messages are never archived: Mailing List traffic, Spam (the option to do so has been deprecated and removed), messages with viruses, system-level messages, and autoresponders.

More Efficient Logging

MDaemon no longer creates empty log files. When items are disabled on the Settings screen their associated log file will not be created at startup. Log files that may already exist when an item is disabled are left in place (not removed). If a log file is missing when an item is enabled then the required log file will be created instantly. This change applies to all log files that the core MDaemon engine manages. Log files for Dynamic Screening, Instant Messaging, XMPP, WDaemon, and WebMail run external to MDaemon and therefore haven't changed. Several other logging-related changes include: making ATRN session logs look correct, making all logs consistent in colors and how they log Session and Child IDs, and the MultiPOP server no longer tears-up and tears-down sessions for accounts that are already over quota and therefore there is no longer wasteful logging in these cases. Finally, the Router log was only logging

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

INBOUND and LOCAL queue message parsing. It now also logs REMOTE queue parsing when delivery attempts are made. This way you don't have to search the Router log and the SMTP(out) logs to see when a message was processed.

Improved Active Directory Integration

You can now configure MDaemon's Active Directory integration feature to create an MDaemon account when you add someone to an Active Directory group, and when you remove someone from an Active Directory group their corresponding MDaemon account will be disabled (but not deleted). To utilize this functionality, you must use an alternative Active Directory search filter. See: Active Directory » Authentication 809, for more information.

On Active Directory's Authentication 809 screen there is now a separate "*Contact search filter*" option for contact searches. Previously, contact searching was done using the user search filter. There's also a separate test button for the contact search filter. Active Directory searches have been optimized so that when the search filters are identical a single query updates all data. When they are different two separate queries are necessary.

The following fields have been added to the ActiveDS.dat file templates, so that they are included in contact records when Active Directory monitoring creates or updates address books: `abTitle=%personalTitle%`, `abMiddleName=%middleName%`, `abSuffix=%generationQualifier%`, `abBusPager=%pager%`, `abBusIPPhone=%ipPhone%`, and `abBusFax=%FacsimileTelephoneNumber%`.

Public folder contacts are now deleted by default when the associated account is deleted from Active Directory. However, the contact is only deleted if it was created by the Active Directory integration feature. The setting to control this is located on the Active Directory Monitoring 812 screen.

When the Active Directory monitoring system creates or updates an account and finds a mailbox value that is too long to fit in MDaemon's limited space for the mailbox value, it will truncate the mailbox value as before but now it will also create an alias using the full size mailbox value. Also, when an account or alias is created, the note's section of the account's Administrative Roles 741 screen is updated for auditing purposes.

The Mailing List Manager's Active Directory 290 screen now allows you to enter an Active Directory attribute for the full name field of list members.

Changes to account properties in Active Directory can trigger the recreation of an MDaemon account, even when the account was previously deleted within MDaemon. To keep accounts from being recreated in this way, a new option was added to Active Directory Monitoring 812. By default, accounts will not be recreated when they were manually deleted within MDaemon.

Improved From Header Screening 560

The "*From Header Modification*" options were moved from the Hijack Detection screen to their own From Header Screening 560 screen, and new options were added. Such as, From Header Screening can now check "From:" header display-names for anything that looks like an email address. If one is found and it does not match the actual sending email address then the displayed address can be replaced with the actual email address. For example, if you are using this feature and the "From:" header looks like

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

this: "`From: 'Frank Thomas <friend@friend.test>' <enemy@enemy.test>`" then it would be changed to: "`From: 'Frank Thomas <enemy@enemy.test>' <enemy@enemy.test>`".

Check for Compromised Passwords

MDaemon can now check a user's password against a compromised password list from a third-party service. It is able to do this without transmitting the password to the service, and if a user's password is present on the list it does not mean the account has been hacked. It means that someone somewhere has used the same characters as their password and it has appeared in a data breach. Published passwords may be used by hackers in dictionary attacks, but unique passwords that have never been used anywhere else are more secure. See Pwned Passwords for more information.

On the Security Settings' Passwords screen, MDaemon now has an option to prevent an account's password from being set to one that is found in the compromised passwords list. It can also check a user's password every certain number of days when they log in, and if it is found, send a warning email to the user and postmaster. The warning emails can be customized by editing message template files in the `\MDaemon\App` folder. Since instructions for how a user should change their password may depend on whether the account is using a password stored in MDaemon or using Active Directory authentication, there are two template files, `CompromisedPasswordMD.dat` and `CompromisedPasswordAD.dat`. Macros can be used to personalize the message, change the subject, change the recipients, etc.

Additional Features and Improvements

With over 250 new features and improvements included in MDaemon 20, there are many not listed in this section. For a comprehensive list of additions, changes and fixes included in MDaemon 20.0, see the Release Notes.

New in MDaemon 19.5

New Webmail Mobile theme

Webmail's Mobile theme has been replaced with a more modern GUI with more features. Message list features now include personalized categories, message snooze, sort by flagged/unread/snoozed, sort columns, and message recall. Calendar features now include Import/Export events as csv or ics files, add external calendars, private access links, publish calendar, and view multiple calendars at one time. Compose features now include deferred delivery, multiple signatures, text/html messages, and email templates. Other features include drag and drop email filters, multiple signatures editor, more folder management options, notifications, drag and drop column management, drag and drop categories management, and more. If running Webmail in IIS, additional configuration steps are needed to utilize the new mobile theme. See Knowledge Base article 1236 for more information.

Client signature management

You can now configure an email signature to be pushed to Webmail and MDaemon Connector for your users. A Default Client Signature can be set or it can be set per

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

domain on the Domain Manager's Client Signatures 200 screen. Use signature macros 133 such as $CONTACTFULLNAME$, $CONTACTEMAILADDRESS$, to personalize the signature with data pulled from the user's contact in the domain's Public Contacts folder. Use the $ATTACH_INLINE:filename$ macro for inline images in the HTML signature. After entering signature text, it will appear in Webmail's Compose options as the "System" signature, and will become the user's default signature. It can be enabled/disabled for Webmail by default under the Webmail Settings 333, or per domain on the Domain Manager 187. For MDaemon Connector, the signature's name and related settings can be configured on the MC Client Settings' Signature 397 screen. This feature requires MDaemon Connector 6.5.0 or newer, and *Push client settings to MC users* 382 to be enabled. The $CLIENTSIGNATURE$ macro can be used in other mail clients to have the server add the client signature to messages.

Categories Page 332

MDaemon's Remote Administration (MDRA) interface now has a Categories 332 page under the Webmail options, for configuring Domain Categories and default Personal Categories.

Additional MDRA Improvements

Many options that previously could only be managed through MDaemon's application interface have been added to MDRA. For a complete list, see the Release Notes.

New in MDaemon 19.0

TLS Server Name Indication (SNI) support 563

MDaemon now supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

XML-API for Folder and Item Management

The XML-API has been expanded to include the ability to manage mailbox folders and items in the folders. Folders can be created, deleted, renamed, and moved using the API. Item operations support email, calendar, contacts, tasks, and notes. Items can be created, deleted, and moved using the API. Full documentation can be found in the MDaemon\Docs\API\XML-API\ folder.

Remote Administration Improvements

MDaemon's Remote Administration (MDRA) web interface has been further expanded to include access to features that formerly could only be administered using a Configuration Session (i.e. MDaemon's application interface), and there are now several options that can only be accessed via MDRA. Consequently, for new MDaemon installations, the "Start MDaemon" Start Menu shortcut will now open a browser to MDaemon Remote Administration by default rather than opening an MDaemon

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Configuration Session. If you wish to change this, edit `\MDaemon\App\MDaemon.ini` and set `[MDLaunch] OpenConfigSession=Yes/No` and `OpenRemoteAdmin=Yes/No`. Set the *Remote Administration URL* at Setup » Web & IM Services » Remote Administration » Web Server 343 if the auto-generated URL does not work or if MDRA runs in an external web server. If a working URL cannot be determined, a Configuration Session will be opened instead. Finally, under the Windows Start menu, in the MDaemon program group, there are now shortcuts to *Open MDaemon Configuration Session* and *Open MDaemon Remote Administration*.

Webmail Improvements

- Webmail users with their *Show Saved Search Folders* option enabled (located in Webmail under Options » Folders) will now be asked if they wish to add an "All Unread" and an "All Flagged" Saved Search folder to their list. They will be asked only one time, the first time they sign-in. If a user chooses "No", he or she can still easily create those Saved Searches manually by clicking the *Create All Unread Saved Search* and *Create All Flagged Saved Search* buttons (also located under Options » Folders). Administrators can prevent Webmail from asking users if they wish to create those searches by adding `DefaultSavedSearchesCheck=Yes` under `[Default:UserDefaults]` in the `MDaemon\WorldClient\Domains.ini` file.
- Modified some *WorldClient* theme icons to make them easier to see.
- Added "(EXPIRED)" to the browser tab title when the session expires, so that if a user is not in the Webmail tab the user will still know that the session expired.
- Added a delete icon for removing common contacts from the autocomplete list.

New in MDaemon 18.5

Signature Macros 128

MDaemon signatures now support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed on the Default Signatures 128 page.

Users can also control the placement of MDaemon signatures in their messages by using the `$SYSTEMSIGNATURE$` macro to place the default/domain signature and `$ACCOUNTSIGNATURE$` to place the account signature.

MDaemon Instant Messaging in Webmail

The WorldClient and LookOut themes now feature a browser-based XMPP client that lets users instant message without needing to run the MDaemon Instant Messenger desktop application or some other XMPP client application. Users can enable it from Webmail's Options | Personalize screen, using the "Enable MDaemon's Instant

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Messaging feature in browser" option. Admins can enable or disable instant messaging per domain using the Domain Manager, per account using the Account Editor, or per group using the Group Manager.

MDaemon includes a new BOSH server to support instant messaging in Webmail. Its settings can now be configured on the XMPP screen 365 (**new in 18.5.1)**.

Exempt Webmail from Location Screening

Added a user option in Webmail to exempt Two Factor Authentication logins from Location Screening. If a user has `BypassLocationScreeningTFA=Yes` in the `[User]` section of their `User.ini` file, and Two Factor Auth is enabled for the user, Location Screening is bypassed. This allows users to login to Webmail in countries that would normally be blocked by Location Screening.

Improved AD Integration

Users whose accounts are set to use Active Directory (AD) authentication can now change their AD password in Webmail if the "AllowADPasswordChange" setting is enabled in \MDaemon\WorldClient\Domains.ini. It is disabled by default.

MDRA Expanded

MDaemon's Remote Administration (MDRA) web interface has been expanded to include access to many features that formerly could only be administered using MDaemon's graphical user interface.

New in MDaemon 18.0

DNSSEC 579

The new DNSSEC (DNS Security Extensions) option allows MDaemon to act as a Non-Validating Security-Aware Stub Resolver, which is defined in RFCs 4033 and 4035 as "an entity that sends DNS queries, receives DNS responses, and is capable of establishing an appropriately secured channel to a security-aware recursive name server that will provide these services on behalf of the security-aware stub resolver." What this means is that during MDaemon's DNS queries in can request DNSSEC service from your DNS servers, setting the AD (Authentic Data) bit in the queries and checking for it in the answers. This can provide an additional level of security during the DNS process for some messages, although not all, because DNSSEC is not yet supported by all DNS servers or for all top-level domains.

When enabled, DNSSEC service is only applied to messages that meet your selection criteria; it can be requested or required as broadly or narrowly as you choose. Simply designate any "`Header Value`" combinations you choose on the DNSSEC screen and MDaemon will request DNSSEC service for any messages matching that criteria whenever performing a DNS query. When the DNS results fail to include authenticated data then no negative consequences result; MDaemon simply falls back to normal DNS behavior. If, however, you wish to *require* DNSSEC for certain messages, add "SECURE" to the header/value combination (e.g. `To *@example.net SECURE`). For those messages, when the DNS results fail to include authenticated data, the message will be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

bounced back to the sender. **Note:** Because DNSSEC lookups take more time and resources, and because DNSSEC is not yet supported by all servers, MDaemon is not configured to apply DNSSEC to every message delivery by default. However, if you wish to request DNSSEC for every message you can do so by included "`To *`" in your criteria.

AntiVirus Mailbox Scanning

There is a new *Scan all messages every [n] day(s)* option under Security » AntiVirus 653 that can be used to scan all stored messages periodically, to detect any infected message that may have passed through the system before a virus definition update was available to catch it. Infected messages will be moved to the quarantine folder and have the `X-MDBadQueue-Reason` header added, so that you can see an explanation when viewed in MDaemon. Messages that cannot be scanned will not be quarantined. There is also a *Configure mailbox scan* option to specify how often you wish to scan the messages and whether you wish to scan all message or only those that are less than a certain number of days old. You can also manually run a mailbox scan immediately.

Exempt Known ActiveSync Devices from Location Screening

Enable the new Exempt from Location Screening 451 option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen. When exempting a device from Location Screening, there is also an option to whitelist the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

New Webmail and MDRA Features

Remember Me

You can now add a "Remember Me" checkbox to the sign-in pages of MDaemon Webmail and MDaemon Remote Administration (MDRA), via options located on the Webmail Settings screen 333 and MDRA Web Server screen 343, respectively. When this option is enabled, users who sign-in via the https port will see the checkbox. If users check this box then their credentials will be remembered for that device. Then any time they use that device to connect to Webmail or MDRA in the future they will be signed in automatically, until such time that they manually sign out of their account or their Remember Me token expires. The *Remember Me* option is disabled by default and applies to all of your domains. If you wish to override this setting for specific Webmail domains then use the *Remember Me* setting located on the Domain Manager's Webmail screen 187 in MDaemon's desktop interface.

By default, users' credentials will be remembered for 30 days before they are forced to sign-in again, but you can use the *Expire Remember Me tokens after this many days* option (located in MDRA) to designate a different number of days if you choose. You can set this option up to 365 days. **Note:** Two-Factor Authentication 703 (2FA) has its

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

own Remember Me expiration key (`TwoFactorAuthRememberUserExpiration=30`), located in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. Therefore 2FA will again be required at sign-in when the 2FA Remember Me token expires, even if the regular token is still valid.

In MDRA there is also a *Reset Remember Me* button that you can use if you suspect that an account may have had a security breach. This will reset the Remember Me tokens for all users, causing them to have to sign-in again.

Email Snooze

In MDaemon Webmail you can now snooze an email in your message list. A snoozed message will be hidden from you for a designated period of time. To snooze a message, right click on it and choose the "Snooze for..." option in the context menu. Then choose how long you wish to snooze the message. The "Choose a date and time" option is only available for browsers that support the date and time inputs. Hidden messages can be viewed in the LookOut theme by clicking the "View Snoozed Messages" icon in the toolbar and the WorldClient theme by choosing "view snoozed" from the view drop-down menu in the toolbar. This feature is on by default. To turn off the feature, go to Options | Personalize in Webmail and find the Inbox Settings. Uncheck the "Enable Message Snooze" box. There are no snooze controls in Lite and Mobile theme, but snoozed messages are still hidden.

Public Calendars

In MDaemon Webmail users can now publish a calendar to a publicly accessible link, and they have the option to password-protect the calendar. To publish a calendar, in Webmail's LookOut or WorldClient theme go to Options | Folders and click the "Share Folder" button next to the calendar you wish to publish. Then, open the Public Access tab and, if desired, fill in the display name or require a password, then click the "Publish Calendar" button. A confirmation dialog will be displayed, and after clicking OK an alert will display the new URL where the calendar is available. There will also be a link displayed on the page once the calendar has been published. To unpublish the calendar, click the "Unpublish Calendar" button. To change the password or the display name, click the "Update" button.

If you wish to disable this globally, change the value of the `EnablePublicCalendars` key to **No** in the `[Default:Settings]` section of the `Domains.ini` file. To disable it on a per user basis, add `CanPublishCalendars=No` to a user's `User.ini` file.

New in MDaemon 17.5

Location Screening 558

Location Screening is a geographically based blocking system that you can use to block incoming SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP, and Minger connections from unauthorized regions of the world. MDaemon determines the country associated with the connecting IP address and then blocks that connection if it is from a restricted location, and adds a line to the Screening log. For SMTP, Location Screening can optionally block only connections using AUTH. This is useful, for example, if you have no users in a specific

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

country but still wish to be able to receive mail from there. That way you would only block those attempting to log in to your server.

The \MDaemon\Geo\ folder contains database files that serve as the master country IP database. The files were provided by MaxMind (www.maxmind.com), and updates can be downloaded from their site if desired.

Dynamic Screening for All Protocols and Services 596

MDaemon's Dynamic Screening system has been greatly expanded to operate with SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery, XML API, Remote Administration, CalDAV/CardDAV, XMPP, and Minger. Authentication failures are tracked across all of these services and IPs addresses can be blocked for all of them. Dynamic Screening can be configured on its new, multi-tabbed dialog under the Security menu.

PIM Attachments

PIM (calendar, contact, tasks, notes) items now support attachments. Attachments can be added to a PIM item via Webmail, Outlook Connector, or CalDAV/CardDAV. When scheduling a meeting, any attachments will be sent to the meeting attendees.

PGP Key-exchange During SMTP 614

The MDPGP dialog contains a new option to enable the automatic transmission of public keys as part of the SMTP message delivery process. To do so, MDaemon's SMTP server will honor an SMTP command called RKEY. When sending an email to a server that supports RKEY, MDaemon will offer to transmit the sender's current, preferred public-key to the other host. That host will respond indicating that it either already has that key ("250 2.7.0 Key already known") or that it needs that key, in which case the key is immediately transferred in ASCII armored form ("354 Enter key, end with CRLF.CRLF") just like an email message. Keys that are expired or revoked are never transmitted. If MDaemon has multiple keys for the sender it will always send the key that is currently marked as preferred. If no key is preferred then the first one found is sent. If no valid keys are available then nothing is done. Only public-keys that belong to local users are offered.

Public-key transfers happen as part of the SMTP mail session that delivers the message from the user. In order for the public-keys transmitted in this way to be accepted, the public-key must be sent along with a message that has been DKIM signed 518 by the domain of the key owner with the i= set to the address of the key owner, which also must exactly match the From: header address of which there can be only one. The "key owner" is taken from within the key itself. Also, the message must arrive from a host in the sender's SPF path 512. Finally, the key owner (or his entire domain via use of wildcards) must be authorized for RKEY by adding an appropriate entry to the MDPGP rules file (instructions are in the rules file for this) indicating that the domain can be trusted for key exchange. All this checking is done automatically for you but you must have DKIM 514 and SPF verification 512 enabled or no work can be done.

The MDPGP log shows the results and details of all keys imported or deleted, and the SMTP session log also tracks this activity. This process tracks the deletion of existing keys and the selection of new preferred keys and updates all participating servers it sends mail to when these things change.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Manage Outlook Add-ins for Outlook Connector Users

Using the new Add-ins screen on the OC Client Settings dialog, you can manage the state of the Outlook Add-ins used by your Outlook Connector users. You can allow any or all of the add-ins to be used normally, or you can disable any that you choose. This feature can be especially useful in cases where you know of a specific add-in that conflicts with the Outlook Connector Client, allowing you to disable that add-in to avoid problems. The Add-ins feature requires Outlook Connector 5.0 or newer.

Webmail Changes

Import/Export Groups/Distributions Lists
In the LookOut and WorldClient themes, an option was added to export and import Groups/Distribution Lists from and to a contact folder in Webmail. The format is MDaemon Webmail specific, since Outlook does not support exporting and importing Groups. The format is as follows:

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

Each line that contains either a Group Name or a Group GUID is considered the beginning of a new group. Any GUID, Full Name or Email on that line is considered the first member of the group/list.

Example from Excel:

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

When importing, the Group GUID is replaced with a freshly generated GUID. If no Group Name is included, the name will be displayed without translation as "ImportedFromCSV_ %GUID%", where %GUID% is replaced with the first five characters of the GUID. Leaving the cells to the right of a group name empty will result in the next line being the first member of the group/list. The Email field is required for a member to be added.

Voice Recorder
Voice Recording was added to the Lookout and WorldClient themes. This feature requires a microphone and is only available in certain browsers. It can be disabled by the admin on a per user basis by adding `EnableVoiceRecorder=No` to the User.ini. Users are limited to five tracks of five minutes each. Attempting to record more than

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

five tracks in a Voice Recorder session will result in either the selected track or the first track being replaced by the new recording (the user will be prompted). After recording is stopped (either automatically or by the user), the track is converted to an mp3 and uploaded to the server. Users have four options regarding each track:

- Save to the desktop
- Save to default WorldClient documents folder
- Send in an email using a quick dialog that only includes To, CC, BCC, Subject, and a plain/text Message Body

  Only the To is required. There are generic Subject and Message Body phrases used when no Subject or Message Body is input by the user.
- Open a new Compose view with the track attached

Users can only act on one track at a time. For example, only one track can be attached to a message. If a user wants to attach multiple tracks to a message, the user will need to save each track to the default documents, and do the attaching from there.

New Folder Management Features
The LookOut and WorldClient themes have new folder management features in the Options » Folders view and in the main folder list view.

In the folder list view (left pane):

- Users can drag and drop to move folders from one parent folder to another.
- Users can rename folders and give favorites nicknames by clicking on them a second time (shortly after folder selection)
- Show Folders by Type is now available in the LookOut theme
- If there is already at least one favorite folder (because favorites are hidden until one is added), users can drag and drop a folder to favorites in order to add it (dragging a folder out of the favorites does nothing).
- The new folder and rename folder dialogs were added to the LookOut theme

In the Options » Folders view, the folder tree is now collapsible, and the New Folder dialog has been moved to an external window like in the WorldClient theme.

New in MDaemon 17.0

XMPP 365 support for WorldClient Instant Messenger 309 (WCIM)

WCIM now uses the XMPP protocol for instant messaging instead of WorldClient's proprietary protocol. This allows the WCIM desktop client to communicate not only with other WCIM clients, but any third-party XMPP clients (including mobile clients) connected to your MDaemon's XMPP server. Additionally, WCIM now has two types of connections: "WCMailCheck" and "WCIMXMPP." WCMailCheck connects to WorldClient for new mail notifications and message counts. WCIMXMPP connects to the XMPP server for instant messaging. Consequently, WCIM users will now have an entry for

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

each type of connection listed on the Connections screen of the client (e.g. "Example.com Mail" and "Example.com WCIM"). When updating to version 17, WCIM will automatically create a WCIMXMPP connection to go with your already existing WCMailCheck connection, and it will migrate your IM contacts from the old system to XMPP. The look and feel of the new WCIM client is essentially the same, but there are some differences, such as how contacts and group chats are managed. See the WCIM client's Help system for more info about what has changed.

WorldClient Dropbox Integration 325

WorldClient is new equipped with direct support for Dropbox, which allows your users to save file attachments to their Dropbox accounts, and to insert direct links to Dropbox files in outgoing messages. To provide this feature to your WorldClient users, you must set up your WorldClient as a Dropbox app on the Dropbox Platform. This is a simple process, requiring you only to sign in to a Dropbox account, create a unique name for an app with Full Dropbox access, specify the Redirect URI to WorldClient, and change one default setting. Then, you will copy and paste the Dropbox App Key and App Secret from there to the options on Dropbox screen in MDaemon. After that your users will be able to link their Dropbox accounts to WorldClient when they next sign in to WorldClient. For step-by-step instructions on how to create your Dropbox app and link it to WorldClient, see: Creating and Linking Your Dropbox App 327.

When you create your Dropbox app it will initially have "Development" status. This allows up to 500 of your WorldClient users to link their Dropbox accounts to the app. According to Dropbox, however, "once your app links 50 Dropbox users, you will have two weeks to apply for and receive Production status approval before your app's ability to link additional Dropbox users will be frozen, regardless of how many users between 0 and 500 your app has linked." This means that until you receive production approval, Dropbox integration will continue to work but no additional users will be able to link their accounts. Obtaining production approval is a straightforward process to ensure that your app complies with Dropbox's guidelines and terms of service. For more information, see the Production Approval section of the Dropbox Platform developer guide.

Once your WorldClient app is created and configured properly, each WorldClient user will be given the option to connect their account to their Dropbox account when they sign in to WorldClient. The user is required to log in to Dropbox and grant permission for the app to access the Dropbox account. Then the user will be redirected back to WorldClient using a URI that was passed to Dropbox during the authentication process. For security that URI must match one of the Redirect URIs you specified on your app's info page at Dropbox.com. Finally, WorldClient and Dropbox will exchange an access code and access token, which will allow WorldClient to connect to the user's Dropbox account so that the user can save attachments there. The exchanged access token expires every seven days, meaning that periodically the user must reauthorize the account to use Dropbox. Users can also manually disconnect their account from Dropbox, or reauthorize it when necessary, from the Cloud Apps options screen within WorldClient.

Integration with Let's Encrypt 580 via PowerShell script

To support SSL/TLS and HTTPS 561 for MDaemon 563, WorldClient 566, and Remote Administration 570, you need an SSL/TLS Certificate. Certificates are small files issued by a Certificate Authority (CA) that are used to verify to a client or browser that it is connected to its intended server, and that enable SSL/TLS/HTTPS to secure the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

connection to that server. Let's Encrypt is a CA that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

To support using Let's Encrypt's automated process to manage a certificate, MDaemon includes a PowerShell script in the "MDaemon\LetsEncrypt" folder. A dependency of the script, the ACMESharp module v2, requires PowerShell 5.1 and .Net Framework 4.7.2, which means the script will not work on Windows 2003. Additionally, WorldClient must be listening on port 80 or the HTTP challenge cannot be completed and the script will not work. You will need to correctly set the execution policy for PowerShell before it will allow you to run this script. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the WorldClient HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, WorldClient, and Remote Administration.

If you have an FQDN 177 setup for your default domain that does not point to the MDaemon server, this script will not work. If you want to setup alternate host names in the certificate, you can do so by passing the alternate host names on the command line.

Example usage:

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

You do not need to include the FQDN for the default domain in the `AlternateHostNames` list. For example, suppose your default domain is "`example.com`" configured with an FQDN of "`mail.example.com`", and you want to use an alternate host name of "`imap.example.com`". When you run the script, you will only pass "`imap.example.com`" as an alternate host name. Further, if you pass alternate host names, an HTTP challenge will need to be completed for each one. If the challenges are not all completed then the process will not complete correctly. If you do not want to use any alternate host names then do not include the `-AlternateHostNames` parameter in the command line.

If you are running WorldClient via IIS, you will need to pass this script the name of your site using the `-IISSiteName` parameter. You must have Microsoft's Web Scripting tools installed in order for the certificate to be automatically setup in IIS.

Finally, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs. The log includes the starting date and time of the script but not the date and time stamp for each action. Also, notification emails can be sent when an error occurs. This is done using the `$error` variable, which is automatically created and set by PowerShell. If you do not wish to have email notifications sent when an error occurs, do not include the `-To` parameter in the command line.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Option to store mailbox passwords using non-reversible encryption

There is a new Password option 840 to store mailbox passwords using non-reversible encryption. This protects the passwords from being decrypted by MDaemon, the administrator, or a possible attacker. When enabled, MDaemon uses the bcrypt password hashing function, which allows for longer passwords (up to 72 characters), and for passwords to be preserved yet not revealed when exporting and importing accounts. Some features, however, are not compatible with this option, such as weak password detection and APOP & CRAM-MD5 authentication, because they depend on MDaemon being able to decrypt passwords. Non-reversible passwords is enabled by default.

ActiveSync Client Approval

There is a new ActiveSync setting that you can use to require that "New clients must be authorized by an administrator prior to synchronizing" with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This option is available on the Global 413 and Account 748 client settings screens. The global option is Off by default and the account option is set to "Inherit."

ActiveSync Notifications

Two types of administrative notifications have been added to ActiveSync: Sync Rollback Notifications and Corrupt Message Notifications.

Sync Rollback Notifications

The ActiveSync Service can now notify the administrators if a client is repeatedly/frequently sending expired Sync Keys in Sync operations.

These merely inform the admin that the server issued a rollback for a given collection because a client made a sync request with the most recently expired Sync Key. The subject states "ActiveSync Client Using expired Sync Key". This could occur because of a network issue or something about the content previously sent to the client in that collection. In some cases, the item ID will be there, it merely depends upon whether or not the previous sync on that collection sent any items.

Rollback warnings do not mean the client is out of Sync, it means that the client has the potential to go out of Sync and our internal system detected it. Rollback warnings are issued for a collection no more than once per 24 hour period. The following keys can be edited under the [System] header in the `\MDaemon\Data\AirSync.ini` file:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (Default is disabled)
- [System] RollbackNotificationThreshhold=[1-254] : The number of rollbacks that must occur on a given collection prior to a notification being sent to the admin. We recommend a value of at least 5 here, since Network hiccups play a part in this. (Default is 10)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Whether or not to CC the user whose client sent that expired Sync Key. (Default is disabled)

ActiveSync Corrupt Message Notifications

The ActiveSync Service can now notify the administrators if a particular message cannot be processed. These are sent in real time to inform the admin of a mail item that could not be parsed and that further action on this item is not possible. The subject states "Corrupt message notification". These items, in previous versions, could lead to a crash. In most cases, the content of the msg file will not be MIME data. If it is MIME data, it is likely corrupt. You can choose to CC the affected user of these notifications with the CMNCCUser key so that they are aware that an email has arrived in their mailbox that is un-readable. The appropriate action for these is to move the designated msg file from the user's mailbox and analyze it to determine both why it is not able to be parsed and how it came to exist in the state that it is in. The following keys can be edited under the [System] header in the `\MDaemon\Data\AirSync.ini` file:

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

New in MDaemon 16.5

MDPGP Improvements 614

Key Server Support

WorldClient

WorldClient can now act as a basic public-key server. Enable the new MDPGP option to "*Send public-keys over HTTP (WorldClient)*" and WorldClient then will honor requests for your users' public-keys. The format of the URL to make the request looks like this: "`http://<WorldClient-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`". Where `<WorldClient-URL>` is the path to your WorldClient server (for example, "`http://wc.example.com`") and `<Key-ID>` is the sixteen character key-id of the key you want (for example, "`0A1B3C4D5E6F7G8H`"). The key-id is constructed from the last 8 bytes of the key fingerprint - 16 characters in total.

DNS (PKA1)

Enable the new MDPGP option to "*Collect public-keys from DNS (pka1) and cache for [xx] hours*" if you want MDPGP to query for message recipient public-keys over DNS using PKA1. This is useful because it automates the process of obtaining some recipients' public keys, preventing you or your users from having to obtain and import them manually in order to send encrypted messages. When PKA1 queries are made, any key URI found is immediately collected, validated, and added to the key-ring. Keys successfully collected and imported to the key-ring using this method will automatically

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

expire after the number of hours specified in this option or according to the TTL value of the PKA1 record that referred them, whichever value is greater.

Key Handling

Tracking Keys

MDPGP now always tracks keys by their primary key-ids rather than sometimes by the key-id and other times the sub-key-id. Consequently, the MDPGP dialog's list of keys was cleaned up to remove two unnecessary columns. Further, MDPGP now more strictly controls the contents of its "exports" folder. As a result you will always find exported copies of local user keys there. Even though the private keys are encrypted, for extra security you should use OS tools to protect this folder (and indeed the entire PEM folder structure) from unauthorized access.

Preferred Keys

Previously, when multiple different keys for the same email address were found in the key-ring, MDPGP would encrypt messages using the first one that it found. Now you can right-click on any key and set it as preferred, so that MDPGP will use that key when multiple keys are found. If no preferred key is declared, MDPGP will use the first one found. When decrypting a message MDaemon will try each one.

Disabled Keys

Disabled and deleted keys are now tracked in a new file called `oldkeys.txt`. Previously, disabled keys were tracked in the `plugins.dat` file.

MDPGP Signature Verification

MDPGP can now verify embedded signatures found within messages that are not encrypted. Previously it was not able verify signatures unless the message was both signed and encrypted. When viewing a message with a verified signature in WorldClient, a new icon is displayed to indicate it was verified. Signature verification is enabled by default for all non-local users, or you can specify exactly which email addresses can and cannot use the service (see: "*Configure exactly who can and can not use MDPGP services*" on the MDPGP dialog 614).

XMPP Instant Messaging Server 365

MDaemon is now equipped with an Extensible Messaging and Presence Protocol (XMPP) server, sometimes called a Jabber server. This allows your users to send and receive instant messages using third-party XMPP clients, such as Pidgin, Gajim, Swift and many others. Clients are available for most operating systems and mobile device platforms. MDaemon's XMPP instant messaging system is completely independent of MDaemon's WorldClient Instant Messenger chat system; the two systems cannot communicate with each other and do not share buddy lists.

The XMPP server is installed as a Windows service, and the default server ports are 5222 (SSL via STARTTLS) and 5223 (dedicated SSL). The XMPP server will use MDaemon's SSL configuration if it is enabled in MDaemon. Also, some XMPP clients use DNS SRV records for auto-discover of host names. Please refer to http://wiki.xmpp.org/web/SRV_Records for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Users sign-in through their chosen XMPP client using their email address and password. Some clients, however, require the email address to be split into separate components for signing in. For example, instead of "frank@example.com," some clients require you to use "frank" as the Login/Username and "example.com" as the Domain.

For multi-user/group chat service, clients typically display this as "rooms" or "conferences." When you want to start a group chat session, create a room/conference (giving it a name) and then invite the other users to that room. Most clients don't require you to enter a server location for the conference; you only need to enter a name for it. When you are required to do so, however, use "conference.<your domain>" as the location (e.g. conference.example.com). A few clients require you to enter the name and location together in the form: "room@conference.<your domain>" (e.g. Room01@conference.example.com).

Some clients (such as Pidgin), support the user search service, allowing you to search the server for users by name or email address, which makes adding contacts much easier. Usually you will not have to provide a search location, but if asked to do so, use "search.<your domain>" (e.g. search.example.com). When searching, the % symbol can be used as a wildcard. Therefore you could use "%@example.com" in the email address field to display a list of all users with an email address ending in "@example.com."

Centralized Management of OC Client Settings 382

Use the OC Client Settings dialog to centrally manage the client settings of your Outlook Connector users. Configure each screen with your desired client settings and MDaemon will push those settings to the corresponding client screens as necessary, each time an Outlook Connector user connects to the server. The OC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them. If you enable the provided option to "*Allow OC users to override pushed settings*," users can override any pushed settings on their individual clients. If that option is disabled, then all of the client screens are locked; Outlook Connector users can make no changes.

To allow for certain settings that must be different for each user or domain, OC Client Settings supports macros such as $USERNAME$, $EMAIL$, and $DOMAIN$. These macros will be converted to data specific to the user or domain when pushing settings to a client. Take care not to place any static values in any fields that should use a macro, such as putting something like "Frank Thomas" in the Your Name field. To do so would cause every Outlook Connector user who connects to MDaemon, to have his or her name set to "Frank Thomas." For your convenience there is a Macro Reference button on the General 384 screen, which displays a simple list of the supported macros.

For those using MDaemon Private Cloud (MDPC), there is another OC Client Settings dialog on the Domain Manager 174, for controlling the Outlook Connector client settings on a per domain basis.

This feature is disabled by default, and works only for those using Outlook Connector client version 4.0.0 or higher.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

"From:" Header Protection/Modification 554

This new security feature modifies the "From:" header of incoming messages to cause the name-only portion of the header to contain both the name and email address. This is done to combat a common tactic used in spam and attacks where the message is made to appear to be coming from someone else. When displaying a list of messages, email clients commonly display only the sender's name rather than the name and email address. To see the email address, the recipient must first open the message or take some other action, such as right-click the entry, hover over the name, or the like. For this reason attackers commonly construct an email so that a legitimate person or company name appears in the visible portion of the "From:" header while an illegitimate email address is hidden. For example, a message's actual "From:" header might be, `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, but your client might display only `"Honest Bank and Trust"` as the sender. This feature changes the visible portion of the header to display both parts, with the email address given first. In the above example the sender would now appear as `"lightfingers.klepto@example.com -- Honest Bank and Trust,"` giving you a clear indication that the message is fraudulent. This option only applies to messages to local users, and it is disabled by default.

Improved IP Screening 548

The IP Screen now contains an Import button that you can use to import IP address data from an APF or .htaccess file. MDaemon's support for these files is currently limited to the following:

- "deny from" and "allow from" are supported
- only IP values are imported (not domain names)
- CIDR notation is allowed but partial IP addresses are not.
- Each line can contain any number of space-separated or comma-separated IP addresses. For example, "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5", and the like.
- Lines starting with # are ignored.

Automatic Installation of Product Updates 487

Using the Automatic Updates features you can configure MDaemon to inform the postmaster whenever an update is available for one of your installed products, or you can download and install updates automatically. This includes MDaemon, SecurityPlus, and Outlook Connector. Automatically installing updates can be controlled separately for each product, and a server reboot is required each time an update is installed. Installer files are downloaded when the update is detected, but the installation and reboot occur later at whichever hour you have designated. All installation activity is logged in the MDaemon system log, and the postmaster is informed after an update has occurred. See the Updates 487 dialog for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

WorldClient Changes

Categories 332

WorldClient supports categories for email in the LookOut and WorldClient themes. Users can add the Categories column to the message list by going to "Options » Columns" and checking "Categories" in the Message List section. To select categories for one or multiple messages, select the messages and right-click one of them. Use the context menu to set the category.

- Administrators can create custom categories. There are two files for this purpose: `DomainCategories.json` and `PersonalCategories.json`.
- Domain Categories are enabled globally by default. To disable them open `MDaemon\WorldClient\Domains.ini`, and in the `[Default:Settings]` section change the value of "`DomainCategoriesEnabled=`" from "`Yes`" to "`No`".
- Users are able to add and edit their own categories by default. If you wish to disable this option, you can do so per user or globally by changing the value of "`CanEditPersonalCategories=`" from "`Yes`" to "`No`". The user option is located in the `[User]` section of the `User.ini` file and the global option is in the `Domains.ini` file under the `[Default:UserDefaults]` section.
- If Domain Categories are enabled, and a user is not allowed to edit personal categories, the user will only see the categories listed in `DomainCategories.json`.
- If Domain Categories are disabled, and a user is not allowed to edit personal categories, the user will see the categories listed in `PersonalCategories.json`.
- The file `CustomCategoriesTranslations.json` is used to support your custom category names in multiple languages. Add any necessary custom category translatations to that file to make it possible for WorldClient to recognize a category saved to an event, note, or task in one language as the equivalent category in another language.

For more detailed information relating to the files mentioned here, see: `MDaemon\WorldClient\CustomCategories.txt`.

White and Black Lists 340

You can now hide the White List and Black List folders for WorldClient users by default. To do so, open `MDaemon\WorldClient\Domains.ini`, and under `[Default:UserDefaults]` change the value of "`HideWhiteListFolder=`" or "`HideBlackListFolder=`" from "`No`" to "`Yes`". You can hide or show these folders for specific users by editing those same keys in the `User.ini` file under the `[User]` section.

Check for Attachments

In the LookOut and WorldClient themes there is now an option to check a composed message for attachments before sending, when attachments are mentioned in the subject or body of the message. This can help you avoid accidentally sending a message without an attachments when it is supposed to include one.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Two-Factor Authentication 703

You can now control whether or not accounts are allowed to use or required to use Two-Factor Authentication (2FA). There are two new options on the New Accounts 782 template for controlling the default settings for new accounts, and there are corresponding options on the Web Services 703 screen for controlling 2FA for individual accounts.

New in MDaemon 16.0

MDaemon Remote Administration (MDRA) UI Update

The user interface for MDRA no longer uses frames and has been updated to use a mobile first responsive design. Browser support is limited to IE10+, the latest Chrome, the latest Firefox, and the latest Safari on Mac and iOS. Android stock browsers have been known to have issues with scrolling, but Chrome on Android devices works well.

This design is based entirely on the size of the window being used. Whether the user is on a phone, tablet, or PC, the appearance is the same for the same window size. The most important change here is the menu. From 1024 pixels width and below, the menu is hidden on the left side of the browser. There are two methods that can be used to display the menu. If a touch device is in use, swiping to the right will show the secondary menu. Whether or not the device is in use, there is also a "menu" button in the top left corner that will display the secondary menu. Tapping or clicking the menu title with the left arrow next to it at the top of the menu will display the primary menu. The help, about, and sign out menu in the top right corner changes based on the width of the screen as well. From 768 pixels and above, the words Help, About, and Sign Out are displayed. From 481 pixels to 767 pixels, only the icons are displayed. 480 pixels and below displays only a "gear" icon which when clicked or tapped will display a drop down menu with the Help, About, Sign Out options. List views with more than one column have column on/off buttons that are accessed by clicking or tapping the gray right arrow button on the far right of the toolbar container. The settings pages are no longer designed to be exact copies of the MDaemon GUI, but are instead designed to reposition and resize based on the width/height of the browser.

Spambot Detection 556

A new feature called Spambot Detection tracks the IP addresses that every SMTP MAIL (return-path) value uses over a given period of time. If the same return-path is used by in an unusual number of IP addresses in a short period of time, this may indicate a spambot network. Although it could still be a legitimate use of the mail system, experimentation has shown that this can be effective in limited cases at detecting a distributed spambot network as long as the same return-path is utilized throughout. If a spambot is detected, the current connection to it is immediately dropped and the return-path value is optionally blacklisted for a length of time you specify. You can also optionally blacklist all the spambot IPs then known for a user-defined period.

CardDAV 360

MDaemon now supports synchronizing contacts via the CardDAV protocol. MDaemon's CardDAV server allows an authenticated CardDAV client to access the contact

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

information that is stored in MDaemon. Notable CardDAV clients are Apple Contacts (included with Mac OS X), Apple iOS (iPhone), and Mozilla Thunderbird via the SOGO plugin. For more information on CardDAV and configuring CardDAV clients, see: CalDAV & CardDAV 360.

Two Factor Authentication for WorldClient and Remote Administration

MDaemon now supports Two Factor Authentication (i.e. 2-Step Verification) for users signing into WorldClient or MDaemon's Remote Administration web-interface. Any user who signs into WorldClient via HTTPS can activate Two Factor Authentication for the account on the **Options » Security** screen. From then on the user must enter a verification code when signing into WorldClient or Remote Administration. The code is obtained at sign-in from an authenticator app installed on the user's mobile device or tablet. This feature is designed for any client that supports Google Authenticator.

ActiveSync Protocol Migration Client

MDaemon now includes an ActiveSync protocol based Migration Client (`ASMC.exe`). It supports migrating mail, calendars, tasks, notes, and contacts from ActiveSync servers that support protocol version 14.1. Documentation for it can be found in the `\MDaemon\Docs` folder.

XML API for Management Tasks

MDaemon now ships with an XML over http(s) based API. The result of this is that MDaemon Management clients can be written using any language on any platform that can make http(s):// post requests to the server. In MDaemon, this is only available to authenticated Global Admins, but in MDaemon Private Cloud a subset of the available operations is accessible to authenticated domain admins as well. The API also produces a website with documentation on the API specification. The installation default is to have it installed at `http://servername:RemoteAdminPort/MdMgmtWS/`, however, this can be set to any url for the sake of additional security.

The available operations include:

- Help
- CreateDomain
- DeleteDomain
- GetDomainInfo
- UpdateDomain
- CreateUser
- DeleteUser
- GetUserInfo
- UpdateUser
- CreateList
- DeleteList

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- GetListInfo
- UpdateList
- AddDomainAdministrator
- DeleteDomainUsers
- GetDomainList
- GetVersionInfo
- GetQueueState
- GetServiceState
- SetAddressRestriction
- GetAddressRestriction

At this time, command line management clients have been written/tested in Javascript, Powershell, VBScript, C, C++ and Visual Basic. A simple HTML and Javascript test site has been used as a proof of concept for a web based management console that operates within several popular browsers. While not tested yet, it is fully expected that this API should work fine from web servers using PHP, Perl, and other development platforms.

See:

Introduction 12
Upgrading to MDaemon 23.5.0 59
MDaemon's Main Display 68

1.4 Upgrading to MDaemon 23.5.0

Below is a list of special considerations and notes that you may need to be aware of when upgrading to MDaemon version 23.5.0 from a previous version. For a comprehensive list of additions, changes and fixes included in MDaemon 23.5.0, see the Release Notes.

Version 23.5.0

- There are no special considerations unique to MDaemon 23.5.0 when updating from the previous version. If you are updating from an earlier version, please review the special notes below for all versions released since that version.

Version 23.0.2

- Outbreak Protection has been restored. Please review your Outbreak Protection settings 624, as they may have been reset to their default values.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Version 23.0.1

- Cyren Anti-Virus has been replaced with IKARUS Anti-Virus. Cyren recently announced its plans to discontinue operations with little warning. This necessitated the need for us to find a new anti-virus partner. After a thorough evaluation, IKARUS Anti-Virus stood out for its excellent detection rate and speed. It offers reliable protection from malicious and potentially hostile programs, and it combines traditional anti-virus defense methods with the latest proactive technologies. IKARUS Anti-Virus automatically updates its definitions every 10 minutes. Scanning with IKARUS is disabled if your AntiVirus license is expired.
- Cyren Outbreak Protection been removed. Cyren recently announced its plans to discontinue operations with little warning. We are actively researching and considering viable anti-spam technologies as suitable additions to the existing anti-spam mechanisms found in our software products.
- IMAP keyword flags support can now be enabled or disabled via the setting `[Special] IMAPKeywordFlags=Yes/No` in `\MDaemon\App\MDaemon.ini`. IMAP keyword flags are disabled by default when updating MDaemon from a version before 23, to avoid the potential loss of message tags in Thunderbird mail clients. When Thunderbird connects to an IMAP server that supports keyword flags, it overwrites its local message tags with tags read from the server, which are initially blank. IMAP keyword flags are enabled by default for new installs and when updating from version 23.0.0.

Version 22.0.0

- 32-bit MDaemon has been discontinued. MDaemon 22.0 and newer will only be available in 64-bit. If you are currently running a 32-bit version on a supported 64-bit operation system, you can simply install the 64-bit version on top of the existing installation.
- The minimum length for strong passwords 840 must now be at least 8 characters. If your minimum length was set to fewer than 8 characters before updating to MDaemon 22, it will be changed to 8. The default minimum length for strong passwords on new installs is now 10.
- MDaemon is moving away from using the terms "whitelist" and "blacklist". In many cases, they are now "allow list" and "block list". Features that had a "white list" to exempt IPs, addresses, etc., now have an "exempt list". The per-user spam filter contacts folders are now named "Allowed Senders" and "Blocked Senders". The folders for all accounts will be renamed when MDaemon 22 starts up for the first time.

Version 21.5.0

- The `X-MDOrigin-Country` header, which Location Screening 558 can add to messages, will now contain the two-letter ISO 3166 country and continent codes instead of full country and continent names. Be sure to update any filters you may have that look for particular values in this header.
- With the renaming of the Webmail "Mobile" theme to "Pro," there is a possible side effect for users who are using the Mobile theme and have the Remember

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Me option enabled. These users may find that they cannot open attachments. To fix this, they must simply sign out of their Webmail account and then sign in again.

Version 21.0.2

- The settings at Setup » Preferences » Miscellaneous to copy all system-generated postmaster notifications to global admins and domain admins now apply to more notifications, such as Account Freeze and Disable, No Such User, Disk Error, Low Disk Space, and Beta and AV expiration. If you do not feel it appropriate for your administrators to receive these notifications, you must disable these settings.

Version 20.0.3

- MDaemon will comment out the line "`AlertExceedsMax yes`" in ClamAV's `clamd.conf` file, due to it causing too many "`Heuristics.Limits.Exceeded`" AV scan failures.

Version 20.0.1

- The network resource access settings at Setup | Preferences | Windows Service now configure the MDaemon service (and the Remote Administration and XMPP Server services) to run as the specified account, instead of MDaemon running as SYSTEM and then it running specific processes and threads as that account. The installer will update the services to run as the specified account when updating to this version.
- Because of changes to and deprecation of many settings in clamd.conf, the installer will now overwrite existing clamd.conf. If you have customized your clamd.conf you may need to review and make changes to clamd.conf after installation.

Version 20.0.0

- Please carefully read the section in the full release notes labeled as task [8930] as it involves changes to the Active Directory integration system and you may find things that were broken in the past now starting to work. Please be aware of all changes made in that area and carefully read that section of the release notes.
- MDaemon 20.0 requires Windows 7, Server 2008 R2, or newer.
- Preferences » Miscellaneous 489 has two new checkboxes that control whether system generated notification emails periodically sent to the Postmaster alias should also be sent to Global and Domain level administrators. By default, these options are both enabled. Domain administrators are restricted to receiving only those emails which are for their domain and the Release Notes. Global administrators receive everything including the Queue Summary report, Statistics report, Release Notes, 'No Such User' found (for all domains), Disk Error notifications, Account Freeze and Disable notifications for all domains (which, like Domain admins, they can unfreeze and re-enable), warnings about licenses and beta test versions about to expire, Spam Summary reports, and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

perhaps others as well. If you do not feel it appropriate for your administrators to receive these notifications you must disable these settings.

- How autoresponders are stored has changed. The text for an accounts autoresponder is now stored as `OOF.MRK` files within the account's DATA folder which is a new sub-folder inside the account's root mail folder. Autoresponder script files are no longer kept in the APP folder and they are not shared between accounts. When MDaemon starts for the first time it will migrate all existing autoresponder files and settings to the correct places for every account. The `AUTORESP.DAT` file is obsolete and will be deleted along with every account specific `.RSP` file (`OutOfOffice.RSP` and non-account specific files will remain for reference and sample purposes). If you wish to quickly assign a single autoresponder configuration to multiple accounts you can use the new Publish button found at Account Settings » Autoresponder 708. This button will copy the existing autoresponder script text and all settings for the current account to other accounts that you select. There is also an Edit autoresponder file 708 button that lets you edit the default autoresponder script (`OutOfOffice.rsp`). This default is copied into an accounts `OOF.MRK` if the `OOF.MRK` is missing or empty.
- How account signature files are stored has changed. Signature files are now stored as `SIGNATURE.MRK` within the account's DATA folder, which is a new subfolder inside the account's root mail folder. When MDaemon starts for the first time it will migrate all existing signature files to the correct places for every account. The root MDaemon Signatures folder will no longer contain account-specific signature files, but it remains in place as it may still contain items needed by MDaemon Remote Administration and the Content Filter. The original Signatures folder was backed up to `\Backup\20.0.0\Signatures\` prior to migration. Finally, every account's `ADMINNOTES.MRK` has been moved from the account's root mail folder to the new DATA subfolder.
- Spam Filter » White List (automatic) 672 has had the default value changed to disabled for the option "*...only whitelist addresses that authenticate using DKIM*". Having this enabled turns out to be a little restrictive for many and prevents address book white listing from working for MultiPOP and DomainPOP mail. Re-enable the setting if this is not to your liking.
- The Preferences » UI 477 option to "*Center all UI dialogs*" has been reset to a default of "enabled" for everybody. If you prefer otherwise you can disable it. This prevents screens from being created partially out of frame, but it can occasionally cause multiple overlapping screens to be harder to select.
- Security Manager » Screening » Location Screening 558 - The default for this feature has been changed from disabled to enabled. When Location Screening is enabled the connecting country/region will always be logged (if known) even when the particular country/region is not being actively blocked. So, even if you do not wish to block any country you can still enable Location Screening (without selecting any countries to block) so that country/region can be shown and logged. Since the default setting for this has changed, you should take a look at your Location Screening configuration for correctness. MDaemon will insert the header "`X-MDOrigin-Country`" that lists the country and region for content filtering or other purposes.
- The hard-coded fixed size limit of 2 MB for spam filter scans has been removed. There is now no theoretical limit to the size of a message that can be scanned.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

It is still possible, however, to configure your own limit in case this is a problem, but using "0" in the option now means no limit. You should review the Spam Filter » Settings 681 screen to make sure this option is set to your desired value.

- Added 'Sender Domain' and 'Recipient Domain' columns to the Queues screens in the main UI. As a result of this a one-time reset of saved column widths had to be done. Once you set the column widths to your liking they will be remembered.
- By default the Host Screen is now applied to MSA connections. This option is located at: Security Manager » Screening » Host Screen 550.
- By default MDaemon IMAP, WebMail, and ActiveSync servers no longer provide access to the shared folders of disabled accounts. You can change this with a new settings at Server Settings » Public & Shared Folders 113.

Version 19.5.2

- The "*Max RSET commands allowed*" options on the Server Settings » Servers 86 screen have been removed since they are essentially less flexible duplicates of the same functionality found on the SMTP Screen 552. The SMTP Screen version is part of the Dynamic Screening system which takes into account more factors (e.g. it has a white list, considers authentication status, etc). Your old values were moved to the SMTP Screen. Please check them to ensure the values there are as you expect. The correct default (and recommended) values for the options are: *Block IPs that send this many RSETs* set to "**20**", and *Close SMTP session after blocking IP* option set to **enabled/checked**.

Version 19.5.1

- The LetsEncrypt 580 functionality has been updated to use ACME v2. This update is required because LetsEncrypt is discontinuing support for ACME v1. PowerShell 5.1 and .Net Framework 4.7.2 are now required in order to use LetsEncrypt.

Version 19.5.0

- Some settings, such as the registration keys, have been moved from `\MDaemon\App\MDaemon.ini` to `\MDaemon\LocalData\LocalData.ini`. If you need to revert to a previous version of MDaemon, earlier installers will not find the settings at the new locations, and will therefore ask you to enter a registration key. This can be avoided by copying the settings back to `MDaemon.ini`, or by restoring a backup of `MDaemon.ini`, first.

Version 19.0.0

- MDaemon's Remote Administration (MDRA) web interface has been further expanded to include access to features that formerly could only be administered using a Configuration Session (i.e. MDaemon's application interface), and there are now several options that can only be accessed via MDRA. Consequently, for new MDaemon installations, the "Start MDaemon" Start Menu shortcut will now open a browser to MDaemon Remote Administration by default rather than opening an MDaemon Configuration Session. If you wish to change this, edit

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

\MDaemon\App\MDaemon.ini and set [MDLaunch] OpenConfigSession=Yes/No and OpenRemoteAdmin=Yes/No. Set the *Remote Administration URL* at Setup » Web & IM Services » Remote Administration » Web Server 343 if the auto-generated URL does not work or if MDRA runs in an external web server. If a working URL cannot be determined, a Configuration Session will be opened instead. Finally, under the Windows Start menu, in the MDaemon program group, there are now shortcuts to *Open MDaemon Configuration Session* and *Open MDaemon Remote Administration*.

- SyncML has been deprecated and removed.
- MDaemon's disk space calculations were being made inconsistently in several places (for example, sometimes using 1000, sometimes using 1024 bytes for a kilobyte computation). This has been fixed to use 1024 consistently. As a result your users' disk space quota values may be slightly different than in previous versions. Please check and make whatever adjustments (if any) you feel are required.
- The option, "Only send antivirus update notification on failure 649" is now enabled by default. When updating to MDaemon 19, this option will be enabled the first time MDaemon is started.

See:

Introduction 12
New in MDaemon 23.5 15
MDaemon's Main Display 68

1.5 Getting Help

Support Options

Support is a vital part of the total MDaemon Technologies customer experience. We want you to get the most from our products long after the initial purchase and installation and we are dedicated to ensuring that any issues are resolved to your satisfaction. For the latest Customer Service information, Technical Support Options, Self-support Resources, Product Information, and more, visit the MDaemon Technologies support page at: www.mdaemon.com/support/

MDaemon Beta Testing

MDaemon Technologies maintains active beta testing teams for our products. If you would like information about joining the MDaemon beta team, send a message to MDaemonBeta@mdaemon.com.

The Beta Team is for those who wish to acquire MDaemon updates before their general release and aid in their testing; it is not a technical support alternative. Technical support for

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

> MDaemon will only be provided through those methods outlined at: www.mdaemon.com/support/.

Contact Us

Hours of Operation
M-F 8:30 am - 5:30 pm Central Standard Time
Excludes weekends and U.S. holidays
Customer Service or Sales
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
sales@helpdesk.mdaemon.com

Technical Support
www.mdaemon.com/support/

Training
training@mdaemon.com

Business Development/Alliances
alliance@mdaemon.com

Media/Analysts
press@mdaemon.com

Channel/Reseller Inquiries
Please refer to the Channel Partner page for additional information.

Corporate Headquarters

MDaemon Technologies
4550 State Highway 360, Suite 100
Grapevine, Texas 76051
U.S. Toll Free: 866-601-ALTN (2586)
International: 817-601-3222
Fax: 817-601-3223

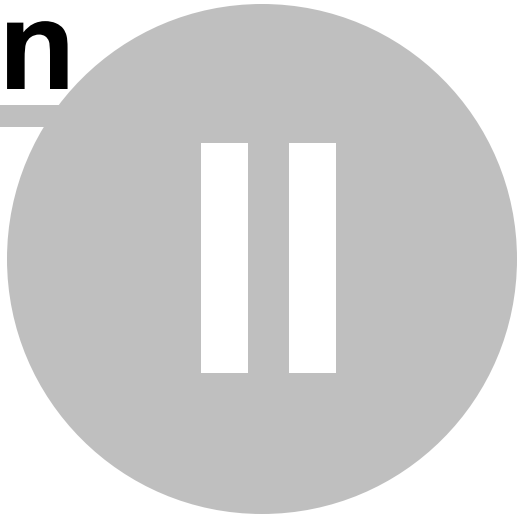
Trademarks

Copyright © 1996-2023 MDaemon Technologies. Alt-N®, MDaemon®, and RelayFax® are trademarks of MDaemon Technologies.

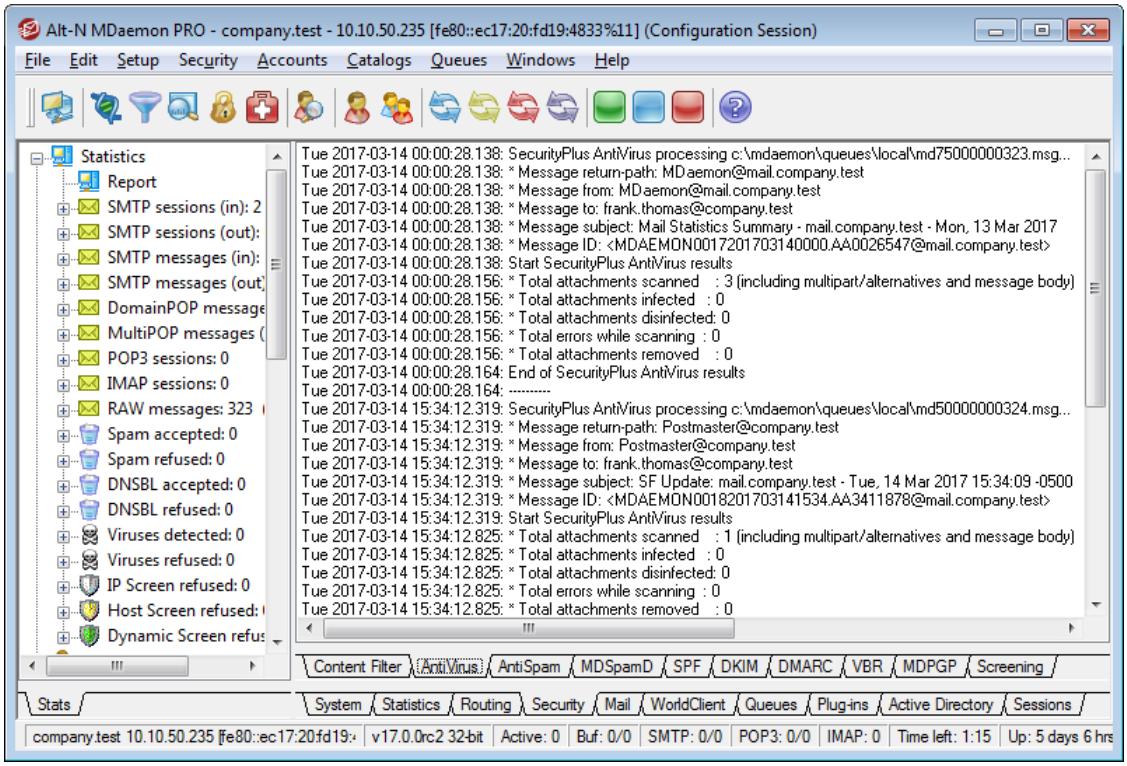
Apple is a trademark of Apple Inc. Microsoft and Outlook are trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section



2 MDaemon's Main Display



MDaemon's main graphical user interface (GUI) gives you important information regarding MDaemon's resources, statistics, active sessions, and queued mail waiting to be processed. It also contains options for easily activating/deactivating MDaemon's various servers. The GUI's tabbed panes keep you up to date on how the server and its incoming and outgoing connections are performing.

Stats

The Stats pane is the default left pane of MDaemon's main interface. This pane contains four sections: Statistics, Accounts, Queues, and Servers.

The *Statistics* section contains statistics regarding the number of messages sent and received by MDaemon as well as statistics for POP and IMAP sessions, Spam accepted and refused, viruses, and more. These stats are counted from the time MDaemon starts, and there is a right-click shortcut menu that can be used to clear the counters.

When you click the "reset root node counters" option, all of the counters will be reset, not merely the one you right-click. Further, there is an option at Setup » Preferences » GUI that can be used to "*Preserve root node mail counters across reboots*." Otherwise they will be reset whenever the server is rebooted.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The *Accounts* section contains entries for MDaemon, MDaemon Connector, and ActiveSync. Each entry lists the number of accounts used and the number of accounts left, depending on your product license.

The *Queues* section contains an entry for each message queue and the number of messages (if any) that each queue contains. You can right-click on each of the queue entries to open a shortcut menu containing one or more of the following options, depending on which queue you select:

View Queue — this option switches the main pane to the Queues tab and displays the selected queue. A list of all messages the queue contains will be displayed, and you can right-click any message to open a shortcut menu containing numerous options similar to those available in the Queue & Statistics Manager such as Copy, Move, Edit, and so on.

Queue and statistics manager — open the Queue and Statistics Manager to the Queue Page with the selected queue displayed.

Process Now — this option "re-queues" all messages contained in the queue and attempts to process them normally for delivery. If you attempt to process messages contained in the Holding queue, Bad queue, or the like then the messages may encounter the same errors that put them there in the first place and return them to the same queue.

Freeze/unfreeze queue — temporarily pauses processing for the selected queue, or continues the processing if it is currently paused.

Release — releases messages from the Holding Queue. MDaemon will attempt to deliver the messages regardless of errors encountered — they will not be returned to the Holding Queue even if they encounter the same errors that caused them to be moved there originally.

Re-Queue — This is available for the Holding Queue, and has the same effect as *Process Now* above.

Enable/disable queue — activates or deactivates the Holding Queue. When disabled, messages will not be moved to the Holding Queue regardless of errors encountered.

The *Servers* section contains an entry for each server within MDaemon, and each entry lists the current state of the server: "Active" or "Inactive". Listed below each server's entry is an entry for each domain (when applicable) and the port and IP address currently in use by that server or domain. The shortcut menu provides a control for toggling each server between the Active and Inactive state. When a server is inactive its icon will turn red.

Event Tracking and Logging

The default right-hand pane of the main interface contains a group of tabs that display MDaemon's current actions and the status of its various servers and resources, and they are continually updated to reflect current server conditions. Each active session and server action is logged onto the appropriate tab once each action is complete. The information displayed on these tabs is mirrored in the log files kept in the Logs directory, if you have chosen to log such activity.

The primary pane of MDaemon's GUI contains the following tabs:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

System — at program startup, the System tab displays a log of the Initialization Process, which can alert you to possible problems with MDaemon's configuration or status. It also displays activity such as enabling/disabling any of MDaemon's various servers.

Statistics — this tab will display a server statistics report corresponding to the information contain in the various root node counters on the Stats tab in the Stats and Tools pane. If you wish to change the font or font size used for this report you can do so by editing the following keys in the MDaemon.ini file:

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

Further, at midnight each night, the Postmaster and all addresses listed on the Recipients 649 screen of the Content Filter will get a copy of this report via email. This is the same report that is generated when you use the "Status" email command listed in General Email Controls 883. If you do not wish this report to be sent, then disable the "*Send stats report to postmaster at midnight*" option located on the Miscellaneous 489 screen under Preferences.

Routing — displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

Security — click this tab and several other security-related tabs will appear above it.

Content Filter — MDaemon's Content Filter 631 operations are listed on this tab. When a message matches the criteria of one of the Content Filter's message rules, the relevant information related to that message and the actions taken are logged here.

AntiVirus — AntiVirus 630 operations are listed on this tab. When a message is scanned for viruses, the relevant information related to that message and the action taken is logged here.

AntiSpam — displays all of MDaemon's spam filtering 660 and prevention activities.

MDSpamD — lists all activity of the MDaemon Spam Daemon 670.

SPF — displays all Sender Policy Framework 512 activities.

DKIM — lists all DomainKeys Identified Mail 514 activities.

DMARC — lists all DMARC 523 activities.

VBR — this tab displays VBR Certification 538 activities.

MDPGP — this tab displays MDPGP 614 activities.

Screening — this tab displays Tarpitting 588 and Dynamic Screening 552 activities.

Auth Failures — This tab (and corresponding log file) contains a detailed entry for every SMTP, IMAP, and POP logon attempt that fails. The information includes the Protocol used, the Session ID (so you can search other logs), the IP of the offender, the raw Logon value they tried to use (sometimes this is an alias), and the Account that matches the logon (or 'none' if no account

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

matches).You can right-click on a line in this tab and have the IP address of the offender added to the block list(s).

MTA-STS — Displays all SMTP MTA Strict Transport Security (MTA-STS) related activity.

Mail — click this tab and several other mail-related tabs will appear above it.

SMTP (in) — all incoming session activity using the SMTP protocol is displayed on this tab.

SMTP (out) — all outgoing session activity using the SMTP protocol is displayed on this tab.

IMAP — mail sessions using the IMAP protocol are logged on this tab.

POP3 — when users collect email from MDaemon using the POP3 protocol, that activity is logged here.

MultiPOP — this tab displays MDaemon's MultiPOP mail collection activities.

DomainPOP — this tab displays MDaemon's DomainPOP activity.

LDAP — displays LDAP server activity.

Minger — displays Minger 847 server activity.

RAW — RAW or system generated message activity is logged on this tab.

MDaemon Connector — displays all MDaemon Connector 379 activities.

Webmail

Webmail — displays MDaemon Webmail's mail activities.

ActiveSync — this tab displays ActiveSync activity.

Queues — this tab gives access to another row of tabs above it with one tab corresponding to each message queue, such as: Local, Remote, Holding, Quarantine, Bayesian Spam, and so on.

Plug-ins — displays all activities related to any MDaemon plug-ins.

Active Directory — displays all Active Directory related activity.

Sessions — click this tab and several other tabs will appear above it. These tabs display an entry for each active connection to MDaemon. Whether the connection is SMTP in or out, POP in or out, IMAP, Webmail, or ActiveSync, information about each active session is displayed here. Double-click on an active session to display a Session Window 82, which displays the transcript of the SMTP session as it progresses.

The information displayed on these tabs has no affect on the amount of data that is actually stored in the log files. However, MDaemon does support a great deal of flexibility with regard to the amount and type of information that is logged in those files. See the Logging 159 dialog for more information on logging options.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Event Tracking Window's Shortcut Menu

If you right-click in any of the Event Tracking pane's tabs it will open a shortcut menu. Various options are provided on this menu that can be used to select, copy, delete, or save the contents of a given tab. The menu's *Print/Copy* option will open any currently selected text in Notepad, which can then be used to print the data or save it to a file. The *Delete* option will delete the text you have selected. The *Search* option will open a window in which you can specify a word or phrase to search for in the log files. MDaemon will search all log files for the text string and then all session transcripts containing that string will be combined into a single file and opened in Notepad for your review. A practical use of this feature would be to search for a particular Message-ID, which would provide a compilation from all the logs of all session transcripts containing that Message-ID. On some tabs there are also options to report messages to MDaemon.com that have been misclassified as spam or containing a virus, or that should have been classified as such (i.e. false positives or false negatives). Reported messages will be analyzed and passed along to third-party vendors for corrective action.

The layout of the MDaemon GUI is not limited to the default positions described above. You may switch their position by clicking Windows » Switch Panes on the menu bar.

Composite Log View

Located on the Windows menu of MDaemon's menu bar is the Composite Log View option. Clicking this option will add a window to the GUI that will combine the information displayed on one or more of the main pane's tabs. Use the options on the Composite Log 161 screen of the Logging dialog to designate the information that will appear in that window.

Performance Counters

MDaemon supports Windows Performance Counters, which allow monitoring software to track MDaemon's status in real time. There are counters for the number of active sessions for the various protocols, number of messages in the queues, server active / inactive states, MDaemon up time, and session and message statistics.

To use the performance counters, start System Monitor by going to Control Panel | Administrative Tools | Performance, or by running "perfmon". These are 32-bit counters so on 64-bit machines you must run "mmc /32 perfmon.msc". Click on Add Counters, select the MDaemon performance object, then select and Add the counters that you want to see. To see the performance counters from MDaemon running on another machine you must have the "Remote Registry" service enabled and access through any firewalls.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Session Window 82
Tray Icon 80
Shortcut Menu 81
Composite Log 161

2. .1 AutoDiscovery Service

MDaemon supports the AutoDiscovery service, which allows users to configure their email clients to connect to their accounts by providing only their email address and password, rather than having to know other configuration details such as mail server names and ports. Most clients support the service, although a few have only limited support for it. The AutoDiscovery service is enabled by default, but you can manually enable or disable it from MDaemon's main application interface. Under **Servers** in the Stats pane, right-click **AutoDiscovery Service**, and click **Enable/Disable AutoDiscovery Service**.

Clients in which the AutoDiscovery service is fully supported will use the domain name in the user's email addresss to do a DNS service (SRV) record lookup for Service Type _autodiscover._tcp and connect to that server to get additional information. Therefore to support AutoDiscovery you must create DNS SRV records for AutoDiscovery and the services it supports. MDaemon's implementation of the AutoDiscovery service supports: ActiveSync 408 (airsync), IMAP, POP, SMTP, DAV, and 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.
```

Note: a few clients will always look at `autodiscover.{domain}.{tld}` first. So having the AutoDiscovery service record point to a server named `autodiscover.{domain}.{tld}` could help in that regard. In the following example, however, the AutoDiscovery server is `adsc.example.com`.

Example:

Domain name: example.com

The admin should set up a _tcp service record for service type _autodiscover

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

In this case, it points to `adsc.example.com`, which has an A record pointing to `192.168.0.101`

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The client will then connect to that server, and ask for connection point information for some specific protocols: ActiveSync, IMAP, XMPP, SMTP, DAV, etc...

The AutoDiscovery service then looks up the protocols requested and returns the proper server names for those protocols. i.e. For ActiveSync, it would return the server name defined in the _tcp service record _airsync, which in this example, would be eas.{domain}.{tld}

If Outlook were calling AutoDiscovery, it would return the IMAP and SMTP Servers, represented for the _tcp service records of _imap and _msa, resulting in the servers being returned as imap4.example.com and msa.example.com.

Here is an example of setting up Auto Discovery Services correctly. This assumes that you wish to use unique names for each protocol, but is easily adapted to use say a common name, such as mail.example.com.

```
;
;  Database file example.com.dns for 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
;
```

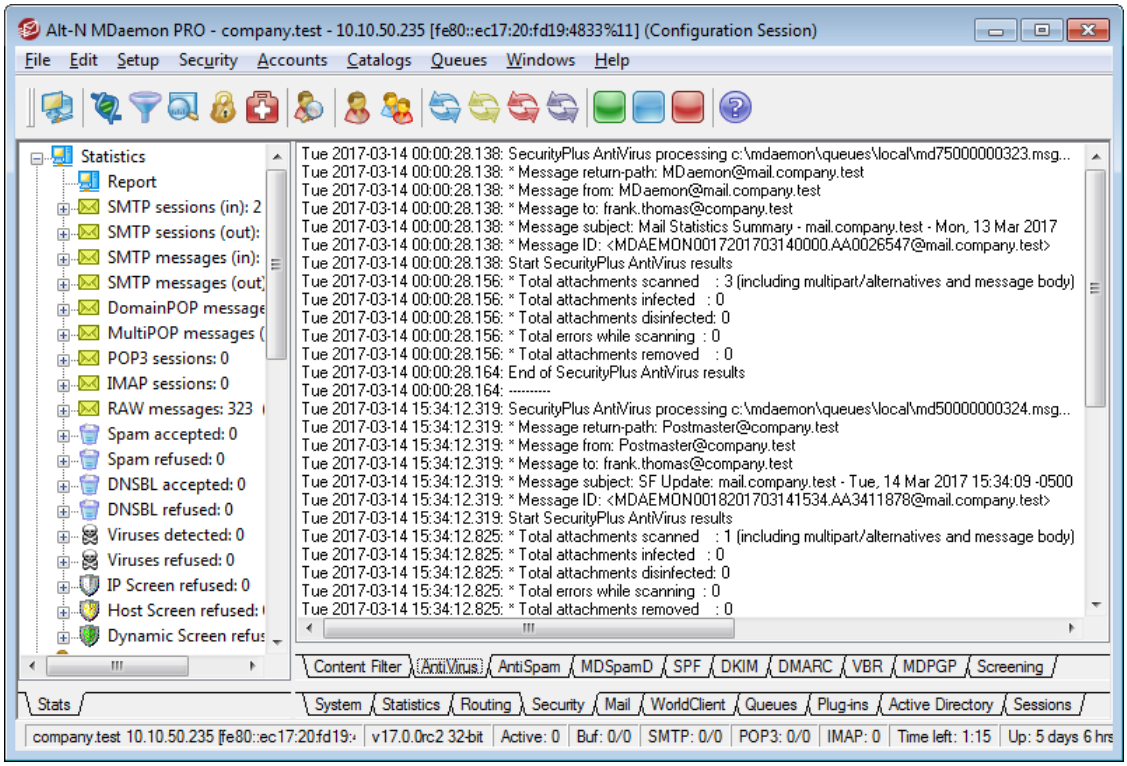
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
_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.
```

See:

For more general information on AutoDiscover, see the Microsoft document: Autodiscover for Exchange.

2.2 Event Tracking and Logging



MDaemon's main graphical user interface (GUI) gives you important information regarding MDaemon's resources, statistics, active sessions, and queued mail waiting to be processed. It also contains options for easily activating/deactivating MDaemon's various servers. The GUI's tabbed panes keep you up to date on how the server and its incoming and outgoing connections are performing.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Stats

The Stats pane is the default left pane of MDaemon's main interface. This pane contains four sections: Statistics, Accounts, Queues, and Servers.

The *Statistics* section contains statistics regarding the number of messages sent and received by MDaemon as well as statistics for POP and IMAP sessions, Spam accepted and refused, viruses, and more. These stats are counted from the time MDaemon starts, and there is a right-click shortcut menu that can be used to clear the counters.

When you click the "reset root node counters" option, all of the counters will be reset, not merely the one you right-click. Further, there is an option at Setup » Preferences » GUI that can be used to "*Preserve root node mail counters across reboots*." Otherwise they will be reset whenever the server is rebooted.

The *Accounts* section contains entries for MDaemon, MDaemon Connector, and ActiveSync. Each entry lists the number of accounts used and the number of accounts left, depending on your product license.

The *Queues* section contains an entry for each message queue and the number of messages (if any) that each queue contains. You can right-click on each of the queue entries to open a shortcut menu containing one or more of the following options, depending on which queue you select:

View Queue — this option switches the main pane to the Queues tab and displays the selected queue. A list of all messages the queue contains will be displayed, and you can right-click any message to open a shortcut menu containing numerous options similar to those available in the Queue & Statistics Manager such as Copy, Move, Edit, and so on.

Queue and statistics manager — open the Queue and Statistics Manager to the Queue Page with the selected queue displayed.

Process Now — this option "re-queues" all messages contained in the queue and attempts to process them normally for delivery. If you attempt to process messages contained in the Holding queue, Bad queue, or the like then the messages may encounter the same errors that put them there in the first place and return them to the same queue.

Freeze/unfreeze queue — temporarily pauses processing for the selected queue, or continues the processing if it is currently paused.

Release — releases messages from the Holding Queue. MDaemon will attempt to deliver the messages regardless of errors encountered — they will not be returned to the Holding Queue even if they encounter the same errors that caused them to be moved there originally.

Re-Queue — This is available for the Holding Queue, and has the same effect as *Process Now* above.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable/disable queue — activates or deactivates the Holding Queue. When disabled, messages will not be moved to the Holding Queue regardless of errors encountered.

The *Servers* section contains an entry for each server within MDaemon, and each entry lists the current state of the server: "Active" or "Inactive". Listed below each server's entry is an entry for each domain (when applicable) and the port and IP address currently in use by that server or domain. The shortcut menu provides a control for toggling each server between the Active and Inactive state. When a server is inactive its icon will turn red.

Event Tracking and Logging

The default right-hand pane of the main interface contains a group of tabs that display MDaemon's current actions and the status of its various servers and resources, and they are continually updated to reflect current server conditions. Each active session and server action is logged onto the appropriate tab once each action is complete. The information displayed on these tabs is mirrored in the log files kept in the Logs directory, if you have chosen to log such activity.

The primary pane of MDaemon's GUI contains the following tabs:

System — at program startup, the System tab displays a log of the Initialization Process, which can alert you to possible problems with MDaemon's configuration or status. It also displays activity such as enabling/disabling any of MDaemon's various servers.

Statistics — this tab will display a server statistics report corresponding to the information contain in the various root node counters on the Stats tab in the Stats and Tools pane. If you wish to change the font or font size used for this report you can do so by editing the following keys in the MDaemon.ini file:

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

Further, at midnight each night, the Postmaster and all addresses listed on the Recipients 649 screen of the Content Filter will get a copy of this report via email. This is the same report that is generated when you use the "Status" email command listed in General Email Controls 883. If you do not wish this report to be sent, then disable the "*Send stats report to postmaster at midnight*" option located on the Miscellaneous 489 screen under Preferences.

Routing — displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

Security — click this tab and several other security-related tabs will appear above it.

Content Filter — MDaemon's Content Filter 631 operations are listed on this tab. When a message matches the criteria of one of the Content Filter's message rules, the relevant information related to that message and the actions taken are logged here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

AntiVirus — AntiVirus[630] operations are listed on this tab. When a message is scanned for viruses, the relevant information related to that message and the action taken is logged here.

AntiSpam — displays all of MDaemon's spam filtering[660] and prevention activities.

MDSpamD — lists all activity of the MDaemon Spam Daemon[670].

SPF — displays all Sender Policy Framework[512] activities.

DKIM — lists all DomainKeys Identified Mail[514] activities.

DMARC — lists all DMARC[523] activities.

VBR — this tab displays VBR Certification[538] activities.

MDPGP — this tab displays MDPGP[614] activities.

Screening — this tab displays Tarpitting[588] and Dynamic Screening[552] activities.

Auth Failures — This tab (and corresponding log file) contains a detailed entry for every SMTP, IMAP, and POP logon attempt that fails. The information includes the Protocol used, the Session ID (so you can search other logs), the IP of the offender, the raw Logon value they tried to use (sometimes this is an alias), and the Account that matches the logon (or 'none' if no account matches).You can right-click on a line in this tab and have the IP address of the offender added to the block list(s).

MTA-STS — Displays all SMTP MTA Strict Transport Security (MTA-STS) related activity.

Mail — click this tab and several other mail-related tabs will appear above it.

SMTP (in) — all incoming session activity using the SMTP protocol is displayed on this tab.

SMTP (out) — all outgoing session activity using the SMTP protocol is displayed on this tab.

IMAP — mail sessions using the IMAP protocol are logged on this tab.

POP3 — when users collect email from MDaemon using the POP3 protocol, that activity is logged here.

MultiPOP — this tab displays MDaemon's MultiPOP mail collection activities.

DomainPOP — this tab displays MDaemon's DomainPOP activity.

LDAP — displays LDAP server activity.

Minger — displays Minger[847] server activity.

RAW — RAW or system generated message activity is logged on this tab.

MDaemon Connector — displays all MDaemon Connector[379] activities.

Webmail

Webmail — displays MDaemon Webmail's mail activities.

ActiveSync — this tab displays ActiveSync activity.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Queues — this tab gives access to another row of tabs above it with one tab corresponding to each message queue, such as: Local, Remote, Holding, Quarantine, Bayesian Spam, and so on.

Plug-ins — displays all activities related to any MDaemon plug-ins.

Active Directory — displays all Active Directory related activity.

Sessions — click this tab and several other tabs will appear above it. These tabs display an entry for each active connection to MDaemon. Whether the connection is SMTP in or out, POP in or out, IMAP, Webmail, or ActiveSync, information about each active session is displayed here. Double-click on an active session to display a Session Window 82, which displays the transcript of the SMTP session as it progresses.

The information displayed on these tabs has no affect on the amount of data that is actually stored in the log files. However, MDaemon does support a great deal of flexibility with regard to the amount and type of information that is logged in those files. See the Logging 159 dialog for more information on logging options.

Event Tracking Window's Shortcut Menu

If you right-click in any of the Event Tracking pane's tabs it will open a shortcut menu. Various options are provided on this menu that can be used to select, copy, delete, or save the contents of a given tab. The menu's *Print/Copy* option will open any currently selected text in Notepad, which can then be used to print the data or save it to a file. The *Delete* option will delete the text you have selected. The *Search* option will open a window in which you can specify a word or phrase to search for in the log files. MDaemon will search all log files for the text string and then all session transcripts containing that string will be combined into a single file and opened in Notepad for your review. A practical use of this feature would be to search for a particular Message-ID, which would provide a compilation from all the logs of all session transcripts containing that Message-ID. On some tabs there are also options to report messages to MDaemon.com that have been misclassified as spam or containing a virus, or that should have been classified as such (i.e. false positives or false negatives). Reported messages will be analyzed and passed along to third-party vendors for corrective action.

The layout of the MDaemon GUI is not limited to the default positions described above. You may switch their position by clicking Windows » Switch Panes on the menu bar.

Composite Log View

Located on the Windows menu of MDaemon's menu bar is the Composite Log View option. Clicking this option will add a window to the GUI that will combine the information displayed on one or more of the main pane's tabs. Use the options on the Composite Log 161 screen of the Logging dialog to designate the information that will appear in that window.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Performance Counters

MDaemon supports Windows Performance Counters, which allow monitoring software to track MDaemon's status in real time. There are counters for the number of active sessions for the various protocols, number of messages in the queues, server active / inactive states, MDaemon up time, and session and message statistics.

To use the performance counters, start System Monitor by going to Control Panel | Administrative Tools | Performance, or by running "perfmon". These are 32-bit counters so on 64-bit machines you must run "mmc /32 perfmon.msc". Click on Add Counters, select the MDaemon performance object, then select and Add the counters that you want to see. To see the performance counters from MDaemon running on another machine you must have the "Remote Registry" service enabled and access through any firewalls.

See:

Session Window 82
Tray Icon 80
Shortcut Menu 81
Composite Log 161

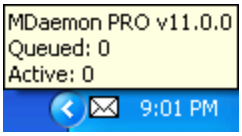
2.4 Tray Icon

Whenever the MDaemon server is running, its icon will be visible in the system tray. However, apart from simply letting you know whether the server is running, the icon is also dynamic and will change colors based upon the current server status. The following is a list of the icon indicators:

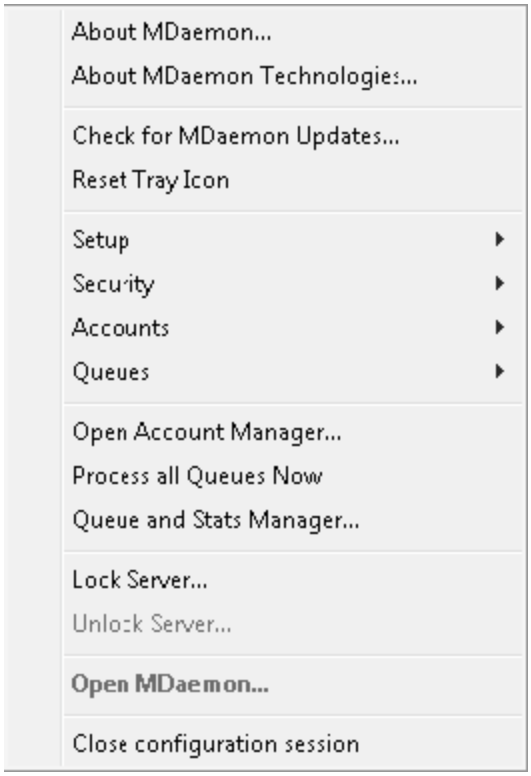
	All okay. No mail in local or remote queues.
	All okay. Mail in local or remote queues.
	Available disk space below threshold (see Setup » Preferences » Disk 482).
	Network is down, dialup failed, or disk is full.
Icon Blinking	A newer version of MDaemon is available.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

There is additional information about the server available through the icon's tool tip. Pause the mouse pointer over it and the tool tip will appear, displaying the number of currently queued messages and active session.



Shortcut Menu



Right click on MDaemon's tray icon to open the shortcut menu. This menu gives you quick access to virtually all of MDaemon's menus without having to open the main user interface.

Click the "About MDaemon..." options in the top section of the shortcut menu to find out more about MDaemon or MDaemon Technologies.

In the next section, click "Check for MDaemon Updates..." to see if there is a newer version of MDaemon available for download.

In the third section you can access the following MDaemon menus: Setup, Security, Accounts, and Queues. Each of these cascading menus is identical to the menu of the same name located on the menu bar of the main interface.

The fourth section has options to open the Account Manager and Queue and Statistics manager, and one that will cause all of MDaemon's mail queues to be processed.

Next, there are commands to lock and unlock MDaemon's interface (See "Locking/Unlocking MDaemon's Main Interface" below) followed by the "Open MDaemon..." menu selection, used for opening/restoring MDaemon's interface when it is minimized to the system tray.

The last option is "Close configuration session," which closes the MDaemon

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

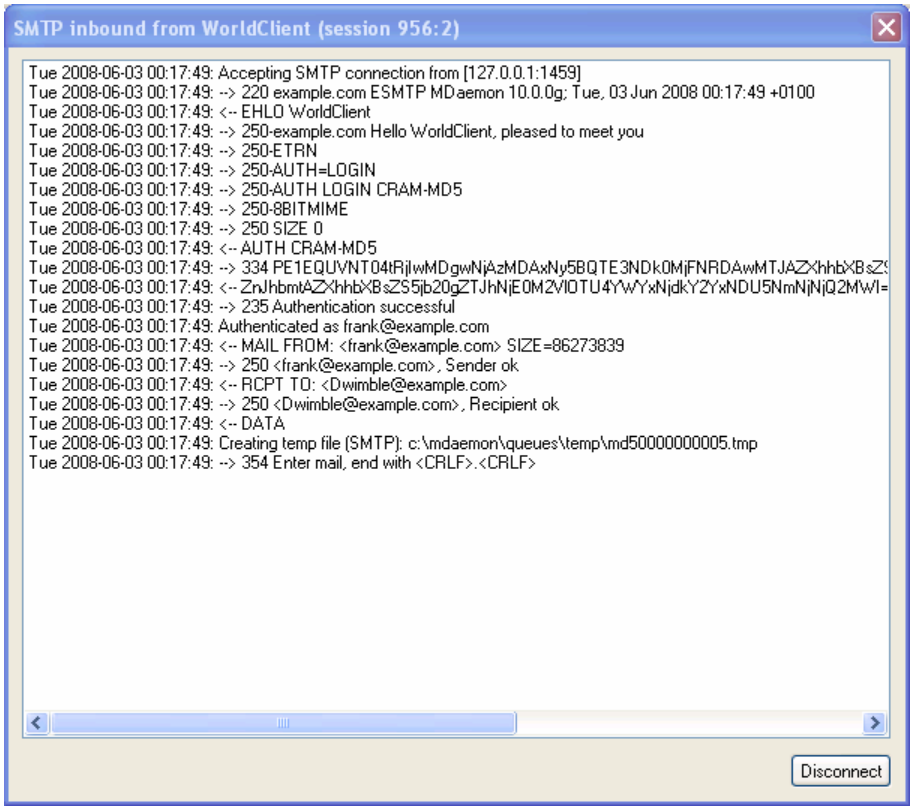
interface. Closing the configuration session does not shutdown the MDaemon service.

Locking/Unlocking MDaemon's Main Interface

To lock the user interface, minimize MDaemon, click the "Lock server..." menu item and then enter a password into the box that opens. After confirming the password by entering it a second time, MDaemon's user interface will be locked. It cannot be opened or viewed, but MDaemon will continue to function normally. You will, however, still be able to use the "Process all queues now..." shortcut option to process the mail queues manually. To unlock MDaemon, open the "Unlock MDaemon" dialog by double-clicking the tray icon, or by right-clicking the icon and then choosing "Unlock Server..." Then, enter the password that you created when you locked it.

2.5 Session Window

When you double-click an active session on one of the Session tabs[69] of the main GUI, this will open the session window corresponding to that entry. The session window will display the SMTP transcript of that session as it progresses. You can click Disconnect on this window if you wish to interrupt and disconnect that session in progress.



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

2.6 MDaemon's SMTP Work Flow

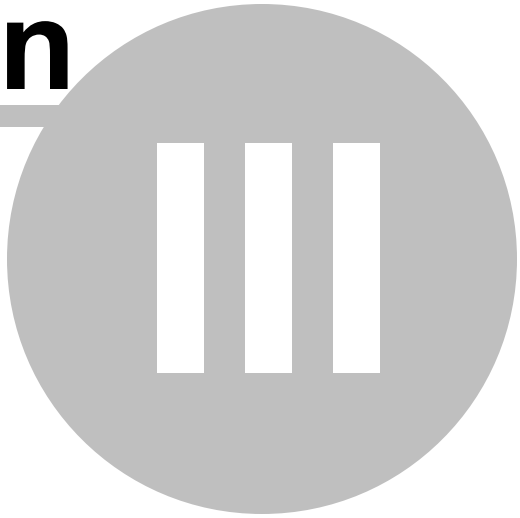
When an incoming SMTP connection is made, MDaemon goes through a complex series of processing steps to determine whether to accept the message for delivery, and what to do with it once it is accepted. The following chart is a graphical representation of this work flow for inbound SMTP messages.

The extent to which these steps are executed is dependent upon your particular configuration. One or more steps might be skipped if a given feature is disabled in your configuration.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section

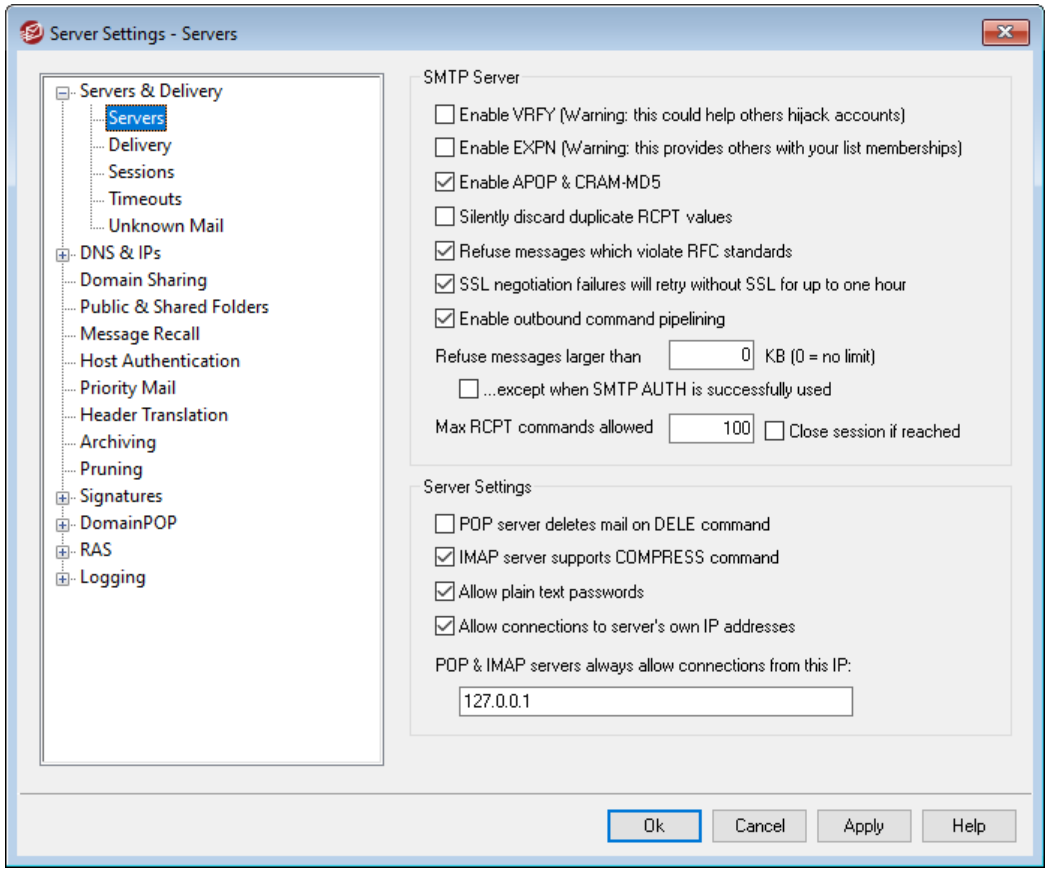


3 Setup Menu

3.1 Server Settings

3.1.1 Servers & Delivery

3.1.1.1 Servers



SMTP Server

Enable VRFY
Click this switch if you wish to respond to SMTP VRFY commands. This command is sometimes used by servers that use an SMTP call forward or call back feature to attempt to confirm the validity of email addresses on your server. This is disabled by default.

Enable EXPN
Click this checkbox if you want MDaemon to honor EXPN commands.

Enable APOP & CRAM-MD5
By default MDaemon's servers (POP, IMAP, and so on) do not honor the APOP and CRAM-MD5 methods of authentication. This type of authentication requires passwords to be stored using reversible encryption, which is not recommended for

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

security purposes, in order to protect passwords from being decrypted by MDaemon, the administrator, or a possible attacker. Consequently, this option is not compatible with the Passwords option 840 to "*Store mailbox passwords using non-reversible encryption*," nor with Active Directory authentication. If, however, you are not using SSL/TLS then APOP and CRAM-MD5 could provide extra security by making it possible for users to be authenticated without sending clear text passwords.

Silently discard duplicate RCPT values
Enable this option if you want the SMTP server to ignore duplicate recipients in the same SMTP session. MDaemon will accept and then discard the duplicate recipients. This option is disabled by default.

Refuse messages which violate RFC standards
Enable this option if you wish to reject messages during the SMTP process that are not compliant to RFC internet standards. To pass the compliance test the message must:

1. Be greater than 32 bytes in size (the minimum size necessary to include all required parts).
2. Have either a FROM: or a SENDER: header.
3. Have no more than one FROM: header.
4. Have no more than one SUBJECT: header, though no subject header is required.

Messages using authenticated sessions or from trusted domains or IP addresses are exempt from this requirement.

SSL negotiation failures will retry without SSL for up to one hour
This option allows you to temporarily retry host IPs without SSL when they encounter an SSL error during an outbound SMTP session. This resets every hour.

Enable outbound command pipelining
By default MDaemon supports the SMTP Service Extension for Command Pipelining (RFC 2920), which means it will send MAIL, RCPT, and DATA commands in batches instead of individually, which improves performance over high latency network links. SMTP pipelining is always used for inbound connections, and it is enabled by default for outbound connections. Clear this checkbox if you do not with to use it for outbound connections.

Refuse messages larger than [xx] KB (0=no limit)
Setting a value here will prevent MDaemon from accepting or processing mail that exceeds a certain fixed size. When this option is enabled MDaemon will attempt to use the ESMTP SIZE command specified in RFC-1870. If the sending agent supports this SMTP extension then MDaemon will determine the message size prior to its actual delivery and will refuse the message immediately. If the sending agent does not support this SMTP extension then MDaemon will have to begin acceptance of the message, track its size periodically during transfer, and finally refuse to deliver the message once the transaction has completed. Use "0" in this option if you do not wish to set a size limit. If you wish to exempt authenticated sessions from SIZE checks, use the "*...except when SMTP AUTH is successfully used*" option below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...except when SMTP AUTH is successfully used
Check this box if you wish to exempt messages from the message size limitation when the SMTP session is authenticated.

Max RCPT commands allowed
Use this option if you wish to limit the number of RCPT commands that can be sent per message. Use "0" if you do not wish to set a limit.

Close session if reached
Check this box if you wish to close the session immediately if the maximum allowed number of RCPT commands is reached.

Server Settings

POP server deletes mail on DELE command
Click this option if you wish MDaemon to delete messages immediately when they are retrieved and the DELE command is received, even if the POP session does not complete properly.

IMAP server supports COMPRESS command
Click this box if you wish to support the IMAP COMPRESS extension (RFC 4978), which compresses all data sent to and from the client. COMPRESS will increase CPU and memory usage per IMAP session.

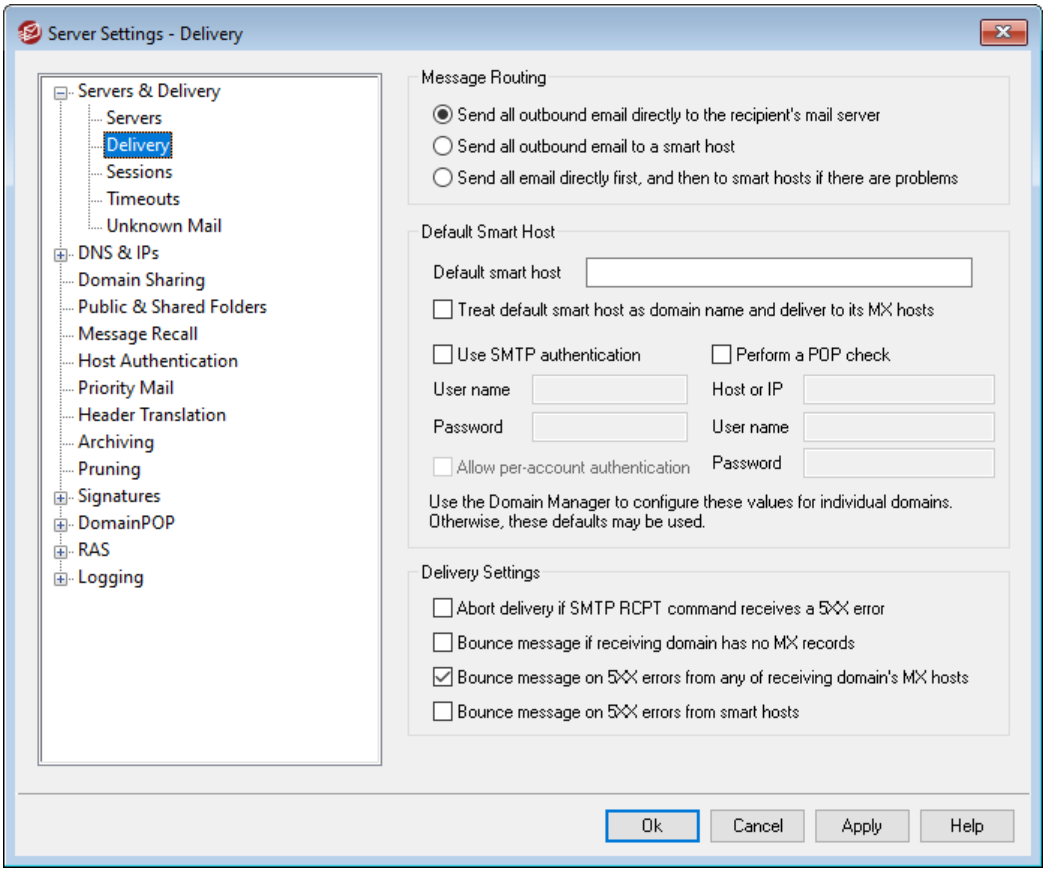
Allow plain text passwords
This option governs whether or not MDaemon will accept passwords sent in plain text to the SMTP, IMAP, or POP3 servers. If disabled, the `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN`, and `SMTP AUTH LOGIN` commands will return an error unless the connection is using SSL.

Allow connections to server's own IP addresses
When this option is enabled, MDaemon can connect to itself.

POP & IMAP servers always allow connections from this IP
The POP and IMAP servers will always accept connections from the IP Address entered into this field regardless of screening and shielding settings.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.1.2 Delivery



Message Routing

Send all outbound email directly to the recipient's mail server
When this option is chosen, MDaemon will attempt to deliver mail directly instead of passing it to another host. MDaemon will place undeliverable messages into its retry system and continue to attempt to deliver them according to the parameters and time intervals that you set on the Retry Queue 856 screen of the Mail Queues dialog.

Send all outbound email to a smart host
Select this option if you want outbound email, regardless of its destination domain, to be spooled to another host or server for routed delivery. If selected, outbound email will be sent to the *Default Smart Host* specified below. Typically, this feature is useful during high volume periods when direct message delivery would result in an excessive taxation of server resources. If a message cannot be delivered to the designated server then it will be moved into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 856 screen of the Mail Queues dialog.

Send all email directly first, and then to smart hosts if there are problems
This option is a combination of the previous two delivery options. First MDaemon will attempt to deliver outbound email directly to the server, but if it is unable to deliver it, it will instead send the email to the *Default Smart Host specified below*.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Undeliverable mail is email destined for hosts that could not be resolved to an actual IP address (such as an unregistered gateway to a remote network) or email destined for a host that was resolved properly but could not be connected to directly or is refusing direct connections. Rather than return such mail to its sender, this option causes MDaemon to pass the message off to a more powerful MTA. Sometimes the mail system run by your ISP may have routed methods of mail delivery to which your local server may not have direct access. If, however, a message cannot be delivered to the designated smart host then it will be moved to into the retry system and MDaemon will continue to attempt to deliver it according to the parameters and time intervals that you set on the Retry Queue 856 screen of the Mail Queues dialog. At each subsequent delivery attempt, MDaemon will again first try to deliver the message directly to its recipient and then to the designated smart host.

Default Smart Host

Default smart host
Specify your ISP or mail host's name or IP address here. This is generally the SMTP server on your ISP.

Do not enter MDaemon's Default Domain or IP addresses into this text box. This entry should be an ISP or other mail server that can relay mail for you.

Treat default smart host as domain name and deliver to its MX hosts
Enable this option if you want MDaemon to treat the *Default smart host* as a domain name, querying its DNS record and delivering to its MX hosts.

Use SMTP authentication

Click this check box and enter your login credentials below if the *Default Smart Host* requires authentication. These login credentials will be used for all outbound SMTP messages sent to the smart host. If, however, you choose to use the *Allow per-account authentication* option below, then MDaemon will authenticate to the host separately for each message, using the sending account's *Smart Host Access* credentials designated on the Mail Services 701 screen of the Account Editor.

User name
Enter your user name or login here.

Password
Use this option to specify your smart host login password.

Perform a POP check first
If your smart host requires a POP3 check before it will accept messages from you, click this check box and enter your required credentials below.

Host or IP
Enter the host or IP address to which you wish to connect.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

User name
This is the POP account's login or account name.

Password
This is the POP account's password.

Allow per-account authentication
Click this checkbox if you wish to use per-account authentication for outbound SMTP messages sent to the *Default Smart Host* specified above. Instead of using the *User name* and *Password* credentials provided here, each account's *Smart Host Access* credentials, designated on the Mail Services 701 screen, will be used instead. If no smart host credentials have been designated for a given account, the above credentials will be used instead.

If you wish to configure *per-account authentication* to use each account's *Email password* instead of its optional *Smart host password*, then you can do so by editing the following key in the `MDaemon.ini` file:

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

Enabling the `ISPAUTHUsePasswords=Yes` option will over time effectively communicate all your accounts' local mail passwords to your smart host. This could pose a risk to mail security, since it is providing sensitive information to another server. You should not use this option unless you are using a smart host that you absolutely trust and you believe it is necessary to do so. Further, you should note that if you use this option and give your users permission to change their *Email password* via Webmail or some other means, then changing the *Email password* will also effectively change the *Smart host password*. This could cause smart host authentication to fail for an account when its *Email password* is changed locally but the corresponding *Smart host password* isn't changed at your smart host.

Abort delivery if SMTP RCPT command receives a 5xx error
Enable this option if you wish MDaemon to abort its attempt to deliver a message when it receives a 5xx fatal error in response to the SMTP RCPT command. This option is disabled by default.

Bounce message if receiving domain has no MX records
Ordinarily when MDaemon checks the receiving domain's DNS records, it will look for MX records and then for an A record when no MX records are found. If neither are found then it will bounce the message back to the sender as undeliverable. Click this option if you want MDaemon to immediately bounce the message when no MX record is found, instead of allowing it to then look for an A record also. This option is Disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

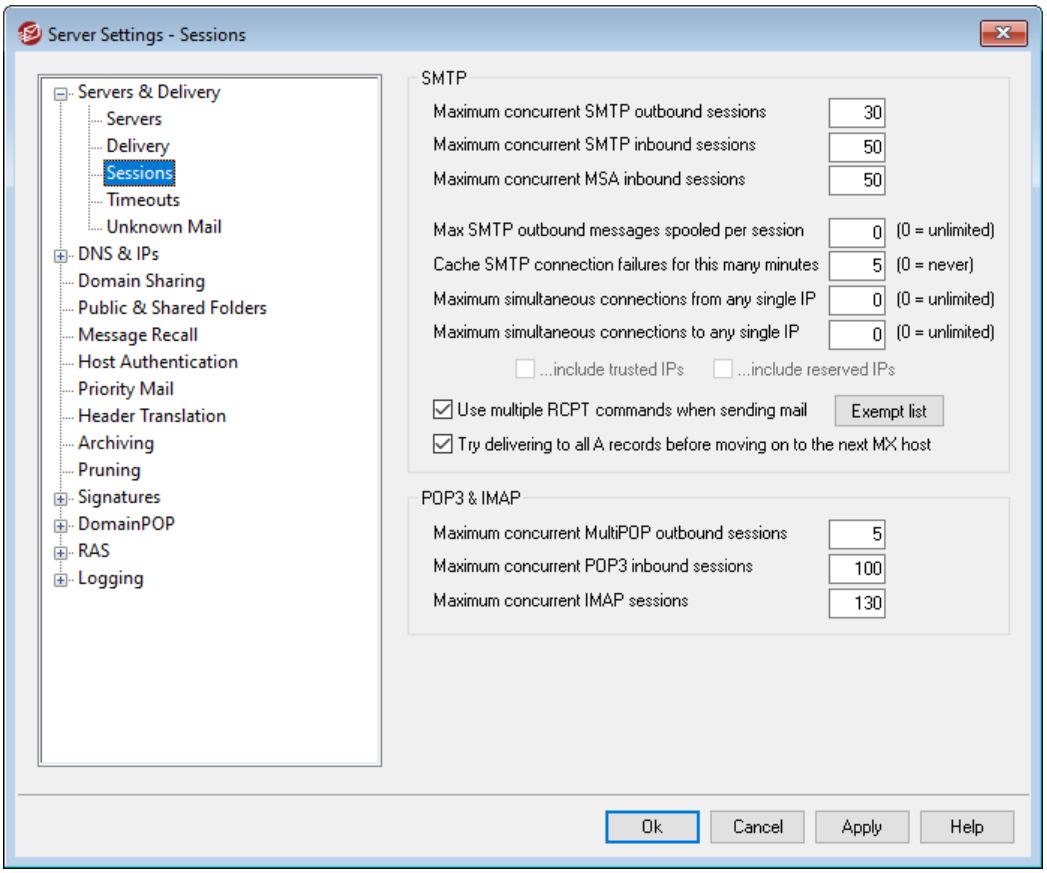
Bounce message on first 5XX error from any of receiving domain's MX hosts
When this checkbox is enabled, MDaemon will return/bounce the message when it receives a 5xx fatal error response from an MX host. Consequently, it won't continue trying to deliver the message to any subsequent MX hosts that may be designated for the recipient's domain. If this option is disabled, MDaemon won't bounce the message as long as at least one of the MX hosts returns a 4xx non-fatal error response. This option is enabled by default.

Bounce message on 5xx errors from smart hosts
Use this option if you wish to return/bounce a message when it receives a 5xx fatal error response from your smart hosts.

See:

Retry Queue 856
Mail Services 701

3.1.1.3 Sessions



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SMTP

Maximum concurrent SMTP outbound sessions
The value entered here represents the maximum possible outbound SMTP sessions that will be created when it is time to send outbound mail. Each session will send outbound messages until either the queue is empty or the *Maximum SMTP outbound messages spooled per session* setting has been reached. For example, if the outbound mail queue has twenty messages waiting when it is time to send mail and the value of this setting is five, then five sessions will be simultaneously created and each will consecutively deliver four messages.

This option is set to 30 by default, but you may wish to experiment with the number of sessions in order to find the setting that will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded or your Windows machine will run out of resources and you will lose delivery efficiency. Remember, each SMTP session created by MDaemon will deliver messages consecutively and therefore four sessions delivering two messages each might perform better and faster than eight threads delivering only one message each. A good place to start would be five to ten threads when using a 56k modem and twenty to thirty for broadband

Maximum concurrent SMTP inbound sessions
This value controls the number of concurrent inbound SMTP sessions that the server will accept before it begins responding with a "Server Too Busy" message. The default value is 50.

Maximum concurrent MSA inbound sessions
Use this option to designate the maximum number of concurrent mail submission agent (MSA) inbound sessions allowed.

Maximum SMTP outbound messages spooled per session
This setting places a limit on the number of individual messages that each session will send before it stops delivering mail and frees itself from memory. Ordinarily, you should leave this control set to zero, which will cause each session to continue delivering messages until the queue is empty.

Cache SMTP connection failures for this many minutes (0 = never)
When an SMTP connection to a given host fails, MDaemon will cease trying to connect to that host for the number of minutes specified in this option. This can prevent MDaemon from needlessly attempting to connect to a problem host over and over again when, for example, it has multiple messages designated for that host and yet discovers that it is down when making the first delivery attempt. The default setting is “5” minutes. Use “0” if you do not wish to cache SMTP failures.

Maximum simultaneous connections from any single IP (0 = unlimited)
This is the maximum number of simultaneous connections allowed from a single IP address before it will be blocked. Use "0" if you do not wish to set a limit.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Maximum simultaneous connections to any single IP (0 = unlimited)
Use this option to limit the number of simultaneous connections that will be allowed to a single IP address during mail delivery. Use "0" if you do not wish to limit simultaneous connections.

This option is useful to prevent making too many connections at once to various IP addresses. During delivery, if a message would require a connection to an IP that would exceed this connection limit, then the connection is skipped and the next MX host (or smart host) is used. If no additional hosts are available the message is queued for the next delivery cycle. By default, this option is disabled, which preserves existing behavior.

...include trusted IPs
By default, connections to trusted IP addresses are exempt from the *Maximum simultaneous connections to any single IP* option. Check this box if you would like to enforce it for trusted IPs as well.

...include reserved IPs
Also by default, connections to IP addresses reserved for intranet use are exempt from this feature. These are `127.0.0.*`, `192.168.*.*`, `10.*.*.*`, and `172.16.0.0/12`. Check this box if you would like to enforce it for reserved IP addresses as well.

Use multiple RCPT commands when sending mail
By default MDaemon uses smart spooling, that is it will use multiple RCPT commands within a session when sending mail. Uncheck this box if you wish to use only one RCPT command per session.

Exempt list
This button opens the Smart Spooling Exempt List. When MDaemon sends messages to domains on this list, it will NOT use smart spooling; only one RCPT command will be used per session.

Try delivering to all A records before moving on to the next MX host
On delivery errors or failures, by default MDaemon will attempt delivery to every A record for an MX host before moving on the the next MX host. Disable this option if you want MDaemon to move on the the next MX host immediately after encountering an error rather than try all A records first.

POP3 & IMAP

Maximum concurrent MultiPOP outbound sessions
The value entered here represents the maximum possible outbound POP sessions that will be created when it is time to collect MultiPOP mail. Each session will collect this type of mail until all MultiPOP servers have been processed, and all mail has been collected. For example, if there are fifteen MultiPOP sessions amongst all of your users and the value of this setting is set to three, then each session will collect mail from five MultiPOP sources.

You should experiment with the number of sessions to determine what number will yield the best performance for your bandwidth. It is possible to specify so many

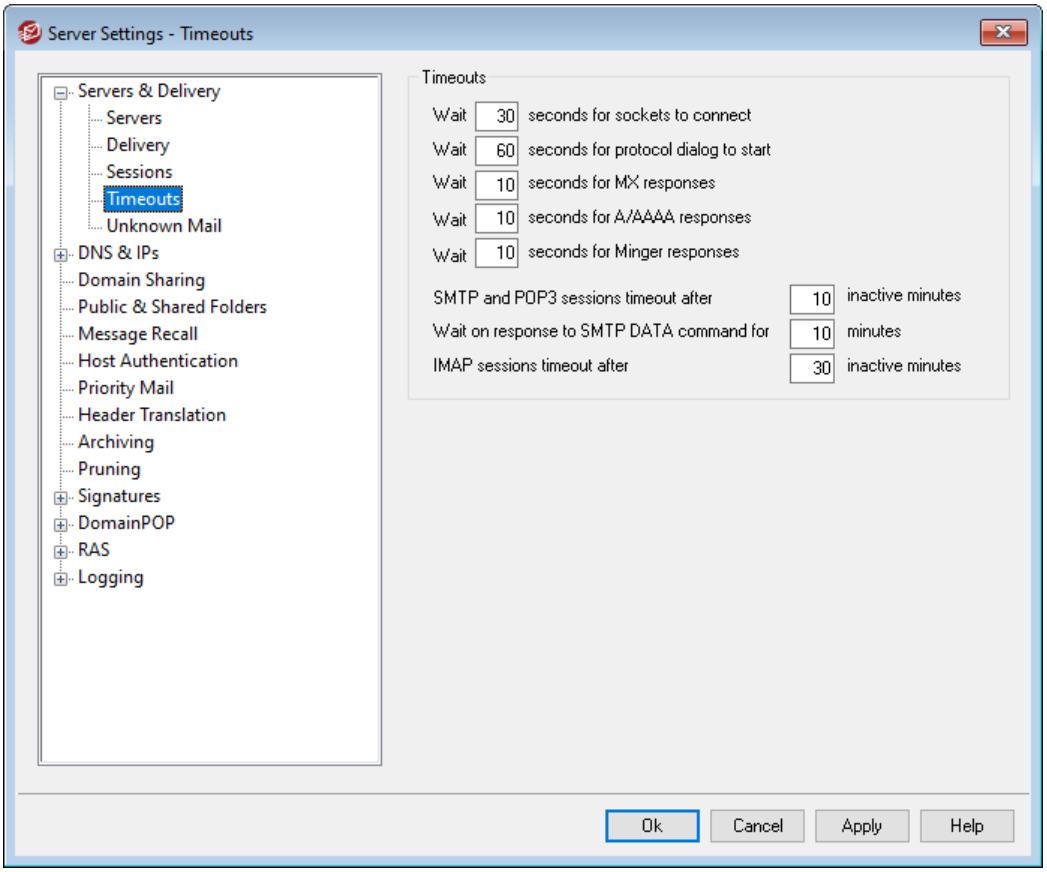
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

sessions that your bandwidth will be overloaded, or your Windows machine will run out of resources and you will lose processing efficiency. Remember that each POP sessions created by MDaemon will collect mail until all sources have been exhausted. Therefore, four sessions collecting mail from twenty sources might perform better and faster than twenty sessions collecting from a single source.

Maximum concurrent POP3 inbound sessions
This value controls the maximum number of concurrent POP inbound mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

Maximum concurrent IMAP sessions
This value controls the maximum number of concurrent IMAP mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

3.1.1.4 Timeouts



Timeouts

Wait xx seconds for sockets to connect
After initiating a connection request MDaemon will wait this many seconds for the remote system to accept the connection. If the remote system does not respond

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

within this time frame, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 89 screen of the Server Settings dialog.

Wait xx seconds for protocol dialog to start
Once a connection has been established with a remote host, this is the number of seconds that MDaemon will wait for the remote host to begin the SMTP or POP3 protocol dialog. If the remote host does not begin the protocol session within this time frame, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 89 screen of the Server Settings dialog.

Wait XX seconds for MX responses
While using DNS services to resolve 'MX' hosts for remote domains, MDaemon will wait for responses to its 'MX' queries for this number of seconds. If the DNS server does not respond within this time frame MDaemon will attempt to deliver the message to the IP address specified in the remote host's 'A' DNS record. If that attempt fails, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 89 screen of the Server Settings dialog.

Wait XX seconds for A/AAAA responses
This timer governs how long MDaemon will wait while attempting to resolve a remote host's IP address. If the attempt fails, MDaemon will send the message to a specified *smart host* or place it into the retry system, depending upon which option you have chosen on the Delivery 89 screen of the Server Settings dialog.

Wait XX seconds for Minger responses
This is the number of seconds that MDaemon will wait for a response from a Minger 847 server.

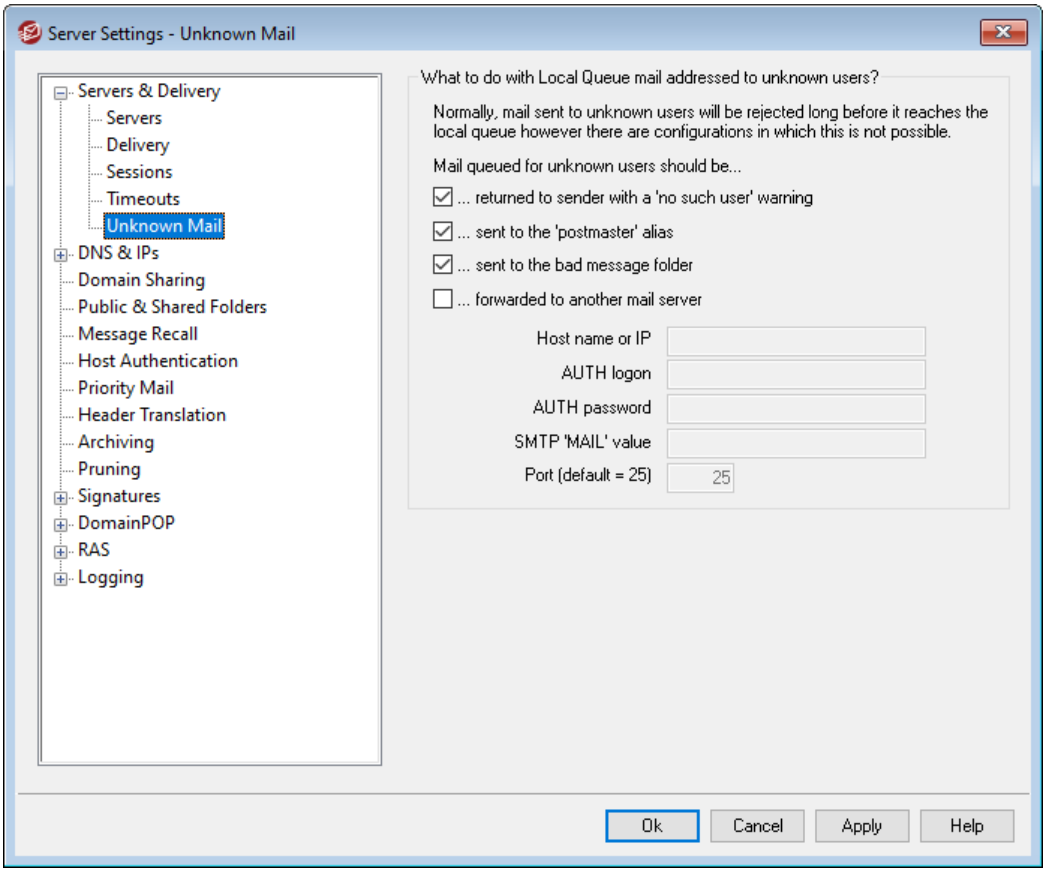
SMTP and POP3 sessions timeout after XX inactive minutes
If a successfully connected and operating session remains inactive (no i/o) for this length of time, MDaemon will abort the transaction. MDaemon will try again at the next scheduled processing interval.

Wait on response to SMTP DATA command for XX minutes
This option governs how long MDaemon will wait for the "`250 Ok`" response after sending the `DATA` command during the SMTP process. Since some receiving servers perform lengthy anti-spam, anti-virus, or other necessary operations at that time, this option can be used to give them time to complete those tasks. The default is 10 minutes.

IMAP sessions timeout after xx inactive minutes
If an IMAP session has no activity for this number of minutes, MDaemon will close the session.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.1.5 Unknown Mail



Mail queued for unknown users should be...

...returned to sender with a 'no such user' warning
When this option is enabled, messages that arrive at the server destined for unknown yet supposedly local users will be returned to the message originator. If you wish to customize the contents of the "No Such User" warning email, you can do so by creating a text file called "`NoShUser.dat`" and placing it in the "`MDaemon\app\`" folder.

...sent to the 'Postmaster' alias
By default, messages that arrive at the server destined for unknown yet supposedly local users will be forwarded to whatever user has been aliased as the postmaster. Disable this option if you do not wish to send these messages to the Postmaster.

...sent to the bad message folder
By default, messages that arrive at the server destined for unknown yet supposedly local users will be routed to the bad message queue. Clear this checkbox if you do not wish to send these messages to the bad message queue.

...forwarded to another mail server
Use this option if you wish to forward messages to another mail server when they are addressed to unknown local users.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Host name or IP
Specify the host name or IP address to which you wish to forward the messages.

The following applies globally anywhere within MDaemon where you are allowed to specify a host to forward, copy, or send email to. If you enclose the host in brackets (e.g. `[example.com]`), MDaemon will skip MX record lookups when delivering to that host. For example, if this option contained "`example.com`" then MX lookups would be performed normally. If, however, that option contained "`[example.com]`" then only the A-record lookup would be performed.

AUTH logon/password
Enter any necessary logon/password credentials for the mail server to which you are forwarding messages addressed to unknown users.

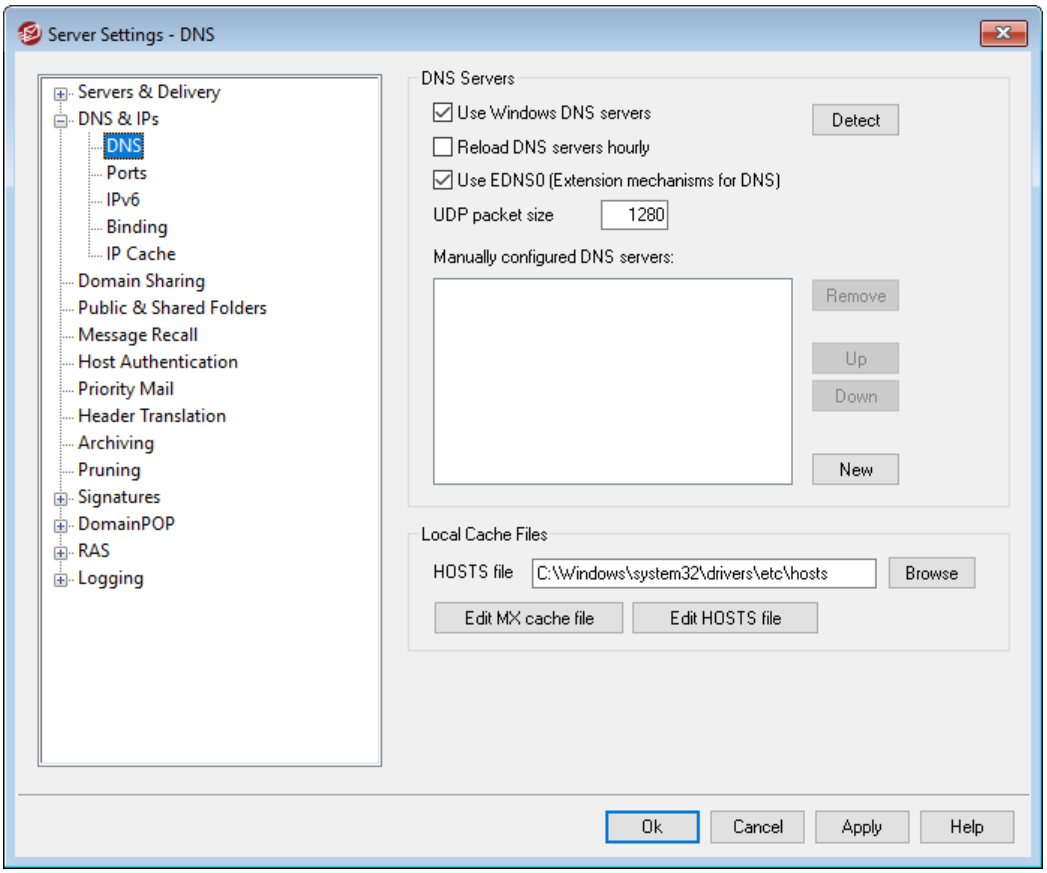
SMTP 'MAIL' value
This address will be used in the SMTP "`Mail From:`" statement, used during the session handshaking with the accepting host. Normally the sender of the message is used in this portion of the SMTP envelope. If you require an empty command (`MAIL FROM <>`) then enter "`[trash]`" into this option.

Port (default = 25)
This is the TCP port that MDaemon will use to send the messages. The default value is port 25.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.2 DNS & IPs

3.1.2.1 DNS



DNS Servers

Use Windows DNS servers
When this option is selected, MDaemon will use all DNS servers found within your Windows TCP/IP configuration. MDaemon will try each DNS server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you include additional DNS servers in the *Manually configured DNS Servers* option below, MDaemon will try those servers as well. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

Reload DNS server hourly
Check this box if you wish to reload the DNS server every hour. This is disabled by default.

Use EDNS0 (Extension Mechanisms for DNS)
By default MDaemon supports Extension Mechanisms for DNS (see RFC 2671). Clear this checkbox if you not wish to support it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

UDP packet size
This option controls the UDP packet size. The default size is 1280 bytes.

Manually configured DNS servers
MDaemon will use all DNS servers specified here when performing DNS lookups. MDaemon will try each server once per lookup operation and in sequence until it exhausts the complete list of DNS servers or finds the first one that works. If you enable the *Use Windows DNS servers* option above, MDaemon will also query all DNS servers found within your Windows TCP/IP configuration. Finally, at startup the System log will display each DNS server and indicate its source (i.e. manually configured or taken from Windows).

Local Cache Files

Hosts file...
Before querying the DNS servers, MDaemon will first attempt to resolve an address by processing the Windows HOSTS file. If this file contains the IP address of the domain in question, MDaemon will not need to query the DNS server.

You must enter the complete path and filename rather than just the filename. MDaemon will attempt to use the following value as the default location of this file:

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

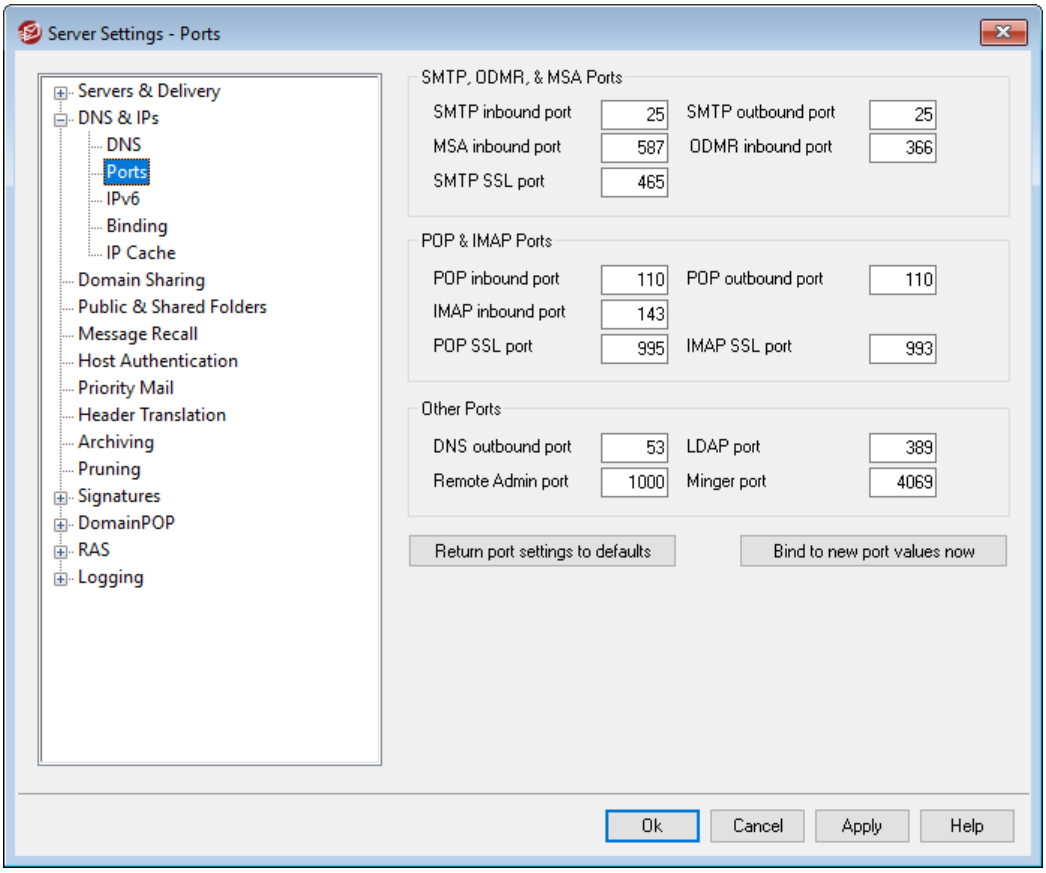
The HOSTS file is a Windows file that contains the A-record or primary IP address for domain names. MDaemon also allows you to specify MX-record IP addresses within a file called MXCACHE.DAT. This file can be found within the MDaemon\APP\ folder. Click **Edit MX cache file** below and read the comments at the top of the file for more information.

Edit MX cache file
Click this button to view or edit the MXCACHE.DAT file.

Edit hosts file
Click this button to view or edit the HOSTS file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.2.2 Ports



SMTP, ODMR, & MSA Ports

SMTP inbound port
MDaemon will monitor this TCP port for incoming connections from SMTP clients. This is the main SMTP port, which in most cases should be left at the default setting of port 25.

SMTP outbound port
This port will be used when mail is sent to other SMTP servers.

MSA inbound port
This is a Message Submission Agent (MSA) port that can be used by your users as an alternative to the *SMTP inbound port* specified above. Transmission on this port requires AUTH, therefore users sending on that port must configure their mail clients appropriately to ensure that their connections are authenticated. Further, because some ISPs block port 25, your remote users might be able to circumvent that restriction by using the MSA port instead. If you do not wish to designate an MSA port then set the value to "0" to disable it.

Connections to the MSA port are exempt from PTR and reverse lookups, Host and IP screening, the IP Shield, and Tarpitting.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

> MSA port connections continue to utilize dictionary attack connection limiting.

ODMR inbound port
MDaemon will monitor this port for incoming On-Demand Mail Relay (ODMR) connections, such as `ATRN` from Gateway Domains.

SMTP SSL port
This is the port dedicated to SMTP mail sessions using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 561 for more information.

POP & IMAP Ports

POP inbound port
MDaemon will monitor this port for incoming connections from remote POP clients.

POP outbound port
This port will be used when MDaemon retrieves mail from POP servers.

IMAP inbound port
MDaemon will monitor this port for incoming IMAP requests.

POP SSL port
This is the port dedicated to POP mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 561 for more information.

IMAP SSL port
This is the port dedicated to IMAP mail clients using a Secure Sockets Layer (SSL) connection. See SSL & Certificates 561 for more information.

Other Ports

DNS outbound port
Enter the Port you want MDaemon to use for sending and receiving datagrams to the DNS server.

LDAP port
MDaemon will post database and address book information to your LDAP server on this port.

See: LDAP Address Book Support 815

Remote Admin port
This is the port that MDaemon will monitor for Remote Administration 341 connections.

Minger port
This is the port that the Minger 847 server will monitor for connections.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Return port settings to defaults
This button returns all the port settings to their standard values.

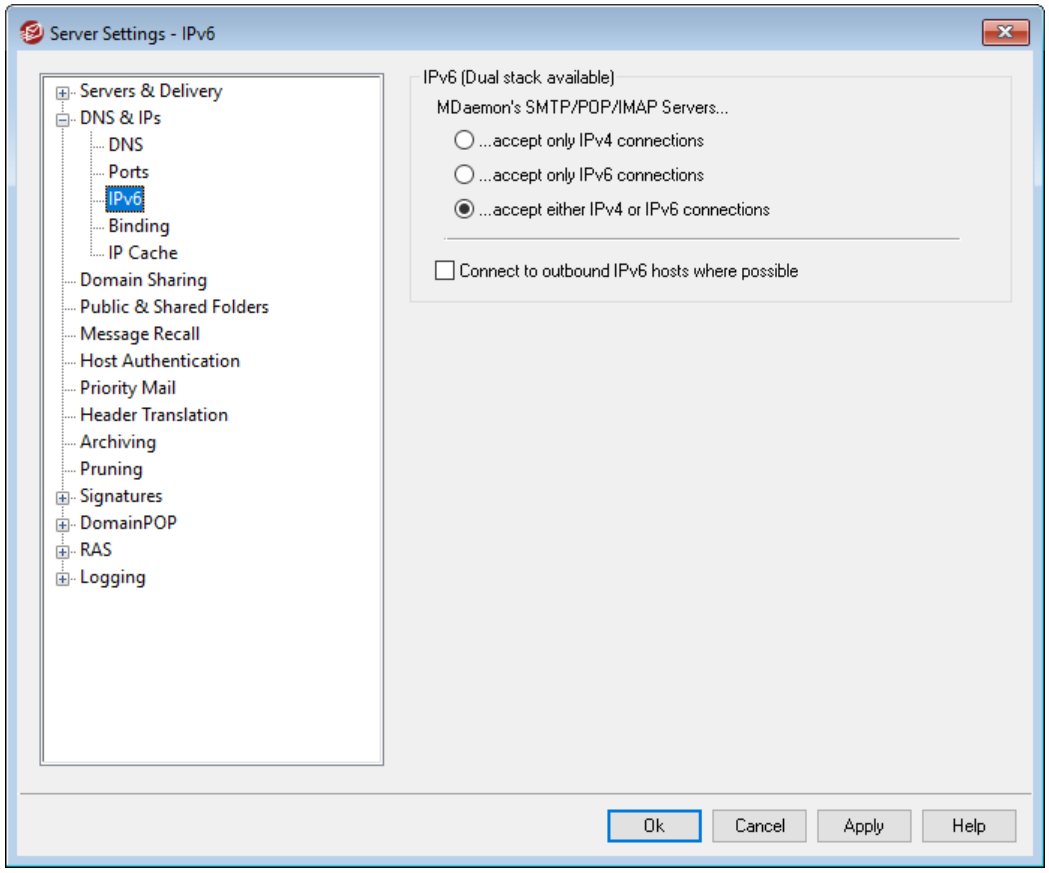
Bind to new port values now
When you alter the values of any of the port settings you will need to press this button to have your changes take immediate effect. Otherwise, your changes will not be put into place until the next time the server is started.

The preceding port settings are critical for proper server operation and should not be altered unless you are certain that you must do so. Being able to configure the ports that MDaemon uses will allow you to configure the server to operate with proxy systems or other software services that require certain port numbers.

An IP address (a machine) has only one of each available port. If one program attempts to gain access to a port that is already in use by another program, an error message will inform the user that the requested address (IP:PORT) is already in use.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.2.3 IPv6



By default MDaemon detects the level of IPv6 capability that your OS supports and dual-stacks where possible. Otherwise, MDaemon monitor both IPv4 and IPv6 independently.

IPv6

MDaemon's SMTP/POP3/IMAP Servers...

...accept only IPv4 connections
Choose this option if you only wish to accept IPv4 connections.

...accept only IPv6 connections
Choose this option if you only wish to accept IPv6 connections.

...accept either IPv4 or IPv6 connections
Choose this option if you wish to accept both IPv4 and IPv6 connections. This is the default setting, and MDaemon will give precedence to IPv6 connections over IPv4 whenever possible.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

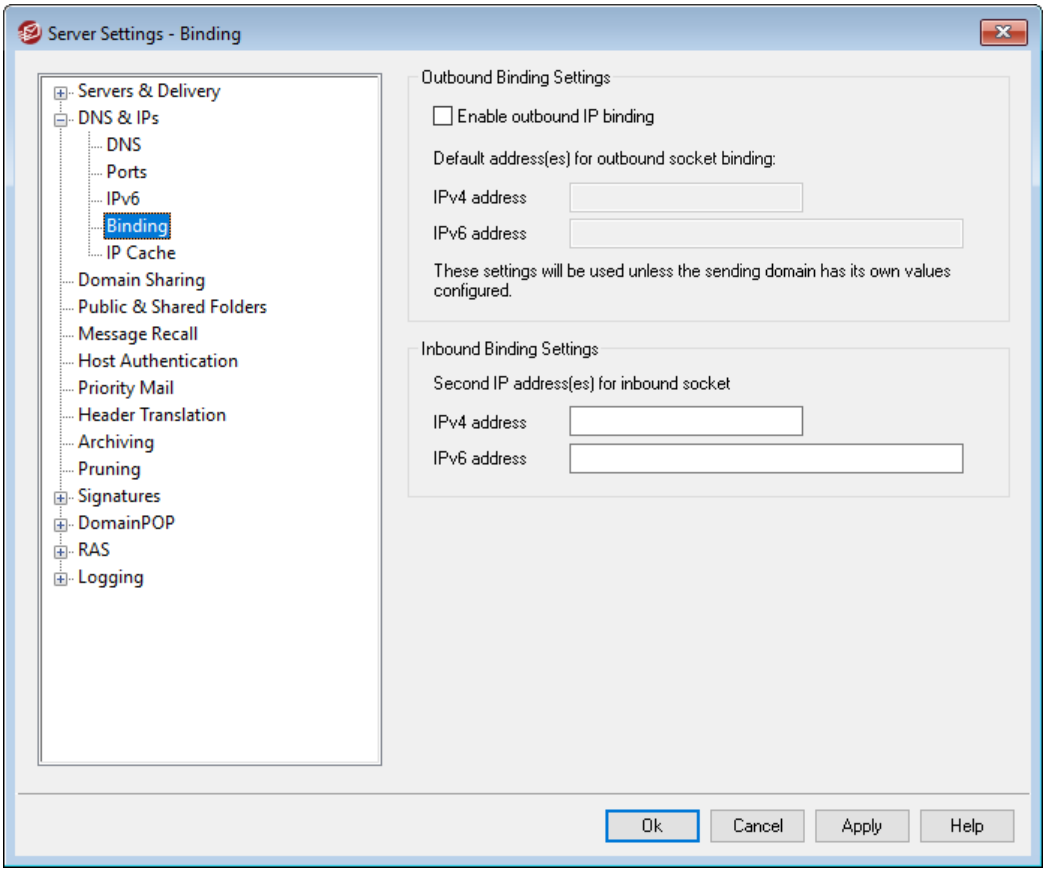
Connect to outbound IPv6 hosts where possible
Enable this option if you want MDaemon to connect to outbound IPv6 hosts whenever possible.

When MDaemon connects to an IPv6 host it must use an IPv6 local address of its own. The IPv6 address is designated on the Domain Manager » Host Name & IP 177 screen. If necessary, an address for outbound socket binding can be specified on the Binding 105 screen.

See:

Binding 105
Domain Manager » Host Name & IP 177

3.1.2.4 Binding



Outbound Binding Settings

Enable outbound IP binding
When this option is checked, MDaemon always binds outbound sockets. For domains that have *This domain recognizes only connections made to these IPs* 177 checked

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

on the Host Name & IP 177 screen, MDaemon uses the domain's configured IP. Otherwise it uses the *Default address(es) for outbound socket binding* specified below.

Default address(es) for outbound socket binding: IPv4/IPv6 address
These are the IP addresses that will be used for outbound socket binding for domains that are not already bound to specific IP addresses on the Domain Manager's Host Name & IP 177 screen.

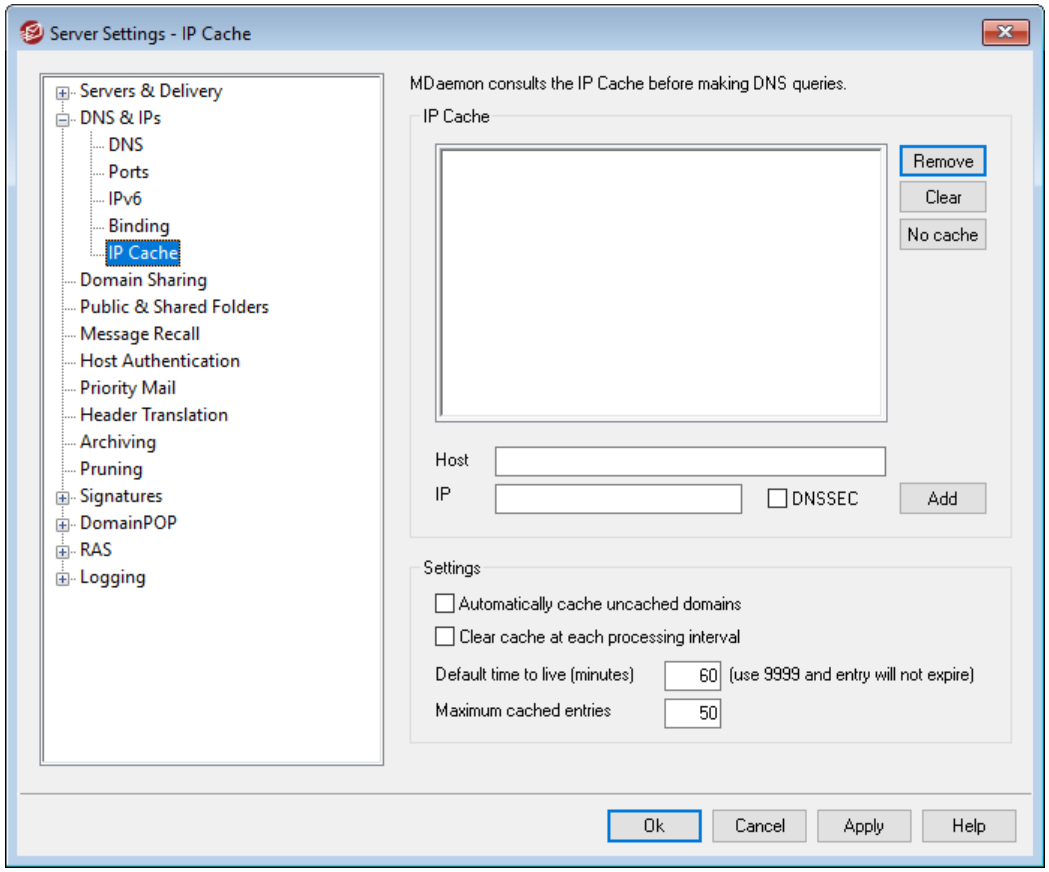
Inbound Binding Settings

Second IP address for inbound socket binding: IPv4/IPv6 address
Use this option if you wish to designate a second set of IP addresses for inbound socket binding 177.

See:

Domain Manager » Host Name & IP 177
IPv6 104

3.1.2.5 IP Cache



In order to speed message delivery and shorten mail processing time, MDaemon caches the IP addresses of all hosts with which it comes in contact. These IPs are stored and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

then the cache is checked each time MDaemon requires a DNS resolution on a host name. If the host name needing resolution is found in the IP cache then the DNS lookup is skipped, which can save a surprising amount of processing time. The settings in this window allow you to manipulate the parameters under which the cache will operate. You may also manually add and remove entries, set whether to use DNSSEC, set the maximum size of the cache, and designate how long entries will remain cached. The IP Cache can be reached from the "Setup » Server Settings » IP Cache" menu selection.

IP Cache

Host
Enter the host that you wish to add to the IP cache.

IP
Enter the IP address that you wish to add to the IP cache.

DNSSEC
Check this box for DNSSEC.

Add
Once you have manually entered a host and IP address, click this button to add it to the cache.

Remove
If you wish to remove a cached IP address from the list, select the entry and then click this button.

Clear
This button will delete all entries in the cache.

No cache
Click this button to bring up a list of domain names and/or IP addresses that you never want MDaemon to add to the IP Cache.

Settings

Automatically cache uncached domains
This option governs MDaemon's internal auto-caching engine. If you want MDaemon to cache domains automatically then enable this option. If you want to build the IP Cache yourself, then clear this checkbox.

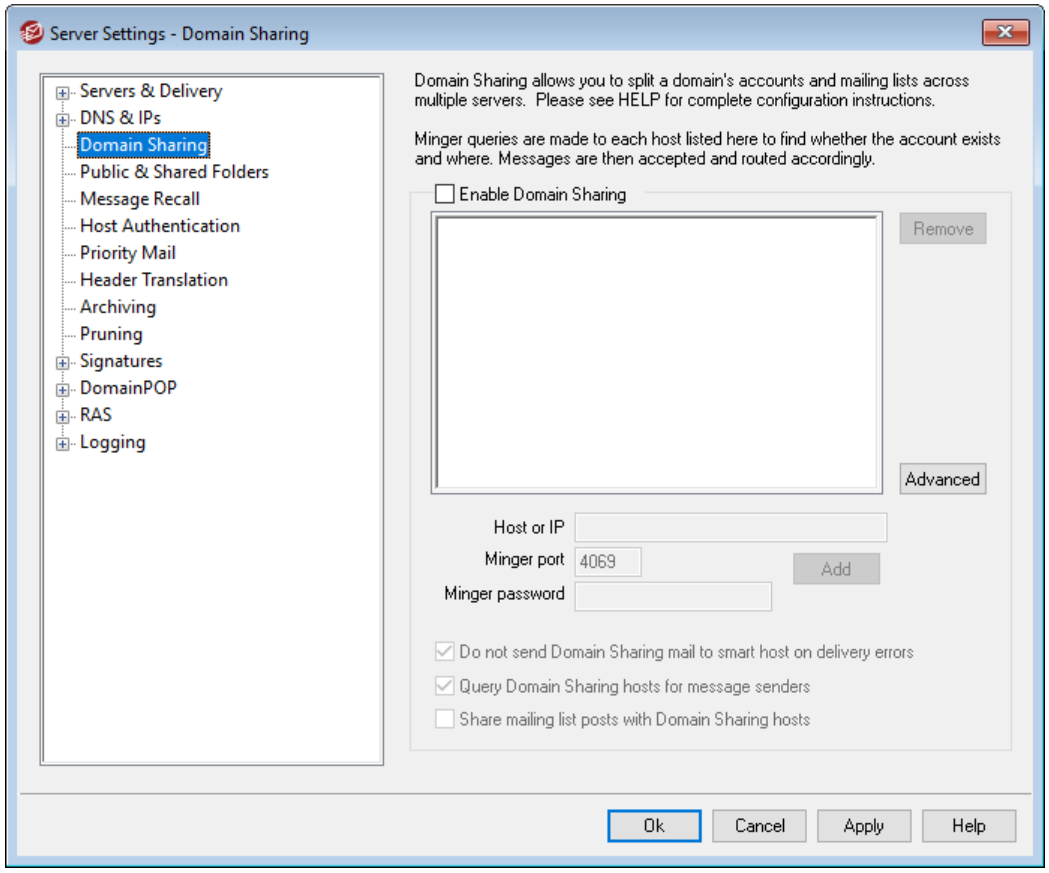
Clear cache at each processing interval
If selected, the entire contents of the cache will be flushed at the start of each mail session. This allows the cache to be refreshed at each processing interval.

Default time to live (minutes)
This is the default value in minutes that an entry will remain in the IP Cache. Once the entry has been in the IP Cache for this number of minutes, MDaemon will remove it. If you want to set a permanent entry in the IP Cache then designate the *Default time to live* as 9999.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Max cached entries
This value determines how large the cache may be. Once this number is reached, the next cache entry will bump the first one out of the cache.

3.1.3 Domain Sharing



Domain Sharing is a feature which allows you to split a domain's users across multiple servers. This makes it possible for you to have MDaemon servers running in different locations, all using the same domain names but with different user accounts. One portion of your domains' user accounts are hosted on one server while another portion of them are hosted on one or more other servers. The Domain Sharing dialog is used to specify where each of these other servers is located. Then, when an incoming message arrives for a local user who does not have a local mailbox, Domain Sharing will use Minger to query the other servers in order to discover whether or not that user has an account on one of them. If the address is found to be valid, MDaemon will accept the message and route it to the server where the account is located.

For example, you could have offices in multiple cities and choose to use Domain Sharing to allow every employee to have an email address ending with, "`@example.com`." Each office's MDaemon would host a portion of `example.com's` email, having accounts only for the local employees who work in that office. Then, every office would be configured

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

to use Domain Sharing, so that everyone's messages would get routed to the correct office.

Because Domain Sharing uses Minger 847 to verify addresses, Minger must be enabled and properly configured on each server in order for queries to function. If, however, an error occurs during a Minger query, such as when one of the servers is temporarily unavailable, MDaemon will respond with a "451" temporary error code so that the sending server can try to deliver the message again later. Further, once an address has been verified, it will be cached for five days so that MDaemon can immediately accept future messages for that address and begin attempting to route those messages to the proper host.

Finally, to avoid potential problems that could occur if the same account were created on multiple servers, MDaemon will query all of the Domain Sharing servers before creating any new account.

There is an option called "*Minger verification lookups also trigger Domain Sharing lookups*," located on the Gateway Editor's Settings 258 screen. This option can be used to cause MDaemon to also query your Domain Sharing hosts whenever Minger Verification 248 is used by a Gateway.

Enable Domain Sharing
Check this box to enable Domain Sharing. After you have enabled Domain Sharing and added all of the Domain Sharing hosts or IP addresses to the list, ensure that you have also enabled and configured Minger 847 so you can respond to queries from those hosts when they attempt to verify your local addresses.

Remove
To delete one of your Domain Sharing entries, select it from the list and click this button.

Advanced
This button opens a file where you can configure domain names that are allowed to use Domain Sharing. When nothing is in this file (the default condition) then all your domains can use Domain Sharing. See the instructions at the top of the file for more information.

Host or IP
Use this box to enter the host or IP address that is sharing one or more of your domains. You can append a colon and port (e.g. `mail.example.com:2525`) if you wish to use a specific, non-default port when sending SMTP messages to the host (this is not the same as the Minger port below).

Minger port
This is the port that Minger will use when querying this host. The default port is 4069.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Minger password (optional)
If the host that you are adding requires a Minger password, enter it here. Setting up Minger to require a password is optional, but it is recommended.

Add
After entering the host or IP, port, and password, click this button to add the new Domain Sharing entry to the list.

Do not send Domain Sharing mail to smart host on delivery errors
When this option is enabled, if MDaemon encounters an error while attempting to deliver Domain Sharing email (e.g. such as when the Domain Sharing host is offline), the email will be kept in the queue[856] rather than sent to the smart host[89]. Sending these emails to the smart host can often lead to a mail loop. This option is enabled by default.

Query Domain Sharing hosts for message senders
By default MDaemon will accept mail from accounts that are found to exist on other Domain Sharing hosts. If you would rather not perform any Domain Sharing lookups on the SMTP MAIL sender, disable this option.

Share mailing list posts with Domain Sharing hosts
Enable this option if you wish to share mailing lists with Domain Sharing hosts. When a message arrives for a mailing list, a copy is created for each Domain Sharing host that also maintains a version of that list (a query is made to check). When these hosts receive their copies they will deliver the message to all of the list members they serve. In this way mailing lists can be split across multiple servers with no loss in functionality. For this to work each Domain Sharing host must include the other hosts IPs in their Trusted IPs[506] configuration. Otherwise list messages might be refused with a 'Sender is not a member of the list' error.

See:

Minger[847]
Domain Manager[174]

3.1.4 Public & Shared Folders

MDaemon supports shared Public and User IMAP folders. Public folders (managed from the Public Folder Manager[300]) are extra folders that do not belong to any particular account but can be made available to multiple IMAP users. User folders are IMAP folders that belong to individual MDaemon accounts. Each shared folder, whether public or user, must have a list of MDaemon users associated with it, and only members of that access list may access it via MDaemon Webmail or an IMAP email client.

When IMAP users access their list of personal folders, they will also see the shared public and shared user folders to which they have been given access. In this way certain mail folders can be shared by multiple users but still require each user's individual logon credentials. Further, having access to a folder doesn't necessarily mean having full read/write or administrative access to it. Specific access rights can be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

granted to individual users, thus allowing you to set different levels of access for each one. For example, you might allow some users to delete messages while restricting that from others.

Once a public or user IMAP folder has been created you can use the Content Filter to set criteria by which certain messages are moved into that folder. For example, it might be useful to make a filter rule that would cause messages containing `support@example.com` in the `TO:` header to be moved into the `Support` public folder. The Content Filter actions 633 "`Move Message to Public Folders...`" and "`Copy Message to Folder...`" make this possible. For shared user folders, you can use your personal IMAP filters 720 to route specific messages to them. In addition to using Content Filters and IMAP filters, you can associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

For added convenience, the Mailing List editor also contains a Public Folder 289 screen that makes it possible for you to configure a public folder for use with a particular list. If you enable this feature then a copy of each list message will be placed into the specified public folder. All public folders are stored in the `\Public Folders\` directory within the MDaemon directory hierarchy.

Webmail Documents Folders

The Webmail themes support document sharing using document folders. Document folders have full Access Control List (ACL) 302 support like other shared folders, which can be used to set permissions and sharing rules, and any types of files can be shared through the system. Webmail users can upload files to their document folders using the built-in tools. When using the LookOut theme, browsers that support the HTML5 Drag and Drop API, such as Chrome and Firefox, can also upload files by dragging them from the desktop into the browser window. Filenames can be searched and renamed, and files can be attached to new messages that are being composed.

You can enable/disable the documents folders (and other shared folders) on a per-domain and per-user basis by editing the `\WorldClient\Domains.ini` file and individual `\Users\..\WC\user.ini` files respectively. You can configure both default settings and customized settings, which will override the defaults. For example:

```
[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
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Setting a Maximum File Size

You can limit the size of individual files that can be uploaded to documents folders by adding this key to the `domains.ini` file: `MaxAttachmentSize=<value in KB>` The default value is `0`, which means there is no limit.

Blocking or Allowing File Types

To prevent certain file types from being uploaded to the documents folder, add the `BlockFileTypes=` key to the `domains.ini` file, listing the files types you wish to block separated by a space or comma. For example, "`BlockFileTypes=exe dll js`".

To allow only certain file types to be uploaded to the documents folder, add the `AllowFileTypes=` key to the `domains.ini` file, listing the files types you wish to allow separated by a space or comma. For example, "`AllowFileTypes=jpg png doc docx xls xlsx`".

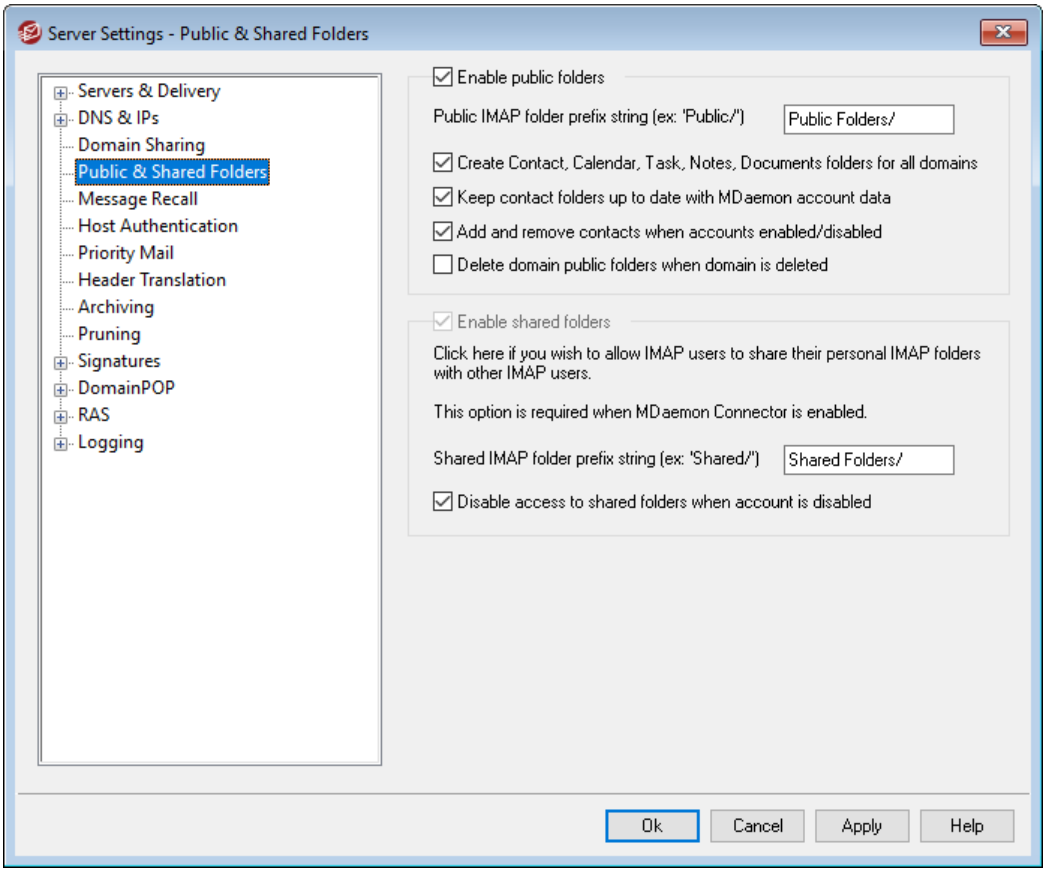
When both keys are used, priority is given to blocked files when there is a conflict; if an extension is in both lists then that extension will be blocked. If a key is used without a value (i.e. no list of extensions), then that key will not be used. File extensions can include a "." (e.g. .exe .dll), but it isn't required.

See:

Public & Shared Folders 113
Public Folder Manager 300
Access Control List 302
Account Editor » Shared Folders 726
Mailing List » Public Folders 289

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.4.1 Public & Shared Folders



To reach the Public & Shared Folders screen, click "Setup » Server Settings » Public & Shared Folders".

Enable public folders

Click this check box if you wish to allow users to gain access to public folders. The users that can access them and the level of access granted is designated under each folder on the Public Folder Manager 300. Clear this check box if you want to hide public folders from all users.

Public IMAP folder prefix string (ex: 'Public/')
Public folders are prefixed with a sequence of up to 20 characters, such as "#" or "Public Folders/". This is to help users easily distinguish public from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote public folders.

Create Contact, Calendar, Task, Journal, and Notes folders for all domains
Click this check box if you wish to ensure that these folders exist for all domains. Whenever a Domain 174 is added to MDaemon, these folders will be created.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Keep contact folders up to date with MDaemon account data
If this option is enabled, MDaemon will keep the contact folders synchronized with its account list.

Add and remove contacts when accounts enabled/disabled
By default when you disable an account, the account will be removed from the domain's public contacts folder. Then if you re-enable the account, it will be added again to the contacts. This option is enabled by default to prevent disabled accounts from showing up in Webmail's auto-complete system.

Delete domain public folders when domain is deleted
Click this check box if you wish to delete a domain's public folders when the domain is deleted.

Enable shared folders

Click this check box if you wish to allow IMAP users to share access to their IMAP folders. The users who can access them and the level of access granted is designated under each folder on the Shared Folders 726 screen of the Account Editor (Accounts » Account Manager » [User Account] » Shared Folders). Clear this check box if you wish to prevent users from being able to share access to their folders, and prevent the aforementioned Shared Folders screen from appearing on the Account Editor.

When using MDaemon Connector 379, this option will be unavailable. You will not be able to deactivate it because user folder sharing is required for MDaemon Connector to function properly.

Shared IMAP folder prefix string (ex: 'Shared/')
Shared user folders are prefixed with a sequence of up to 20 characters, such as "Public Folders/". This is to help users easily distinguish shared from private folders from within their email client. Use this text box to specify the series of characters that you wish to use to denote shared user folders.

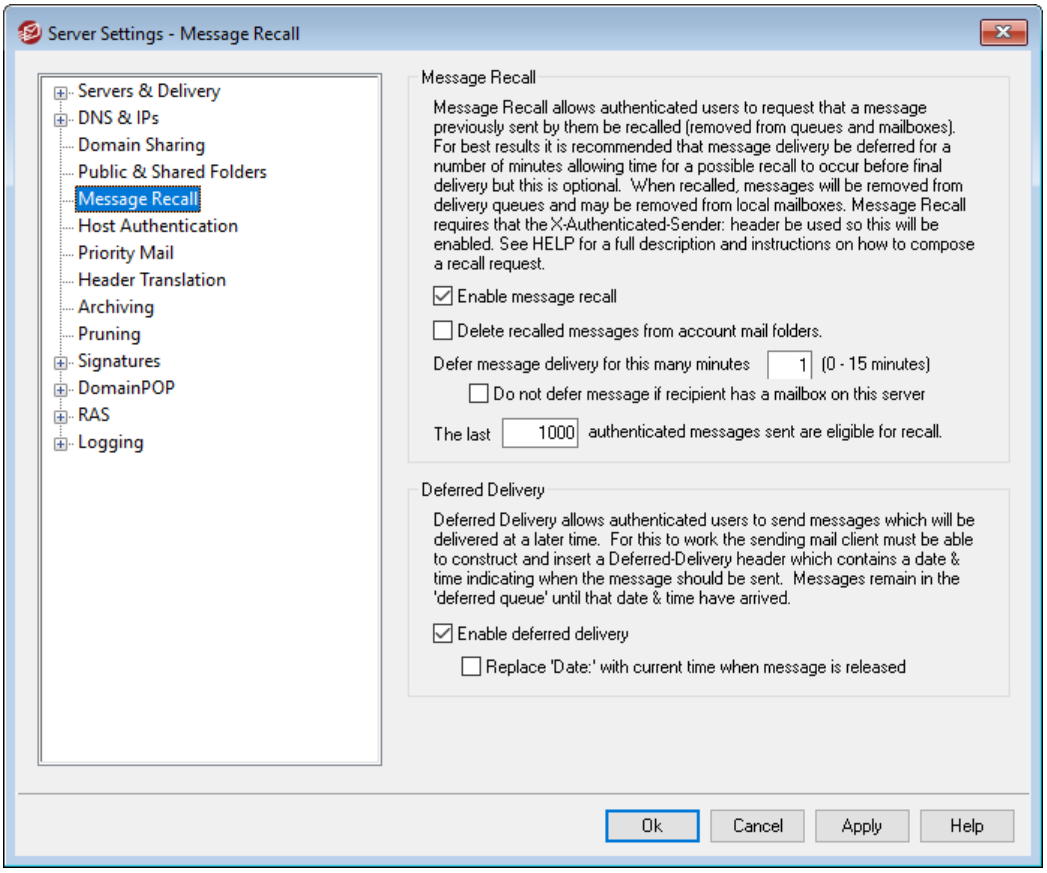
Disabled access to shared folders when account is disabled
By default MDaemon's IMAP, Webmail, and ActiveSync servers do not allow access to the shared folders of disabled accounts. Clear this checkbox if you wish to allow access to account shared folders even if when an account is disabled.

See:

Public Folders Overview 110
Public Folder Manager 300
Access Control List 302
Account Editor » Shared Folders 726
Mailing List » Public Folders 289

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.5 Message Recall



Message Recall System

MDaemon has a message recall system that you can use to delay incoming messages sent by authenticated local users for 0 to 15 minutes, which provides users a short period of time during which they can attempt to stop a message from being delivered. During that delay period the messages are placed in a dedicated Deferred queue rather than going directly to the Inbound mail queue—messages in the Deferred queue have the date they are set to leave the queue encoded into the file name. MDaemon checks the queue once per minute and when it's time for a message to leave the queue it is moved to the Inbound queue and subject to normal message processing and delivery. Activity is logged to the Routing tab and log file.

You can set the delay time to "0" if you wish, but this increases the possibility that a message a user wishes to recall may have already been delivered. Therefore a delay of at least 1 or 2 minutes is recommended to give your users time to realize they want to recall a message, send the recall request, and have time left over for MDaemon to process the request. However, because MDaemon is able to remove recalled messages from the Remote queue(s), where there might already be a delay, some administrators may find this deferred delivery timer unnecessary.

Recalling a Message

There are several ways that users can recall a message.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

1. In MDaemon Webmail, click the Recall button that is displayed when viewing a recently sent message in the Sent Items folder. If clicked before the recall time limit expires, Webmail will send a RECALL message to MDaemon.
2. Send a message to the mdaemon@example.com system account, with the word "RECALL" (without the quotes) as the message's Subject. This will recall the last message that you sent. It will only recall the last message.
3. In the Sent Items folder, locate the message you wish to recall, choose the "Forward as Attachment" option and send the message to the mdaemon@example.com system account, using "RECALL" as the message's Subject.
4. View a message's headers, copy the "Message-ID: <message-ID value>" header, and create a new message with "RECALL Message-ID: <message-ID value>" in the subject (without the quotes).

Regardless of the chosen recall method, MDaemon will send an email back to the user, saying whether or not the recall was successful. When a message is successfully recalled, MDaemon deletes the message from the queue as if it had never been sent. Optionally, if the *Delete recalled messages from account mail folders* option is enabled, MDaemon will also attempt to delete the recalled message from any local user's mail folder where it may have already been delivered. Messages sent to multiple recipients will all be recalled by a single request. Finally, the Message Recall system does not work without the `X-Authenticated-Sender` header to provide security and keep others from recalling messages they did not originate. Therefore, the option to disable that header 485 will be over-ridden if Message Recall is enabled.

Message Recall

Enable message recall
Click this checkbox to activate the message recall system. The option is disabled by default.

Delete recalled messages from account mail folders
Check this box if you also wish to delete recalled messages from the mail folders of your local MDaemon accounts if they have already been delivered before the message is recalled. This can cause messages to disappear from local user mail clients and phones. The option is disabled by default.

Defer message delivery for this many minutes XX (0-15 minutes)
This is the number of minutes that MDaemon will hold incoming messages from authenticated local users. If a RECALL message is received during the delay period then MDaemon will delete the referenced message before any delivery attempt has been made. This option can be set to 0-15 minutes. 1 minutes is the default setting.

Do not defer messages if recipient has a mailbox on this server
Check this box if you do not wish to defer messages when the recipient's mailbox is located on the same MDaemon server as the sender. Note: when using the "*Delete recalled messages from account mail folders*" option

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

above, even messages that were already delivered can be recalled and deleted from a user's mailbox.

The last [xx] authenticated messages sent are eligible for recall
MDaemon remembers the message IDs and locations of a specified number of the most recent emails sent by authenticated users. Recall attempts will fail if the message being recalled isn't within that group of messages. Therefore when using the *Delete recalled messages from account mail folders* option above, this makes it possible to recall messages right out of user mailboxes even after they've already been delivered. By default this option is set to 1000 messages.

Deferred Delivery

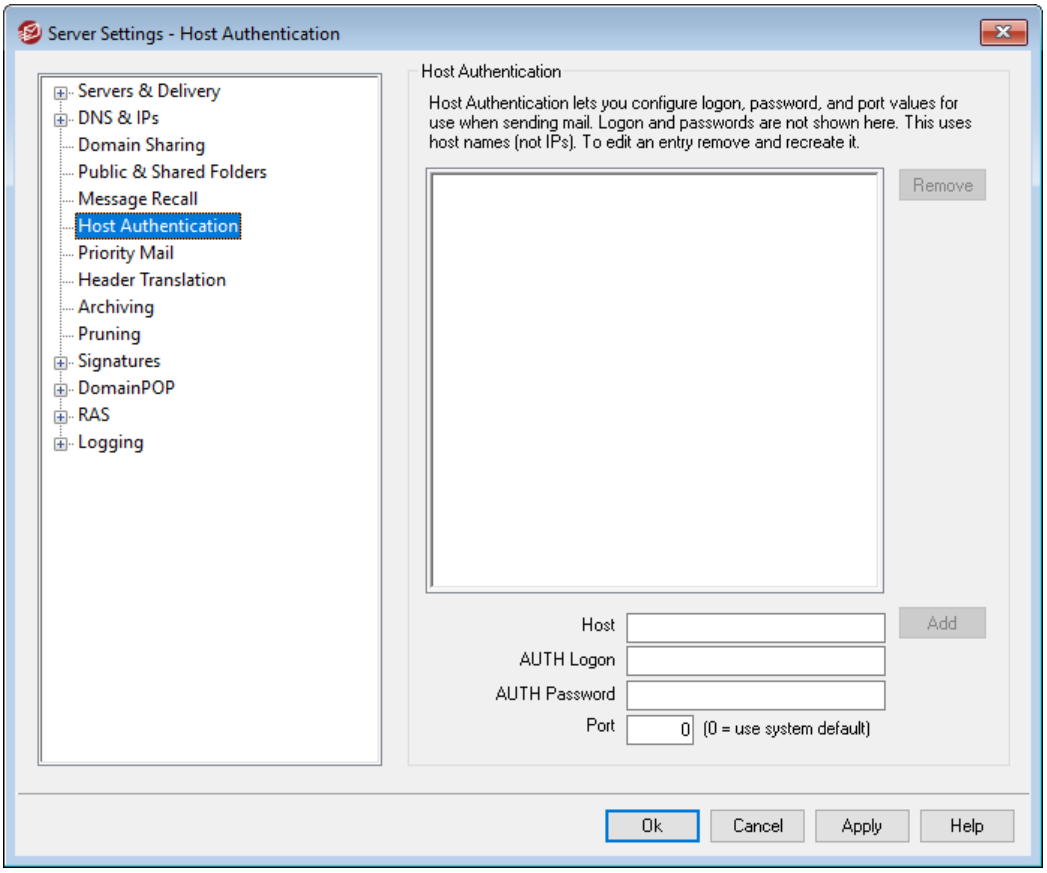
The Deferred Delivery option allows authenticated clients to send messages to be delivered at a scheduled date and time. Webmail includes this option, allowing users to click "Send Later" and specify the date and time to send the message. The message includes the `Deferred-Delivery` message header containing the date and time to attempt to deliver the message. If the Message Recall option is enabled and a recall request is received for a message scheduled for deferred delivery, MDaemon will attempt to remove the recalled message.

Enable deferred delivery
Enable this option if you wish to allow authenticated clients to use the `Deferred-Delivery` header to schedule messages for deferred delivery. When this option is enabled, Webmail users will have the **Send Later** option available in the WorldClient and Lookout themes. The option is disabled by default.

Replace 'Date:' with current time when message is released
Enable this option if you wish to replace the 'Date:' header with the current date and time when a message is released from the Deferred Queue. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.6 Host Authentication

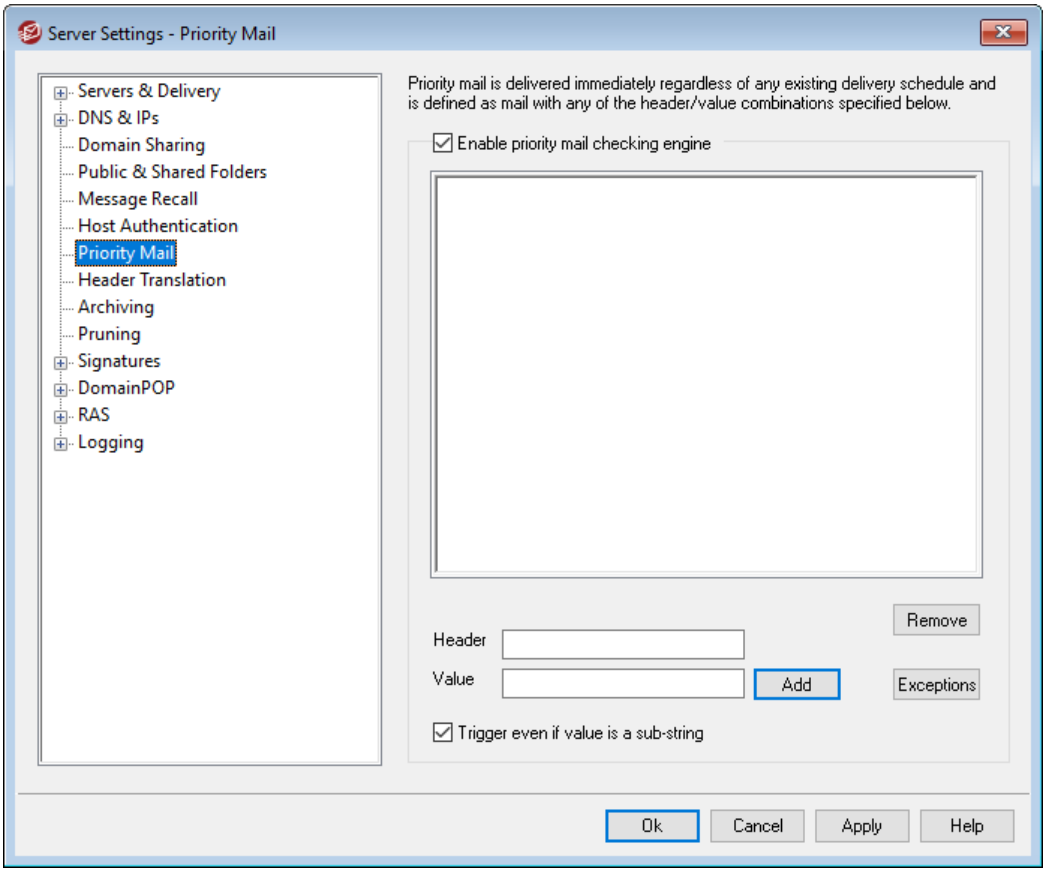


Host Authentication

Use this screen to configure logon, password, and port values for any host. When MDaemon sends SMTP mail to that host the associated credentials found here will be used. Please note that these credentials are a fallback and are only used when other more task-specific credentials are unavailable. For example, if you configure logon and password settings for the Account Editor's forwarding options or the Gateway Manager's Dequeuing options, or any of the many other task specific settings, then those credentials are used and supersede any that are configured here. This feature works with host names only (not IP addresses).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.7 Priority Mail



The Priority Mail screen is reached from the "Setup » Server Settings » Priority Mail" menu selection. It is used to define what constitutes Priority Mail on your system. Priority mail is delivered immediately by MDaemon regardless of scheduled mail processing intervals. When a new message arrives, MDaemon inspects its headers for a set of header/value combinations that you have specified on this dialog. If it finds them, it considers the message a high priority item and attempts to deliver it immediately.

Priority Mail Engine

Enable priority mail checking engine
Check this box to enable the Priority Mail feature. MDaemon will inspect incoming messages for priority status.

Header
Enter the message header in this field. Do not include the ending colon character.

Value
Enter the value that must be found in the specified header in order for the message to be considered high priority.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Trigger even if value is a sub-string
When entering a new Priority Mail setting you may select this feature to enable priority matching of a portion (or sub-string) of a header value. For example, you could create a Priority Mail Setting for the "`To`" header with the value "`Boss`". Then, any email containing "`Boss@anything`" in that header would be considered Priority Mail. If an entry is created without this feature enabled then the value of the header must match the entry exactly; matching only a portion will not be sufficient.

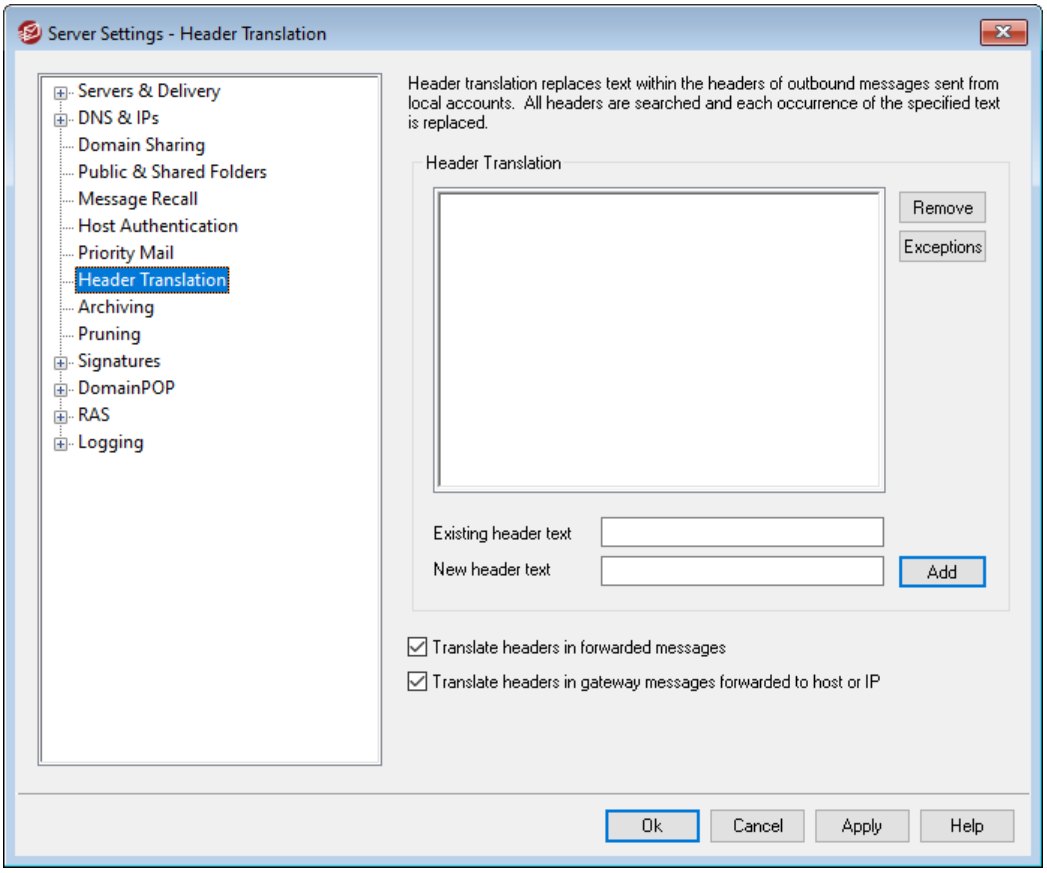
Add
After entering the Header/Value information in the specified text boxes, and after specifying whether this entry will apply to sub-strings, click the *Add* button to create the new Priority Mail entry.

Remove
Click this button to remove a selected entry from the *Current Priority Mail Settings* window.

Exceptions
This allows you to define field/value combinations that will cause a message to be considered an exception to the priority mail settings. This gives you more flexible control over this feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.8 Header Translation



The Header Translation feature can change any portion of text found within a header to a new value whenever a message is detected which must leave your domain destined for a remote host. You specify the text you want to search for and its corresponding replacement value. MDaemon will then search through all the headers in the message and make the replacements. You may also specify headers that MDaemon should **not** modify (such as "Subject:" or "Received:" headers) by clicking the *Exceptions* button on this dialog.

This feature is necessary for some MDaemon configurations in which the local domain name is fictitious or different from the domain name that must appear on outbound mail. In such a situation, Header Translation could be used to change every occurrence of "`@localdomain`" to "`@RemoteDomain`".

Header Translations

This list contains the portions of text that MDaemon will scan for in the outbound message headers, and the text that will be substituted when a match is found.

Remove
Select an entry in the Current Header Translations list and then click this button to remove it from the list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Exceptions
Click this button to open the Header Translation Exceptions 122 dialog. This dialog is used for specifying any Headers that you wish to be omitted from the Header Translation process.

Existing header text
Type the text that you want to be replaced when it is found within the headers of any outbound message.

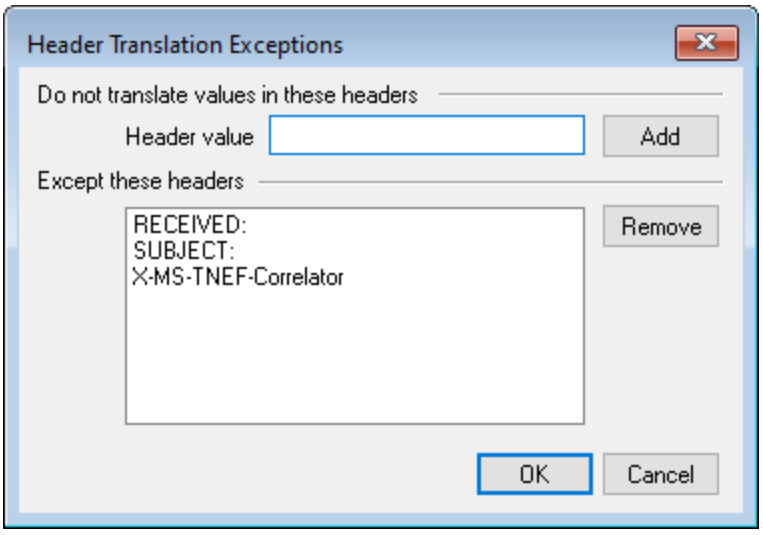
New header text
This text will be substituted for that which you specified in the *Existing header text* field.

Add
Click this button to add the above text parameters to the *Header Translation* list.

Translate headers in forwarded messages
Click this checkbox to cause the header translations to apply also to messages automatically forwarded from a local domain to a non-local domain.

Translate headers in gateway messages forwarded to host or IP
Click this check box if you want the headers to be translated in forwarded domain gateway mail. See the Forwarding 252 screen of the Gateway Editor for more information.

3.1.8.1 Header Translation Exceptions



Do not translate values in these headers

Header value
Enter any header that you want to be omitted from the Header Translation 121 process.

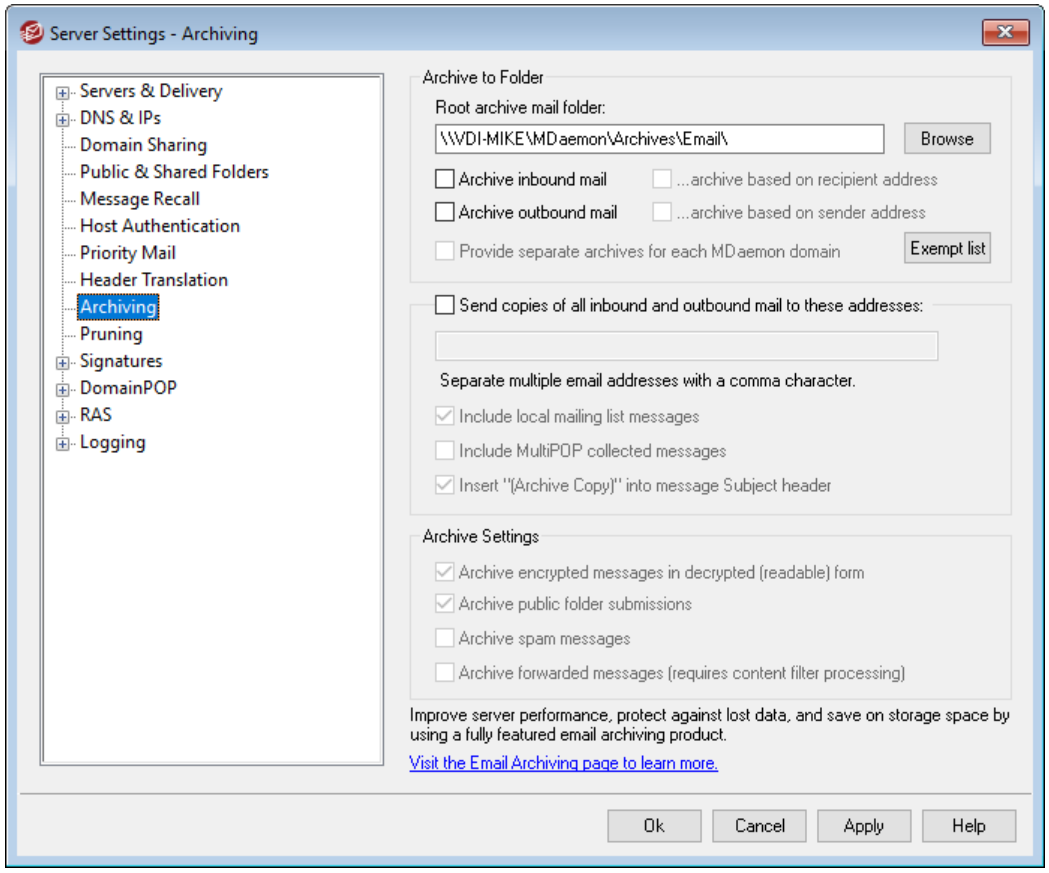
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add
Click this button to add a new header to the list.

Except these headers
MDaemon will not scan these headers when it is substituting header text.

Remove
Select a header in the list and then click this button to remove it.

3.1.9 Archiving



Use this feature to archive all inbound or outbound messages to a folder. The default location for this folder is `C:\MDaemon\Archives\Email\`, but you can set it to any folder you choose. You can choose to archive inbound messages addressed to your local users, outbound messages from your local users, or both. Mailing list traffic, messages being relayed, system-level messages, and autoresponders are never archived. Neither are spam messages or messages with viruses.

Inbound and outbound messages will be stored in `\In\` and `\Out\` subfolders, respectively. They can be further subdivided by using the *...archive based on recipient address* and *...archive based on sender address* options below. Also, separate archives

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

can be maintained for each domain by using the *Provide separate archives for each MDaemon domain* option.

Archived messages are saved in the final state in which they appear in the local user's mail folder, or in the "ready to be delivered" state for outbound messages. This means that if you, for example, have the content filter make some change to a message, such as adding a header to it, then the archived message will contain that change.

To browse the archive folder use one of your mail accounts (or create a new one) and point its Mail Folder 700 to the same folder used for the archive. If multiple people need access to the archive then log in to the archive account and share 726 the desired folders using its Access Control List 302.

There is a hidden, system queue located at: "`\MDaemon\Queues\ToArchive\`". This queue is checked at regular intervals for messages that have been placed there manually, by a plugin, or otherwise. When a message is found there it is immediately archived and deleted. If messages are found that are not eligible for archiving then they are simply deleted. The Routing screen/log will show details whenever a message is successfully archived.

Archive to Folder

Designate your archive mail folder here. By default it is set to `C:\MDaemon\Archives\Email\`, but you can set it to any folder you choose.

Archive inbound mail
Click this check box to save a copy of all messages that are going to a local user. Mailing list messages and messages containing a virus are not archived.

...archive based on recipient address
Click this option if you want the inbound mail archive to be categorized by the recipient's email address.

Archive outbound mail
Click this check box to save a copy of all messages that are from a local user. Mailing list messages and messages containing a virus are not archived.

...archive based on sender address
Click this option if you want the outbound mail archive to be categorized by the sender's email address.

Provide separate archives for each MDaemon domain
Click this option if you want to maintain a separate archive for each domain.

Exempt list
Click this button to open the Archiving Exempt List. Here you can list "to" and "from" addresses that you wish to exempt from archiving.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send copies of all inbound and outbound mail to these addresses

Enter one or more addresses to which you wish to send archival messages. Multiple addresses must be separated by a comma. You may specify local and remote addresses and address aliases.

Include local mailing list messages
When this option is enabled, copies of local mailing list messages will also be sent to the addresses.

Include MultiPOP collected messages
Enable this option if you wish to send messages collected through MDaemon's MultiPOP feature.

Insert "(Archive Copy)" into message Subject header
When this option is enabled, "(Archive Copy)" will be inserted in the `Subject:` header of sent messages.

Archive Settings

Archive encrypted messages in decrypted (readable) form
By default, unencrypted copies of encrypted messages are stored in the archive. If, however, a message can't be decrypted then the encrypted form will be stored instead. Disable this option if you would rather store encrypted versions even when decryption is possible.

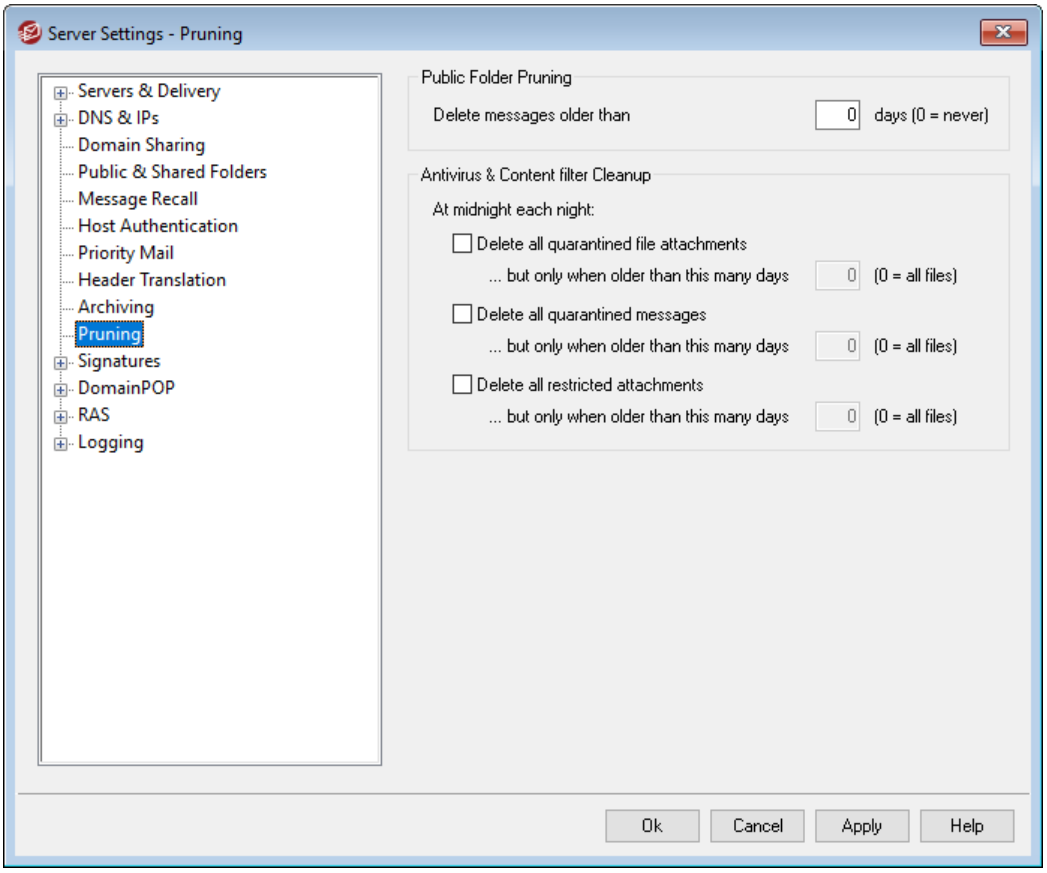
Archive public folder submissions
By default, messages sent to public folder submission addresses are archived. Disable this option if you do not wish to archive those messages.

Archive spam messages
Enable this option if you want the archives and sent copies to include messages that are marked as spam.

Archive forwarded messages (requires content filter processing)
Enable this option if you want the archives and sent copies to include messages that are forwarded. By default these are not archived.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.10 Pruning



Public Folder Pruning

Delete messages older than XX days (0=never)
Specify a number of days in this option if you want old messages to be deleted from Public Folders 110.

Antivirus & Content Filter Cleanup

Delete all quarantined files
Click this option if you want all quarantined file attachments to be deleted each night.

...but only when older than this many days [xx] (0 = all files)
By default all quarantined files will be deleted. Specify a number of days in this option if you only wish to delete files that are older than that value.

Delete all quarantined messages
Click this option if you want all quarantined messages to be deleted each night.

...but only when older than this many days [xx] (0 = all files)
By default all quarantined messages will be deleted. Specify a number of days in this option if you only wish to delete messages that are older than that value.

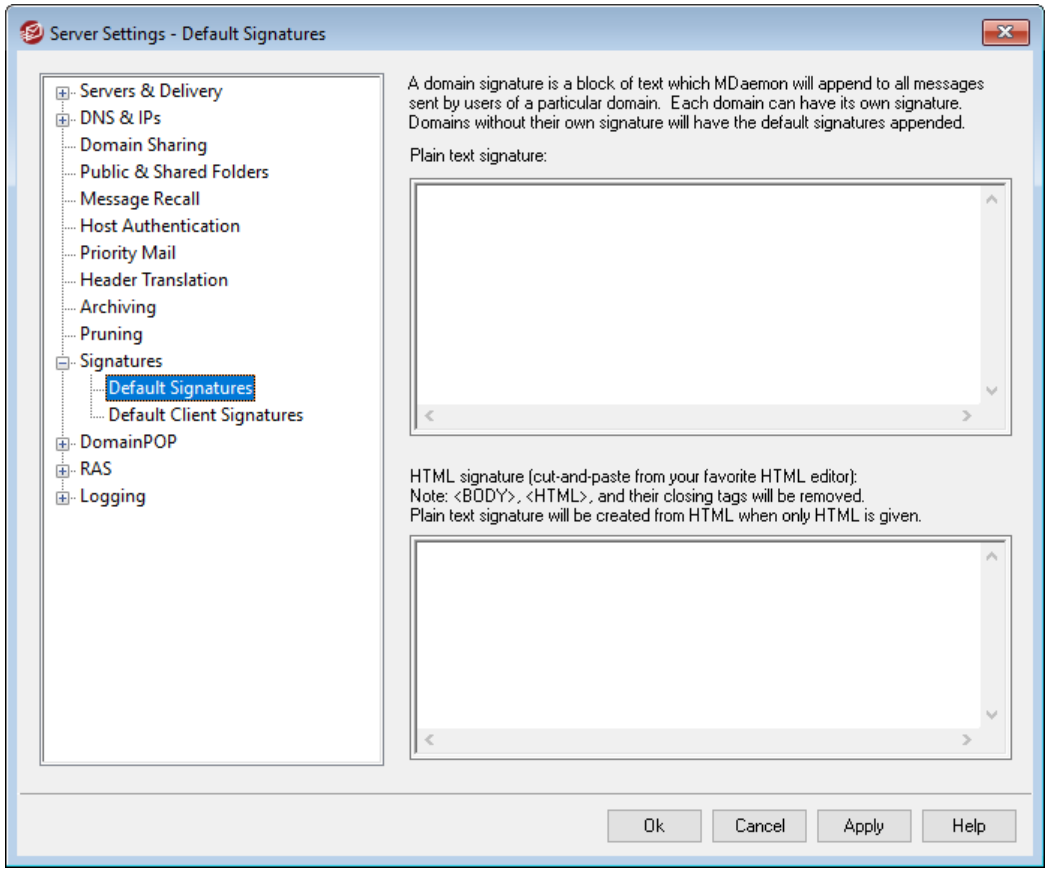
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete all restricted attachments
Click this option if you want all restricted attachments to be deleted each night.

...but only when older than this many days [xx] (0 = all files)
By default all restricted attachments will be deleted. Specify a number of days in this option if you only wish to delete restricted attachments that are older than that value.

3.1.11 Signatures

3.1.11.1 Default Signatures



Use this screen to append a signature to all messages sent by your MDaemon users. Use the Signatures 195 screen on the Domain Manager if you wish to use a different signatures for users of specific domains—when a domain-specific signature exists it will be used instead of the Default Signature. Signatures are added to the bottom of messages, except for mailing list messages using a footer 287, in which case the footer is added below the Signature. You can also use the Account Editor's Signature 737 feature to add individual signatures for each Account. Account signatures are added just before Default or Domain Signatures.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature to be used in the text/html part of multipart messages. If a signature is included here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html will be used to create one.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

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

There are also several ways you can insert inline images into signatures from within MDaemon's Remote Administration 341 web interface:

- On the Default Signatures screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab.
- On the Default Signatures screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Default Signatures screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Default Signatures screen's HTML editor with Chrome, FireFox, MSIE 11+

<body></body> and <html></html> tags are not allowed in signatures and will be removed when found.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Users can control the placement of MDaemon signatures in their emails by placing any of the **Signature Selector** macros into a message wherever they want the signature to appear.

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
Instant Messaging and Web	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
Address	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
Business Related	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

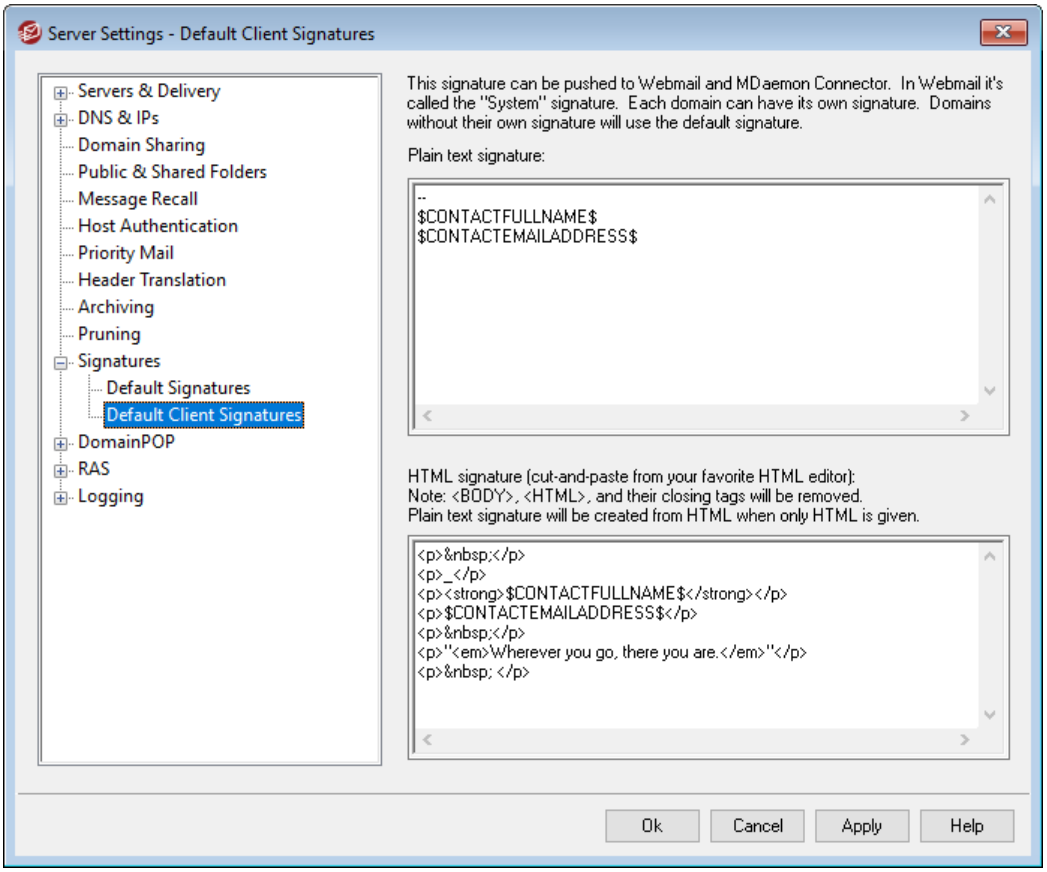
Business assistant	$CONTACTBUSINESSASSISTANT$
Business assistant phone	$CONTACTBUSINESSASSISTANTPHONE$
Business main phone	$CONTACTBUSINESSMAINPHONE$
Business phone	$CONTACTBUSINESSPHONE$
Business phone 2	$CONTACTBUSINESSPHONE2$
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Domain Manager » Signatures 195
Account Editor » Signature 737

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.11.2 Default Client Signatures



Use this screen to create a default client signature that you can push to MDaemon Webmail[333] and MDaemon Connector[397], to be utilized by your users when composing email messages. You can use the macros[133] listed below to personalize the signature, so that it will be unique for each user, including elements like the user's name, email address, phone number, and the like. Use the Client Signatures[200] screen on the Domain Manager if you wish to use a different signature for users of specific domains. When a domain-specific signature exists it will be used instead of the Default Client Signature. Use the *Push client signature*[333] option if you wish to push the client signature to Webmail and the *Push client signature to Outlook*[397] option if you wish to push it to MDaemon Connector. In Webmail's Compose options, the pushed client signature is called "System." For MDaemon Connector you can designate a name for the signature that will appear in Outlook.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html will be used to create one.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

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

There are also several ways you can insert inline images into signatures from within MDaemon's Remote Administration 341 web interface:

- On the Default Client Signature screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Default Client Signature screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Default Client Signature screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Default Client Signature screen's HTML editor with Chrome, FireFox, MSIE 11+

<body></body> and <html></html> tags are not allowed in signatures and will be removed when found.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Users can control the placement of MDaemon signatures in their emails by placing any of the **Signature Selector** macros into a message wherever they want the signature to appear.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Home fax	$CONTACTHOMEFAX$
Other phone	$CONTACTOTHERPHONE$
Instant Messaging and Web	
IM Address	$CONTACTIMADDRESS$
IM Address 2	$CONTACTIMADDRESS2$
IM Address 3	$CONTACTIMADDRESS3$
MMS Address	$CONTACTMMSADDRESS$
Home web address	$CONTACTHOMEWEBADDRESS$
Address	
Home address	$CONTACTHOMEADDRESS$
Home city	$CONTACTHOMECITY$
Home state	$CONTACTHOMESTATE$
Home zip code	$CONTACTHOMEZIPCODE$
Home country	$CONTACTHOMECOUNTRY$
Other address	$CONTACTOTHERADDRESS$
Other city	$CONTACTOTHERCITY$
Other state	$CONTACTOTHERSTATE$
Other zip code	$CONTACTOTHERZIPCODE$
Other country	$CONTACTOTHERCOUNTRY$
Business Related	
Business Name	$CONTACTBUSINESSCOMPANY$
Yomi Business Name	$CONTACTYOMICOMPANYNAME$
Business title	$CONTACTBUSINESSTITLE$
Business office	$CONTACTBUSINESSOFFICE$
Business department	$CONTACTBUSINESSDEPARTMENT$
Business manager	$CONTACTBUSINESSMANAGER$
Business assistant	$CONTACTBUSINESSASSISTANT$
Business assistant phone	$CONTACTBUSINESSASSISTANTPHONE$
Business main phone	$CONTACTBUSINESSMAINPHONE$
Business phone	$CONTACTBUSINESSPHONE$

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

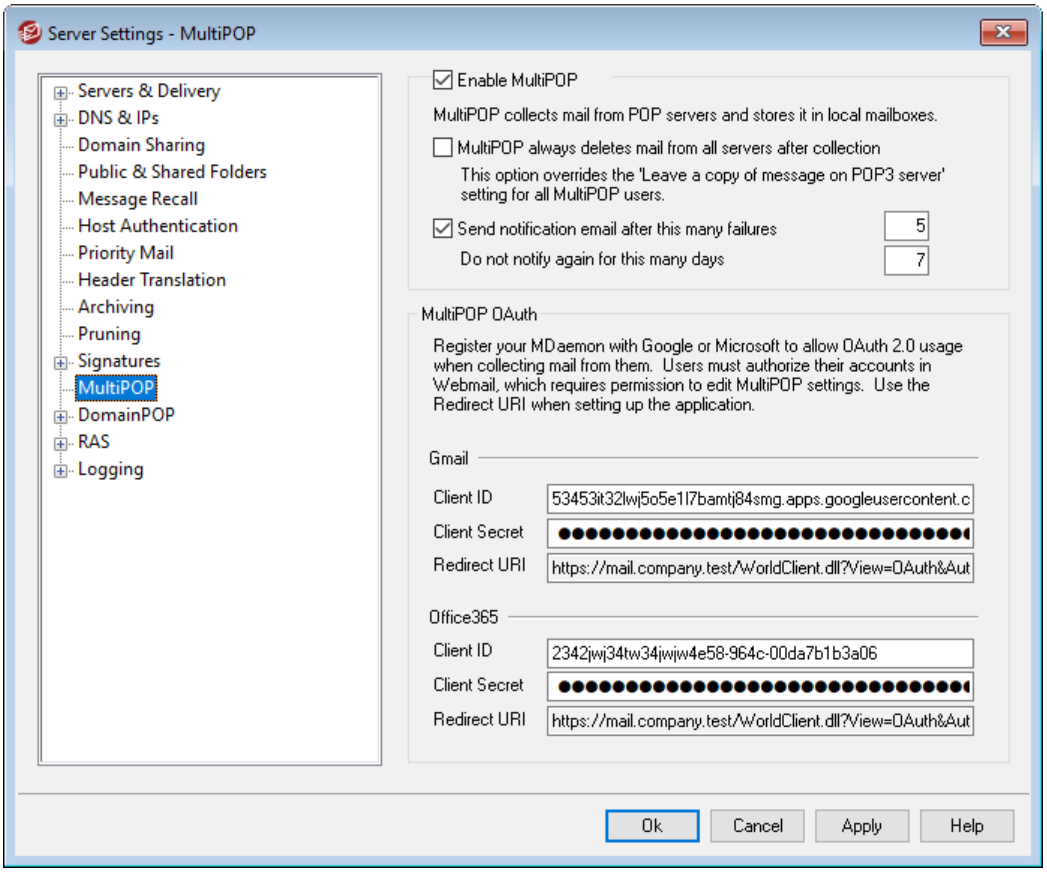
Business phone 2	$CONTACTBUSINESSPHONE2$
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Default Signatures 127
Domain Manager » Signatures 195
Domain Manager » Client Signatures 200
Account Editor » Signature 737
Webmail Settings 333
MC Client Settings » Signature 397

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.12 MultiPOP



Enable MultiPOP

Check this box to enabled the MultiPOP server. MultiPOP collects mail from POP servers on behalf of your users and stores it in the their local mailboxes. The MultiPOP feature allows you to create an unlimited number of POP3 host/user/password combinations for collection of mail messages from multiple sources. This is useful for your users who have mail accounts on multiple servers but would prefer to collect and pool all their email together in one place. Before being placed in the user's mailbox, MultiPOP collected mail is first placed in the local queue so that it can be processed like other mail having Autoresponders and Content filters applied to it. The scheduling options for MultiPOP are located at: Setup » Event Scheduling » Mail Scheduling » MultiPOP Collection 375.

MultiPOP always deletes mail from all servers after collection
Click this check box if you wish to override the *Leave a copy of message on POP server* option (located on the MultiPOP 723 screen of the Account Editor) for all users. All messages will be deleted from each MultiPOP server after they are collected.

Send notification email after this many failures
By default, MDaemon sends a notification email after multiple failures when checking a MultiPOP account. Since temporary failures can be common, this option allows you to specify how many consecutive failures it takes to trigger the notification, and the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

option below allows you to choose how many days to wait between those notifications. The content and recipients of the notification emails can be customized by editing `\MDaemon\App\MPOPFailureNotice.dat`. By default the notifications are sent to the MultiPOP account owner after 5 failures, no more than once every 7 days.

Do not notify again for this many days
By default MultiPOP failure notifications are sent no more than once every seven days. Use this option if you wish to adjust that interval.

MultiPOP OAuth

OAuth 2.0 is a modern authentication method that Gmail and Microsoft (Office) 365 are now requiring (or will soon require) as they disable support for legacy/basic authentication. In order for MDaemon's MultiPOP feature to use OAuth 2.0 to collect mail from Gmail or Office 365 on behalf of your users, you must register your MDaemon server with Google or Microsoft, respectively, creating an OAuth 2.0 application using the Google API Console or Microsoft's Azure Active Directory. This is similar to the procedure required for using MDaemon's Dropbox Integration 325 for your Webmail users.

To set up MultiPOP to collect mail from Gmail or Microsoft (Office) 365 for your users:

1. Turn on the **Enable MultiPOP** option above.
2. Follow the instructions below for **Creating and Linking Your MultiPOP OAuth App** 139 for Gmail or Office 365.
3. On the Account Editor's MultiPOP page 723, **Enable MultiPOP** for each user that you wish to allow to use MultiPOP to retrieve email from Gmail or Office 365.
4. Add the Gmail (`pop.gmail.com:995`) or Office 365 (`outlook.office365.com:995`) account for each of the users, and enable the **Use OAuth** option. Optionally you can have your users do this step for themselves in Webmail 308. **Note:** for Gmail accounts, each Gmail account must be added to the Test Users in your Gmail OAuth app (see the **Publishing Status** note in the *Creating and Linking Your MultiPOP OAuth App* 139 instructions below).
5. On the Account Editor's Web Services 703 page, enable the "**...edit MultiPOP settings**" option for each of those users.
6. Each user must sign in to Webmail, go to their **Mailboxes** page under Options, add their Gmail or Office 365 account (if you didn't already do that for them), and then click **Authorize** to sign in to their Gmail or Office 365 account and proceed through the steps to authorize MDaemon to collect their mail from that location.

Gmail/Office 365

Client ID
This is the unique Client ID assigned to your MultiPOP OAuth 2.0 app when you create it in the Google API Console or Microsoft Azure Active Directory portal. After you create your app, copy its Client ID and paste it here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Client Secret
This is the unique Client Secret assigned to your MultiPOP OAuth 2.0 app when you create it in the Google API Console or Microsoft Azure Active Directory portal. After you create your app, copy its Client Secret and paste it here. **Note:** when creating the Client Secret for an Azure app, you must copy it while creating the app because it will no longer be visible after that. If you fail to copy it at that time then you must delete the secret and create a new one.

Redirect URI
You must specify a Redirect URI when creating your OAuth 2.0 app for Gmail or Office 365. The Redirect URI displayed on the MultiPOP screen is an example built from your Default Domain's 174 SMTP host name 177, which should work for that domain's users when signing in to Webmail. You should add additional Redirect URIs to your app for any additional MDaemon domains your users go to when signing in to Webmail. For example, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" would work for any of your users who go to mail.example.com when signing in to Webmail. See: **Creating and Linking Your MultiPOP OAuth App** below for more information.

Redirect URI example:

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

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

Creating and Linking Your MultiPOP OAuth App

Step-by-step instructions for creating your MultiPOP OAuth 2.0 app.

For Google Gmail

Follow the steps below to create a Google application to allow MultiPOP to authenticate using OAuth 2.0 when collecting mail from Gmail for your users.

1. In your browser, go to the Google API console.
2. If on the Project List, click **NEW PROJECT**, or if on the Manage Resources page, click **(+) CREATE PROJECT**.
3. Type a **Project name,** then click **Edit** if you wish to edit the Project ID, or leave it set to the default value. **Note:** the Project ID cannot be changed after the project is created.
4. In the left pane, go to **APIs & Services | OAuth consent screen**.
5. Select **External**, and click **Create**.
6. Enter the **App name** (e.g. MultiPOP OAuth 2.0 for Gmail), a **Support email address** for users to contact, and a **Developer email address** for Google to contact about changes to your project. That is all that's required on this page for setup, but depending on your particular organization or verification requirements, you can also enter your company logo and links to your Terms of Service 356 and Privacy Policy. The **Authorized domains** fields will be filled in

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

for you automatically when you add the *Redirect URIs* in a later step below. **Note:** This info is used for the Consent screen that will be presented to users for authorizing MultiPOP to collect from Gmail.

7. Click **Save and Continue**.
8. Click **ADD OR REMOVE SCOPES**, and under "Manually add scopes," enter **https://mail.google.com/**. Click **ADD TO TABLE**, then click **Update**.
9. Click **Save and Continue**.
10. Under Test Users, click **ADD USERS**, enter each Gmail account from which you will be collecting mail, and click **ADD** (see the note below about your app's Publishing Status 140).
11. Click **Save and Continue**.
12. On Summary, click **BACK TO DASHBOARD** at the bottom of the page.
13. Click **Credentials** in the left pane, click **(+) Create Credentials**, and select **OAuth client ID**.
14. In the "Application type" drop-down box, select **Web application**, and under "Authorized redirect URIs", click **+ ADD URIs**. Enter the Redirect URI. The Redirect URI displayed on the MultiPOP screen is an example built from your Default Domain's 174 SMTP host name 177, which should work for that domain's users when signing in to Webmail. You should add additional Redirect URIs to your app for any additional MDaemon domains your users go to when signing in to Webmail. For example, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Gmail" would work for any of your users who go to mail.example.com when signing in to Webmail.
15. Click **CREATE**.
16. Copy the values in **Your Client ID** and **Your Client Secret** to the Gmail Client ID and Client Secret boxes on the MultiPOP page.

Publishing Status — These instructions are for creating a Google app with the Publishing Status set to "**Testing**". This requires you to add each specific Google account that will be using the app to collect their mail from Gmail, and it is limited to 100 users. Further, in Webmail when your users are asked to authorize MDaemon to collect their mail from Gmail, a warning message will be displayed "to confirm the user has test access to your project but should consider the risks associated with granting access to their data to an unverified app." Also, authorization expires after seven days, therefore each user would be required to reauthorize collection from Gmail every week.

If you wish to remove these requirements and limitations then you must change your status to "**In Production**", which may or may not require you to go through a verification process. For more information on app verification and publishing status, see the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

following Google articles: Setting up your OAuth consent screen and OAuth API verification FAQs.

For Microsoft (Office) 365

Follow the steps below to create a Microsoft Azure application to allow MultiPOP to authenticate using OAuth 2.0 when collecting Office 365 email for your users.

1. Go to the Microsoft Azure Active Directory page at the Azure Portal and click **App Registrations** in the left pane (you must sign-up for a free or pay-as-you-go Azure account if you don't have one already).
2. Click **+ New Registration**.
3. Enter an application name in the **Name** field (e.g. "Mailbox OAuth for Office 365").
4. For "Supported account types" select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.
5. For "Redirect URI" select **web** and then enter your Office 365 **Redirect URI**. The Redirect URI displayed on the MultiPOP screen is an example built from your Default Domain's 174 SMTP host name 177, which should work for that domain's users when signing in to Webmail. You should add additional Redirect URIs to your app for any additional MDaemon domains your users go to when signing in to Webmail. For example, "https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=Office365" would work for any of your users who go to mail.example.com when signing in to Webmail.
6. Click **Register**.
7. Make note of the **Application (client) ID** (there is a copy to clipboard button beside it). You can find this ID later by clicking **Overview** in the left pane.
8. If you need to add additional Redirect URIs, click the **Redirect URIs: 1 web** link on the right. Click **Add URI** and enter the URI, repeating as necessary, and click **Save**.
9. Click **API Permissions** in the left pane.
10. Click **+ Add a permission**.
11. Click **Microsoft Graph**.
12. Click **Delegated Permissions**.
13. Scroll down to **POP** and select **POP.AccessAsUser.All**, then under **User** select and **User.Read** (User.Read is already selected by default).
14. Click **Add permissions**.
15. In the left pane, click **Certificates & Secrets**.
16. Click **+ New Client Secret**.
17. Enter a description (e.g. "Client secret for Office 365 MultiPOP OAuth app").
18. Select how long before the client secret expires.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

19. Click **Add**.
20. Make note of the generated client secret in the **Value** field (there is a copy to clipboard button beside it). **NOTE:** the client secret will not be viewable again on this page—there will be a **Delete** icon beside the entry so that you can delete it and create a new client secret when necessary.
21. Enter the Application (client) ID and Client Secret values into the **Client ID** and **Client Secret** fields under the Office 365 section of MDaemon's MultiPOP page under Server Settings.

See:

Account Editor | MultiPOP 723
Mail Scheduling | MultiPOP Collection 375

3.1.13 DomainPOP

Use DomainPOP Mail Collection ("Setup » Server Settings » DomainPOP") to configure MDaemon to download mail from a remote POP mailbox for redistribution to your users. This feature works by using the POP3 protocol to download all the mail found in the ISP's POP mailbox associated with the specified logon. Once collected, the messages are parsed according to the settings provided on this dialog and then placed in user mailboxes or the remote mail queue for MDaemon to deliver, just as if the messages had arrived at the server using conventional SMTP transactions.

It is important to note that messages stored in mailboxes and retrieved using the POP3 protocol will be devoid of the important routing information (sometimes called the message's "envelope") that would ordinarily be supplied had the messages been delivered using the more powerful SMTP protocol. Without this routing information, MDaemon is forced to "read" the message and examine the headers in an attempt to determine to whom the message was originally intended. This is not an exact science to say the least. Message headers are sometimes notorious for their lack of sufficient information needed to determine the intended recipient. This lack of what would seem to be a fundamental characteristic of an email message - the recipient - may seem surprising but one must keep in mind that the message was never intended to be delivered to its recipient using the POP protocol. With SMTP, the contents of the message are irrelevant since the protocol itself dictates specifically to the server, during the mail transaction, the intended recipient of the message.

In order to allow for POP retrieval and delivery of mail messages in a reliable and consistent way, MDaemon employs a powerful suite of header processing options. When MDaemon downloads a message from a remote POP source it immediately parses all the relevant headers within that message and builds a collection of potential recipients. Every email address found in the headers that MDaemon inspects is included in the collection.

Once this process is complete, MDaemon's collection of recipients is divided into local and remote sets. Further, all addresses that are parsed and placed into the collection of potential recipients are processed through the Aliases 818 translator before being divided into local and remote sets. Every member of the local set (addresses with a domain that matches one of MDaemon's local domains) will receive a copy of the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

message. What happens to the remote set is governed by the settings in this dialog. You can elect to simply ignore these addresses, forward a summary listing of them to the postmaster, or honor them — in which case MDaemon will actually deliver a copy of the message to the remote recipient. Only under rare circumstances would the need to deliver these messages to remote recipients be warranted.

Care must be taken to prevent duplicate messages or endlessly looping mail delivery cycles. A common problem that results from the loss of the SMTP envelope manifests itself with mailing list mail. Typically, messages distributed by a mailing list do not contain within the message body any reference to the addresses of the recipients. Rather, the list engine simply inserts the name of the mailing list into the `TO:` field. This presents an immediate problem: if the `TO:` field contains the name of the mailing list then the potential exists for MDaemon to download this message, parse the `TO:` field (which will yield the name of the mailing list), and then dispatch the message right back to the same list. This would in turn deliver another copy of the same message back to the POP mailbox from which MDaemon downloaded the original message — thus starting the whole cycle over again. To cope with such problems mail administrators must take care to use the tools and settings that MDaemon provides to either delete mailing list mail or perhaps alias it in such a way that it will be delivered to the proper local recipient(s). You could also utilize the Routing Rules or Content Filters to deliver the message to the correct recipient(s).

Additional concerns when employing this sort of mail collection scheme revolve around the issue of unwanted message duplication. It is very easy for mail that is delivered to the ISP's POP mailbox using SMTP to generate unwanted duplicates, once it has been collected using DomainPOP. For example, suppose a message is sent to someone at your domain and a carbon copy is sent to another person at the same domain. In this situation, SMTP will deliver **two** copies of the same message to your ISP's mailbox — one for each recipient. Each of the two message files will contain references to **both** recipients — one in the `TO:` field and the other in the `CC:` field. MDaemon will collect each of these two identical message files and parse both addresses from each of them. This would result in both recipients receiving one unwanted duplicate message. To guard against this sort of duplication MDaemon uses a control which allows you to specify a header that MDaemon will use to check for duplication. The `Message-ID` field is ideal for this. In the above example, both messages are identical and will therefore contain the same `Message-ID` field value. MDaemon can use this value to identify and remove the second message during the download stage before it can be parsed for address information.

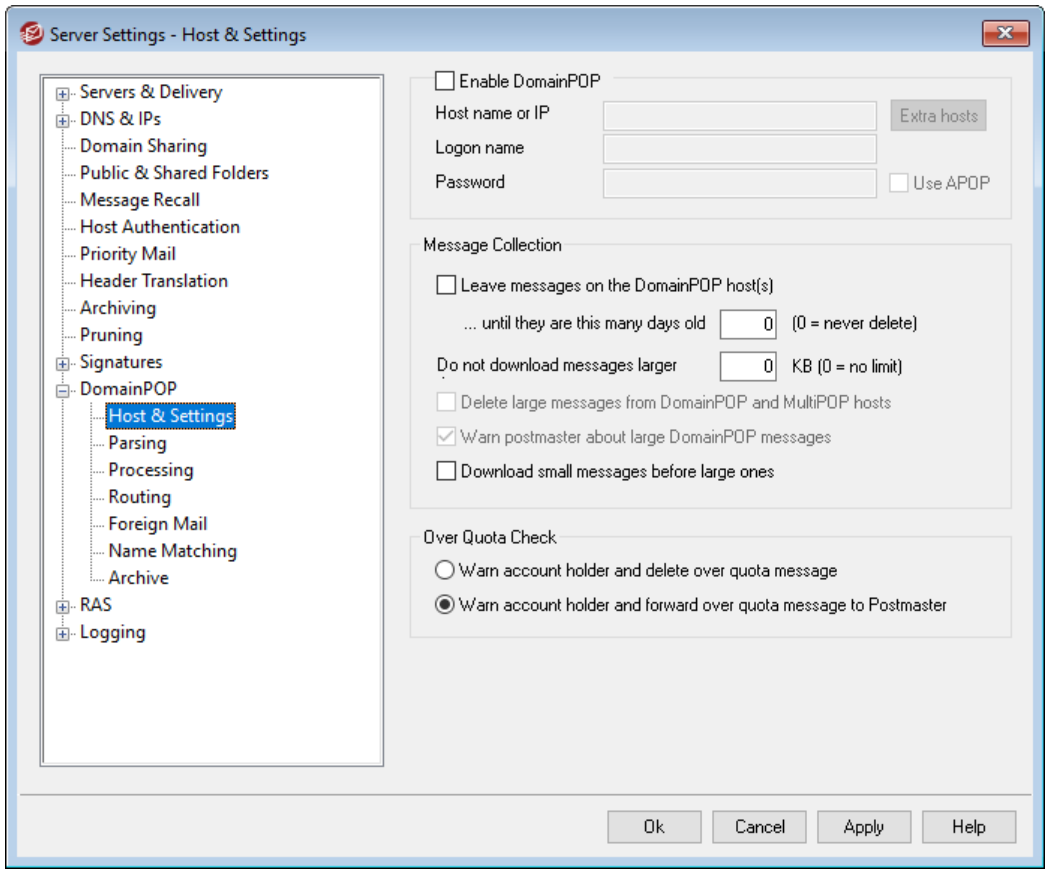
As a final measure guarding against duplicate messages and endless looping delivery cycles, MDaemon employs a means for detecting how many trips or "hops" a message has made through the transport system. Each time an SMTP mail server processes a message it "stamps" the message with a "Received" header. MDaemon counts all such headers when it encounters a message for the first time. If the total number of mail servers exceeds a specified value, it is likely the message is caught in a delivery loop and should be taken out of the mail stream and moved to the bad message directory. This value can be configured under the Retry Queue 856.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Content Filters 630
Mailing Lists 259

3.1.13.1 Host & Settings



DomainPOP Host Properties

Enable DomainPOP mail collection engine
If selected, MDaemon will use the setting provided on this screen to collect mail from a DomainPOP mail host for local redistribution.

Host name or IP
Enter your DomainPOP host's domain name or IP address here.

Extra hosts
Click this button to open the `DpopXtra.dat` file, on which you can designate extra hosts from which to collect DomainPOP mail. See the contents of that file for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Logon name
Enter your login of the POP account used by DomainPOP.

Password
Enter the POP or APOP account's password here.

Use APOP
Click this box if you wish to use the APOP command and CRAM-MD5 authentication when retrieving your mail. This makes it possible to authenticate yourself without having to send clear text passwords.

Message Collection

Leave messages on the DomainPOP host(s)
If selected, MDaemon will download but not remove the messages from your DomainPOP mail host.

...until they are this many days old (0=never delete)
This is the number of days that a message can remain on the DomainPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

Some hosts may limit the amount time that you are allowed to store messages in your mailbox.

Don't download messages larger than [XX] KB (0 = no limit)
Messages greater than or equal to this size will not be downloaded from your DomainPOP mail host. Enter "0" if you want MDaemon to download messages no matter the size.

Delete large messages from DomainPOP and MultiPOP hosts
Enable this option and MDaemon will delete messages that exceed the size designated above. The messages will simply be removed from the DomainPOP and MultiPOP mail hosts and will not be downloaded.

Warn postmaster about large DomainPOP messages
Check this option and MDaemon will send a warning to the postmaster whenever a large message is discovered in the DomainPOP mailbox.

Download small messages before large ones
Enable this checkbox if you want the message downloading order to be based on size — beginning with the smallest and proceeding to the largest.

This option retrieves smaller messages quicker but requires a larger amount of internal sorting and processing.

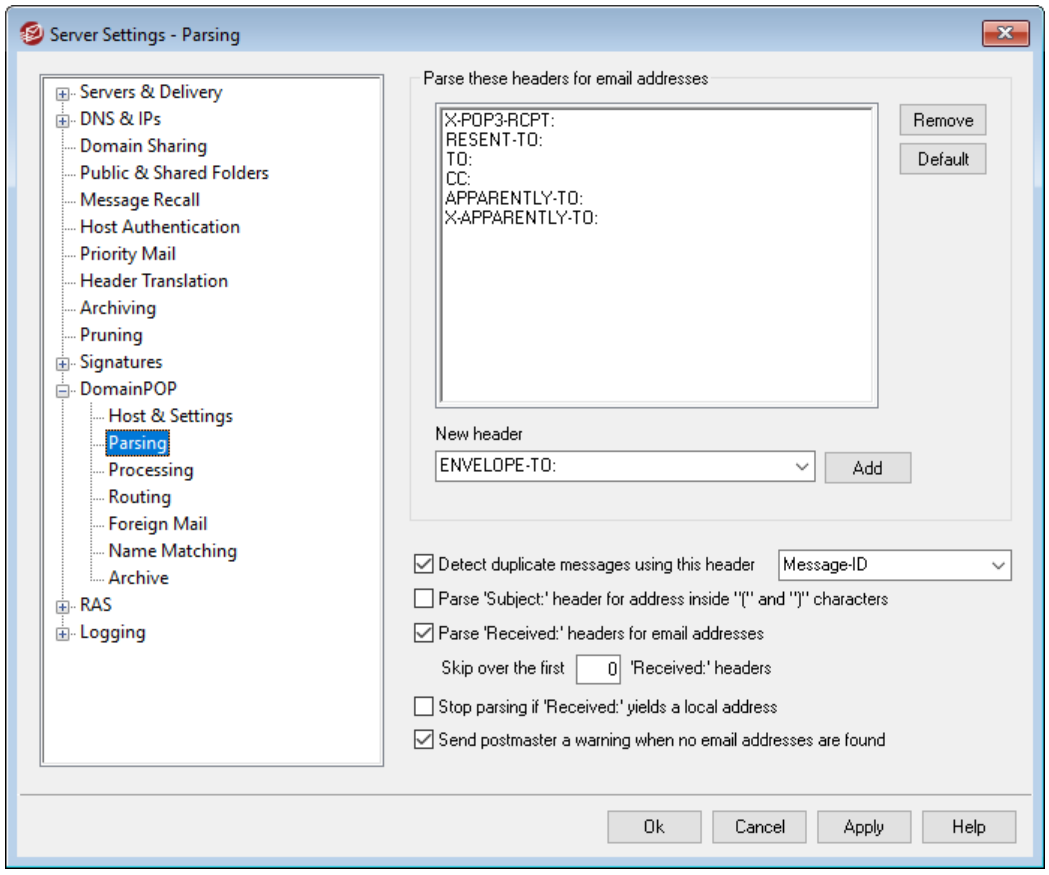
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Over Quota Check

Warn account holder and delete over quota message
When this option is chosen and a message is collected for an account that is over its quota (designated on the Quotas 715 screen of the account editor), MDaemon will delete the message and then send a message to the account holder stating that the account is over its limit.

Warn account holder and forward over quota message to Postmaster
When this option is chosen and a message is collected for an account that is over its quota, MDaemon will forward the message to the Postmaster and send a warning to the user letting him or her know that the account is over its limit.

3.1.13.2 Parsing



Parse these headers for email addresses

This area lists the headers that MDaemon will parse in an attempt to extract addresses. Every header listed here is checked for addresses.

Remove
This button will remove the selected entries from the header list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Default
This button will clear the current contents of the header list and add MDaemon's default list of headers. The default headers are typically sufficient to extract all addresses from the message.

New header
Enter the header you wish to add to the header list.

Add
After specifying a header in the *New header* option, click this button to add it to the list.

Detect duplicate messages using this header
If this option is selected MDaemon will remember the value of the specified header and will not process additional messages collected in the same processing cycle which contain an identical value. The `Message-ID` header is the default header used by this option.

Parse "subject:" header for address inside "(" and ")" characters
When this is selected and MDaemon finds an address contained in "( )" in the "Subject:" header of a message, this address will be added to the message's list of recipients along with any other parsed addresses.

Parse "Received" headers for email addresses
It is possible to store the recipient information ordinarily found only within the message's envelope in the "Received" message headers. This makes it possible for parsers of the mail message to be able to glean the actual recipient address by merely inspecting the Received headers later. Click this checkbox if you wish to parse valid addresses from all of the "received" headers found within the mail message.

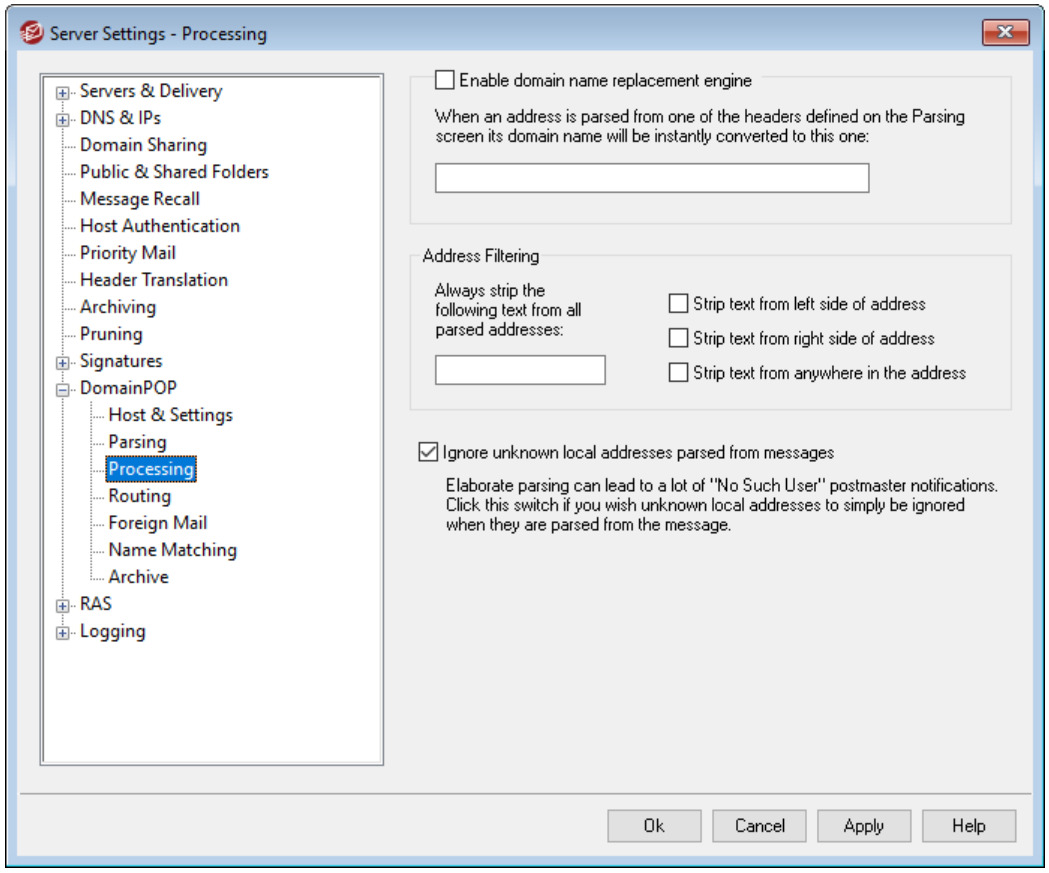
Skip over the first xx "received" headers
In some server configurations you may wish to parse Received headers but need to skip the first few of them. This setting allows you to enter the number of "Received" headers that MD will skip over before beginning its parsing.

Stop parsing if "Received" yields a valid local address
If while parsing a "received" header MDaemon detects a valid local address, this switch will cause all further parsing to stop and MDaemon will not search the message for more potential delivery addresses.

Send postmaster a warning when no email addresses are found
By default MDaemon sends a warning email to the postmaster when no addresses are found by the parsing process. Clear this checkbox if you do not wish to send this warning.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.13.3 Processing



Domain Name Replacement

Enable domain name replacement engine
This option can be used to reduce the number of aliases your site might require. When a message is downloaded, all domain names in all addresses parsed from that message will be converted to the domain name specified here.

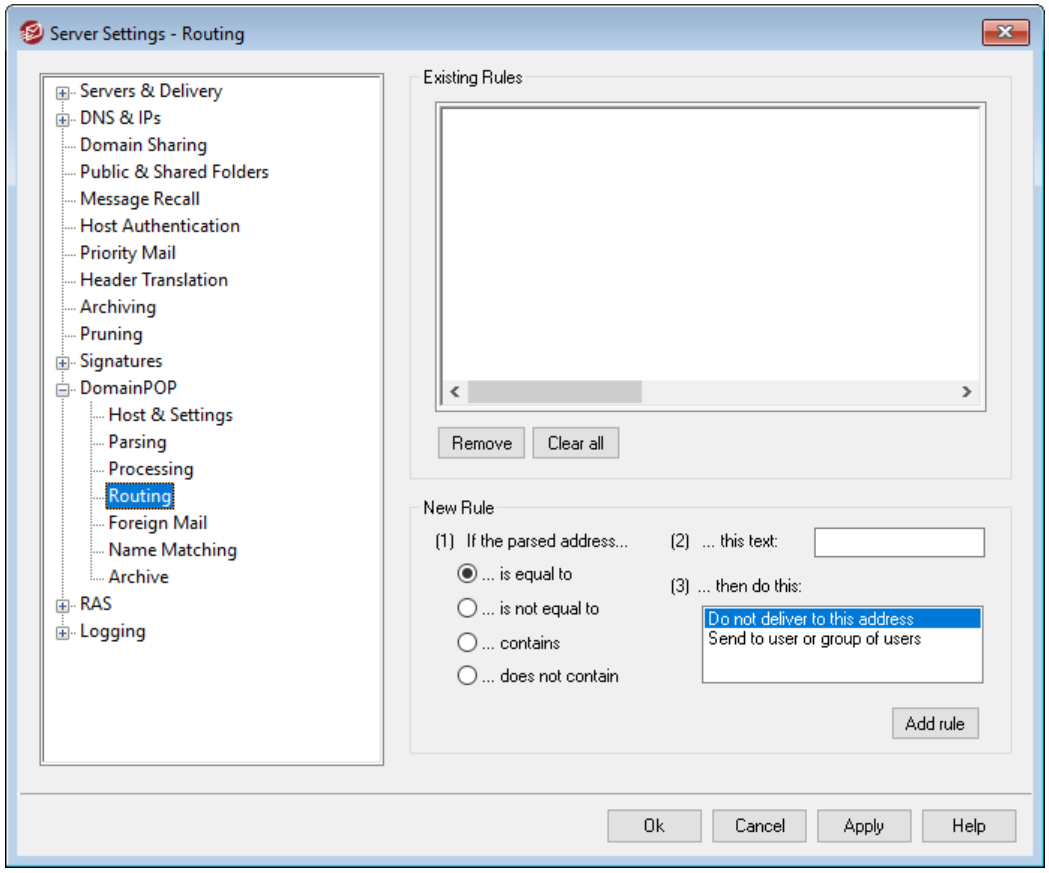
Address Filtering

Always strip the following text from all parsed addresses
Some hosts will stamp each message with a line that indicates who the recipient of the message should be, along with a bit of routing information appended to the address on either the left or right side. This stamp would be perfect to use for parsing the recipient address except that the additional routing information makes this impossible without a lot of account aliasing. Rather than do all that you can simply specify the value of this appended text in the edit control associated with this feature and MDaemon will strip any occurrence of this text from all addresses that it parses.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Ignore unknown local addresses parsed from messages
As mentioned above, the Domain Name Replacement feature will alter the domain name in all email addresses parsed from a message, converting it into the one you specify on this screen. This could create some addresses that do not have a corresponding account your server. Because the domain name but not the mailbox would be valid, MDaemon would consider such addresses unknown local users. Such mail typically generates a "No Such User" message. Check this box if you wish to prevent the Domain Name Replacement Engine from causing these messages to be generated.

3.1.13.4 Routing



Existing Rules
This list shows you the rules that you have created and will be applied to your messages.

Remove
Select a rule from the list and then click this button to delete it.

Clear all
This button removes all existing rules.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New Rule

(1) If the parsed address...

Is equal to, is not equal to, contains, does not contain
This is the type of comparison that will be made when an address is compared to this routing rule. MDaemon will search each address for the text contained in the *"...this text*" option below and then proceed based upon this option's setting — does the address's complete text match exactly, not match exactly, contain the text, or not contain it at all?

(2) ...this text:
Enter the text that you want MDaemon to search for when scanning the addresses.

(3) ...then do this:
This option lists the available actions that can be performed if the result of the rule is true. You can choose from the following actions:

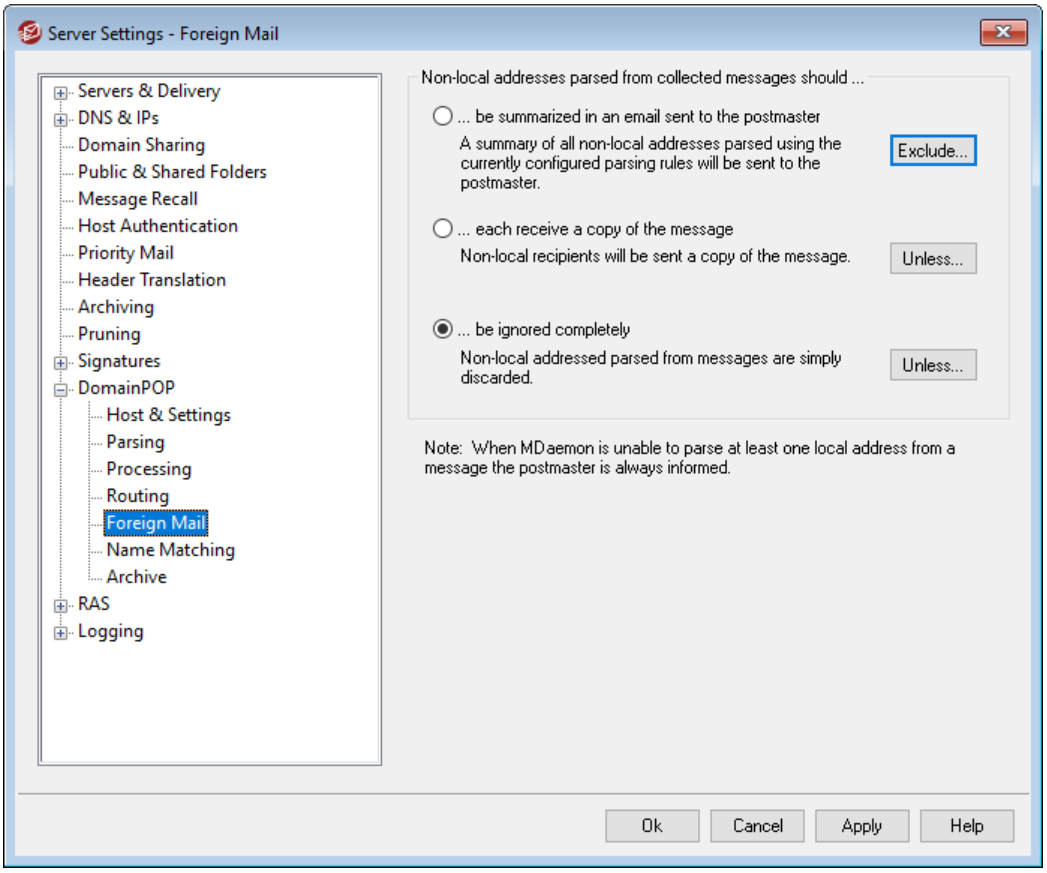
Do not deliver to this address - Selecting this action will prevent the message from being delivered to the specified address.

Send to user or group of users - Selecting this action will open dialog on which you can designate a list of email addresses that should receive a copy of the message being processed.

Add rule
After setting the new rule's parameters, click *Add rule* to add it to the list of rules.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.13.5 Foreign Mail



Non-local addresses parsed from collected messages should...

...be summarized in an email sent to the postmaster
If this option is selected MDaemon will send a single copy of the message to the postmaster along with a summary of the non-local addresses that the parsing engine extracted using the current set of headers and parsing rules.

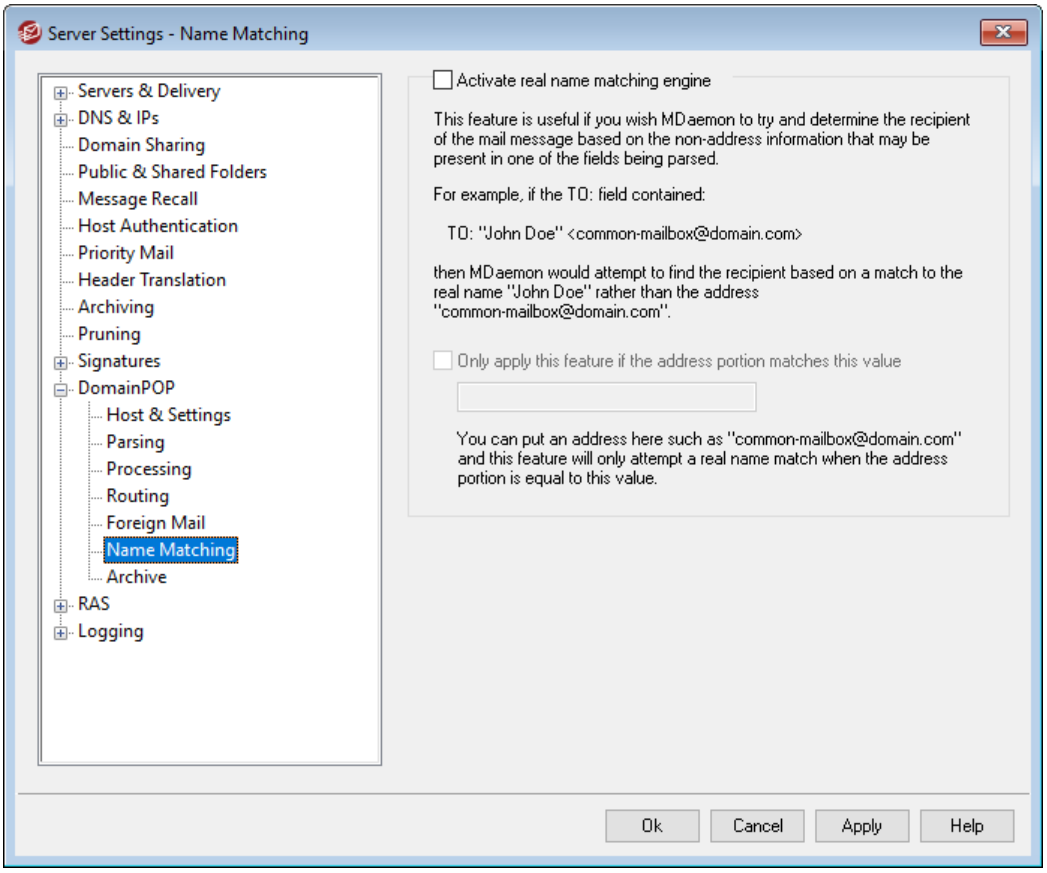
...each receive a copy of the message
If this option is selected MDaemon will deliver a copy of the message to any non-local recipient that it finds within the inspected headers.

...be ignored completely
If this option is selected MDaemon will remove from the recipient list any address that is non-local. It will be as if MDaemon never parsed remote addresses from the original downloaded message.

The *Exclude...* and *Unless...* buttons allow you to define addresses that will be treated as exceptions to the the selected option.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.13.6 Name Matching



The Name Matching feature is only active in conjunction with the DomainPOP Mail Collection engine. If you wish to use this feature, you must make sure that you have DomainPOP enabled. DomainPOP can be reached from the "Setup » Server Settings » DomainPOP" menu selection.

Real Name Matching Engine

Activate real name matching engine
This feature allows MDaemon to determine who should receive a DomainPOP collected message based not upon the parsed email address but upon the text included with the address. This is typically the recipient's real name.

For example, a message's TO header might read:

```
TO: "Michael Mason" <user01@example.com>
```

or

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
TO: Michael Mason <user01@example.com>
```

Name Matching ignores the "user01@example.com" portion of the address. It instead extracts the "Michael Mason" portion and checks to see if this is an MDaemon user. If a match is found to an account's real name then that account's local email address is used for delivery purposes. If no match is made then MDaemon reverts to delivering the message to the email address parsed from the data (user01@example.com in this example).

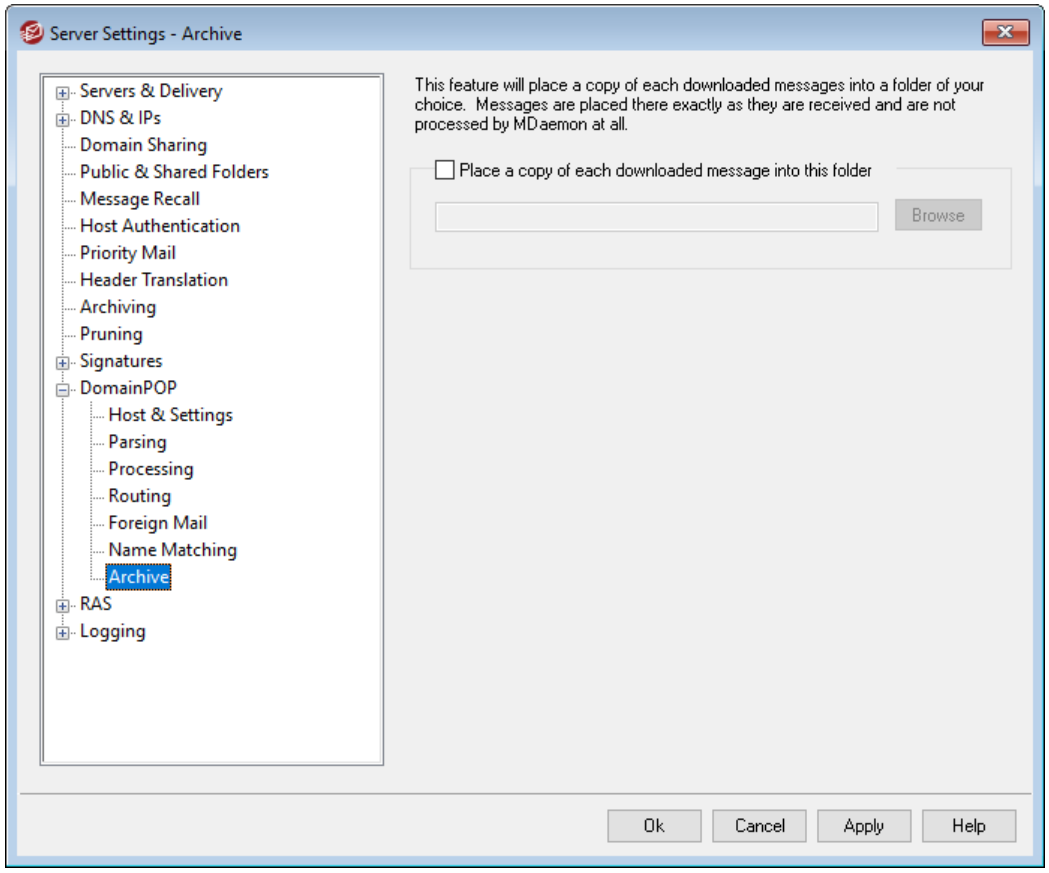
The real name portion of the address may not contain a comma, semi-colon, or colon character.

Only apply this feature if the address portion matches this value
This option allows you to specify an email address that must be present in the extracted data in order for the real name matching process to proceed. This allows you a measure of control over when the Name Matching feature will be employed. For example, you can specify an address such as "user01@example.com" and then only addresses matching this value will be candidates for Name Matching.

Suppose you specify "user01@example.com" in this option. This means that "**`TO: 'Michael Mason' <user01@example.com>`**" will be a candidate for Name Matching while "**`TO: 'Michael Mason' <user02@example.com>`** will not.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.13.7 Archive



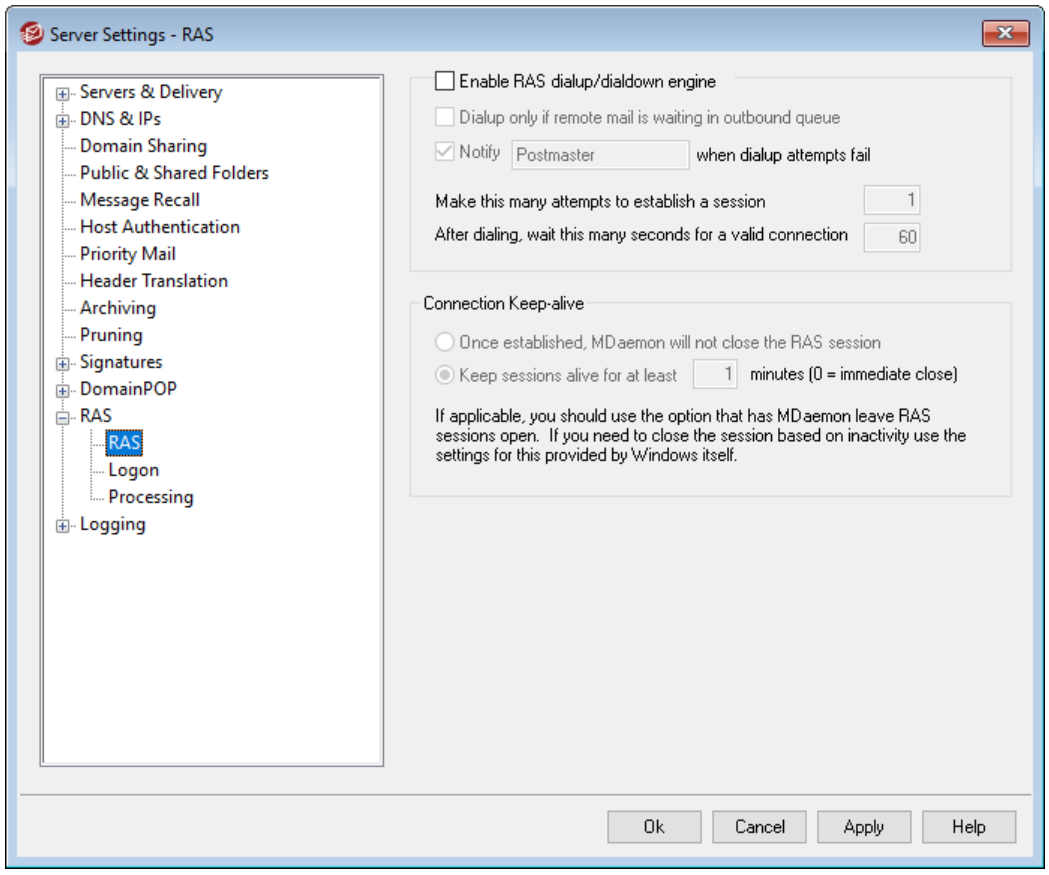
Archive

Place a copy of each downloaded message into this folder
This is a safety feature to ensure that you don't lose any mail due to unforeseen parsing or other errors that might occur when downloading mail in bulk quantities. Check this box if you wish to save a copy of each downloaded message into the folder that you specify. These copies are placed in the folder exactly as they are received and are not processed by MDaemon at all.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.14 RAS

3.1.14.1 RAS



Click the "Setup » Server Settings » RAS" menu selection to configure your RAS Dialup settings. This dialog will only be available if you have Remote Access Services installed on your system. It is used by MDaemon when you need to dial up your ISP just prior to a Remote Mail processing event.

Enable RAS dialup/dialdown engine
When this option is enabled, MDaemon will use the settings specified here to make a connection to a remote host before sending or receiving remote mail.

Dialup only if remote mail is waiting in outbound queue
When this box is checked, MDaemon will not dial the ISP unless there is remote mail waiting in the Remote queue. This may be beneficial in some circumstances but be aware that if MDaemon does not dial up then it cannot do any mail **collecting** either (unless it is delivered across the local LAN).

Notify [address] when dialup attempts fail
When selected, MDaemon will send a message to the specified address when a dialup event fails because of some error.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Make this many attempts to establish a session
MDaemon will attempt to connect to the remote host this many times before giving up.

After dialing, wait this many seconds for a valid connection
This value determines how long MDaemon will wait for the remote computer to answer and complete the RAS connection.

Connection Keep-alive

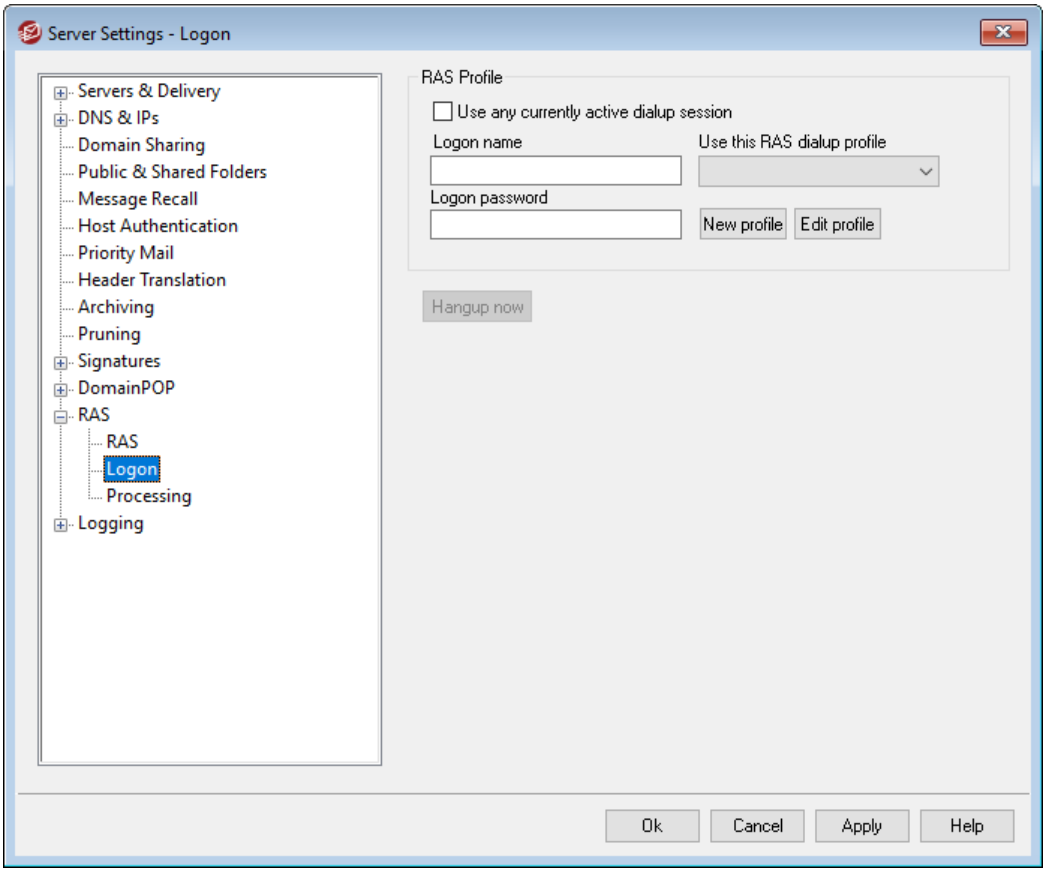
Once established, MDaemon will not close the RAS session
By default, MDaemon will shut down a created connection immediately after all mail transactions have been completed and the session is no longer in use. Selecting this option will cause the connection to remain open even after all transactions have been completed.

MDaemon will never close a connection that it did not create.

Keep sessions alive for at least xx minutes
If enabled, this option will cause an MDaemon created RAS session to remain open for at least the number of minutes specified or until all mail transactions have been completed, whichever is greater.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.14.2 Logon



RAS Profile

Use any currently active dialup session
Click this checkbox if you want MDaemon to be able to utilize other connection profiles when it detects that one is active. Whenever it is time to dialup, MDaemon will first check to see if there is an active connection that it can use rather than dialing.

Logon name
The value specified here is the user identification or login name that will be passed to the remote host during the authentication process.

Logon Password
The value specified here is the password that will be passed to the remote host during the authentication process.

Use this RAS dialup profile
This drop-down list box allows you to select a session profile that has been previously defined through windows Dialup Networking or Remote Access Services Setup.

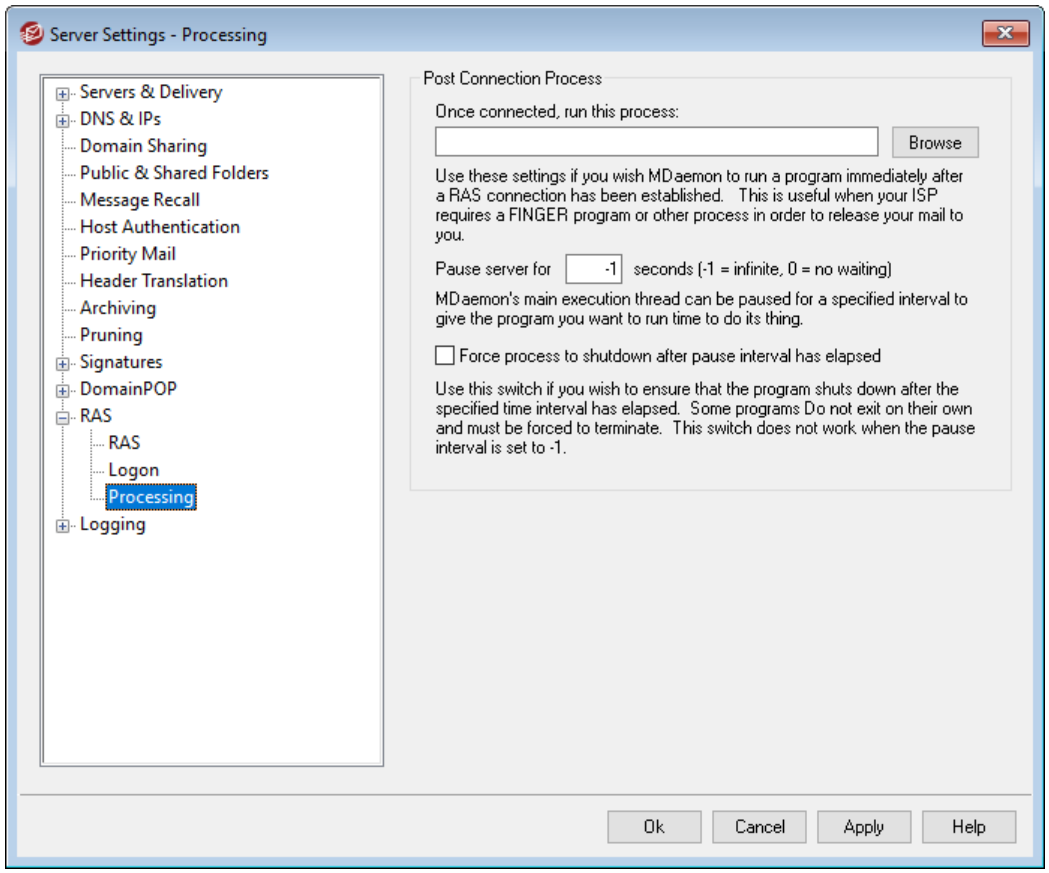
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New profile
Click this button to create a new Dialup Networking or Remote Access Services profile.

Edit profile
Click this button to edit the currently selected Dialup Networking or Remote Access Services profile.

Hangup now
This button will close the connection to the ISP. This button is active only when MDaemon initiated the RAS session.

3.1.14.3 Processing



Post Connection Process

Once connected, run this process
If a program is specified here, MDaemon will spawn a thread and execute the process. This is useful for those who require `Finger` or some other program to unlock the ISP's mailbox.

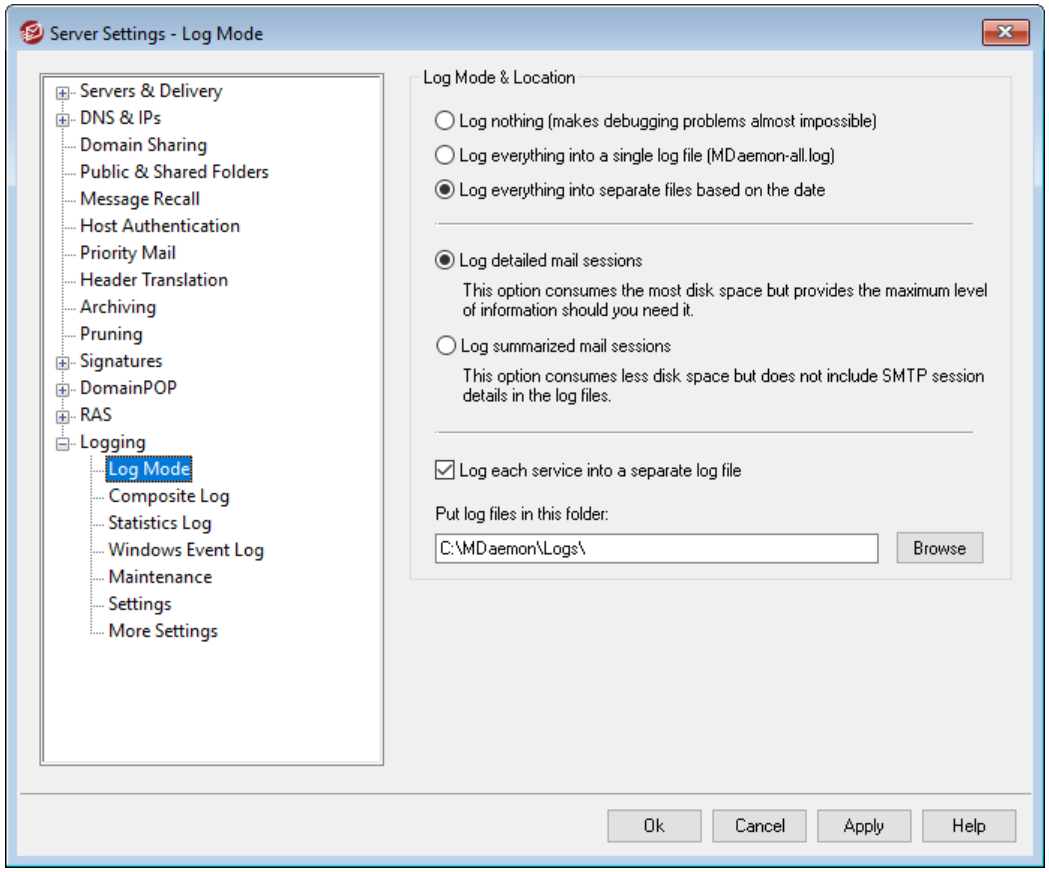
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Pause server for xx seconds (-1 = infinite, 0=no waiting)
If the *Once Connected, Run This Process* control contains a valid entry then the server will pause its operations for the number of minutes specified here while it waits for the executing process to return. Entering "-1" will cause the server to wait indefinitely for the process to return.

Force process to shutdown after pause interval has elapsed
Sometimes the program you need to run may not exit once it has run its course; some programs require user intervention in order to close them down. This is not acceptable when the software must run unattended. If this switch is selected MDaemon will force the process thread to terminate once the number of seconds specified in *Pause Server For XX Seconds* has elapsed. This function does not work when the server is configured to wait indefinitely for the process to return.

3.1.15 Logging

3.1.15.1 Log Mode



Click the "Setup » Server Settings » Logging" menu selection to configure your logging settings. Logging is a useful tool for diagnosing problems and seeing what the server has been doing while unattended.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

There are several options on the Preferences dialog governing the amount of log data that may be displayed in the Event Tracking pane of MDaemon's main interface. For more information, see Preferences » UI 477.

Log Mode & Location

Log nothing
Choosing this option will deactivate all logging. The log files will still be created, but no logging data will be written to them.

We do not recommend using this option. Without logs it can be extremely difficult, if not impossible, to diagnose or debug any potential email-related problems you may encounter.

Log everything into a single log file (MDaemon-all.log)
Choose this option if you wish to log everything into a single, separate file named `MDaemon-all.log`.

Log everything into separate files based on the date
If this option is selected then a separate log file will be generated each day. The name of the file will correspond to the date it was created.

Log detailed mail sessions
A complete transcript of each mail transaction session will be copied to the log file when this option is active.

Log summarized mail sessions
The option causes a summarized transcript of each mail transaction session to be copied to the log file.

Log each service into a separate log file
Click this checkbox to cause MDaemon to maintain separate logs by service rather than in a single file. For example, with this switch set MDaemon will log SMTP activity in the `MDaemon-SMTP.log` file and IMAP activity in the `MDaemon-IMAP.log` file. When running a Configuration Session or Terminal Services instance of the MDaemon interface, this option must be selected in order for the tabs on the interface to display the logged information.

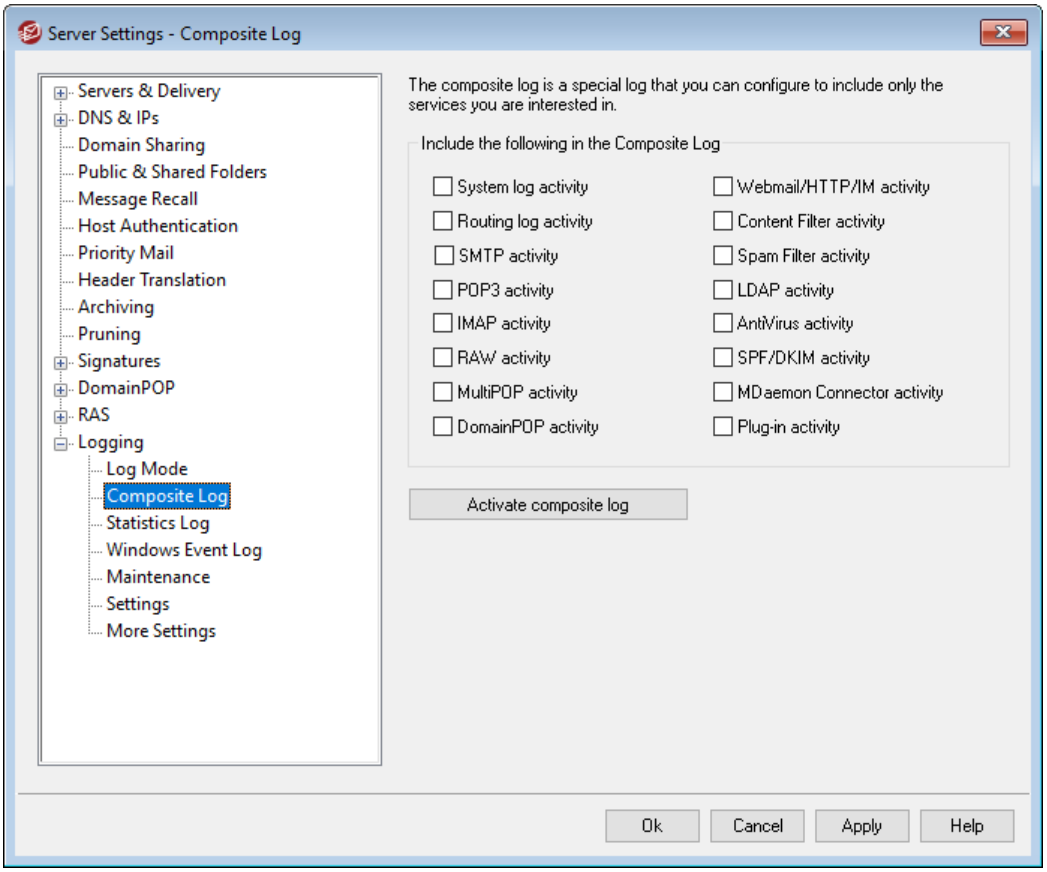
Put log files in this folder:
Use this option if you wish to designate a specific folder path for your log files.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The BadAddress.txt File

In addition to the log files, MDaemon maintains the `BadAddress.txt` file in the logs folder. When delivery to an address results in a 5xx error, the address will be appended to the file. This can help you, for example, identify bad addresses in your mailing lists more quickly than searching the outgoing SMTP logs. This file is automatically removed at midnight each night to prevent it from growing too large.

3.1.15.2 Composite Log



Composite log

Include the following in the Composite Log

Located on the Windows menu of MDaemon's menu bar is a Composite Log View option. Clicking that option will add a window to MDaemon's main display that will combine the information displayed on one or more of the Event Tracker's tabs. Use the controls in this section to designate which tabs' information to combine in that window. The information contained on the following tabs can be combined:

System—Displays MDaemon's system activity such as initializing services and enabling/disabling any of MDaemon's various servers.

Routing—Displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SMTP—All send/receive session activity using the SMTP protocol is displayed.

POP3—When users collect email from MDaemon using the POP3 protocol, that activity is logged.

IMAP—Mail sessions using the IMAP protocol are logged.

RAW—RAW or system generated message activity is logged.

MultiPOP—Displays MDaemon's MultiPOP mail collection activities.

DomainPOP—Displays MDaemon's DomainPOP activity.

Webmail/HTTP/IM—Displays all Webmail and instant messaging activity.

Content Filter—MDaemon's Content Filter operations are listed.

Spam Filter—Displays all Spam Filtering activity.

LDAP—Displays LDAP activity.

AntiVirus—AntiVirus operations are display in the composite view.

SPF/DKIM—Displays all Sender Policy Framework and DKIM activity.

MDaemon Connector—Displays all MDaemon Connector activity.

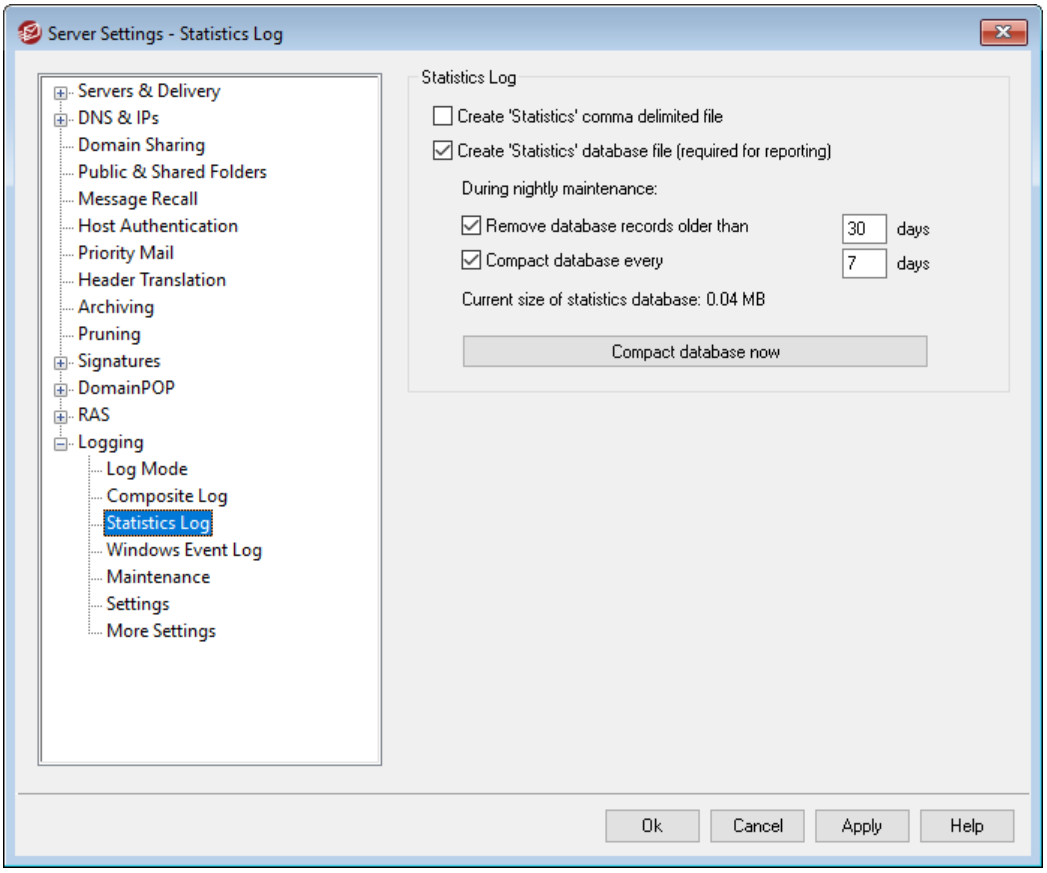
Plugin activity—Logs MDaemon plugin activities to the composite log.

Activate composite log

Click this button to launch the composite log window in MDaemon's main interface. It can also be activated from the Windows menu of MDaemon's menu bar.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.15.3 Statistics Log



Statistics Log

Create 'Statistics' comma delimited file
Use this option if you wish to maintain a comma-delimited statistics file, containing data on the number of inbound and outbound messages processed, spam statistics, antivirus statistics, and the like. This option is disabled by default.

Create 'Statistics' database file (required for reporting)
Check this box if you wish to log statistical information about MDaemon's activity to an SQLite database file. The database contains data on MDaemon's bandwidth usage, number of inbound and outbound messages, spam statistics, and the like. By default this database is stored in the "`MDaemon\StatsDB`" folder and 30 days worth of data are saved, but you can adjust how long to keep the data if you wish to retain more or less than the default 30 days. Data older than the designated limit will be removed during the nightly maintenance process. You can also specify how often MDaemon will compact the database to conserve space.

The Reports page in MDaemon's Remote Administration web interface uses this database to generate a variety of reports available to Global administrators. For each report, data may be generated for several predefined date ranges, or the admin may specify a custom date range. Administrators can choose from the following reports:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Enhanced bandwidth reporting
- Inbound vs. Outbound messages
- Good messages vs. Junk messages (percentage of email that is spam or a virus)
- Inbound messages processed
- Top recipients by number of messages
- Top recipients by message size
- Outbound messages processed
- Top spam sources (domains)
- Top recipients of spam
- Viruses blocked, by time
- Viruses blocked, by name

During nightly maintenance:
The options below govern which database-related tasks MDaemon will perform during the nightly maintenance operation.

Remove database records older than [xx] days
Use this option to designate the number of days worth of statistical database records that you wish to keep. By default this option is enabled and set to 30 days.

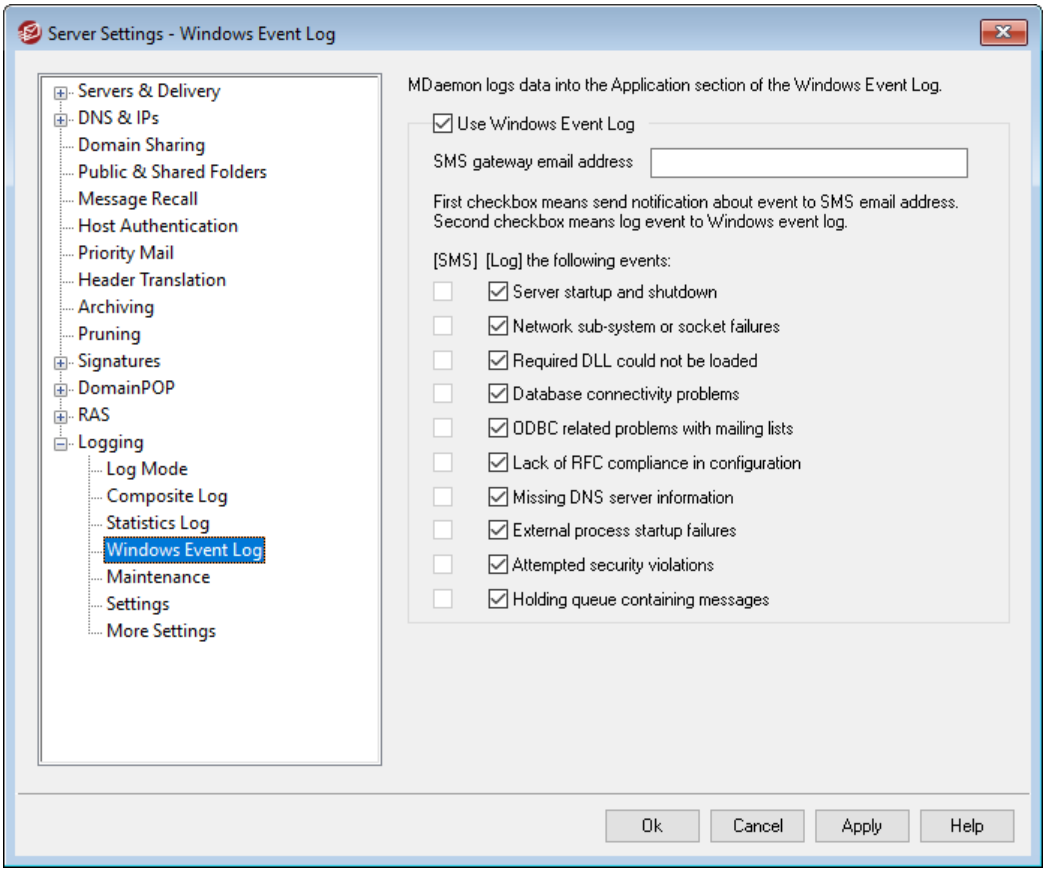
Compact database every [xx] days
Use this option if you wish to periodically compact the database to conserve space. By default this option is enabled and set to compact the database every 7 days.

Current size of statistics database:
The current size of your statistics database is listed here.

Compact database now
Click this button to immediately compact the database.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.15.4 Windows Event Log



Use Windows Event Log
Click this check box if you want to log critical system errors, warnings, and certain other events into the Application section of the Windows Event Log.

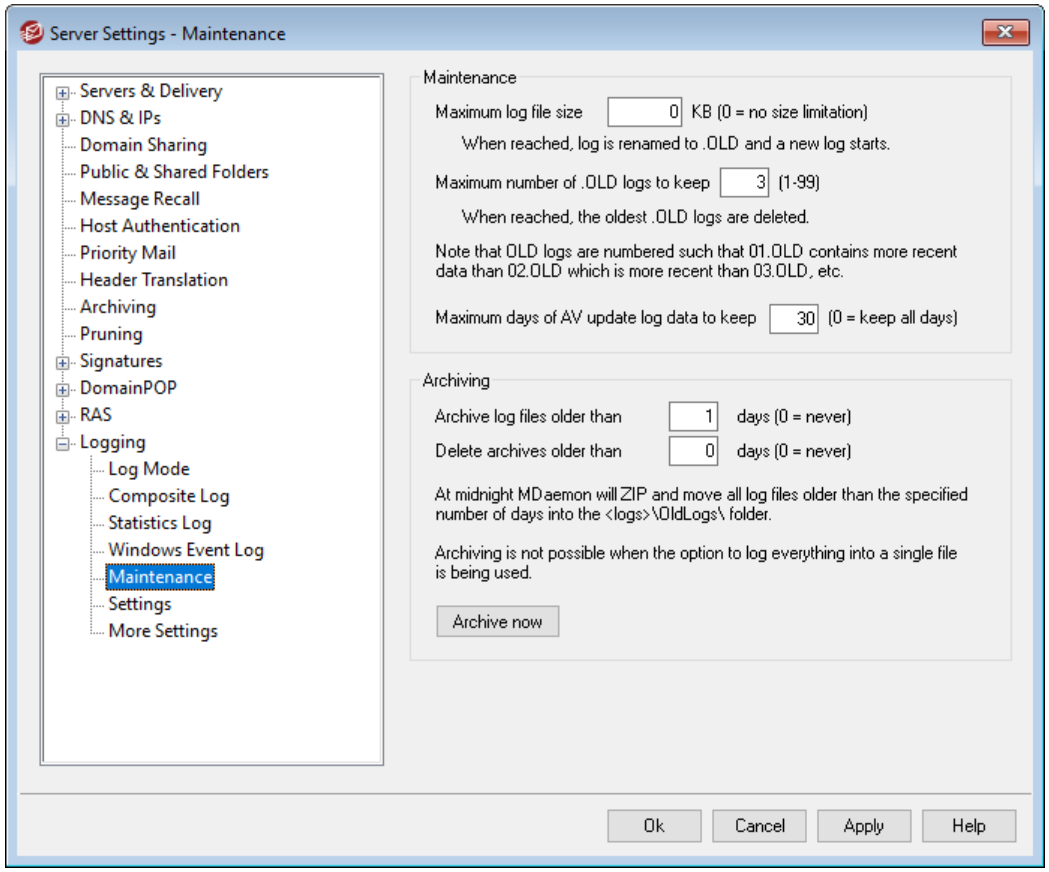
SMS gateway email address
Use this option if you wish to send event data for any of the events designated below to a device in an SMS (text) message. To do so, specify the email address of your phone carrier's email-to-SMS (i.e. text message) gateway, such as Verizon's, which is `PhoneNumber@vtext.com` (e.g. `8175551212@vtext.com`). Then use the checkboxes in the SMS column below to specify the events that you wish to send to the device.

SMS | Log the following events:
Use the SMS options to designate the events you wish to send to a device via text message. Use the Log options to designate the events that you wish to log to the Application section of the Windows Event log. To send SMS messages you must specify the email address of your phone carrier's email-to-SMS gateway in the option above. Further, any event that triggers a notification message to the SMS gateway will cause the remote queue to be processed; the notifications will be treated as and "urgent" email.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The SMS option for *Server startup and shutdown* events will only send an email-to-SMS message for startup events, not shutdown.

3.1.15.5 Maintenance



Maintenance

Maximum log file size [xx] KB
This is the maximum size in kilobytes that a log file may reach. Once this size is reached, the log file is copied to "LOGFILENAME.01.OLD" and a new log is started. If LOGFILENAME.01.OLD already exists then the old file will either be deleted or renamed to "LOGFILENAME.02.OLD," depending on the value set in "*Maximum number of .OLD logs to keep*" below. Use "0" in this option if you do not with to limit the size of the file. This option is set to "0" by default.

Maximum number of .OLD logs to keep (1-99)
When using the option above to limit log file size, this option governs how many iterations of a given .OLD log file will be kept before the oldest is deleted. These backup files are named, "LOGFILENAME.01.OLD," "LOGFILENAME.02.OLD," and so on,

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

with the newest file always listed first. For example, `SMTP(out).log.01.old` has newer data than `SMTP(out).log.02.old`, etc. When the maximum number is reached, the oldest file is deleted when a new file is created.

Maximum days of AV update log data (0=no limit)
This option governs the maximum number of days that the Antivirus update log (i.e. avupdate.log) will keep data. At midnight each night, and also whenever MDaemon starts after upgrading, older data will be deleted from the file. Use "0" in this option if you do not wish to set a time limit. By default the last 30 days of data are kept.

The AV update log is maintained by default and its size is limited to 5120 KB. If you wish to change its size limit or disable AV update logging, the options to do so are located on the AV Updater Configuration 659 dialog, located at: **Security » AntiVirus » AV Updater » Configure updater » Misc**.

Archiving

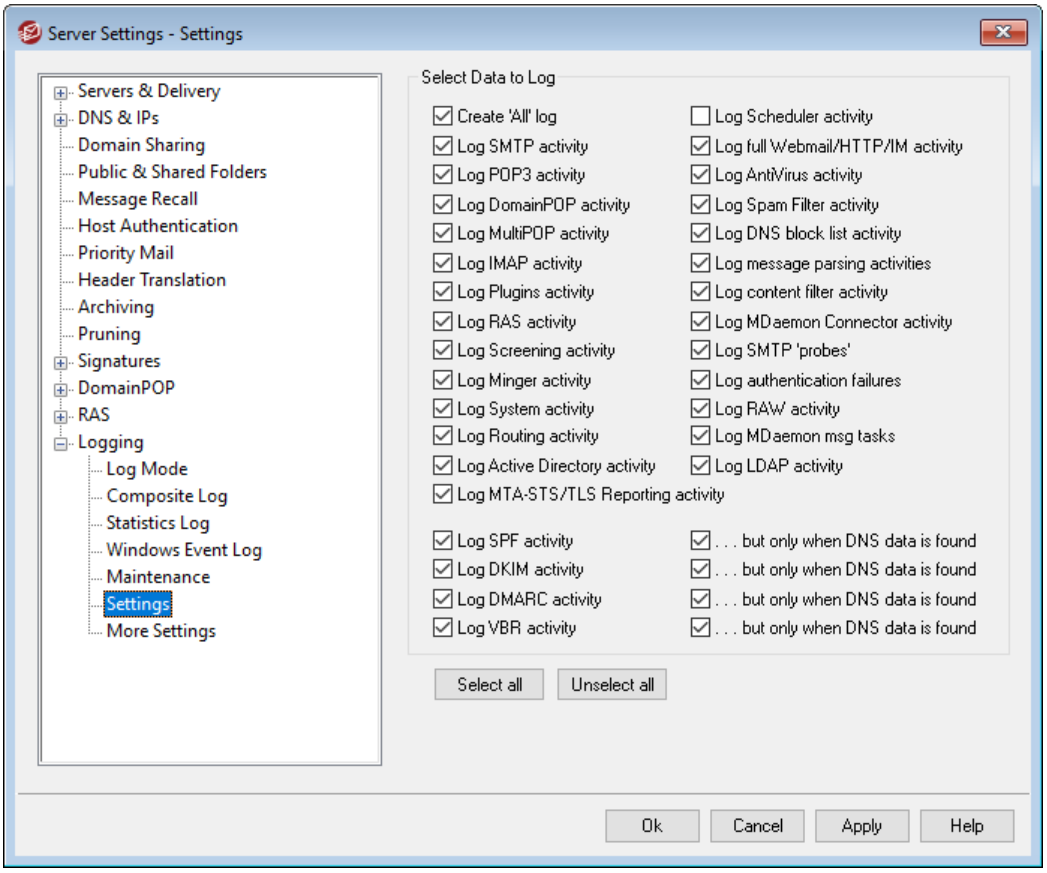
Archive log files older than [XX] days (0=never)
Click this option if you want MDaemon to archive each log file whose age exceeds the number of days specified. Each day at midnight, MDaemon will `ZIP` old `*.log` and `*.old` files and move them to the `\Logs\OldLogs\` subfolder (deleting the original files in the process). This process will not archive or delete files that are in use, nor will it archive files when the "*Log everything into a separate log file (MDaemon-all.log)*" option is selected on the Log Mode 159 screen.

Delete archives older than [XX] days (0=never)
Use this option if you want MDaemon to delete archived log files automatically when their age exceeds the number of days specified here. Use "0" in this option if you do not wish to delete archives automatically. Archive deletion occurs during the daily midnight cleanup event.

Archive now
Click this button to archive old log files immediately rather than waiting for MDaemon to archive them automatically at midnight.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.1.15.6 Settings



Select Data to Log

Create 'All' log
Click this option if you want the "`*-all.log`" file to be generated, which contains a composite of all logged activities.

Log SMTP activity
Enable this option if you want to log all of MDaemon's send/receive SMTP activity.

Log POP3 activity
Click this checkbox to log all POP mail activity. This will log your users' POP mail collection sessions.

Log DomainPOP activity
Click this checkbox to log all DomainPOP mail activity.

Log MultiPOP activity
Click this checkbox to log all of your users' MultiPOP mail collection activity.

Log IMAP activity
Enabling this option causes all of your users' IMAP sessions to be included in MDaemon's log files.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Log Plugins activity
This option logs all plugin-related activities.

Log RAS activity
Click this switch if you want MDaemon to copy RAS dialup/dialdown activities into the log file. This information is useful for diagnosing dialup problems.

Log Screening activity
Click this checkbox if you want MDaemon's Screening activities to be included in MDaemon's log file.

Log Minger activity
Click this checkbox to log Minger server activities.

Log System activity
This option logs system activities.

Log Routing activity
This option logs all Inbound, Local, and Remote queue parsing activities.

Log Active Directory activity
This option is for logging MDaemon-related Active Directory activities.

Log MTA-STS/TLS Reporting activity
Logs all SMTP MTA Strict Transport Security (MTA-STS) related activity.

Log Scheduler activity
Enable this checkbox if you wish to log all of the Event Scheduler's 372 activity.

Log full Webmail/HTTP/IM activity
Click this option if you wish to log all Webmail, HTTP, and MDaemon Instant Messenger activity. When disabled, Webmail and HTTP logs will still be created showing MDaemon Webmail's startup and shutdown times, but other Webmail/HTTP/IM activity will not be logged.

Log AntiVirus activity
This option logs AntiVirus activities

Log Spam Filter activity
Logs all Spam Filter activity.

Log DNS block list activity
This option causes MDaemon to log DNS block list activity. Using this option will allow you to have an easy reference to the sites that were logged as blocked.

Log message parsing activities
MDaemon periodically performs a great deal of message parsing activity when determining to whom a message should be delivered. Enable this switch if you want this information to be included in the log file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Log content filter activity
Click this checkbox if you want to include Content Filter activity in the log file.

Log MDaemon Connector activity
This option governs whether or not MDaemon Connector activities are logged.

Log SMTP 'probes'
Click this option to log SMTP sessions when no message data is transmitted by the sending server (i.e. the sending server does not use the DATA command).

Log authentication failures
Use this option to log authentication failures.

Log RAW activity
Logs MDaemon's RAW message activity.

Log MDaemon msg tasks
Logs message tasks..

Log LDAP activity
Logs all LDAP activity.

Log SPF activity
Click this check box if you wish to log all Sender Policy Framework lookup activities.

> **...but only when DNS data is found**
> If you are logging SPF activities, click this check box if you wish to log only lookups where actual SPF data is found during the DNS lookup, rather than logging all SPF lookups.

Log DKIM activity
Click this option if you wish to log DomainKeys Identified Mail (DKIM) activity.

> **...but only when DNS data is found**
> Click this check box if you are logging DKIM activity but wish to log only those instances where DNS data is found instead of logging all activity.

Log DMARC activity
Click this option if you wish to log DMARC activity.

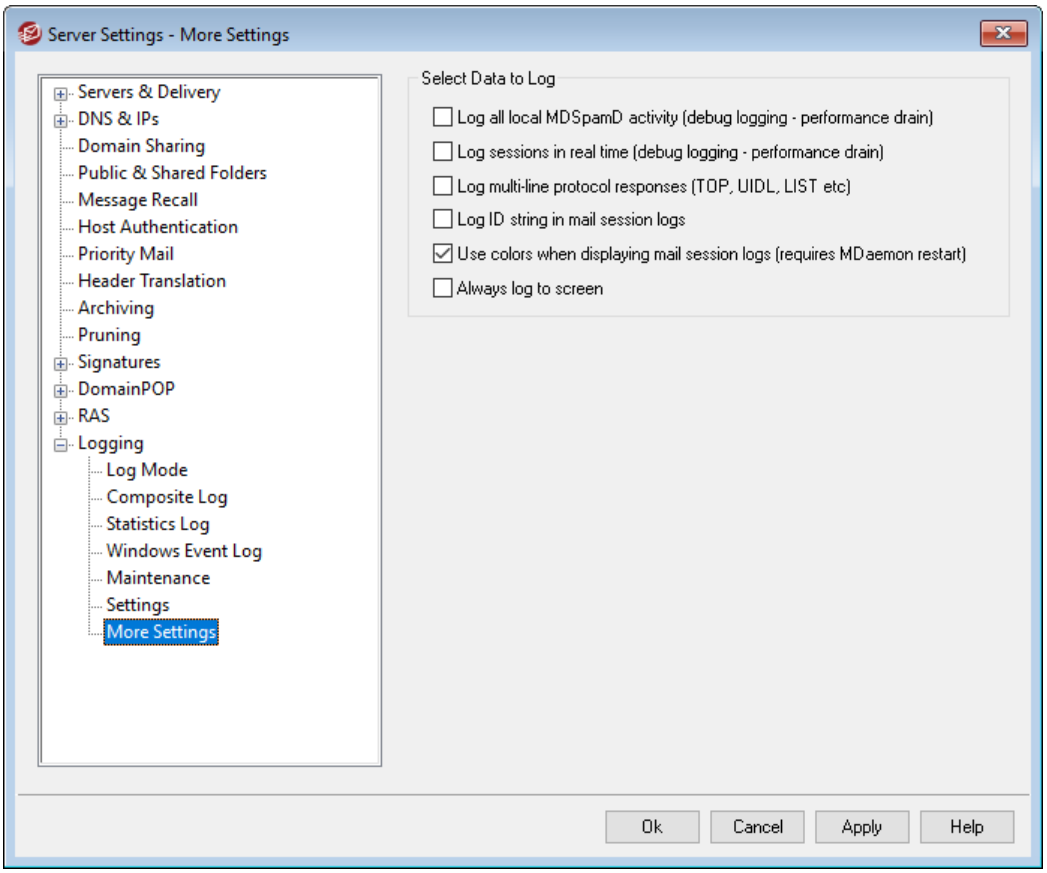
> **...but only when DNS data is found**
> Click this check box if you are logging DMARC activity but wish to log only those instances where DNS data is found instead of logging all activity.

Log VBR activity
Use this option if you wish to log message certification 538.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...but only when DNS data is found
If you are logging message certification activity, click this check box if you wish to log it only when actual certification data is found during the DNS lookup.

3.1.15.7 More Settings



Select Data to Log

Log all local MDSpamD activity (debug logging—performance drain)
Use this option to log all local MDSpamD activities (see Caution below).

Log sessions in real time (debug logging—performance drain)
Ordinarily, session information is logged after the session is completed in order to conserve resources. Click this option if you want session information to be logged as it occurs.

When using either or both of the previous two logging options, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use these options for debugging purposes.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Log multi-line protocol responses (like UIDL and LIST)
Sometimes the responses to protocol requests require more than one line of information. Click this checkbox if you want to log these additional lines.

Enabling this switch could potentially increase the amount of logged information a great deal. Because the number of lines in a response can't be determined in advance, and because some responses have great potential for "filling up" your log file with possibly unnecessary information (POP TOP, for example, lists the actual contents of the message), we do not recommend using this feature if log file size or verbosity is of concern to you.

Log ID string in mail session logs
Click this check box if you wish to include `[%d:%d]` ID strings in session logs.

Use colors when displaying mail session logs (requires MDaemon restart)
Enable this option if you wish to colorize the text displayed on several of the Event Tracking and Logging 69 tabs on MDaemon's user interface. This option is disabled by default, and enabling/disabling it requires an MDaemon restart before the change will take effect. See: "Colorized Session Logs" below for more information.

Always log to screen
Click this option if you want the logged data to be copied to the MDaemon GUI even when it is minimized or running in the tray.

When this control is cleared, log data isn't copied to the Event Tracking pane when MDaemon is running in the system tray. Consequently, the most recent activity won't be listed on any of the Event Tracking pane's tabs when MDaemon is first opened. It will begin displaying newly logged information from that point forward.

Colorized Session Logs

On MDaemon's user interface 69, the tabs that display Routing, SMTP-in, SMTP-out, IMAP, POP, MultiPOP, and DomainPOP activity can be colorized to help visually separate events during a session. This features is disabled by default, but can be enabled via the "*Use colors when displaying mail session logs*" option located at: Logging » More Settings 171 and Preferences » UI 477. The default text colors can be changed by editing the `[Colors]` section of the `LogColors.dat` filein MDaemon's `\APP\` folder. See the chart below for a list of the default colors.

If you want to use colors but don't want to colorize one or more of the listed elements, set value of each of those elements to zero (for example, `SpamFilter=0`). This will cause the chosen elements to use the `Default` color. For `Background` and `SelectedBackground`, however, setting their values to zero doesn't work. If you want to change either of those elements you will have to provide a new color value. Color values are specified in hexadecimal using this form: "`0xbbggrr`", where "bb" is the relative intensity for blue, "gg" for green, and "rr" for red. For example, "`Error=0x0000ff`" sets error text to red. **Please note:** this is the reverse of the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

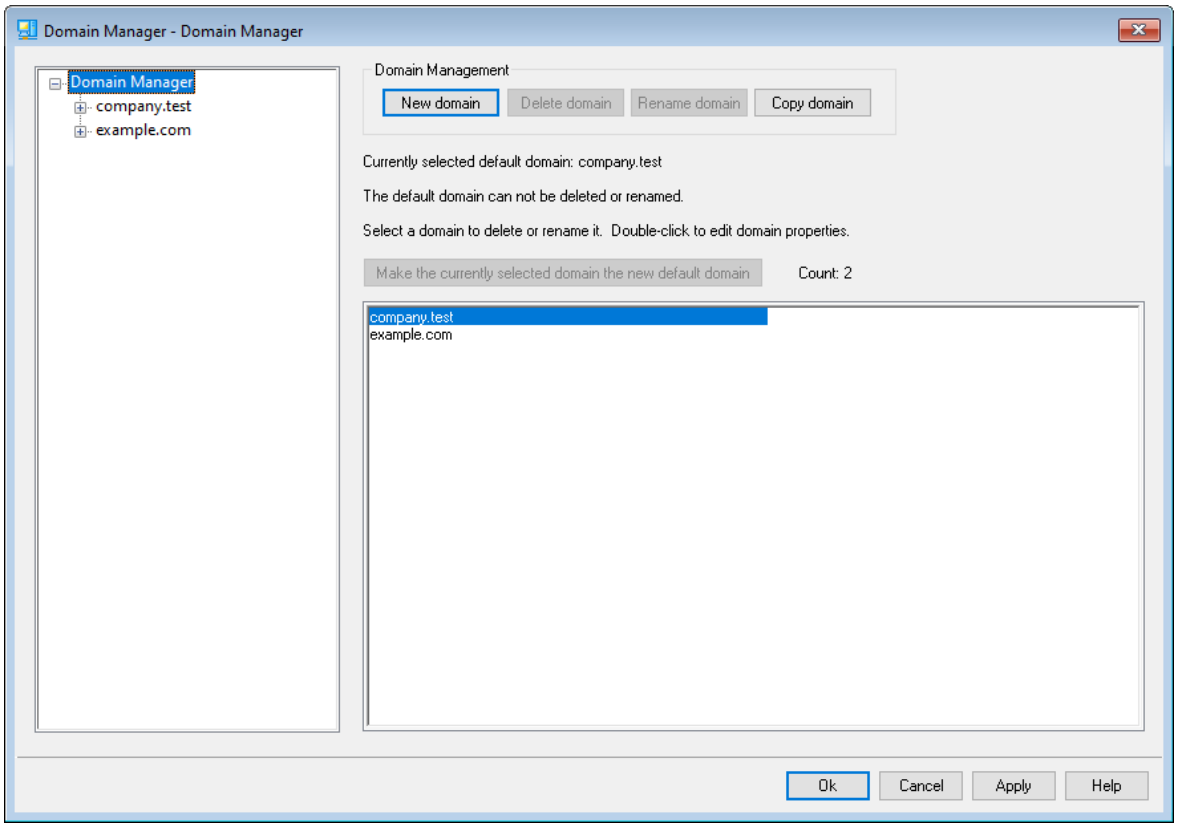
traditional order for color codes, which is typically "rrggbb". If you make changes to the colors, you must restart MDaemon or create a file called COLORS.SEM and place it in MDaemon's \APP\ folder.

Default Log Colors

Background=0x000000	Background color; black
SelectedBackground=0xff0000	Selected background color; blue
Default=0xffffff	Default text color; white
Processing=0x00ffff	Internal processing and parsing activity; default is yellow
DataIn=0x008040	Incoming data from other server; default is dark green
DataOut=0x00ff00	Outgoing data sent to other server; default is bright green
Error=0x0000ff	Error messages; default is red
TCPIP=0xff8000	TCP/UDP/DNS/PTR related activity; default is light blue
SpamFilter=0x0080ff	Spam filtering; default is orange
AntiVirus=0xdda0dd	AntiVirus processing; default is plum
DKIM=0xff00ff	DKIM activity; default is fuchsia
VBR=0x40c0ff	Vouch by Reference activity; default is light orange
SPF=0x808080	Sender Policy Framework activity; default is grey
Plugins=0x0080c0	Any message sent from a plugin; default is brown
Localq=0x00ffff	Local queue routing; default is yellow
Spam=0x0080ff	Spam message routing; default is orange
Restricted=0x40c0ff	Restricted message routing; default is light orange
BlackList=0x808080	Block-listed message routing; default is grey
Gateway=0x00ff00	Gateway message routing; default is light green
Inboundq=0xff8000	Inbound message routing; default is light blue
PublicFolder=0xdda0dd	Public folder message routing; default is plum

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2 Domain Manager



MDaemon contains full support for multiple domains, administered using the Domain Manager. Here you can manager the domain names, IP addresses, account and message pruning settings, Webmail settings, and other domain-specific options for your domains.

MDaemon supports both single and multiple IP addresses, and IP addresses can be unique to individual domains or shared between them. Further, several key features such as Accounts, Mailing Lists, and some Security Settings are on a per domain basis. When you create an account, for example, you must specify the domain to which the new account belongs. The same goes for Mailing Lists. This also means that features such as the IP Screen 548 and IP Shield 507 are tied to domains individually.

Some features, such as Name Matching 152 under DomainPOP 142, are tied exclusively to the Default Domain. The Default Domain is also the domain displayed by default in various options, such as when creating new accounts or mailing lists. Further, to support MDaemon's handling of system messages, the following default Aliases 818 point several reserved mailbox names to MDaemon's default domain name rather than to its other domains:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
listserver@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
list-serv@$LOCALDOMAIN$ = MDaemon@<DefaultDomain>
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Finally, in order to support multiple domains, by default MDaemon requires users to use their full email address (e.g. "user01@example.com") as their login value rather than using just the mailbox portion of the address (i.e. "user01"). Some very old mail clients, however, do not support using '@' in the login field. Therefore to accommodate those clients you can specify an alternate character on the System 480 screen under Preferences. Further, this value can be up to 10 characters long, making it possible to provide a string of characters to serve as the delimiter instead of only a single character such as '$'. For example, using '**.at.**' will allow you to make logon values of "user02.at.example.com". You can also disable the full email address requirement, allowing the use of only the mailbox portion of the address as the login value, but that is not recommended and can cause problems when you have more than one domain.

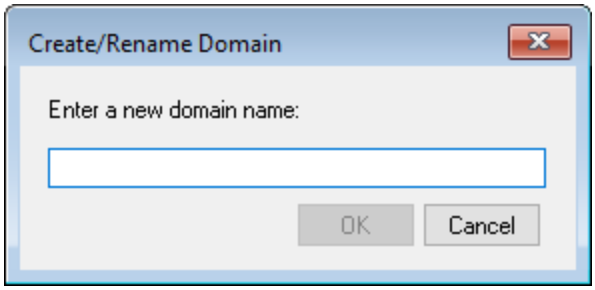
Domains List

The area on the left side of this dialog contains the list of your domains, with links to each screen used for configuring the various domain-specific settings. The Default Domain is listed first and all other domains are listed alphabetically. The list on the right is used for deleting and renaming domains, and for designating the Default Domain. You can double-click a domain in this list to switch to the domain and configure its settings.

Domain Management

New domain

To create a new domain: click *New domain*, enter the domain name in the Create/Update Domain dialog, and click *OK*.



Typically the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name. Alternatively, you may choose to use an internal-only or otherwise non-valid, non-public domain name (such as "company.mail") for your domain name. When configuring your server in this way it may be necessary to use the Header Translation 121 feature, and/or the Domain Name Replacement Engine 148, to enable proper mail distribution.

Delete domain

To delete a domain: select the domain from the list below, click *Delete domain*, and then confirm your decision to delete the domain by clicking *Yes*.

You cannot delete or rename the default domain. If you wish to delete or rename it then you must first designate a different

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

domain as the default domain.

Rename domain
To change a domain name: select a domain from the list below, click *Rename domain*, type the new domain name in the Create/Update Domain dialog, and click *OK*.

Copy domain
If you wish to create a new domain with settings that match another domain, select a domain from the list, click this button, and then specify a name for the new domain. Accounts, lists, and the like will not be copied to the new domain.

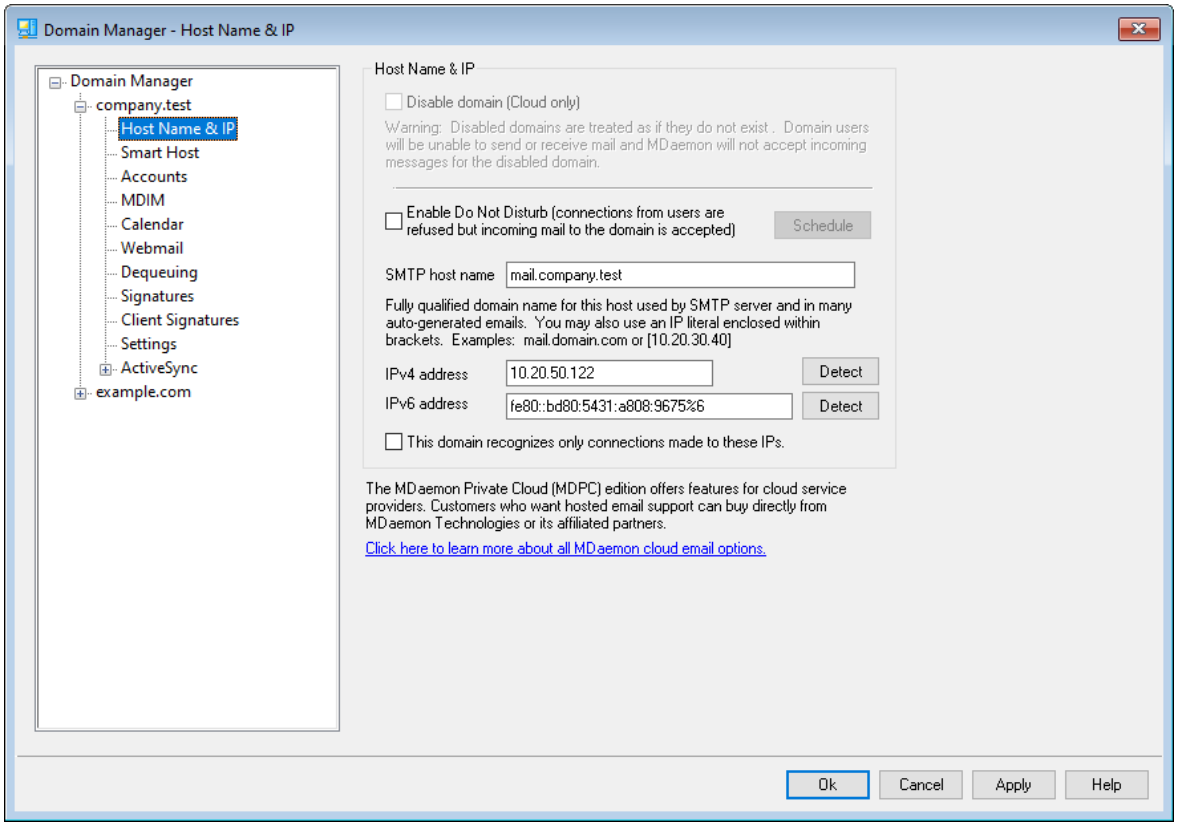
Make the currently selected domain the new default domain
If you wish to change MDaemon's default domain, select the desired domain from the list below and click this button.

See:

Preferences » System 480

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.1 Host Name & IP



Host Name & IP

Disable domain (Cloud only)
Click this checkbox if you wish to disable the domain. Disabled domains are treated by MDaemon as if they do not exist. Domain users will not be able to send or receive mail and MDaemon will not accept incoming mail for the domain. This option is only available in MDaemon Private Cloud.

Enable Do Not Disturb
Use this option to activate Do Not Disturb for a domain. When active the domain will refuse all connections from all users for all services, but it will still accept messages from the outside world.

Schedule
Click this button to schedule when Do Not Disturb starts and stops. For example, if you configure May 1, 2020 to June 30, 2020 from 5:00pm to 7:00am, Monday thru Friday then this means that no mail services will be available for that domain's users on those days, beginning at 5:00pm and resuming at 7:01am, so long as the current date falls on or between May 1 and June 30, 2020. Erasing the scheduled start date deactivates the schedule and has the effect of **putting the domain on 'Do Not Disturb' forever**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SMTP host name
This value is the Fully Qualified Domain Name (FQDN) that will be used in the `SMTP HELO/EHLO` instruction when sending mail for this domain. For incoming connections, if the *This domain recognizes only connections made to the host IP address* option below is used, the domain is bound to its own IP address and the proper FQDN will be used for connections made to that domain. Using that option, however, is not strictly required for this to work. But, if you have two or more domains using the same unbound IP address then the FQDN used will be the one that is associated with the domain that is first in alphabetical order.

In most cases the FQDN will be either the *Domain name* or a subdomain of it (for example, "`mail.example.com`"), but an IP literal syntax such as "`[192.0.2.0]`" may also be used. When no FQDN value is specified, MDaemon will use the Default Domain's FQDN.

IPv4/IPv6 address
Enter the IPv4 and IPv6 addresses to associate with this domain. If an IP address is missing MDaemon will automatically try to detect a suitable address for use.

Detect
Use these buttons to detect the IPv4 and IPv6 IP addresses that are eligible for use in the corresponding IP address options. You can then choose from the IP addresses listed.

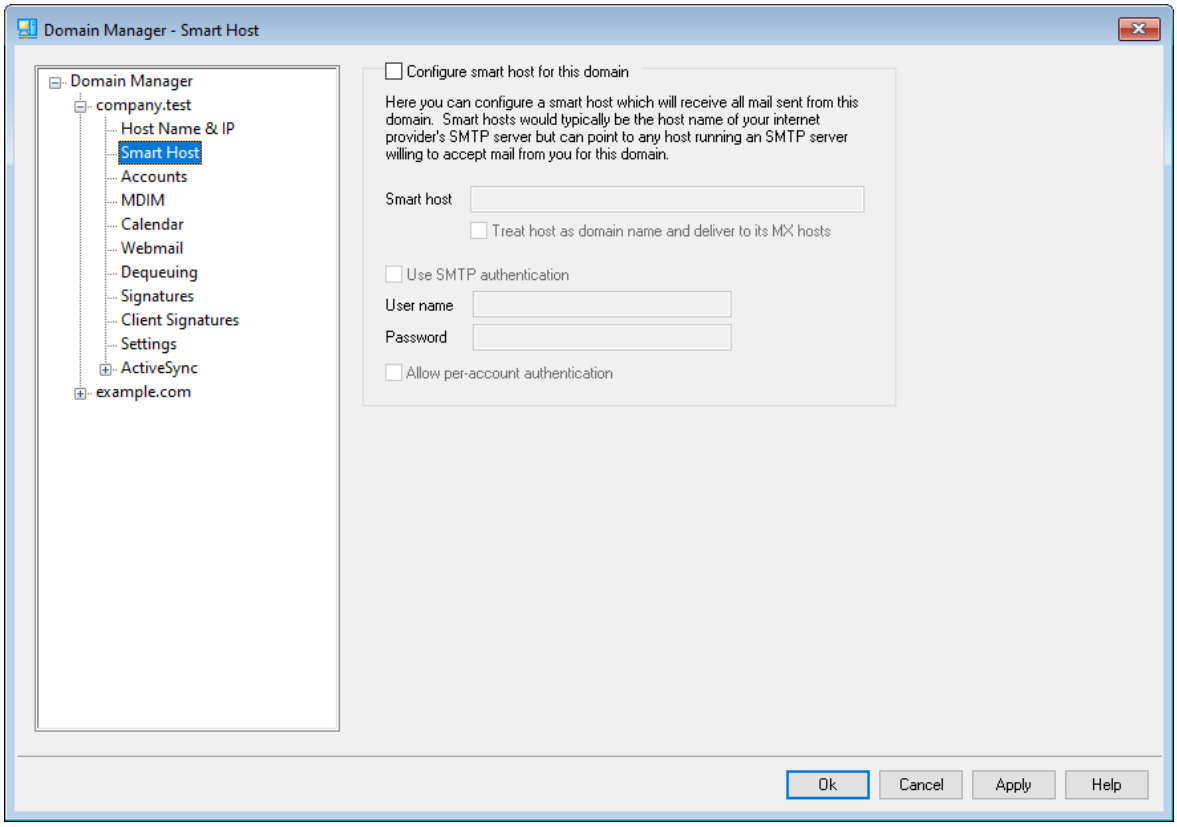
This domain recognizes only connections made to these IPs
Click this checkbox if you wish to restrict this domain's incoming connections to the IP addresses specified above. By default this only applies to inbound connections. Outbound socket binding is governed by an option under "Server Settings » Binding 105."

See:

Domain Manager 174
Preferences » System 480
Binding 105
IPv6 104

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.2 Smart Host



Configure smart host for this domain

If you wish to route this domain's outbound mail through a specific Smart Host rather than using MDaemon's default Delivery 89 options, enable this checkbox and specify the smart host below. All of the domain's outbound mail will be routed to the host.

Smart host

Specify your ISP or mail host's name or IP address here. This is generally the SMTP server of your ISP.

> Do not enter MDaemon's Default Domain or IP addresses into this text box. This entry should be an ISP or other mail server that can relay mail for you.

Treat host as domain name and deliver to its MX hosts

Check this box if you wish to treat the host as a domain name rather than a specific server, thus causing MDaemon to retrieve any MX hosts associated with the domain and connect to them.

Use SMTP authentication

Click this check box and enter your login credentials below if the *Smart Host* requires authentication. These login credentials will be used for all outbound SMTP

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

messages sent to the smart host. If, however, you choose to use the *Allow per-account authentication* option below, then MDaemon will authenticate to the host separately for each message, using the sending account's *Smart Host Access* credentials designated on the Mail Services 701 screen of the Account Editor.

User name
Enter your user name or login here.

Password
Use this option to specify your smart host login password.

Allow per-account authentication
Click this checkbox if you wish to use per-account authentication for outbound SMTP messages sent to the *Smart Host* specified above. Instead of using the *User name* and *Password* credentials provided here, each account's *Smart Host Access* credentials, designated on the Mail Services 701 screen, will be used instead. If no smart host credentials have been designated for a given account, the above credentials will be used instead.

If you wish to configure *per-account authentication* to use each account's *Email password* instead of its optional *Smart host password*, then you can do so by editing the following key in the `MDaemon.ini` file:

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

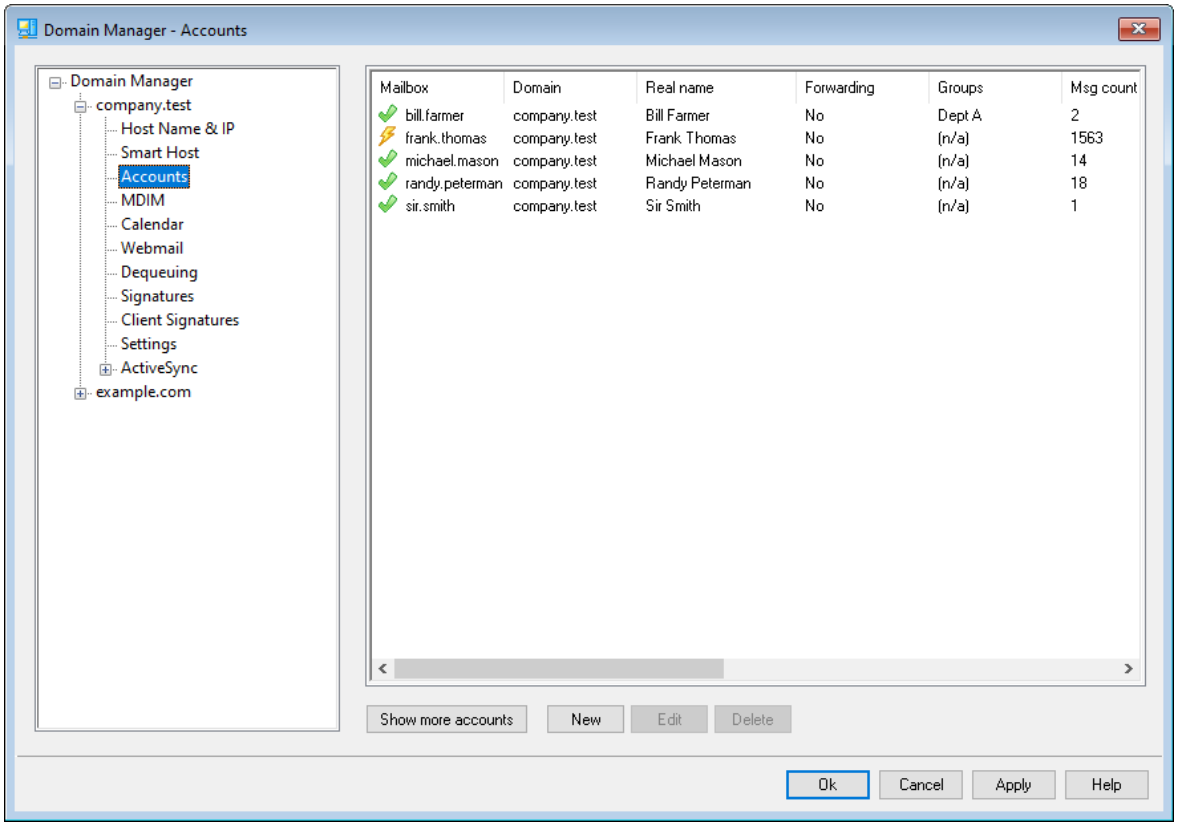
Enabling the `ISPAUTHUsePasswords=Yes` option will over time effectively communicate all your accounts' local mail passwords to your smart host. This could pose a risk to mail security, since it is providing sensitive information to another server. You should not use this option unless you are using a smart host that you absolutely trust and you believe it is necessary to do so. Further, you should note that if you use this option and give your users permission to change their *Email password* via Webmail or some other means, then changing the *Email password* will also effectively change the *Smart host password*. This could cause smart host authentication to fail for an account when its *Email password* is changed locally but the corresponding *Smart host password* isn't changed at your smart host.

See:

Domain Manager 174
Server Settings » Delivery 89
Account Editor » Mail Services 701

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.3 Accounts



The Accounts page displays a list of all of this domain's MDaemon accounts. Each entry in the list contains Account Status Icons (see below), the mailbox, the "real name" of the account holder, any groups to which the account belongs, the message count, and the amount of disk space used (in MB). This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Account Status Icons

Account is a global or domain administrator.

Full access account. Both POP and IMAP access are enabled.

Restricted access account. Either POP, IMAP, or both are disabled.

Account is frozen. MDaemon will still accept mail for the account, but the user cannot send or check mail.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Disabled account. All access to the account is disabled.

New
Click this button to open the Account Editor[697] in order to create a new account.

Edit
Select an account from the list and then click this button to open it in the Account Editor[697]. You can also double-click the account to open it.

Delete
Select an account from the list and then click this button to delete it. You will be asked to confirm your decision to delete the account before MDaemon will proceed.

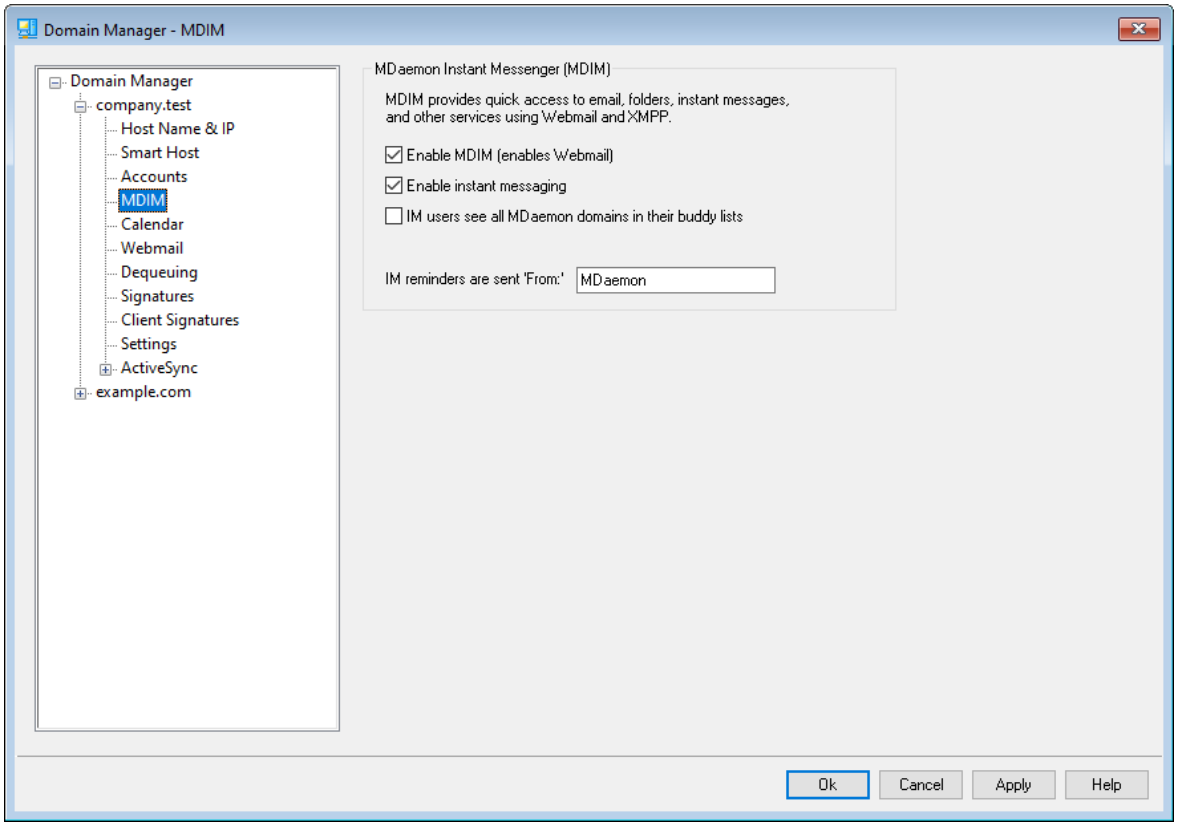
Show more accounts
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500.

See:

Account Manager[694]
Account Editor[697]
New Accounts Template[775]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.4 MDIM



This screen controls various aspects of MDaemon Instant Messenger (MDIM) 309 for this domain. The initial settings on this screen are determined by the Default MDaemon Instant Messenger 320 settings located on the Web & IM Services dialog. MDIM services can be enabled or disabled for specific accounts or groups via the Web Services 703 and Group Properties 766 screens respectively.

MDaemon Instant Messenger (MDIM)

Enable MDIM (enables Webmail)
Enable this option if you wish to make MDaemon Instant Messenger available for download from within Webmail by default for the domain's users. They can download it from the *Options » MDaemon Instant Messenger* page. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier. This option also makes it possible for MDIM to use the My Mail Folders features, allowing users to check for new email and open Webmail directly from the MDIM shortcut menu. MDIM is enabled by default.

Enable instant messaging
By default, accounts can use MDIM and third-party XMPP 365 clients to instant message other members of their domain. Clear this checkbox if you do not wish to allow this domain's users to use instant messaging.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

IM users see all MDaemon domains in their buddy lists
Click this option if you want this domain's users by default to be able to add contacts to their buddy list from all of your MDaemon domains. When this option is disabled, contacts must be on the same domain. For example, if your MDaemon is hosting mail for example.com and example.org, activating this option for example.com means that example.com users can add instant messaging contacts from both domains. Disabling it means that example.com users can only add other example.com users. This option is disabled by default.

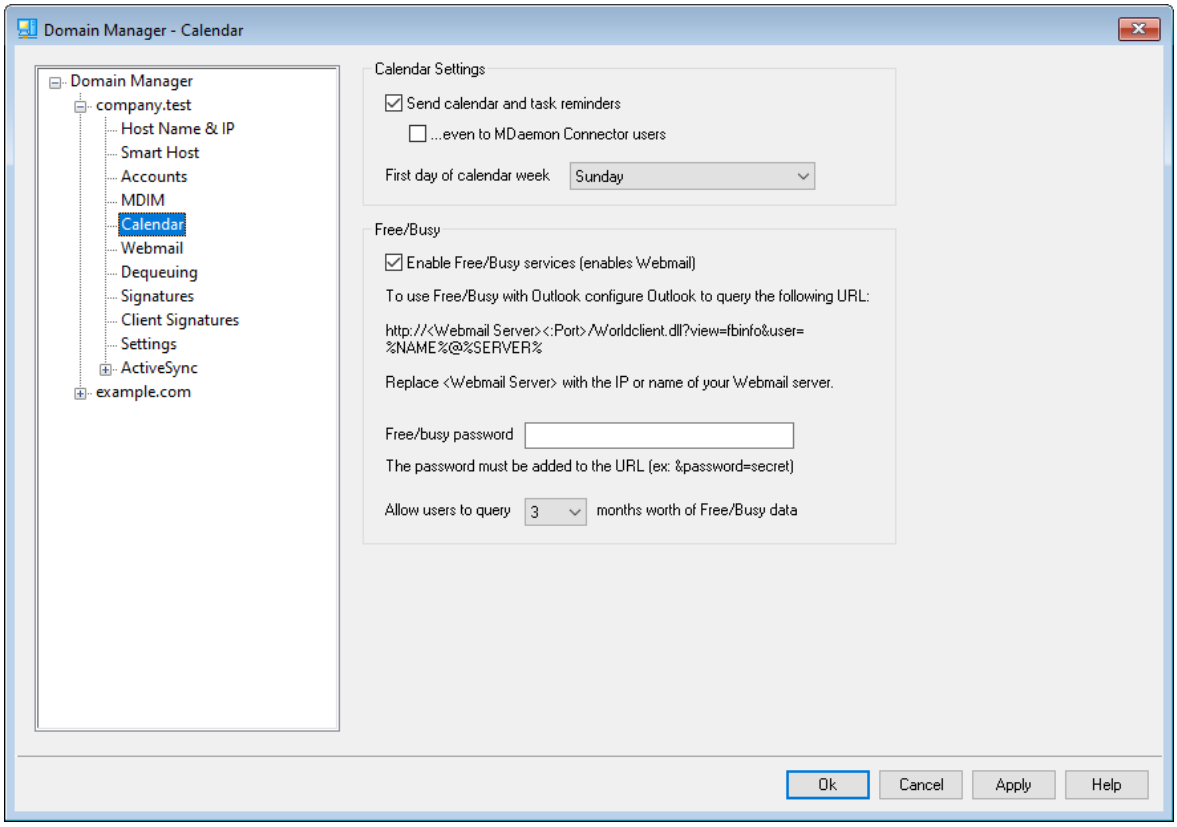
IM reminders are sent 'From:' [*text*]
When an appointment is scheduled on a user's Webmail calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message to the user. Use this text box to specify the name that you wish the message to appear to be 'From:'.

See:

Domain Manager 174
Webmail » MDIM 320
Account Editor » Web Services 703
Group Properties 766

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.5 Calendar



This screen controls MDaemon's Calendar features for this domain. The initial settings on this screen are determined by the Calendar 322 screen located on the Web & IM Services dialog.

Calendar Settings

Send calendar and task reminders
Click this checkbox if you wish to allow Webmail's calendar and task reminders to be sent to your users via email and MDaemon Instant Messenger.

...even to MDaemon Connector users
If you have enabled the "*Send calendar and task reminders*" option above, click this option if you also wish to enable reminders for MDaemon Connector 379 users.

First day of week
Choose a day from the drop-down list. The selected day will appear in the calendars as the first day of the week.

Free/Busy

MDaemon includes a Free/Busy server, which makes it possible for a meeting planner to view the availability of potential meeting attendees. To access this feature, click Scheduling within Webmail when creating a new appointment. This opens a Scheduling window containing the list of attendees and a color-coded calendar grid

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

with a row for each one. Each attendee's row is color-coded to indicate the times at which he or she might be available for a meeting. There are colors for Busy, Tentative, Out of Office, and No information. There is also an Auto-Pick Next button that makes it possible for you to query the server for the next time slot at which all attendees may be available. When you have finished creating the appointment it will send an invitation to all of the attendees, who can then accept or decline.

Webmail's Free/Busy server is also compatible with Microsoft Outlook. To use it, configure Outlook to query the URL listed below for Free/Busy data. In Outlook 2002, for example, the Free/Busy options are located under "Tools » Options » Calendar Options... » Free/Busy Options..."

Free/Busy server URL for Outlook:

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Replace "<Webmail>" with the IP address or domain name of your Webmail server, and "<:Port>" with the port number (if you aren't using the default web port). For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

For more on how to use Webmail's Free/Busy features to schedule your appointments, see the online Help system within Webmail.

Enable Free/Busy services (enabled Webmail)
Click this option if you wish to provide access to the Free/Busy server features to users.

Free/Busy password
If you wish to require a password when users attempt to access the Free/Busy server features via Outlook, include the password here. This password must be appended to the URL listed above (in the form: "&password=FBServerPass") when the users configure their Free/Busy settings within Outlook. For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

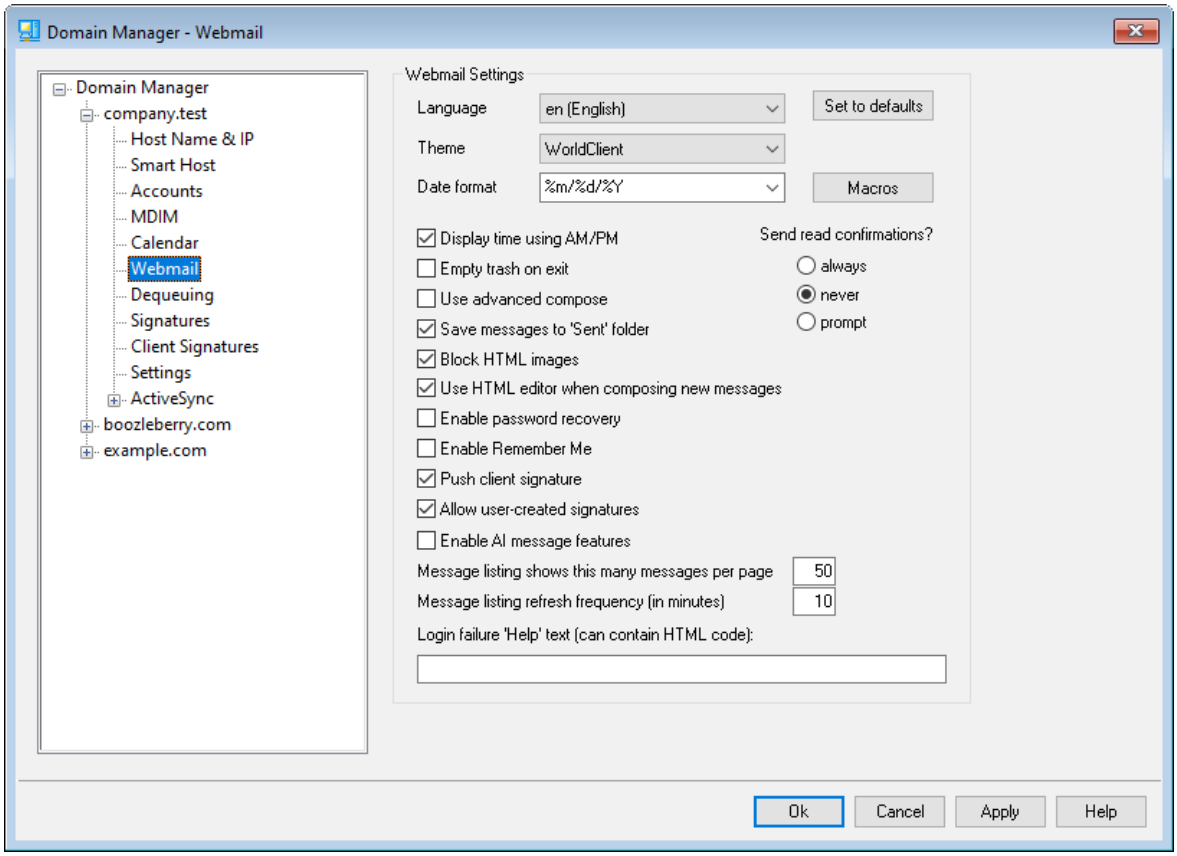
Allow users to query X months worth of Free/Busy data
Use this option to designate how many months worth of Free/Busy data your users may query.

See:

Webmail » Calendar 322

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.6 Webmail



This screen governs various Webmail client-level options for this domain. When a user signs in to Webmail, these options govern how Webmail initially works for that user. Many of these settings can then be customized by the user via the Options pages within Webmail. The default settings of this screen are determined by the Webmail » Settings 333 screen located on the Web & IM Services dialog.

Webmail Settings

Set to defaults
This button resets a domain to the Default Webmail Settings 333.

Language
Use the drop-down list box to choose the default language in which the Webmail interface will appear when your users first sign in to the selected domain. Users can change their personal language setting on the Webmail Sign-in page, and through an option in Options » Personalize within Webmail.

Theme
Use this drop-down list box to designate the default Webmail theme to use for the selected domain's users whenever they sign in for the first time. The users can personalize the theme setting from Options » Personalize within Webmail.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Date format
Use this text box to designate how dates will be formatted for the selected domain. Click the *Macros* button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

%A — Full weekday name

%B — Full month name

%d — Day of month (displays as "01-31")

%m — Month (displays as "01-12")

%y — 2-digit year

%Y — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in Webmail as "`12/25/2011`".

Macros
Click this button to display the list of macro codes that can be used in the *Date format*.

Send read confirmations?
This option governs how Webmail will respond to incoming messages that contain a request for read confirmation.

always
If this option is selected, MDaemon will send a notification to the sender indicating that the message was read. The Webmail user who received the message will not see any indication that the read confirmation was requested or responded to.

never
Choose this option if you want Webmail to ignore read confirmation requests.

prompt
Select this option if you wish to ask Webmail users whether or not to send a read confirmation each time a message is opened that requests it.

Display time using AM/PM
Click this option if you want a 12-hour clock with AM/PM to be used within Webmail for times displayed for this domain. Clear the check box if you want to use a 24-hour clock for the domain. Individual users can modify this setting via the "*Display my hours in an AM/PM format*" option located on the Options » Calendar page within Webmail.

Empty trash on exit
This option causes the user's trash to be emptied when he or she signs out from Webmail. Individual users can modify this setting from the Options » Personalize page within Webmail.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use advanced compose
Check this box if you wish the domain's users to see the Advanced Compose screen in Webmail rather than the normal Compose screen by default. Individual users can modify this setting from Options » Compose within Webmail.

Save messages to 'Sent' folder
Click this option if you want a copy of each message that you send to be saved in your mailbox's *Sent* folder. Individual users can modify this setting from the Options » Compose page within Webmail.

Block HTML images
Enable this check box if you wish to prevent remote images from being displayed automatically when viewing HTML email messages in Webmail. In order to view the images the user must click the bar that appears above the message in the browser window. This is a spam prevention feature, because many spam messages contain images with special URLs that identify the email address of the user who viewed the images, thus confirming to the spammer that it is a valid, working address. This option is enabled by default.

Use HTML editor when composing new messages
Check this box if you want the domain's users to see the HTML compose editor by default in Webmail. They can control this setting for themselves from Options » Compose within **Webmail**.

Enable password recovery
If enabled, domain users who have permission to edit their password 703 will be able to enter an alternate email address in Webmail, which can be sent a link to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in Webmail on the Options » Security page. Once set, if the user attempts to log in to Webmail with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page. This feature is disabled by default.

You can enable or disable this option on a per-user basis by adding the following key to a Webmail user's `user.ini` file (e.g. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (or "=No" to disable the option for the
user)
```

Allow Two Factor Authentication Remember Me (also applies to Remote Admin)
When someone uses Two-Factor Authentication (2FA) when signing in to Webmail or Remote Admin, there is ordinarily a Remember Me option available to the user on the 2FA authentication page, which will prevent the server from requiring 2FA again from that user for a set number of days (see the "*Enable Remember Me*" option below). Clear this checkbox if you do not wish to display the 2FA Remember Me option, which means all users with 2FA enabled will have to enter a 2FA code every time they sign in. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable Remember Me
Check this box if you want there to be a *Remember Me* checkbox on the MDaemon Webmail sign-in page when the domain's users connect via the https 316 port. If users check this box at sign-in, their credentials will be remembered for that device. Then any time they use that device to connect to Webmail in the future they will be signed in automatically, until such time that they manually sign out of their account or their Remember Me token expires.

By default, user credentials are remembered for a maximum of 30 days before the user is forced to sign in again. If you wish to increase the expiration time then you can do so by changing the value of the *Expire Remember Me tokens after this many days* option in the MDaemon Remote Administration (MDRA) 341 web-interface. You can also change it by editing the `RememberUserExpiration=30` key in the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. The expiration value can be set to a maximum of 365 days. **Note:** Two-Factor Authentication 703 (2FA) has its own Remember Me expiration key (`TwoFactorAuthRememberUserExpiration=30`), located in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. Therefore 2FA will again be required at sign-in when the 2FA Remember Me token expires, even if the regular token is still valid.

The *Remember Me* option is disabled by default and applies only to this domain. The global option is located on the Webmail Settings 333 screen.

Because *Remember Me* allows users to have a persistent login on multiple devices, users should be discouraged from using it on public networks. Further, if you ever suspect that an account may have had a security breach, in MDRA there is a *Reset Remember Me* button that you can use to reset Remember Me tokens for all users. This will require all users to sign-in again.

Push client signature
Check this box if you wish to push the Client Signatures 200 to this domain's Webmail users. In Webmail, this will create a signature called "System" under the signature options at: **Options » Compose**. Users can then choose to have this signature automatically inserted into the compose view when composing a new message. If this option is enabled but you have not created a client signature on the Domain Manager's Client Signatures screen, the Default Client Signatures 132 option will be used instead. If there is no default client signature either, then there will be no System signature option in Webmail.

Allow user-created signatures
Check this box if you wish to allow this domain's users to create their own custom signatures in Webmail. Users can then choose which signature they wish to insert into the compose view automatically when composing messages. When you do not allow user-created signatures, but the *Push client signature* option above is enabled, only the Client Signature 132 (i.e. the System signature in Webmail) can be inserted automatically. In Webmail, the signature options are located at: **Options » Compose**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable AI message features
Check this box if you wish to enable support for MDaemon's AI Message Features in MDaemon Webmail for this domain. The default state of this option is inherited from the setting of the same name located on the main Webmail Settings 333 dialog. Changing this domain-specific setting will override that default option. **Note:** enabling AI message features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services 703 screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features. See: "Webmail's AI Message Features 191" below for important information and cautions about using these features.

Message listing shows this many messages per page
This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from Options » Personalize within Webmail.

Message listing refresh frequency (in minutes)
This is the number of minutes that Webmail will wait before automatically refreshing the Message Listing. Individual users can modify this setting from Options » Personalize within Webmail.

Login failure 'Help' text (can contain HTML code)
You can use this option to specify a sentence of text (either plain text or HTML) to display on the Webmail sign-in page when a user encounters a problem signing in. The text is displayed below the following default text: "*Incorrect Logon, please try again. If you need assistance please contact your email administrator.*" This text could be used to direct users to a page or contact info for help regarding signing in to Webmail.

In order for this feature to work accurately with multiple domains, a valid SMTP host name 177 setup is required for each domain, otherwise the default domain's 174 text will be used. Therefore, for example, if you have multiple domains but direct all Webmail users to a single host name for sign-in, the correct, domain-specific *Login failure 'Help' text* may not be displayed.

Webmail's AI Message Features

As of MDaemon 23.5.0, the Pro theme in MDaemon's Webmail client includes various Artificial Intelligence (AI) features to help assist your users in managing their email and increasing productivity. These features are optional and disabled by default, but can be enabled for any user you choose.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

With these features, in MDaemon Webmail you can use AI to:

- Give you a summary of the contents of an email message.
- Suggest a reply to the message, according to several guidelines that you can instruct the AI to use. You can set the *Tone* of the reply to be professional, respectful or casual. The *Position*, or stance, to take in the reply can be set to interested or not interested, agree or disagree, or skeptical. The *Attitude* the reply should convey can be set to confident, excited, calm, or apologetic. Last, you can designate the *Length* of the reply, ranging from very brief to detailed.
- Assist you in composing a new email message, based on some text you have already included. As with the *Suggest a Reply* option above, you can also designate the Tone, Position, Attitude, and Length for the AI to use when composing the message.

The *Enable AI message features* option on the main Webmail Settings 333 dialog controls whether or not support for the AI features is enabled by default for your domains. There is an option of the same name located on the Domain Manager's Webmail 187 dialog that can be used to override that main setting for specific domains. **Note:** enabling AI Message Features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services 703 screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features.

Enabling accounts to use MDaemon's AI message features allows them to submit and receive information to and from third-party generative AI services, specifically ChatGPT by OpenAI. Administrators and users should therefore be aware that this introduces several potential privacy concerns due to the feature's ability to process personal data and generate potentially sensitive information. To address privacy concerns, it's vital for organizations to train their employees to use AI responsibly. **Note:** Data submitted to/from Open AI is not stored on the local server or on our network.

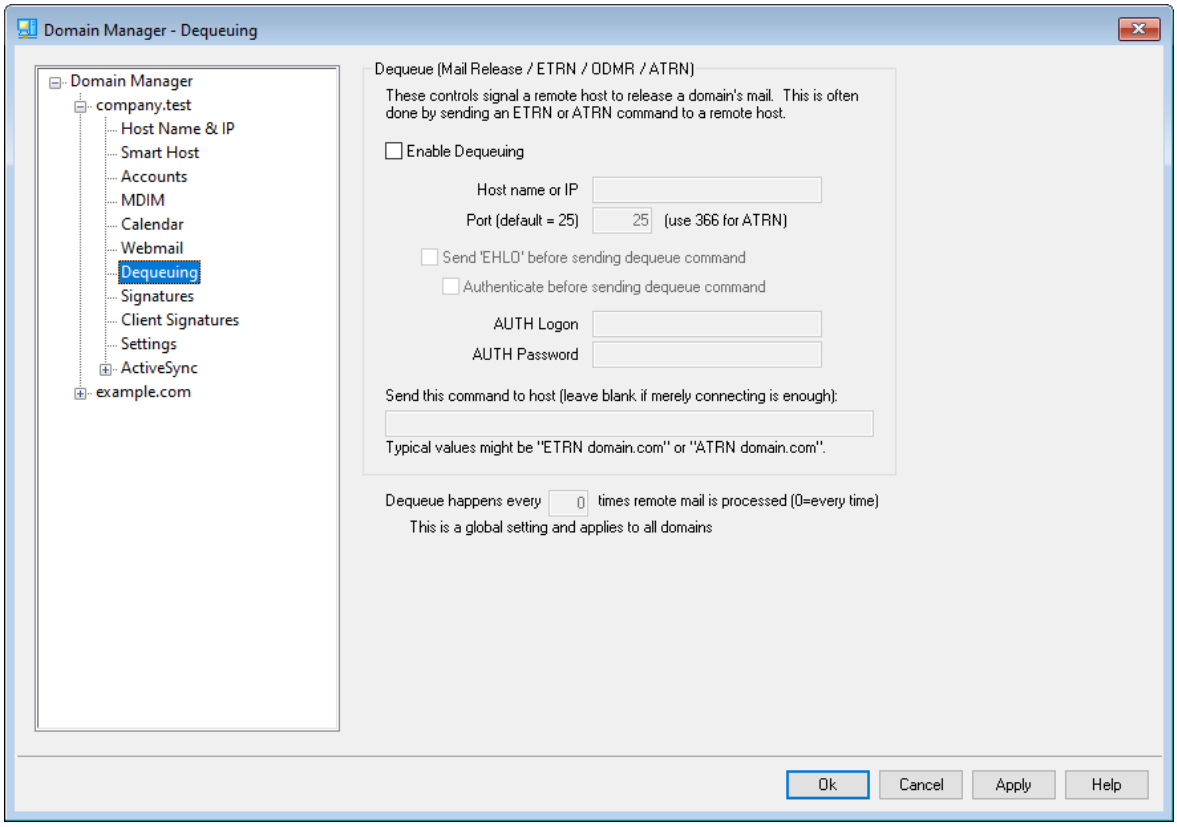
You can find MDaemon Technologies' AI Usage Policy at our Artifical Intelligence (AI) Information Page. On that same page there is also a link to OpenAI's Terms of Use.

See:

Webmail » Settings 333

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.7 Dequeuing



Dequeue (Mail Release/ ETRN/ODMR/ATRN)

Enable Dequeuing
When it is time to process remote mail MDaemon can connect to any server on any port and send any string that you wish to send. This is useful when you need to signal a remote server to release your mail by sending some string to them. For example, `ATRN`, `ETRN`, or `QSND`. You can also use this feature when a `FINGER` or `TELNET` session is briefly required in order for your remote host or ISP to determine that you are online.

Host name or IP
This is the host that will be signaled to release your mail.

Port
Enter the port on which you wish to make the connection. The default is 25 (the SMTP port), which is appropriate for the `ETRN` or `QSND` signaling method. Port 366 is typically used for `ATRN`, and port 79 is used for `FINGER`.

Send "EHLO" before sending the text string
If you enable this checkbox then you should be connecting to an SMTP server to signal release of your mail. This switch causes an SMTP session to be initiated with the specified host and allows the session to progress just beyond the SMTP "`EHLO`" stage before sending the unlock string.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Authenticate before sending the text string (required for ATRN)
As a security measure, some hosts or servers require clients to authenticate using ESMTP AUTH before releasing waiting messages. If this is the case for your mail host, click this checkbox and enter the required authentication credentials below.

Authentication is required when using the ATRN command to dequeue your email.

AUTH Logon
Enter the AUTH logon parameter here that is required by your host.

AUTH Password
Enter the AUTH password here.

Send this command to host (leave blank if merely connecting is enough)
This control is for specifying the text string that needs to be sent in order for your mail to be released. For example, the `ETRN` method requires the text "`ETRN`" followed by the domain name of the site being queued. Other methods require different text to be sent. Consult your ISP if you need more information on what to send to unlock your mail queue. If you have a choice of the method to use, we recommend using On-Demand Mail Relay (ODMR) 194 whenever possible. ODMR requires the ATRN command to be used in this option.

Dequeue happens every [xx] times remote mail is processed (0=every time)
By default the dequeue signal will be sent each time that remote mail is processed. Entering a number into this control will prevent the dequeue signal from being sent every time. It will be sent every x number of times as designated. For example, setting this value to "3" would cause the signal to be sent every third time that remote mail is processed.

This is a global setting and applies to all domains.

3.2.7.1 On-Demand Mail Relay (ODMR)

When you require a queue/dequeue method for hosting and releasing your email, we recommend using On-Demand Mail Relay (ODMR) whenever possible. This method is superior to ETRN and other methods in that in requires authentication before mail is released. Further, it utilizes an ESMTP command called `ATRN` that does not require the client to have a static IP address, because it immediately reverses the flow of data between the client and server, releasing the messages without having to make a new connection to do so (unlike ETRN).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

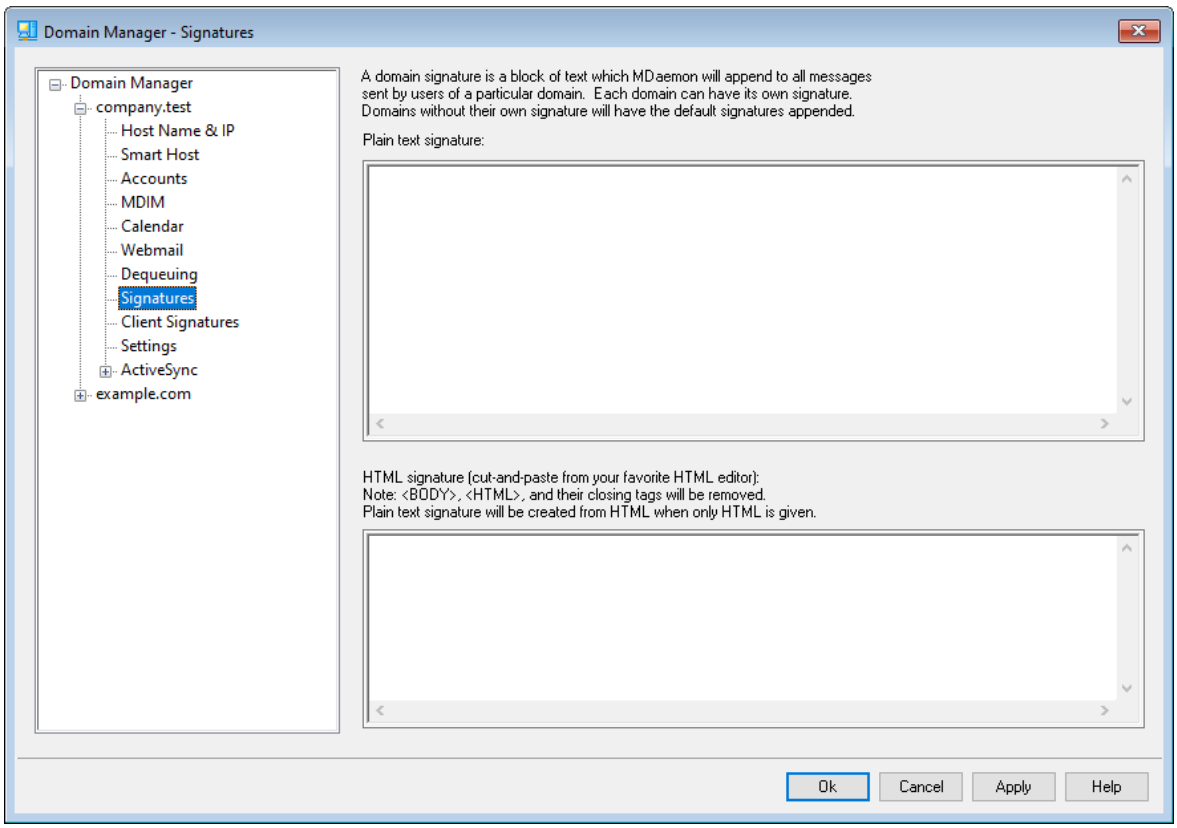
MDaemon fully supports ODMR on the client side via using the ATRN command and authentication controls on the Mail Release 193 screen, and on the server side using the Domain Gateways features on the Dequeuing 253 screen of the Gateway Editor.

Some mail servers do not support ODMR, therefore you should check with your provider before attempting to use it.

See:

Gateway Editor » Dequeuing 253

3.2.8 Signatures



Use this screen to append a signature to all messages sent by this domain's users. If no signature is specified here then the Default Signature 127 will be appended instead. Signatures are added to the bottom of messages, except for mailing list messages using a footer 287, in which case the footer is added below the signature. You can also use the Account Editor's Signature 737 feature to add individual signatures for each Account. Account signatures are added just before Default or Domain Signatures.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature, to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html will be used to create one.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

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

There are also several ways you can insert inline images into signatures from within MDaemon's Remote Administration 341 web interface:

- On the Signatures screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Signatures screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Signatures screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Signatures screen's HTML editor with Chrome, FireFox, MSIE 11+

<body></body> and <html></html> tags are not allowed in signatures and will be removed when found.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Users can control the placement of MDaemon signatures in their emails by placing any

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

of the **Signature Selector** macros into a message wherever they want the signature to appear.

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
Instant Messaging and Web	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
Address	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
Business Related	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

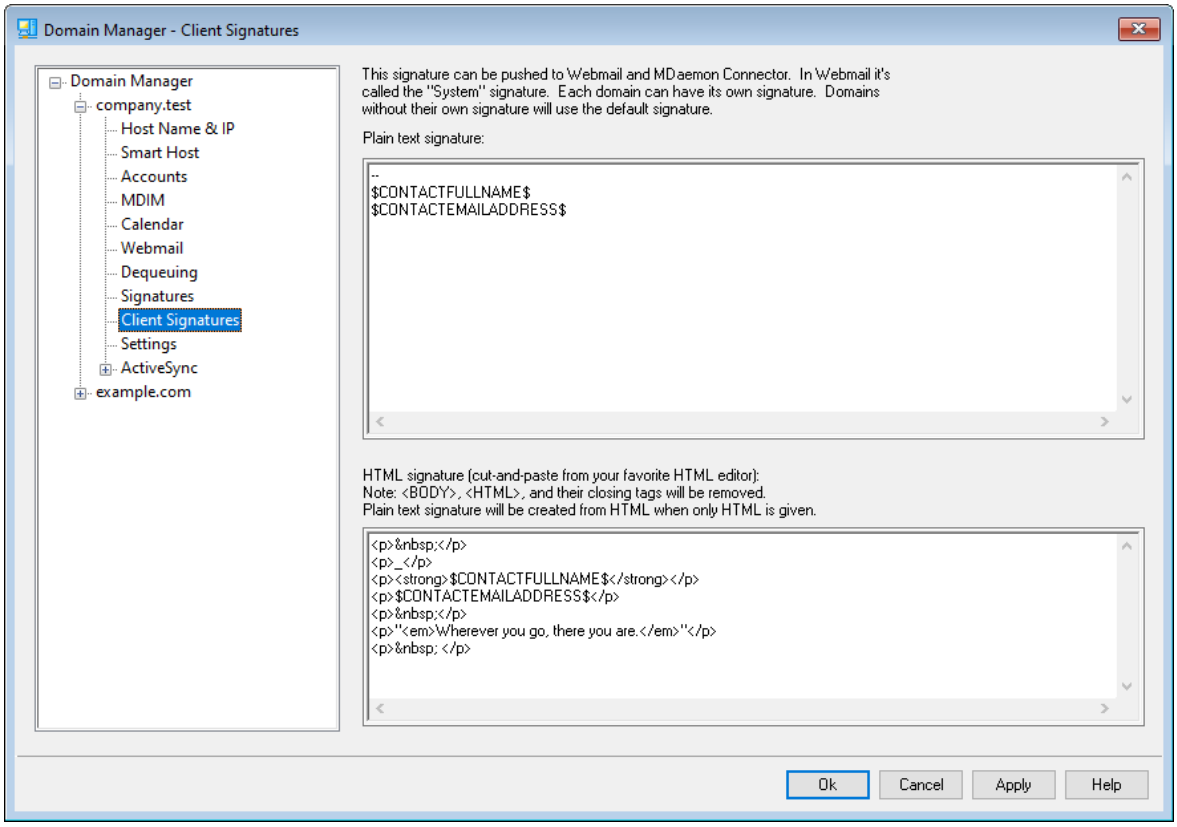
Business main phone	$CONTACTBUSINESSMAINPHONE$
Business phone	$CONTACTBUSINESSPHONE$
Business phone 2	$CONTACTBUSINESSPHONE2$
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Default Signatures 127
Account Editor » Signature 737

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.9 Client Signatures



Use this screen to create a client signature for this domain that you can push to MDaemon Webmail 187 and MDaemon Connector 397, to be utilized by your users when composing email messages. You can use the macros 201 listed below to personalize the signature, so that it will be unique for each user, including elements like the user's name, email address, phone number, and the like. Use the Default Client Signatures 132 screen if you wish to create a different signature that will be used when no domain-specific client signature has been made. When a domain-specific signature exists it will be used instead of the Default Client Signature. Use the *Push client signature* 187 option if you wish to push the client signature to Webmail and the *Push client signature to Outlook* 397 option if you wish to push it to MDaemon Connector. In Webmail's Compose options, the pushed client signature is called "System." For MDaemon Connector you can designate a name for the signature that will appear in Outlook.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages, use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature*

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

area above, MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html will be used to create one.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

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

There are also several ways you can insert inline images into signatures from within MDaemon's Remote Administration 341 web interface:

- On the Client Signature screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Client Signature screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Client Signature screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Client Signature screen's HTML editor with Chrome, FireFox, MSIE 11+

<body></body> and <html></html> tags are not allowed in signatures and will be removed when found.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Users can control the placement of MDaemon signatures in their emails by placing any of the **Signature Selector** macros into a message wherever they want the signature to appear.

Signature Selector

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Other phone	$CONTACTOTHERPHONE$
Instant Messaging and Web	
IM Address	$CONTACTIMADDRESS$
IM Address 2	$CONTACTIMADDRESS2$
IM Address 3	$CONTACTIMADDRESS3$
MMS Address	$CONTACTMMSADDRESS$
Home web address	$CONTACTHOMEWEBADDRESS$
Address	
Home address	$CONTACTHOMEADDRESS$
Home city	$CONTACTHOMECITY$
Home state	$CONTACTHOMESTATE$
Home zip code	$CONTACTHOMEZIPCODE$
Home country	$CONTACTHOMECOUNTRY$
Other address	$CONTACTOTHERADDRESS$
Other city	$CONTACTOTHERCITY$
Other state	$CONTACTOTHERSTATE$
Other zip code	$CONTACTOTHERZIPCODE$
Other country	$CONTACTOTHERCOUNTRY$
Business Related	
Business Name	$CONTACTBUSINESSCOMPANY$
Yomi Business Name	$CONTACTYOMICOMPANYNAME$
Business title	$CONTACTBUSINESSTITLE$
Business office	$CONTACTBUSINESSOFFICE$
Business department	$CONTACTBUSINESSDEPARTMENT$
Business manager	$CONTACTBUSINESSMANAGER$
Business assistant	$CONTACTBUSINESSASSISTANT$
Business assistant phone	$CONTACTBUSINESSASSISTANTPHONE$
Business main phone	$CONTACTBUSINESSMAINPHONE$
Business phone	$CONTACTBUSINESSPHONE$
Business phone 2	$CONTACTBUSINESSPHONE2$

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

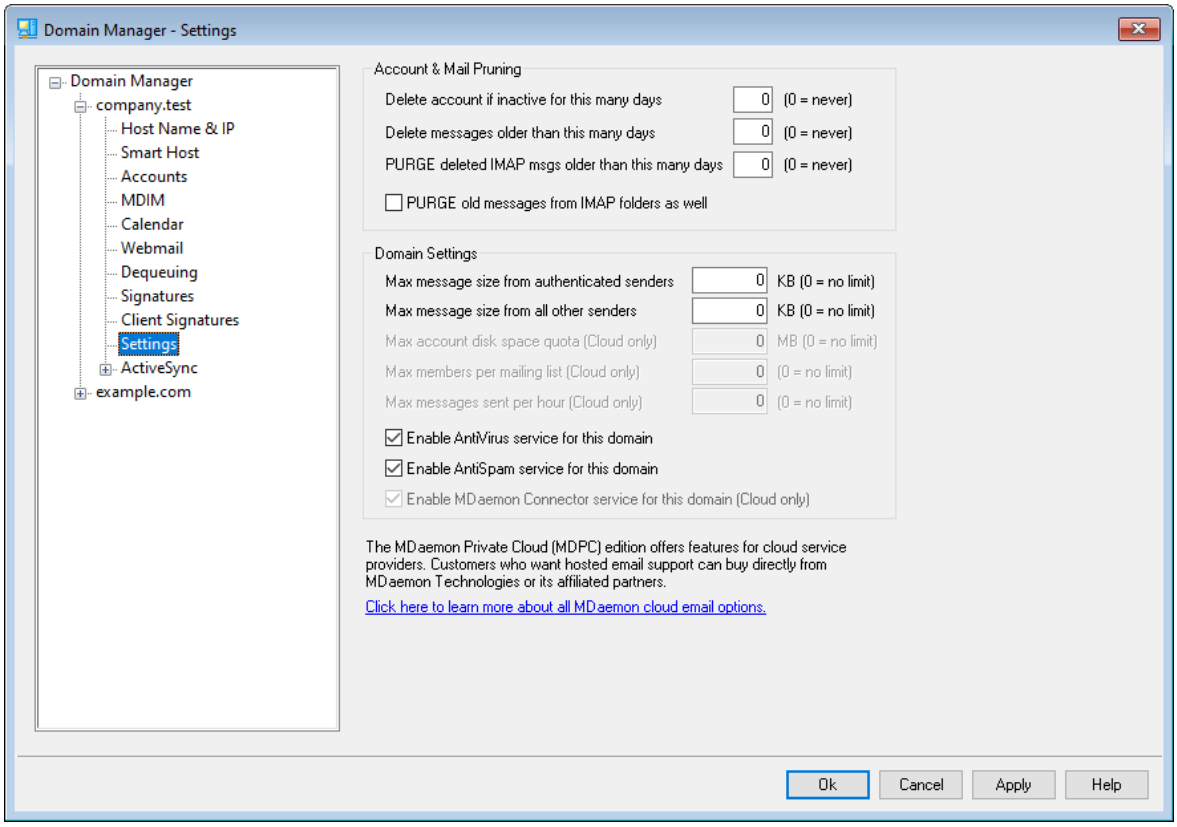
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Default Client Signatures 132
Default Signatures 127
Domain Manager » Signatures 195
Account Editor » Signature 737
Domain Manager » Webmail Settings 187
MC Client Settings » Signature 397

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.10 Settings



Account & Mail Pruning

These options are used to designate when or if inactive accounts or old messages will be deleted by MDaemon. Each day at midnight MDaemon will remove all messages and accounts that have exceeded the time limits stated. There are similar options on the Account Editor's Quotas 715 screen that can be used to override these settings for individual accounts.

See `AccountPrune.txt` in the "...`MDaemon\App\`" folder for more information and command line options.

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow an account belonging to this domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age. **Note:** This option's setting does not apply to messages contained in IMAP folders unless you also enable the "*PURGE old messages from IMAP folders as well*" option below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in your users' folders. Messages flagged for deletion longer than this number of days will be purged from their mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than this many days*" option above to apply to messages in IMAP folders as well. When this control is disabled, regular messages contained in IMAP folders will not be deleted due to their age.

Domain Settings

Max message size from authenticated senders [xx] KB (0=no limit)
Use this option if you wish to set a limit on the size of messages that an authenticated sender can send to the domain. The value is in Kilobytes and set to "0" by default, which means no limit. If you wish to set a message size limit for non-authenticated senders, use the "*...all other senders*" option below.

Max message size from all other senders [xx] KB (0=no limit)
Use this option if you wish to set a limit on the size of messages that a non-authenticated sender can send to the domain. The value is in Kilobytes and set to "0" by default, which means no limit. If you wish to set a message size limit for authenticated senders, use the previous option.

Max account disk space quota [xx] MB (0=no limit) (Cloud only)
Use this option if you wish to set a limit on how much disk space the domain can use. This option is only available in MDaemon Private Cloud.

Max members per mailing list [xx] (0=no limit) (Cloud only)
Use this option if you wish to set a maximum number of members allowed for each of this domain's mailing lists. There is a corresponding global option on the Mailing List Manager's Settings 262 screen. This option is only available in MDaemon Private Cloud.

Max messages sent per hour [xx] (0=no limit) (Cloud only)
Use this option if you wish to designate a maximum number of messages that the domain can send per hour. Once this limit is reached, further messages are left in the queue until the count resets. Message counts are reset hourly and when the server is restarted. This option is only available in MDaemon Private Cloud.

Enable AntiVirus service for this domain
Click this check box if you want the AntiVirus 630 settings to be applied to this domain.

Enable AntiSpam service for this domain
Click this check box is you want MDaemon's current Spam Filter settings to be applied to this domain.

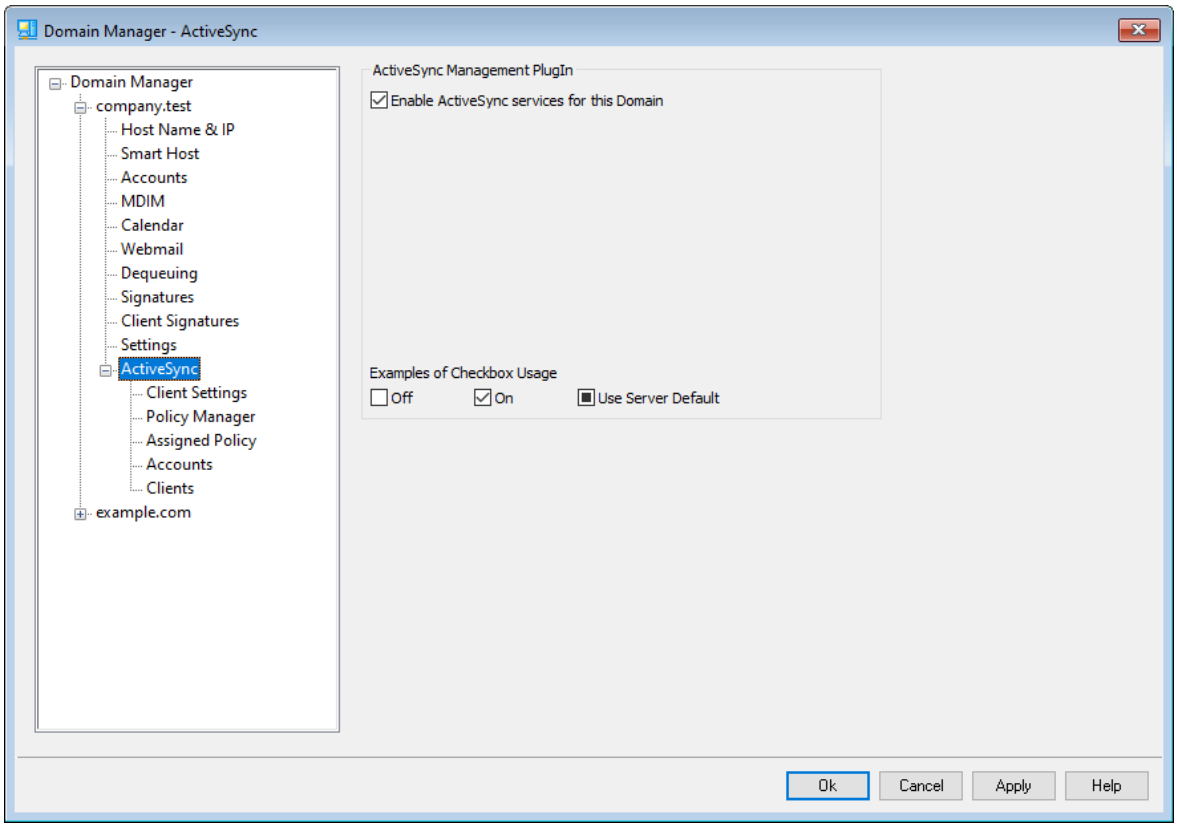
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable MDaemon Connector service for this domain (Cloud only)
Check this box if you wish to enable the MDaemon Connector 379 service for this domain.

See:

Account Editor » Quotas 715

3.2.11 ActiveSync



Use this section of the Domain Manager to administer the domain's ActiveSync 408 settings. You can manage the ActiveSync settings and defaults for all domains from the ActiveSync Manager's Domains 426 screen.

ActiveSync for MDaemon Management Plugin

Enable ActiveSync Service for this Domain
This option controls whether or not the domain's users will by default be able to use an ActiveSync client to access their email and PIM data. By default the state of this setting is inherited from the Default ActiveSync State 426, but you can override that setting if you choose by toggling the checkbox to either on or off. This setting can also be overridden for any accounts 442 or clients 451 that you do not wish to use the domain's setting. **NOTE:** If you disable ActiveSync for this domain, a confirmation box will open to ask if you wish to revoke ActiveSync access for all of the domain's

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

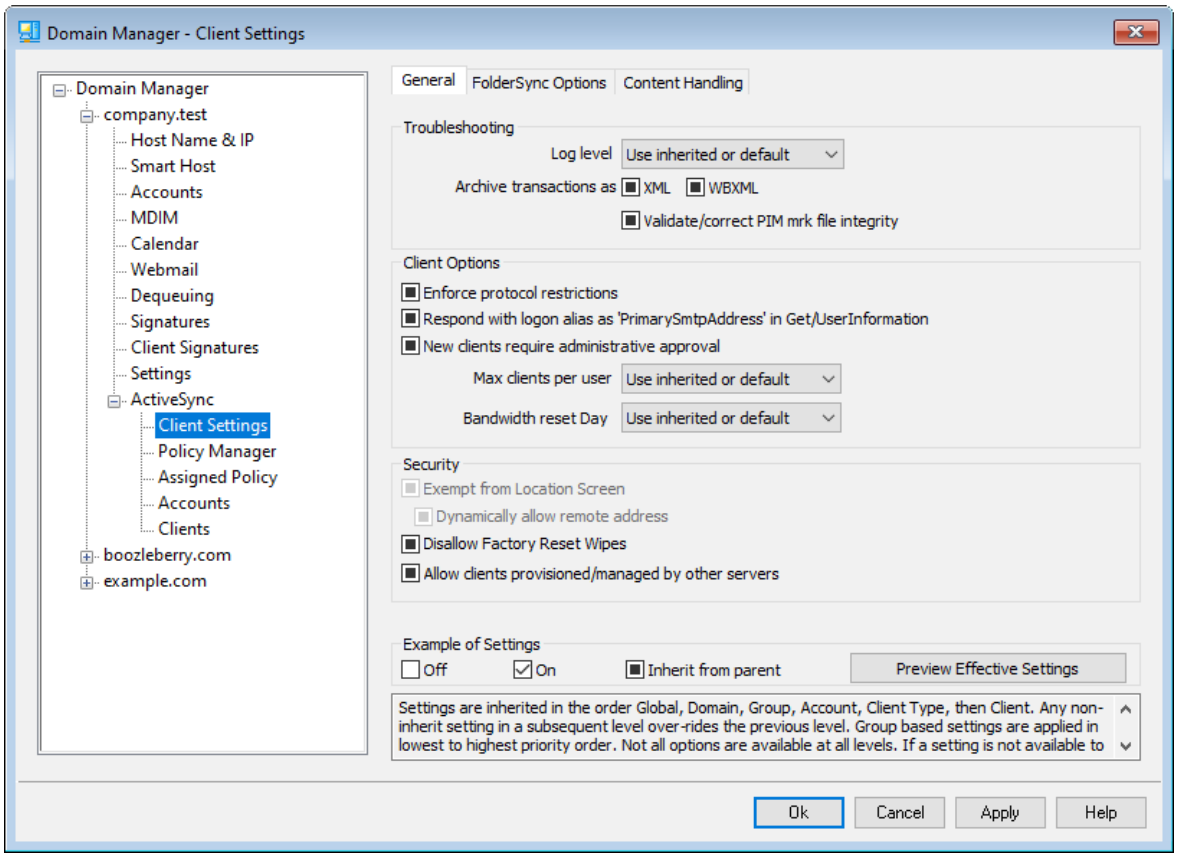
users. Choose **No** if you wish to allow any of the domain's users who currently use ActiveSync to continue using it. If you choose **Yes**, then ActiveSync will be disabled for all of that domain's users.

This setting simply controls whether or not any of the domain's accounts will be permitted to use ActiveSync by default, when the ActiveSync service is running. The global option to **Enable the ActiveSync protocol** 408 must be enabled in order for ActiveSync to be accessible to permitted domains or accounts.

See:

ActiveSync » Domains 426
ActiveSync » Accounts 442
ActiveSync » Clients 451

3.2.11.1 Client Settings



This screen allows you to manage the default settings for accounts and clients associated with the domain.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the global Client Settings 413 screen. Similarly, this domain's accounts 181 will inherit their settings from this screen, since it is their parent screen. Any changes made to the options on this screen will be reflected on those account screens. Below that, individual clients 232 also have settings screens that inherit their settings from the account-level settings. This configuration makes it possible for you to make changes to all of the domain's accounts and clients simply by making changes to this one screen, while also making it possible for you to override those settings for any account or client as needed.

General

Troubleshooting

Log level
ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug	This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.
Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.
Inherit	By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders 113 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders 726 to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients 451 and client types 466 that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol 424 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias 818 for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

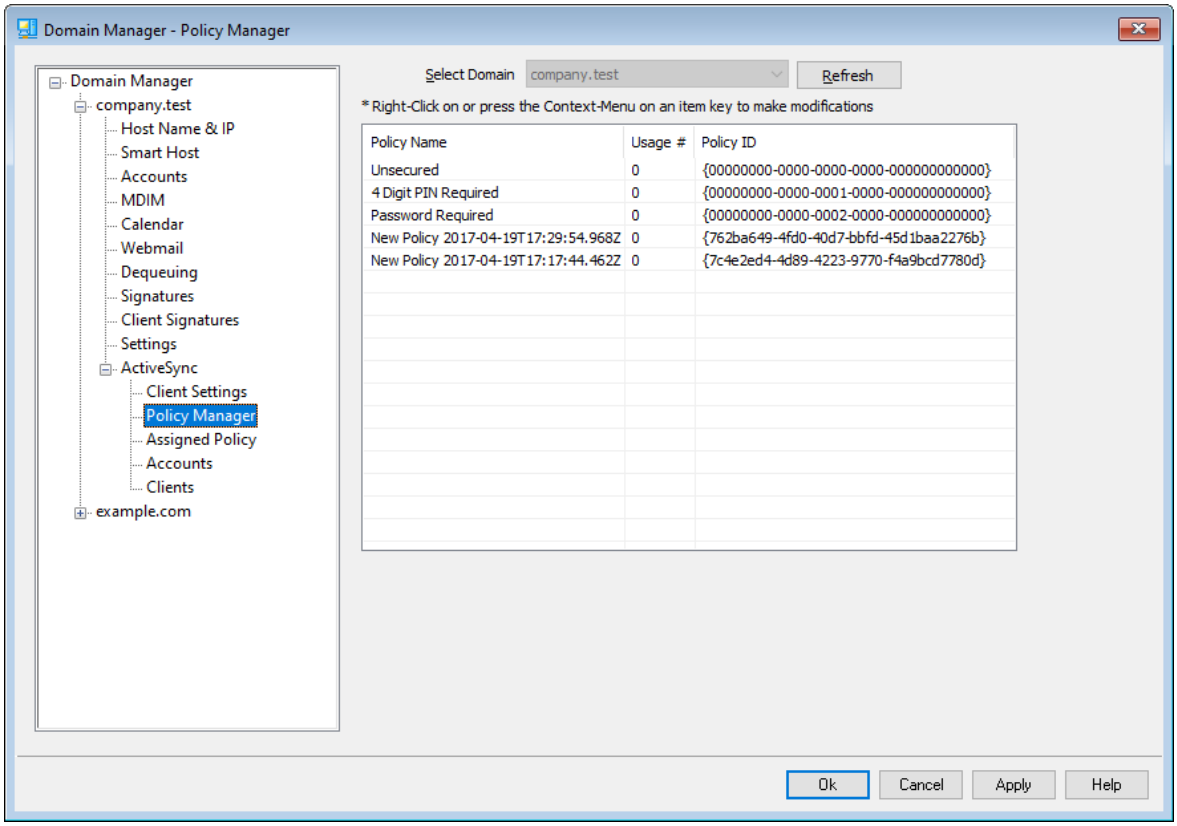
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 413
ActiveSync » Accounts 442
ActiveSync » Clients 451

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.11.2 Policy Manager



Use this screen to manage the ActiveSync Policies that can be assigned to user devices to govern various options. Predefined policies are provided, and you can create, edit and delete your own. Default and overriding policies can can be assigned to the domain and each account 442 and client 451 on their respective Assigned Policy screens.

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy to a device, it will not be applied to the device until the next time it connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

ActiveSync Policies

Right-click the list to open the shortcut menu with the following options:

Create Policy
Click this option to open the ActiveSync Policy Editor 215, used for creating and editing your policies.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete
To delete a policy, select a custom policy from the list and then click **Delete**. Click **Yes** to confirm the action. The predefined policies cannot be deleted.

Edit Policy
To edit a policy, right-click a custom policy from the list and then click **Edit Policy**. After making your desired changes in the policy editor, click **OK**. The predefined policies cannot be edited.

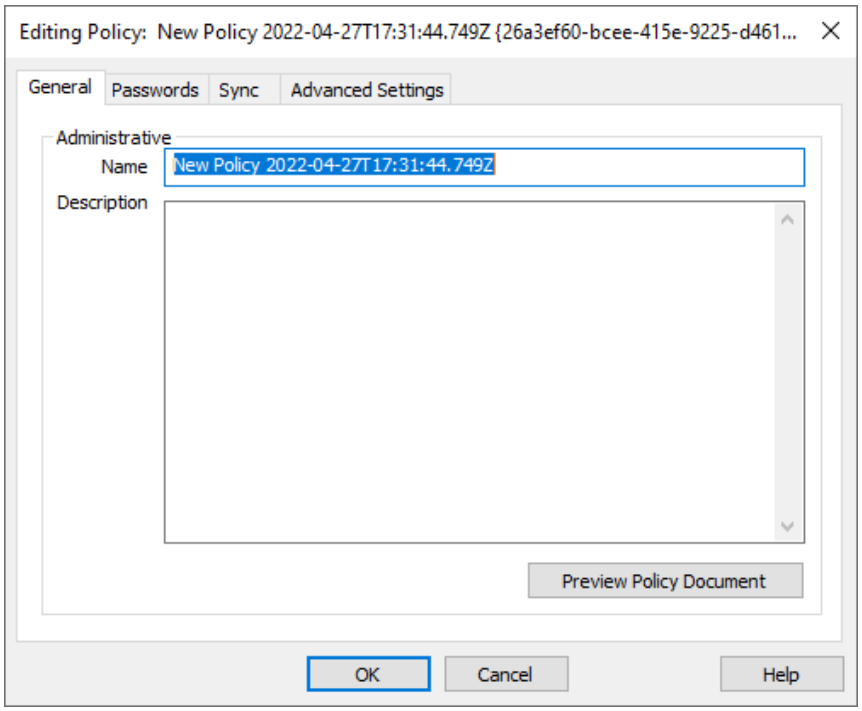
View Policy Usage
Right-click a policy and then choose this option to view a list of all domains, accounts, and clients that are set to use this policy.

ActiveSync Policy Editor

The ActiveSync Policy Editor has four tabs: General, Passwords, Sync, and Advanced Settings. The Advanced Settings tab is hidden unless you activate *Enable editing of advanced policy options* 408, located on the ActiveSync System screen.

General

Use this screen to designate a name and description for your policy. You can also preview the XML policy document.



Administrative

Name
Specify a name for your custom policy here.

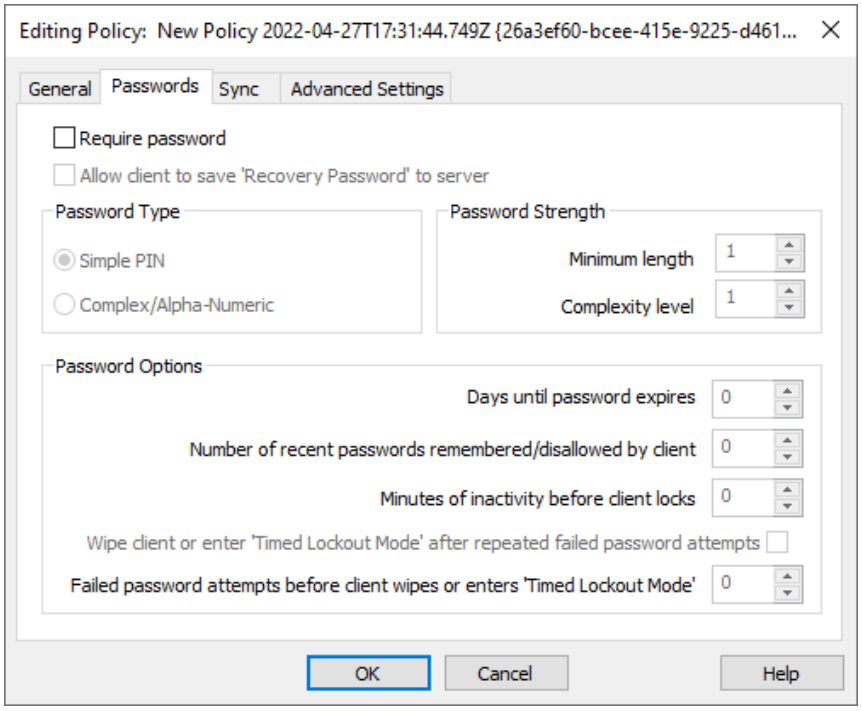
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Description
Use this area to describe your custom policy. This description appears on the Apply Policy dialog when selecting a policy to apply to a domain, account, or client.

Preview Policy Document
Click this button to preview the XML policy document for this policy.

Passwords

Password options and requirements for the policy are designated on this tab.



Require password
Check this box if you wish to require a password on the device. It is disabled by default.

Allow device to save 'Recovery Password' to server
Enable this option if you wish to allow clients to use ActiveSync's Recovery Password option, which allows a device to save a temporary recovery password to the server to unlock the device if the password is forgotten. The administrator can find this recover password under the client's Details 451. Most devices do not support this feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Password Type

Simple PIN
How this option is implemented is largely dependent on the device, but selecting *Simple PIN* as the password type generally means that no restrictions or complexity requirements are placed on the device password, other than the *Minimum password length* option below. This allows simple passwords such as: "111," "aaa," "1234," "ABCD" and the like.

Complex/Alpha-Numeric
Use this policy option if you wish to require more complex and secure device passwords than the *Simple PIN* option. Use the *Complexity level* option below to define exactly how complex the password must be. This is the default selection when a password is required by the policy.

Password Strength

Minimum length
Use this option to set the minimum number of characters that the device password must contain, from 1-16. This option is set to "1" by default.

Complexity level
Use this option to set the complexity level requirement for *Complex/Alpha-numeric* device passwords. The level is the number of different types of characters that the password must contain: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters (such as punctuation or special characters). You can require from 1-4 character types. For example, if this option were set to "2", then the password must contain at least two of the four character types: uppercase and numbers, uppercase and lowercase, numbers and symbols, and so on. This option is set to "1" by default.

Password Options

Days until password expires (0=never)
This is the number of days allowed before the device's password must be changed. This option is disabled by default (set to "0").

Number of recent passwords remembered/disallowed by device (0=none)
Use this option if you wish to prevent the device from reusing a specified number of old passwords. For example, if this option is set to "2" and you change your device password, you will not be able to change it to either of the last two passwords that were used. The option is disabled by default (set to "0").

Minutes of inactivity before device locks (0=never)
This is the number of minutes that a device can go without any user input before it will lock itself. This password option is disabled by default (set to "0").

Wipe device or enter 'Timed Lockout Mode' after repeated failed password attempts
When this option is enabled and the user fails the designated number of

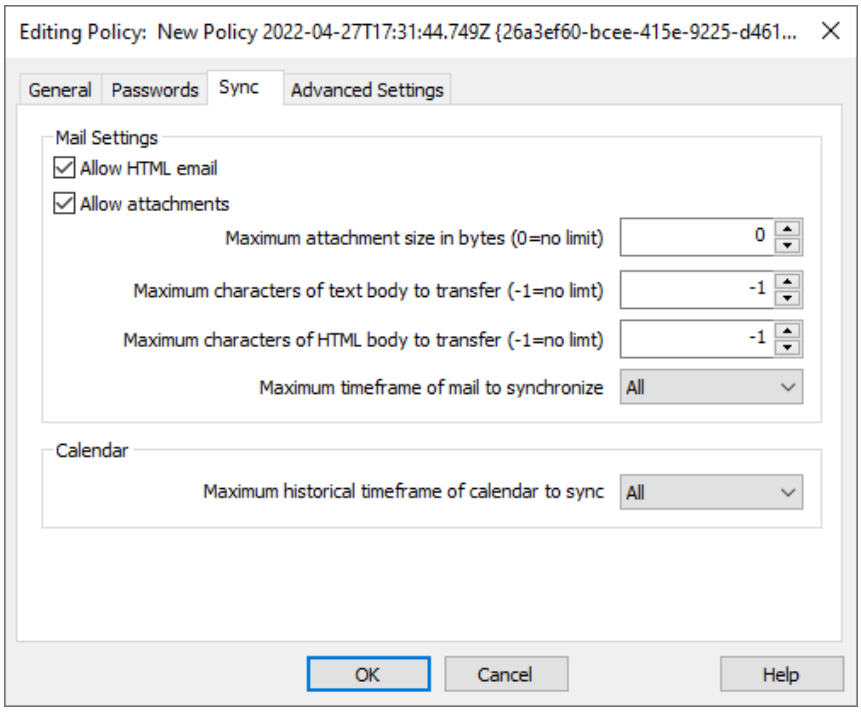
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

password attempts, the device will either lock itself for a certain amount of time or perform a wipe of all data, depending on the device. This option is disabled by default.

Failed password attempts before device wipes or enters 'Timed Lockout Mode'
When the "*Wipe device..*" option above is enabled and a user fails this many password attempts, the device will be wiped or the 'Timed Lockout Mode' will be triggered, depending on the device.

Sync

This screen contains various settings governing HTML email, allowing attachments, limiting the number of characters to transfer, and the maximum mail and calendar timeframes to sync.



Mail Settings

Allow HTML email
By default HTML-formatted email can be synced/sent to ActiveSync clients. Uncheck this box if you wish to send only plain text.

Allow attachments
Allows the device to download file attachments. This option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Max attachment size in bytes (0=no limit)
This is the maximum size of attachment that can be automatically downloaded to the device. There is no size limit set for this option by default (set to "0").

Maximum characters of text body to transfer (-1=no limit)
This is the maximum number of characters in the body of plain text-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum characters of HTML body to transfer (-1=no limit
This is the maximum number of characters in the body of HTML-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum timeframe of mail to synchronize
This is the amount of past email, by date range from today, that can be synchronized by the device. By default this is set to "All," meaning that all email can be synchronized no matter how old it is.

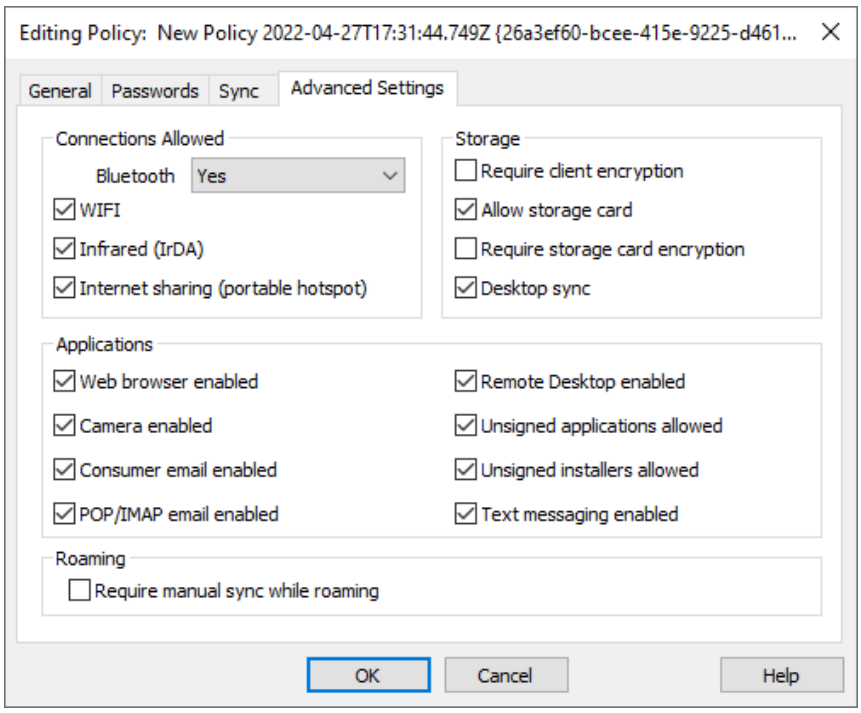
Calendar

Maximum historical timeframe of calendar to sync
This is how far back from today that past calendar entries can be synchronized by the device. By default this is set to "All," meaning that all past entries can be synchronized no matter how old they are.

Advanced Settings

The Advanced Settings tab contains options governing the types of connections allowed, whether certain applications can be enabled, storage and encryption, and roaming.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



This tab is hidden unless you activate *Enable editing of advanced policy options*[408], located on the ActiveSync for MDaemon screen.

Connections Allowed

Bluetooth
Use this option to designate whether or not Bluetooth connections are allowed on the device. You can choose **Yes** to allow Bluetooth connections, **No** to prevent them, or **Handsfree** to restrict Bluetooth to Handsfree only. This option is set to **Yes** by default.

WIFI
Allows WIFI connections. Enabled by default.

Infrared (IrDA)
Allows Infrared (IrDA) connections. Enabled by default.

Internet sharing (portable hotspot)
This option allows the device to use Internet sharing (portable hotspot). It is enabled by default.

Storage

Require device encryption
Click this option if you wish to require encryption on the device. Not all devices will enforce encryption. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow storage card
Allows a storage card to be used in the device. This is enabled by default.

Require storage card encryption
Use this option if you wish to require encryption on a storage card. This is disabled by default.

Desktop sync
Allows Desktop ActiveSync on the device. Enabled by default.

Applications

Web browser enabled
Allows the use of a browser on the device. This option is not supported on some devices, and it may not apply to 3rd party browsers. It is enabled by default.

Camera enabled
Allows the use of a camera on the device. This option is enabled by default.

Consumer email enabled
Device allows the user to configure a personal email account. When disabled, the types of email accounts or services that are prohibited is entirely dependent on the particular ActiveSync client. This option is enabled by default.

POP/IMAP email enabled
Allows access to POP or IMAP email. Enabled by default.

Remote Desktop enabled
Allows the client to use Remote Desktop. Enabled by default.

Unsigned applications allowed
This option allows unsigned applications to be used on the device. This is enabled by default.

Unsigned installers allowed
This option allows unsigned installers to be run on the device. This is enabled by default.

Text messaging enabled
This option allows text messaging on the device. Text messaging is enabled by default.

Roaming

Require manual sync while roaming
Use this policy option if you wish to require the device to synchronize manually while roaming. Allowing automatic synchronization while roaming

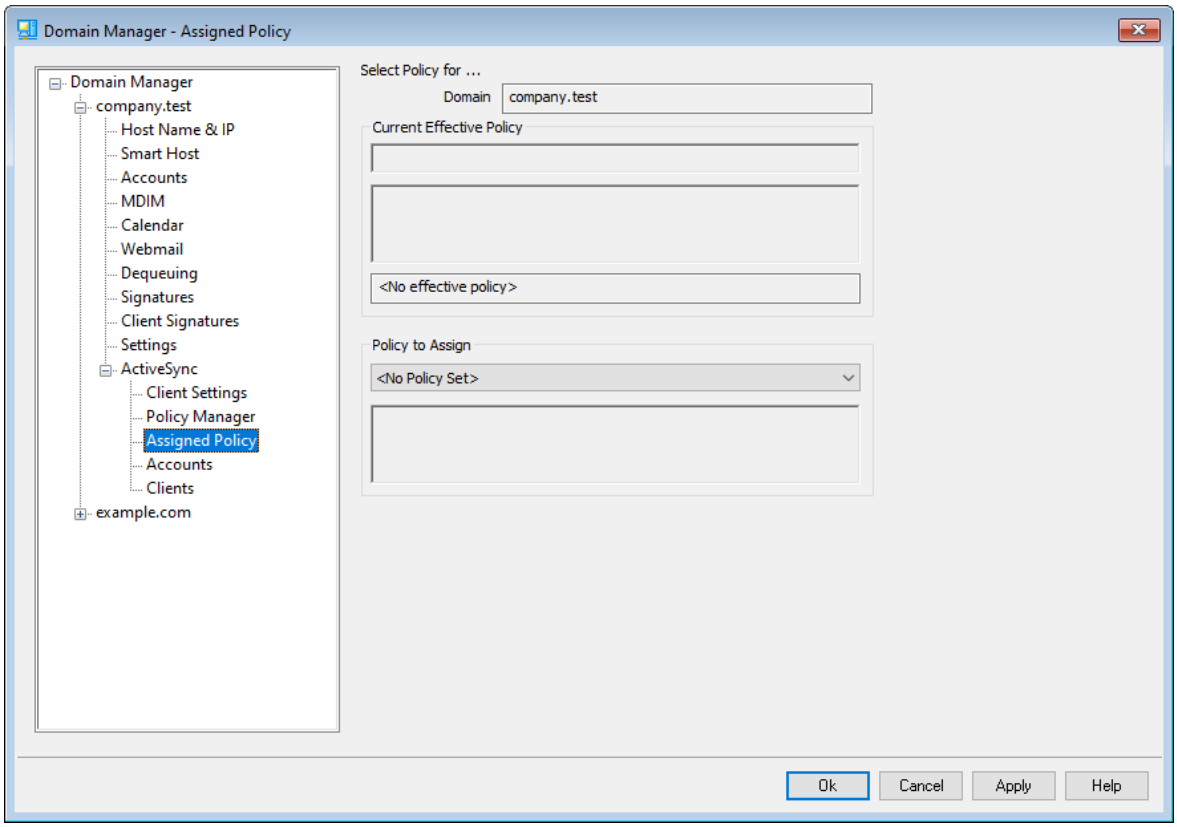
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

could increase data costs for the device, depending on its carrier and data plan. This option is disabled by default.

See:

Domain Manager » Assigned Policy 222
ActiveSync » Accounts 442
ActiveSync » Clients 451

3.2.11.3 Assigned Policy



Use this screen to assign the default ActiveSync policy 214 for the domain. When an ActiveSync client connects using one of this domain's accounts, this is the policy that will be assigned to the client, unless an alternate policy has been set specifically for that account.

Assigning a Default ActiveSync Policy

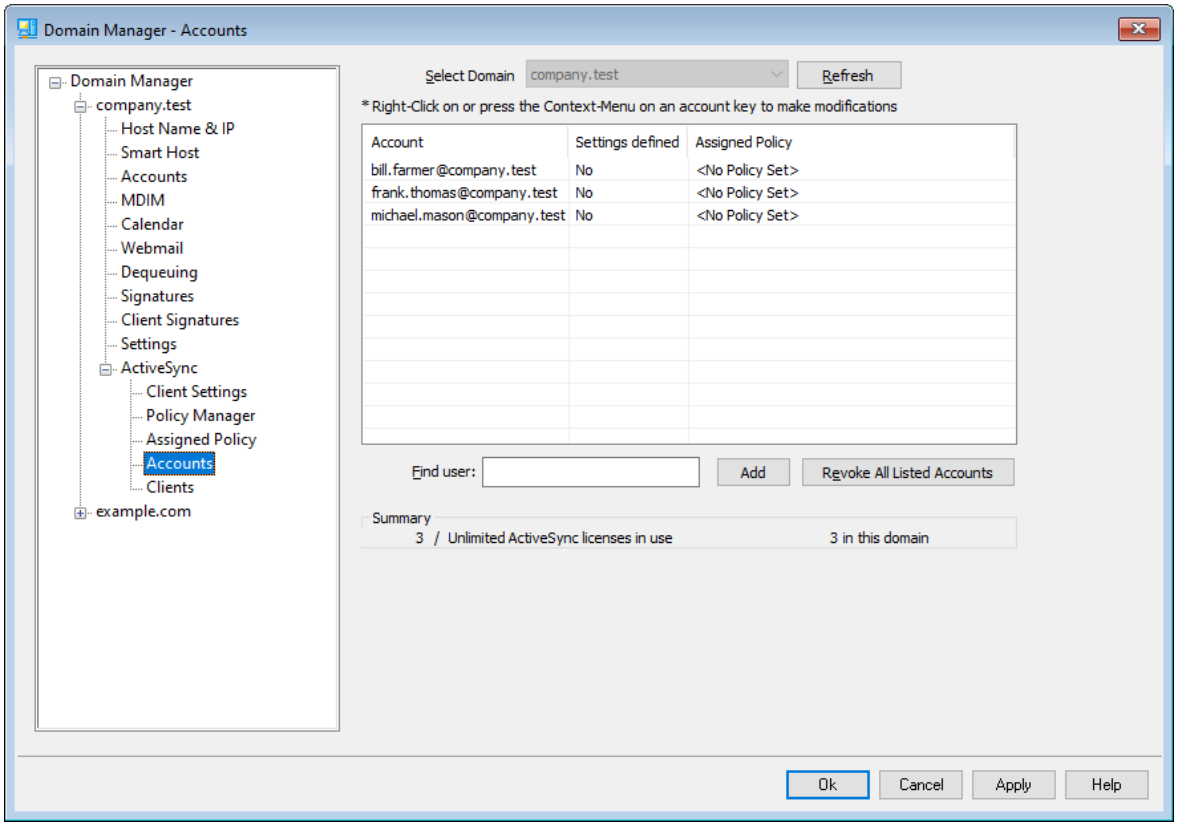
To assign a default ActiveSync policy for the domain, click the **Policy to Assign** drop-down list, select the desired policy, and click **Ok**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Domain Manager » Policy Manager 214
ActiveSync » Accounts 442
ActiveSync » Clients 451

3.2.11.4 Accounts

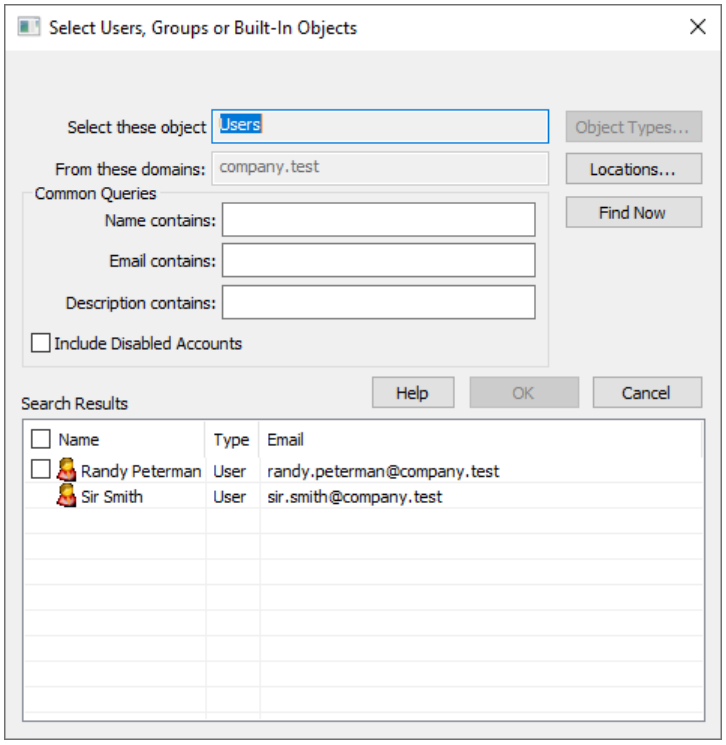


Use this screen to designate the domain's accounts that are authorized to use ActiveSync, and you can edit each authorized account's client settings and assign its ActiveSync policy.

Authorizing Accounts

Click **Add** to manually authorize one or more of the domain's accounts to use ActiveSync. This opens the Select Users dialog for finding and selecting the accounts.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description[697]. Leave these fields blank if you want the search results to contain every user that matches the Locations specified above.

Include Disabled Accounts
Check this box if you wish to include disabled accounts[697] in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired users in the Search Results and click **OK** to add them to the list of authorized accounts.

Revoking Accounts

To revoke an account's authorization to use ActiveSync, select it from the list and click **Revoke Selected Account**. If you wish to revoke all accounts, click the **Revoke All Accounts** button.

If you have enabled the option to *Authorize all accounts upon first access via ActiveSync protocol*[442], revoking an account's

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

access will remove it from the list, but the next time a device connects for the account it will be authorized again.

Assigning an ActiveSync Policy

To assign a Policy 434 to the account:

1. Select an account from the list.
2. Click **Assign Policy**. This opens the Apply Policy dialog.
3. Click the **Policy to Assign** drop-down list and choose the desired policy.
4. Click **OK**.

This policy will be assigned to any new device that connects for this account.

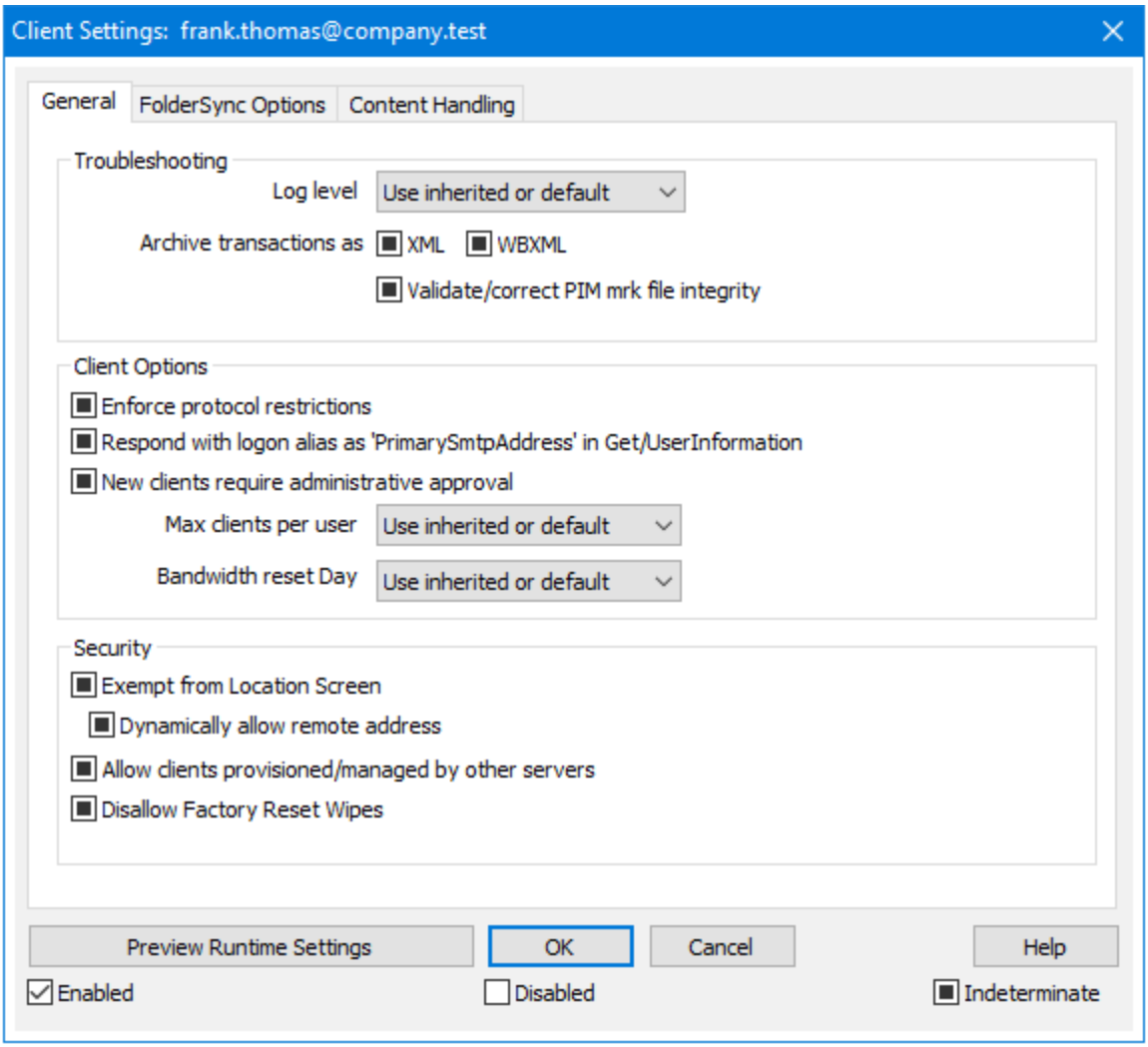
Searching the List of Authorized Accounts

If you have a large number of accounts authorized to use ActiveSync, you can use the **Find user** box to search the list for a specific account. Simply type the first few letters of the account's email address to select the user.

Settings

Select an account and click **Settings** to manage the Client Settings for the account. These settings will be applied to any ActiveSync clients that connect for the account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the domain's Client Settings 208 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the domain-level setting for this account.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder

By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders

By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders

By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy

Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching

Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)

By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders

Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

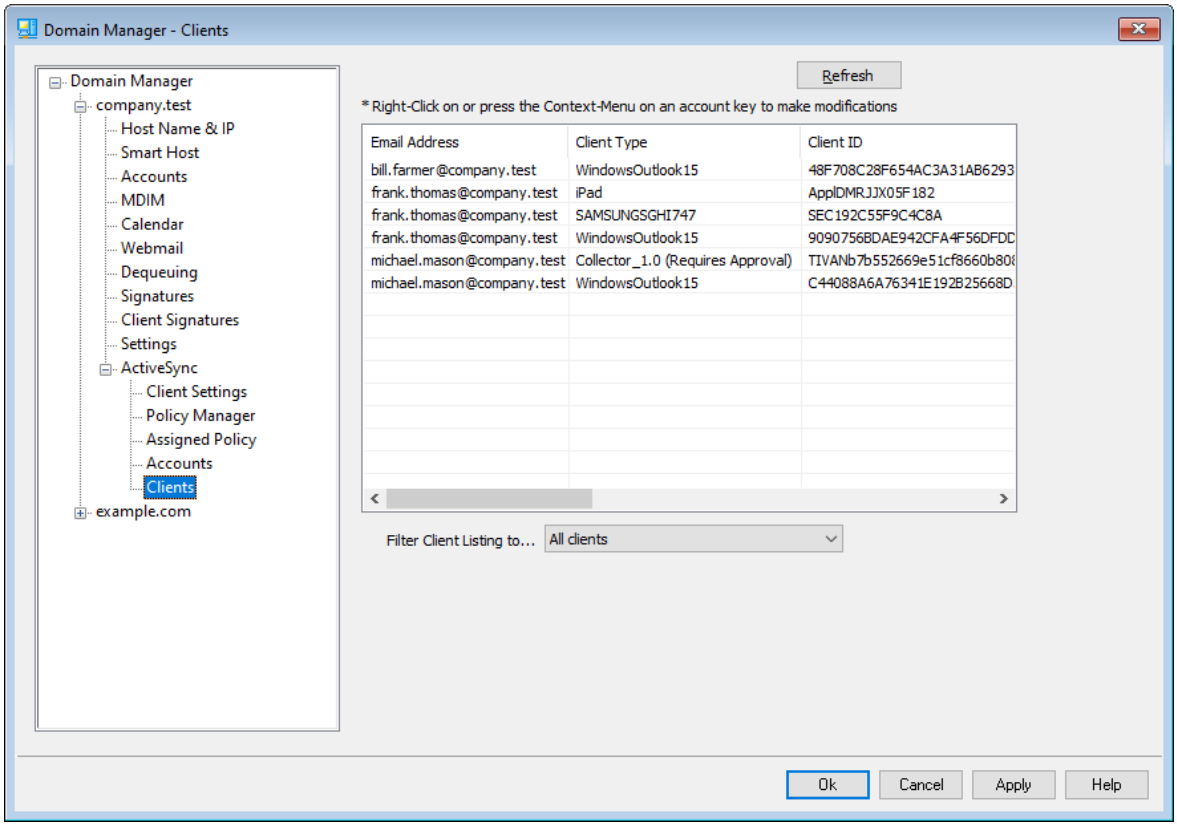
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 413
ActiveSync » Domains 426
ActiveSync » Clients 451

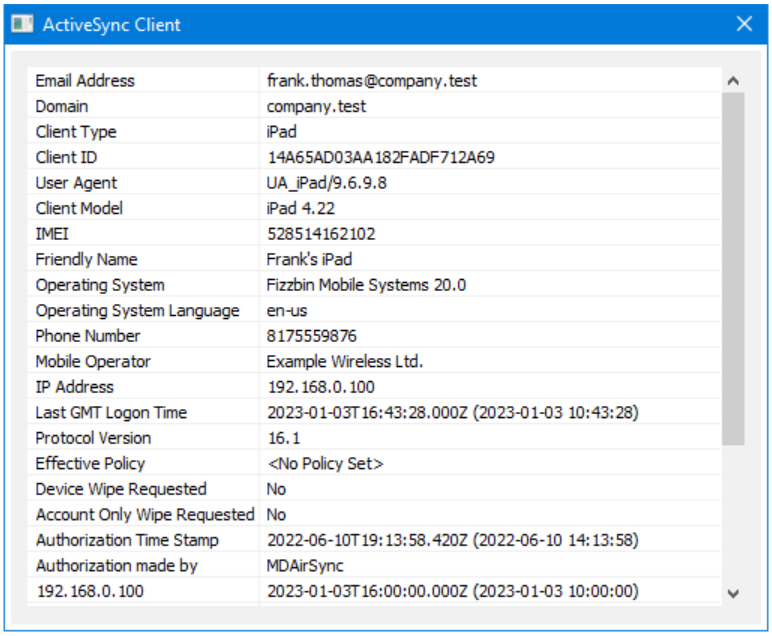
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.2.11.5 Clients



This screen contains an entry for each ActiveSync device associated with the domain.

ActiveSync Client Details



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Double-click an entry, or right-click the entry and click **View Client Details**, to open the Client Details dialog. This screen contains information about the client, such as its Client Type, Client ID, last login time, and the like.

Client Settings

Right-click a client and click **Customize Client Settings** to manage its Client Settings. By default these settings are inherited from the Client Type settings, but they can be adjusted however you like. See Managing a Device's Client Settings 234 below.

Assigning an ActiveSync Policy

To assign a Policy 434 to the device:

1. Right-click a device in the list.
2. Click **Apply Policy**. This opens the Apply Policy dialog.
3. Click the **Policy to Assign** drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Right-click an entry and then click **View Statistics** to open the Client Statistics dialog, containing various usage stats for the client.

Reset Statistics

If you wish to reset a client's statistics, right-click the client, click **Reset Statistics**, and then **OK** to confirm the action.

Removing an ActiveSync Client

To remove an ActiveSync client, right-click the client and click **Delete**, and then **Yes**. This will remove the client from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same client, MDaemon will treat the client as if it had never before been used on the server; all client data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Client

When a policy 434 has been applied to a selected ActiveSync client, and the client has applied it and responded, then there will be a Full Wipe option available for that client. To do a Full Wipe, right-click the client (or select it if you are using MDRA) and click **Full Wipe**. The next time the client connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the client, this may remove everything on it, including downloaded apps. Further, as long as the client's ActiveSync entry exists, MDaemon will continue to send the wipe request any time that device connects in the future. If at some point you wish to delete the client, make sure you add it to the Block List 420 first, so that it cannot connect again in the future. Finally, if a wiped device is recovered and you wish to allow it to connect again, you should select the device and click **Cancel Wipe Actions**. You must also remove it from the Block List.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Account Wiping an ActiveSync Client

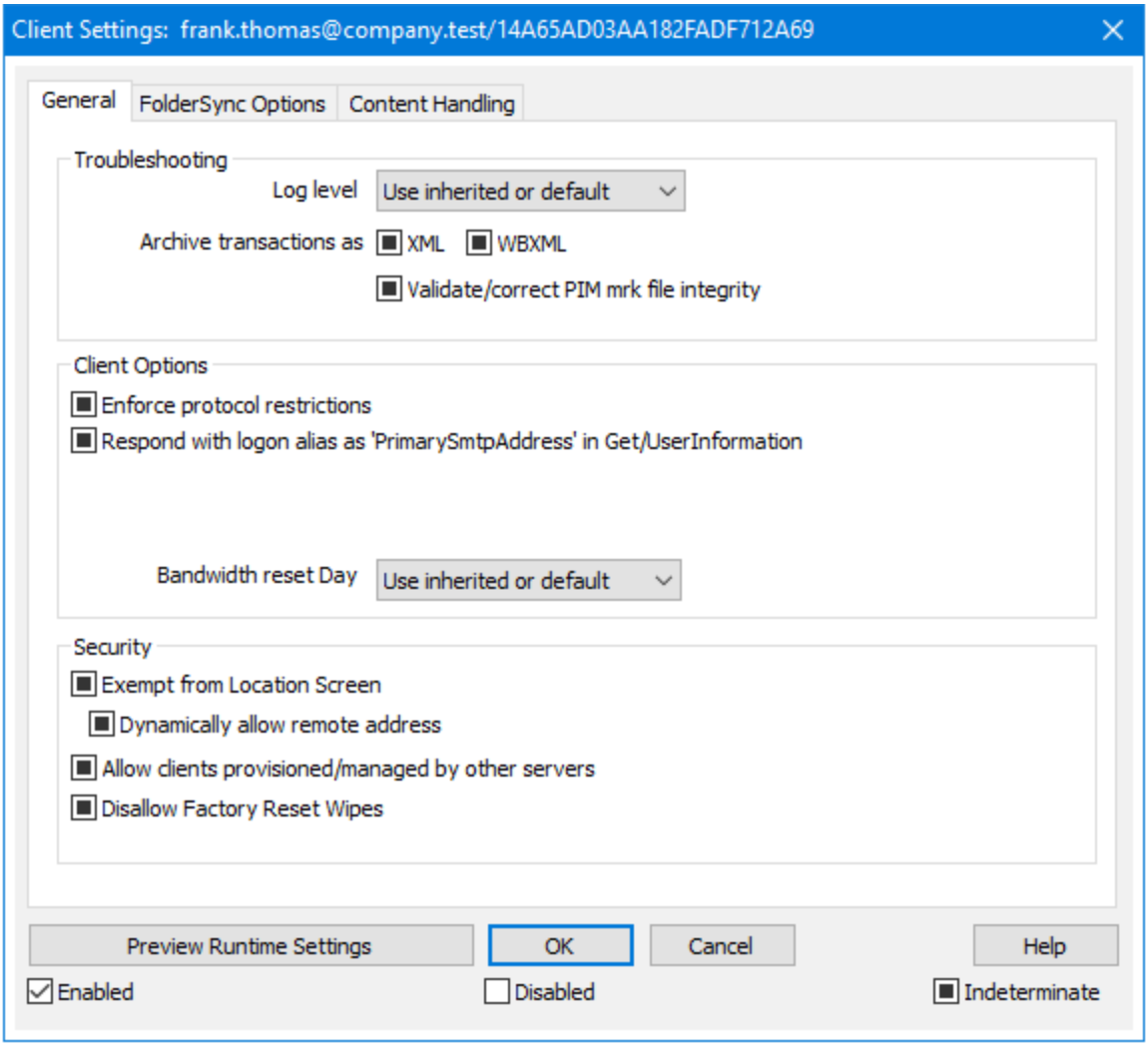
To wipe the account's mail and PIM data from the client or device, right-click and click **Account Wipe Account Mail and PIM from client**. The *Account Wipe* option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

Authorizing Client

If the "*New clients require administrative approval*" option on the ActiveSync Client Settings 413 screen is set to require approval, select a client and click Approve client to sync, to authorize it for synchronization with the server.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the Client-Types Client Settings 466 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the client-type-level setting for this device.

General

Troubleshooting

Log level
ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug	This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.
Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.
Inherit	By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission[302] for both the subfolder (i.e. child folder) and all parent public folders[300] above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol 424 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias 818 for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Accounts 442
ActiveSync » Security 420

3.3 Gateway Manager

The Gateway Manager is reached from the Setup » Gateway Manager... menu selection. This feature provides a limited yet useful secondary level of support for hosting multiple domains or acting as a backup mail server for someone.

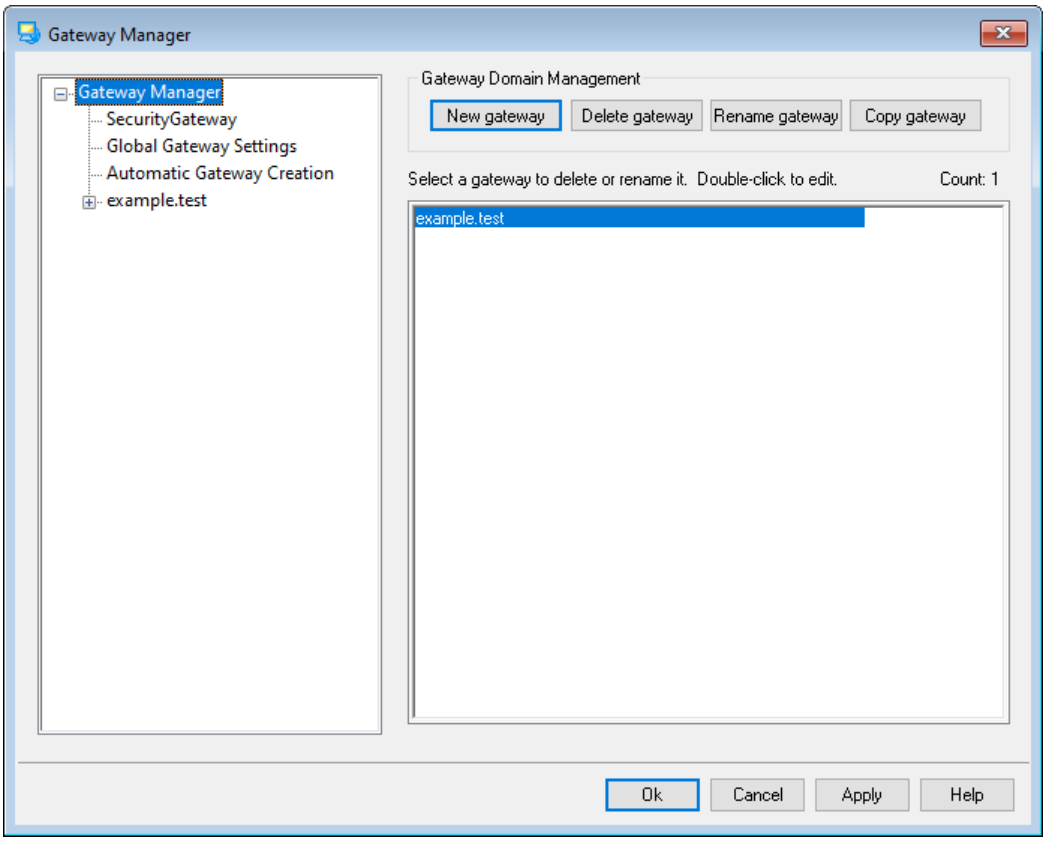
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

For example:

> Suppose you wish to act as a backup server or mail-drop for a third party, receiving its incoming email and storing it in a folder on your server, but you do not wish to host its domain fully, maintaining its individual user accounts. Let's use "example.com" as its name.
>
> The first thing you will do is create the gateway by clicking **New gateway** on the Gateway Manager and then entering "example.com" as its name. Now all mail that MDaemon receives for that domain will be separated from the main mail stream and placed in the folder designated on the gateway's Domain 247 screen, regardless of the specific individuals to which each message is addressed.
>
> Next, you will designate the collection or delivery methods that you wish to allow or use to get the domain's email to its actual email server, where its user accounts are hosted. There are two ways to do this: use the *Deliver stored messages each time MDaemon processes remote mail* option on the Domain screen 247, or use the Dequeuing 253 options. Optionally, you can also create an MDaemon account and change its Mail Folder 700 to the same storage folder 247 that your gateway uses. This will allow a mail client to connect to MDaemon to collect example.com's email.
>
> Finally, you will likely have to edit the DNS settings for example.com so that your MDaemon server is a designated MX host for that domain.

There are many other features and options available, but the above example is the basic form that a typical gateway will take. If, however, you require an atypical configuration then you may have to do some things differently, such as when you wish to use a domain name that doesn't actually exist on the Internet, like "company.mail." Receiving messages for an otherwise invalid domain name such as that is possible, but the domain name must be "hidden" inside a default domain 174 address. Using that method, addresses can be constructed that will pass through the default domain and on to the gateway. For example, if your default domain is example.com and you have a gateway for company.mail, then someone could send a message to "bob@company.mail" by using the address, "bob{company.mail}@example.com." Since "example.com" is the registered domain hosted by MDaemon, this message would be delivered properly, but when MDaemon received the message in that format it would convert the address to "bob@company.mail" and deliver the message to the folder specified for that gateway. Of course the simplest method is still to register a valid domain name for the gateway and then point its DNS or MX record to example.com.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Gateway List

The navigation pane on the left side of this dialog contains the list of your gateways, with links to each screen used for configuring the various gateway-specific settings. It also provides access to the Global Gateway Settings 243 and Automatic Gateway Creation 245 screens. The list on the right is used for deleting and renaming domains. You can double-click a gateway in this list to switch to the gateway editor for configuring its settings.

Gateway Domain Management

New gateway

To create a new gateway: click **New gateway**, enter the gateway name (e.g. example.mail) in the Create/Rename Gateway Domain dialog, and click **OK**.

Typically the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name. Alternatively, you may choose to use an internal-only or otherwise non-valid, non-public domain name (such as "company.mail") for your gateway name. This, however, would require you to use the nested domain name method outlined in the example above, or require you to utilize some other content filtering scheme to get the messages where they belong.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete gateway
To delete a gateway: select it from the list and click **Delete gateway**, and click **Yes** to confirm your decision.

Rename gateway
To change a gateway's name: select it from the list, click **Rename gateway**, type the new name in the Create/Rename Gateway Domain dialog, and click **OK**.

Copy gateway
If you wish to create a new gateway with settings that match another gateway, select a gateway from the list, click this button, and then specify a name for the new gateway.

Gateway Editor

The Gateway Editor is used for editing each gateway's settings. It includes the following screens:

Domain 247
Use this screen to enable/disable the gateway, designate the folder used for storing the domain's messages, and configure other delivery and attachment-handling options.

Verification 248
If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, you can use this dialog to specify that server and thus verify the validity of recipient addresses of incoming messages. When a recipient address is found to be invalid the message will be rejected. With this method you can avoid having to assume that all recipients of a domain's messages are valid.

Forwarding 252
With this screen you can declare a host or address to which the domain's mail will be forwarded as soon as it arrives. There are also options for stating whether a copy of these messages should be kept locally and for designating the port on which the forwarded messages should be sent.

Dequeuing 253
Using the options on this screen, you can configure MDaemon to respond to ETRN and ATRN requests made on behalf of the domain in order to dequeue its messages. You can also configure several other dequeuing related options.

Quotas 256
This dialog is used for assigning a limit to the amount of disk space that the domain may use and the maximum number of messages that may be stored.

Settings 258
This screen contains a number of other options that will apply to the selected domain gateway. For example, you can enable/disable AntiVirus and AntiSpam

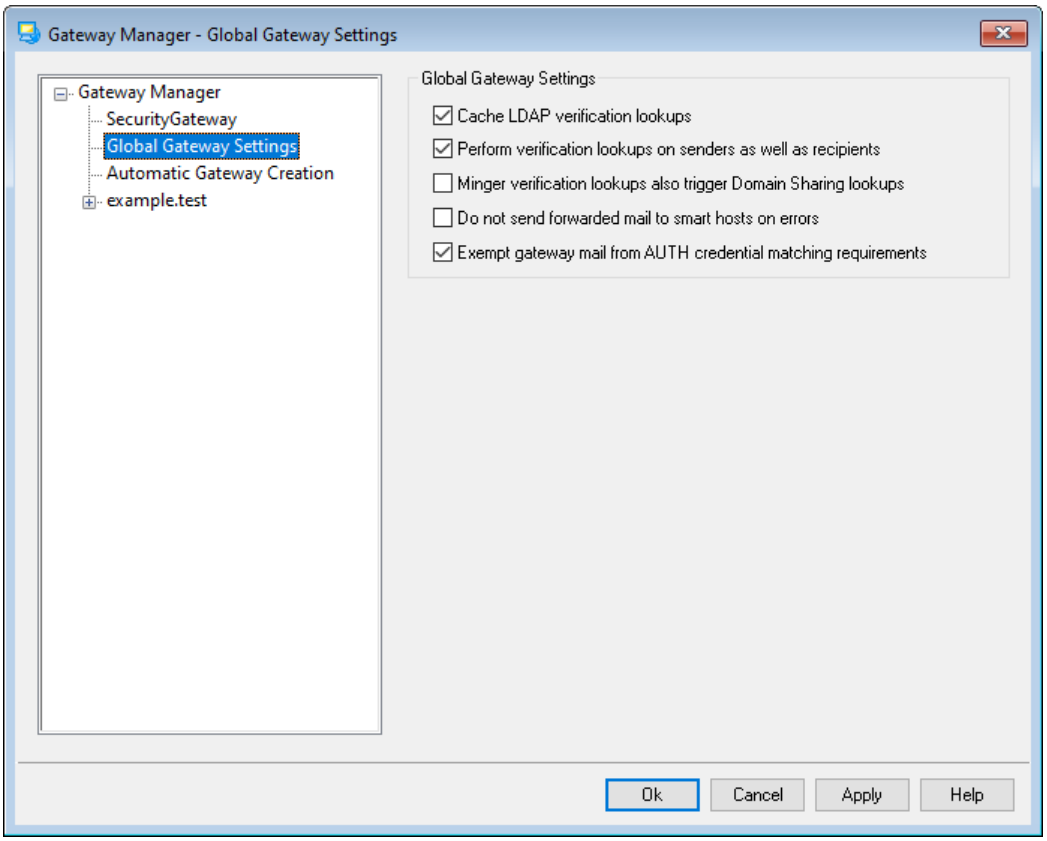
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

scanning for the gateway, designate whether or not authentication is required when dequeuing mail, designate an authentication password, and several other options.

See:

Global Gateway Settings 243
Automatic Gateway Creation 245
Domain Manager 174

3.3.1 Global Gateway Settings



Global Gateway Settings

The following options are global options. They aren't limited to any particular gateway.

Cache LDAP verification lookups
Click this checkbox if you wish to cache the results of LDAP verification 248 queries for your domain gateways.

Perform verification lookups on senders as well as recipients
By default, when the address verification options 248 are enabled for a gateway, MDaemon will attempt to verify recipients and senders of the gateway's messages. Disable this option if you wish to verify only the recipients.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Minger verification lookups also trigger Domain Sharing lookups
When this option is enabled and Minger[847] is used by any of your gateways for address verification, in addition to querying the Minger host designated on the Verification screen[248], MDaemon will also query your Domain Sharing[108] hosts. This option applies to all gateways set to use Minger for address verification.

Do not send forwarded mail to smart host on errors
Click this option to prevent the sending of forwarded emails to the host specified above when delivery errors occur. This option is disabled by default.

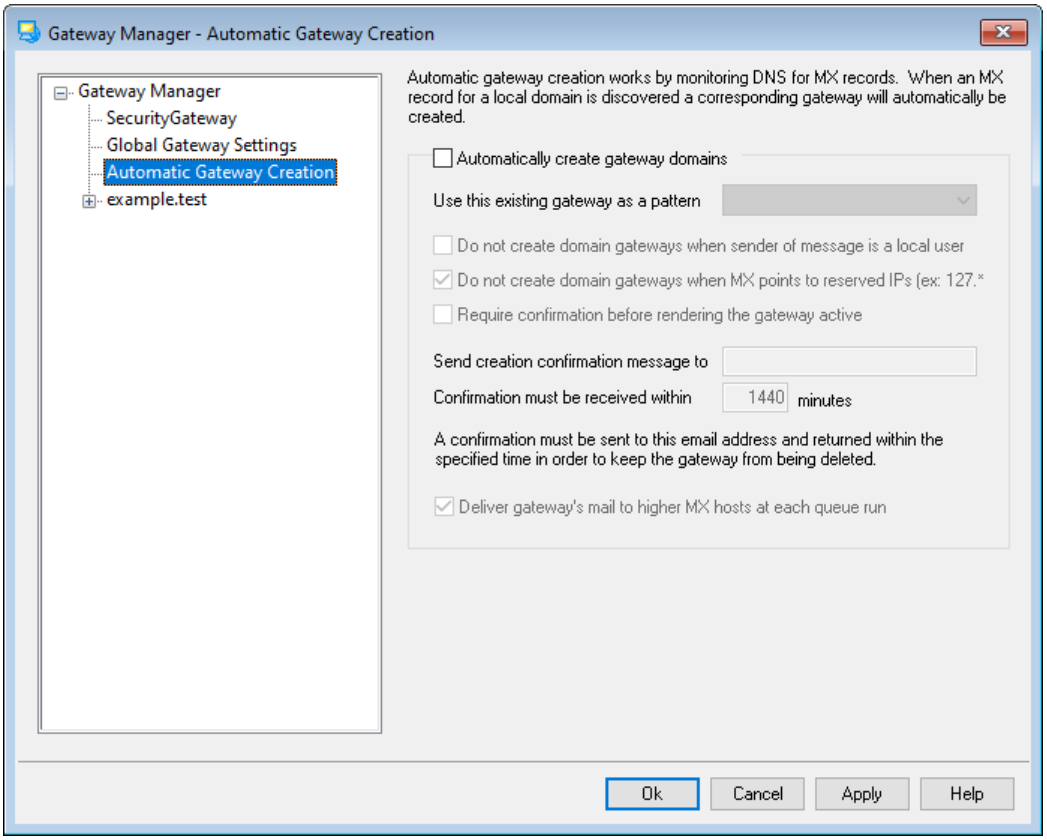
Exempt gateway mail from AUTH credential matching requirements
By default gateway mail is exempt from the following two options located on the SMTP Authentication[509] screen: "*Credentials used must match those of the return-path address*" and "*Credentials used must match those of the 'From:' header address*". Disable this option of you do not wish to exempt gateway mail from these requirements, but disabling it could cause some problems for gateway mail storage and forwarding.

See:

Gateway Manager[239]
Gateway Editor » Verification[248]
Minger[847]
Domain Sharing[108]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.3.2 Automatic Gateway Creation



Automatic Gateway Creation

This feature is used to automatically create a Domain Gateway [239] for a previously unknown domain when another source attempts to deliver that domain's messages to MDaemon, and a DNS query lists MDaemon's location as a valid MX record.

For example:

With automatic gateway creation enabled, if MDaemon's Default Domain IP address is `192.0.2.0` and a message is delivered via SMTP for an unknown domain `example.com`, MDaemon will perform MX and A-record queries on `example.com` to see if `192.0.2.0` is a known mail relay host for it. If the results of the DNS queries state that MDaemon's IP address is a valid MX host for `example.com` then MDaemon will automatically create a new Domain Gateway for it and accept its email. Messages for `example.com` will then be stored in a special folder and, if you so choose, spooled to higher level MX hosts at each remote mail processing interval. This feature effectively enables you to become a backup server for another domain by simply configuring the DNS system to use your IP as an alternate MX host.

To help secure this feature, MDaemon can be configured to send a confirmation request to an email address of your choice. While MDaemon is waiting for the confirmation response, messages for the domain will be accepted and stored but not delivered. Confirmation requests must be replied to within an amount of time that you designate or the automatically created gateway will be removed and all stored

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

messages deleted. If confirmation is received before the time has expired then the stored messages will be delivered normally.

It might be possible for a malicious person or "spammer" to attempt to exploit this feature by configuring their DNS server to list your MDaemon's IP address as one of their MX hosts. Automatic Gateway Creation must therefore be used with caution. To aid in preventing possible exploitation we recommend utilizing the *Send creation confirmation message to...* feature whenever possible.

Automatically create gateway domains
Click this checkbox if you want MDaemon to automatically create Domain Gateways based upon the results of DNS queries.

Use this existing gateway as a pattern
Choose a Domain Gateway from this drop-down list and MDaemon will use its settings as a template for all future automatically created gateways.

Don't create domain gateways when sender of message is a local user
Enable this control if you do not want messages originating from local users to trigger automatic gateway creation.

Don't create domain gateways when MX points to reserved IPs
Click this check box if you wish to prevent an automatic gateway creation when the MX record points to a reserved IP address such as 127.*, 192.*, or the like.

Require confirmation before rendering the gateway active
When this control is enabled, MDaemon will send a confirmation message to the email address of your choice in order to determine whether the automatically created gateway is valid. MDaemon will continue to accept messages for the domain in question but will not deliver them until confirmation is received.

Send creation confirmation message to
Use this text box to designate the email address to which confirmation messages will be sent.

Confirmation must be received within XX minutes
This control is for designating the number of minutes that MDaemon will wait for a response to any given confirmation message. If this time limit expires then the Domain Gateway in question will be deleted.

Deliver gateway's mail to higher MX hosts at each queue run
If you want MDaemon to attempt to deliver this gateway's messages to higher level MX hosts each time that the remote queue is processed then enable this control.

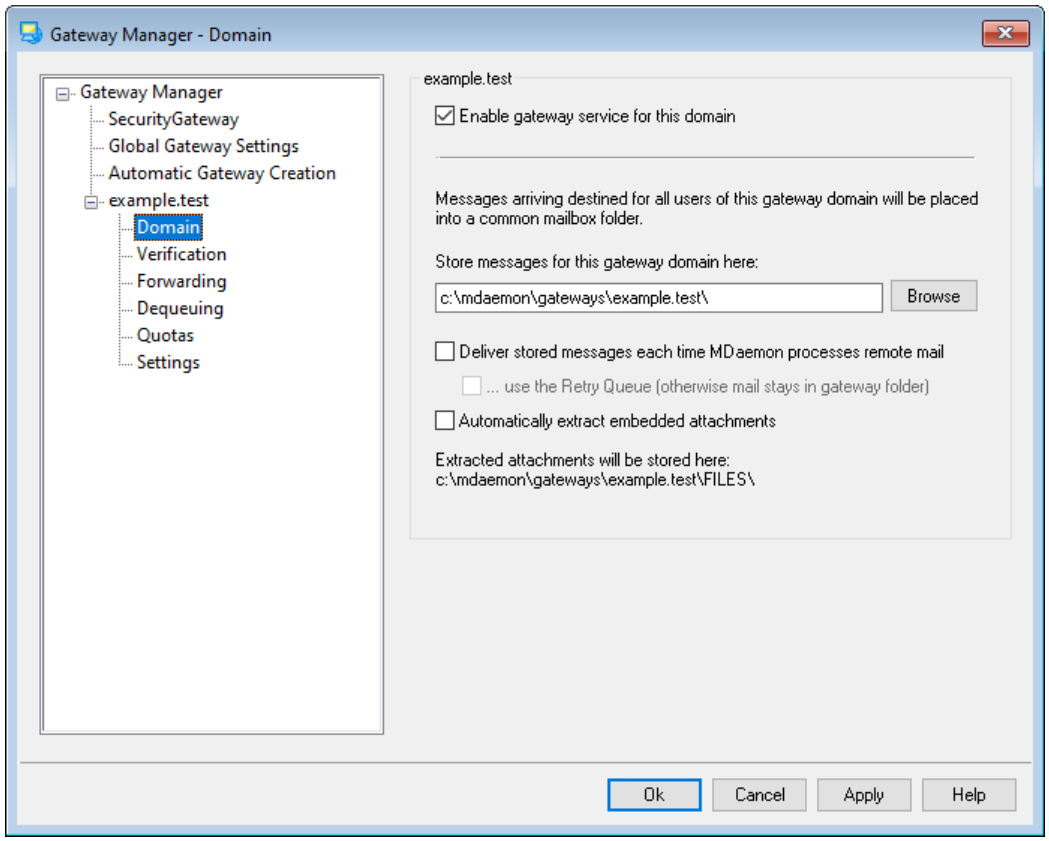
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Gateway Manager 239

3.3.3 Gateway Editor

3.3.3.1 Domain



Gateway Domain

Enable gateway service for this domain
Check this box to enable the domain gateway.

Store messages for this gateway domain here:
Enter the directory where you wish to store incoming mail for the domain. All of its messages will be stored in the same folder regardless of the individual recipients to which each message is addressed.

Deliver stored messages each time MDaemon processes remote mail
Ordinarily, when MDaemon receives mail that is intended for one of its gateways, it will store the mail until that domain connects to MDaemon to collect it. In some situations you may want MDaemon to attempt to deliver the mail directly via SMTP rather than waiting for the domain to collect it. When this option is enabled, MDaemon will attempt to deliver the domain's messages each time remote mail is processed. The gateway's mailbox will temporarily act as a remote queue and

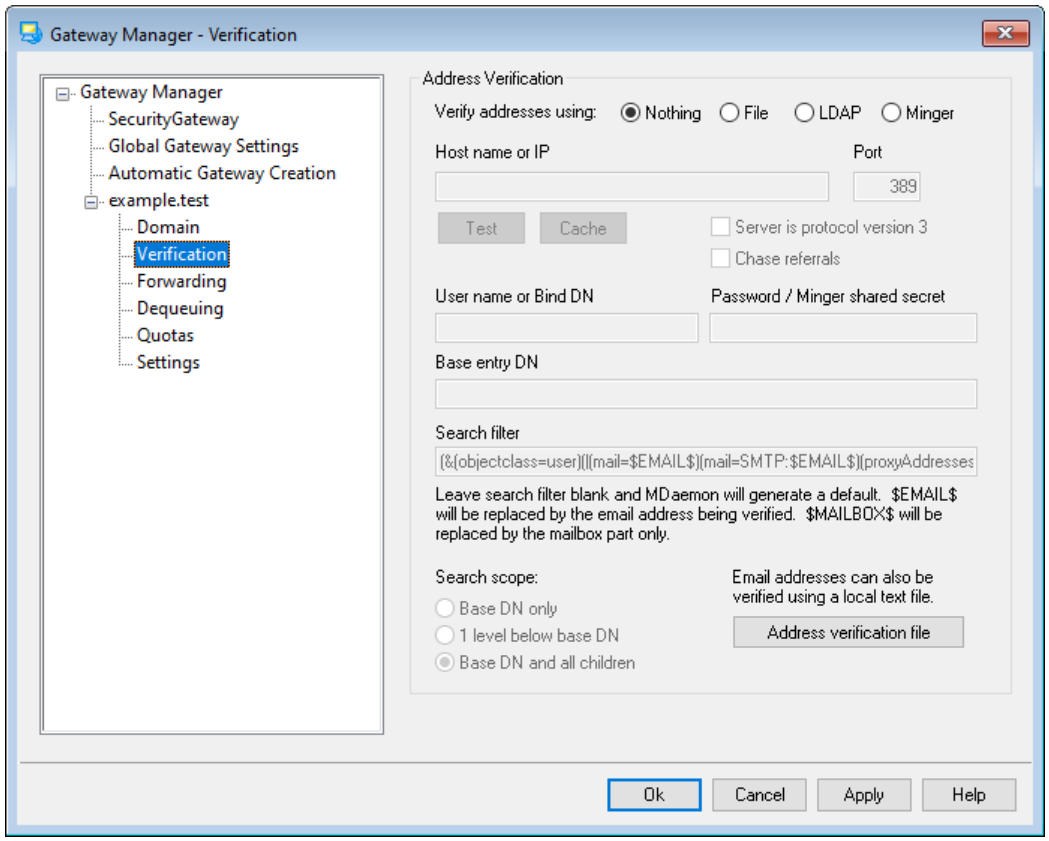
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

delivery will be attempted. Any messages that cannot be delivered will simply remain in the gateway's mailbox until they are collected by the domain or are successfully delivered later; they will not be moved into the remote queue or retry system. However, if you do not have the domain's DNS properly configured, or if you have your MDaemon configured to pass all outgoing messages to some other host for delivery, then you could cause those message to get caught in a mail loop and then eventually be treated as undeliverable.

Use the Retry Queue (otherwise mail stays in gateway folder)
Enable this option if you wish to use the Retry Queue 856 mechanism for delivering mail. This is disabled by default, meaning that gateway mail will be held in the gateway folder forever, even if it can't be delivered.

Automatically extract embedded attachments
Some mail systems require attached files be extracted before submission of mail messages to the mail stream. To facilitate this, MDaemon can auto-extract incoming MIME attachments and place them in the `\Files\` subfolder underneath the domain's message folder. Check this box if you wish to automatically extract attachments.

3.3.3.2 Verification



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

One common problem with domain gateways and mail-drops is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if you act as a gateway for example.com and a message comes for user01@example.com then you have no way of knowing whether or not there is actually a mailbox, alias, or mailing list corresponding to that address on example.com's email server. Thus you have no choice but to assume that the address is valid and accept the message. Further, since spammers commonly send messages to many invalid addresses, this problem can result in large amounts of junk email being accepted for the gateway.

MDaemon contains a method to prevent this by verifying the recipient addresses. If the remote domain's server is configured to keep an LDAP or Active Directory server up to date with all of its mailboxes, aliases, and mailing lists, or if it runs a Minger server to provide remote address verification, then you can use the options on this screen to specify the LDAP, Active Directory, or Minger server where this information is stored. Then, when a message arrives for example.com, you can lookup the recipient's address on the other server and discover whether or not it is valid.

Address Verification

Verify addresses using:

Nothing
Choose this option if you do not wish to use email address verification for this domain gateway. MDaemon will treat all of the domain's incoming messages as if the recipient is a valid address, since it will have no way of identifying which addresses actually exist for that domain.

File
Choose this option if you wish to use the GatewayUsers.dat file as the definitive list of addresses that will be used to verify whether or not the recipient of an incoming message for this domain is valid. This is a global list of addresses, applicable to all of your domain gateways, and even if you have chosen to use one of the other verification methods, this list will still be used as an extra source of valid addresses. When using the *File* option, however, it will be the only verification option used. You can open and edit the valid address list by clicking the *Address verification file* button below.

LDAP
Choose this option to activate remote address verification via LDAP or Active Directory. Whenever a message arrives for the remote domain its LDAP or Active Directory server will be queried to determine whether or not the recipient is valid. If it isn't valid the message will be rejected. If MDaemon is unable to connect to the LDAP/AD server then it will assume the address is valid.

Minger
Choose this option if you wish to query the domain's Minger server to verify recipient addresses for this domain. If MDaemon is unable to connect to the server then it will assume the address is valid. There is also a global option located on Global Gateway Settings 243 that you can use to cause MDaemon to query your Domain Sharing 108 hosts as well.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Host name or IP
Enter the host name or IP address of the domain's LDAP/Active Directory or Minger server. This is the LDAP/AD or Minger server to which MDaemon will connect in order to verify that the recipient of an incoming message is a valid address at the domain for which this MDaemon is acting as a gateway or backup server.

Port
Specify the port that the domain's LDAP/AD or Minger server is using. MDaemon will use this port when verifying address information via LDAP, Active Directory, or Minger.

Test
Click this button to test whether or not you have the remote address verification settings configured properly. MDaemon will simply attempt to connect to the designated LDAP/AD server and verify that it responds to the specified information.

Cache
Click this button to open the LDAP/Minger cache. You can enable/disable the cache on Global Gateway Settings 243.

Server is protocol version 3
Click this checkbox if want gateway verification to use LDAP protocol version 3 with your server.

Chase referrals
Sometimes an LDAP server doesn't have a requested object but may have a cross-reference to its location, to which it can refer the client. If you want gateway verificaiton to chase (i.e. follow) these referrals, enable this option. This is disabled by default.

User name or Bind DN
Enter the User name or DN of the account that has administrative access to the domain's LDAP/AD server so that MDaemon can verify the recipients of incoming messages addressed to the domain for which it is acting as a gateway or backup server. This is the DN used for authentication in the bind operation.

Password or Minger shared secret
This password will be passed to the domain's LDAP/AD server along with the *Bind DN* value for authentication. If using a Minger server then this is the shared secret or password used.

Base entry DN
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will query your LDAP/AD server for address verification.

Search filter
This is the LDAP/AD search filter that will be used when querying your server to verify addresses. MDaemon will setup a default search filter that should work in most cases.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Search scope:

This is the scope or extent of your LDAP/AD searches.

Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

1 level below base DN
Use this option if you wish to extend your LDAP/AD search to one level below the supplied DN in your DIT.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

Address verification file
Click this button to open the Gateway Valid Email Address List (i.e. the `GatewayUsers.dat` file). This contains a list of addresses that MDaemon will consider to be valid recipients for incoming messages addressed to your domain gateways. Regardless of the verification option selected above, MDaemon will use this list as an extra source of valid address data. When using the *File* option above, however, it will be the definitive and only verification option used.

Using multiple configurations for LDAP verification queries

You can specify multiple LDAP configurations for your gateway domains. To specify extra sets of LDAP parameters, setup your first set normally and then manually edit the `GATEWAYS.DAT` file using Notepad.

Your new set of parameters should be created using the following format:

```
LDAPHost1=<host name>
LDAPPort1=<port>
LDAPBaseEntry1=<base entry DN>
LDAPRootDN1=<root DN>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

For each new set of parameters, increase the numeral in each parameter's name by 1. For example, in the sample set above, each parameter's name ends with "1". To create an additional set each name would end with "2". In another set, each would end "3", and so on.

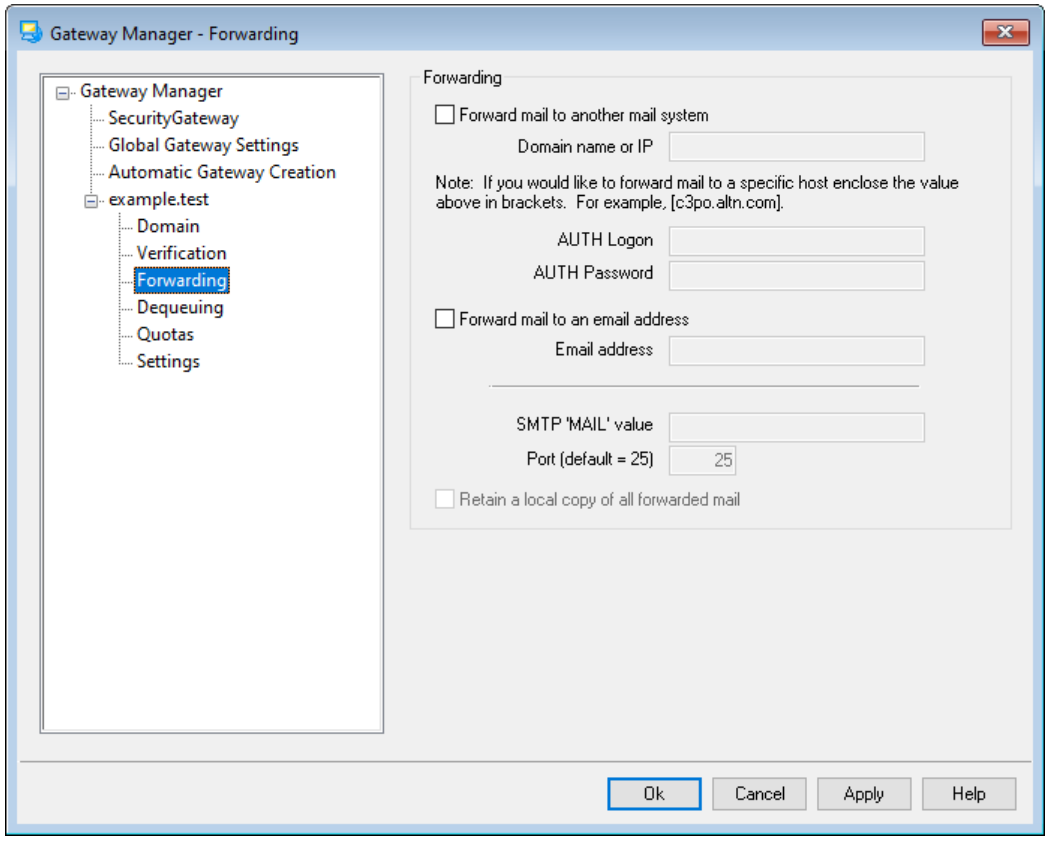
When the LDAP queries take place, MDaemon will perform multiple LDAP queries in sequence to find a match. If an error or a match is found no further checks are performed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

LDAP/Address Book Options 815
Minger 847

3.3.3.3 Forwarding



Forwarding

Forward mail to another mail system
Sometimes it is advantageous to simply forward a copy of all messages for a domain as they arrive. If you wish to configure MDaemon to do this, enter the name or IP

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

address of the domain to which copies of incoming mail for this domain should be sent. If you wish to forward the messages to a specific host then place the value in brackets (for example, `[host1.example.net]`). Use the AUTH Logon/Password option to include any necessary logon credentials for the server to which you are forwarding the messages.

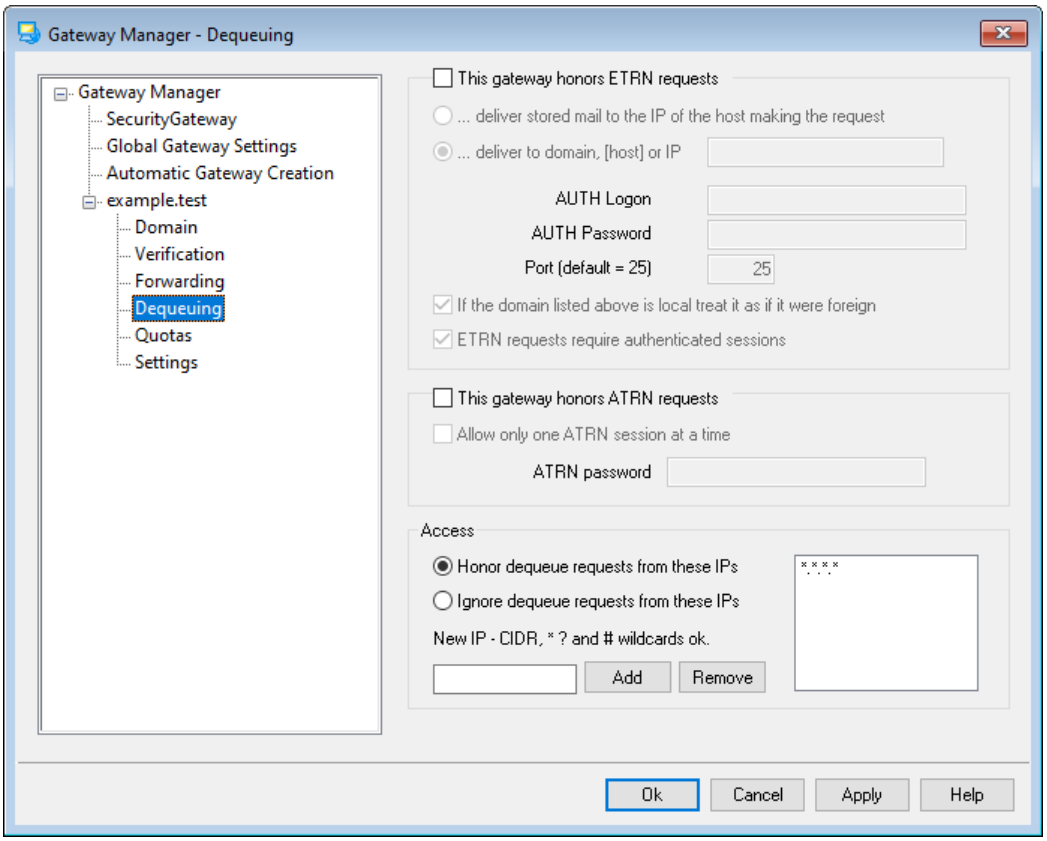
Forward mail to an email address
Use this feature if you wish to forward to a specific email address all email messages destined for this client domain.

SMTP 'MAIL' value
MDaemon will use this address in the SMTP "Mail From" transaction when forwarding the messages.

Port (default = 25)
MDaemon will use this port when forwarding the messages.

Retain a local copy of all forwarded mail
Select this option if you want MDaemon to retain an archival copy of each message locally once it has been forwarded.

3.3.3.4 Dequeuing



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ETRN

This gateway honors ETRN requests
When this switch is enabled MDaemon will respond to ETRN requests made by qualified hosts on behalf of the domain for which MDaemon is acting as an email gateway. The ETRN command is an SMTP extension that signals a server storing mail for a particular domain that it is time to begin spooling the mail. When MDaemon receives an ETRN request for a domain, it will immediately begin spooling the stored mail for delivery using subsequent SMTP transactions. Please note that the SMTP session that issues an ETRN request will not be the one that receives any stored mail. MDaemon will use subsequent independent SMTP transactions to send any mail it has stored for the domain. This preserves the message envelope and is more secure. Also note that the host to which MDaemon will spool any stored mail may not immediately begin reception of these messages. ETRN only guarantees that any stored mail is *spooled* for delivery. The actual *process* of delivery is subject to other administrator-imposed restrictions and may have to wait in the outbound mail queue for the next scheduled remote mail processing event to take place. Because of these limitations we recommend using On-Demand Mail Relay (ODMR) 194 and its ATRN command rather than ETRN. This method is not supported by all clients and servers, however, and will therefore only be available to client domains using a server that does so. MDaemon fully supports ODMR on both the client and server side.

By default MDaemon requires that the connecting host issuing the ETRN request first authenticate itself via ESMTP AUTH using the *Domain name* 247 and Gateway *ATRN password* as its login credentials. If you do not wish to require authentication than you can disable it on Settings 258 by clearing *ETRN dequeuing requires authentication*.

...deliver stored mail to the IP of the host making the request
Selecting this option will cause MDaemon to send any stored mail to the IP address of the machine that made the ETRN request. The requesting machine must be running an SMTP server to receive these messages.

...deliver to domain, [host] or IP
This is the host name, domain name, or IP address to which any stored mail will be sent when an ETRN request is received and honored. The receiving machine must be running an SMTP server to receive these messages. Note: when a domain name is specified in this option, A and MX records may be used, depending on the DNS results during delivery. If you wish to deliver the messages to a particular host then place the host name in brackets (for example, `[host1.example.net]`) or specify an IP address instead of a domain name. Enter any *AUTH Logo/Password* credentials needed to deliver to the location.

Port (default = 25)
Use this option to specify the port on which the domain's mail will be spooled.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If the domain listed above is local treat it as if it were foreign
Activate this control if the domain is local but you want its mail to be spooled as if it is remote.

ETRN requests require authenticated sessions
When honoring ESMTP ETRN requests, this option will be used by default to require the connecting host to first authenticate using the ESMTP AUTH command. When this option is enabled, you must designate an authentication password in the "ATRN password" option below.

Clear this checkbox if you do not wish to require authentication of hosts making ETRN requests.

ATRN

This gateway honors ATRN requests
Enable this option if you want MDaemon to respond to `ATRN` commands from the gateway's domain. `ATRN` is an ESMTP command used in On-Demand Mail Relay (ODMR) 194, which is currently the best relay method available for mail hosting. It is superior to ETRN and other methods in that in requires authentication before mail is dequeued and does not require a static IP address. A static IP address isn't required because the flow of data between MDaemon and the client domain is immediately reversed and the messages are de-spooled without having to make a new connection, unlike `ETRN`, which uses a separate connection after the `ETRN` command is sent. This enables client domains with a dynamic (non-static) IP address to collect their messages without having to use POP3 or DomainPOP, because the original SMTP envelope is preserved.

ATRN requires a session using the AUTH command. You can configure the authentication credentials on the Settings 258 screen.

Allow only one ATRN session at a time
Click this check box if you wish to restrict ATRN to one session at a time.

ATRN password
When using ATRN to dequeue this gateway's mail, or when you are requiring authentication via the *ETRN dequeuing requires authentication* option on the Settings screen, designate the gateway's ATRN password here.

The domain for which MDaemon is acting as an email gateway must use its domain name as the logon parameter. For example, if the domain gateway is "example.com" and is using ATRN to dequeue its mail, then it would authenticate using the login credentials "example.com" and the password specified here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Access

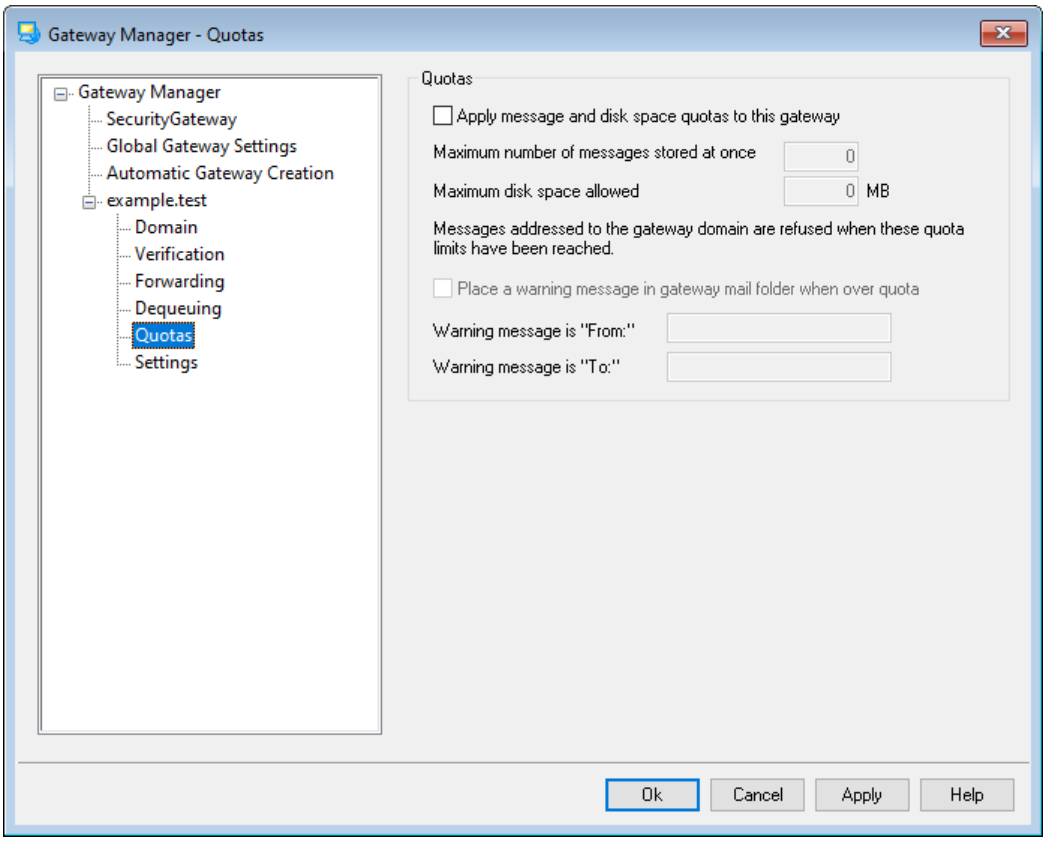
Honor dequeue requests from these IPs
Select this switch and MDaemon will honor ETRN/ATRN requests made from any IP listed in the associated address list.

Ignore dequeue requests from these IPs
Select this switch and MDaemon will ignore ETRN/ATRN requests that are made from any IP listed in the associated address list.

Add new IP
To add a New IP to the current list simply enter the IP into this text box and click the *Add* button.

Remove
Click this button to remove a selected entry from the list of IP addresses.

3.3.3.5 Quotas



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Quotas

Apply message and disk space quotas to this gateway
Enable this option if you wish to designate a maximum number of messages allowed to be stored for the domain or a maximum amount of disk space (in kilobytes) that it can use. This includes any decoded file attachments in its Files directory. When a quota is reached, any further incoming messages addressed to the domain will be refused.

Maximum number of messages stored at once
Use this box to designate the maximum number of messages that MDaemon will store for this gateway domain. Use "0" in this option if you do not wish to limit the number of messages.

Maximum disk space allowed
Specify the maximum allowed disk space here. When messages and files stored for the domain reach this limit, any further incoming messages for the domain will be refused. Use "0" if you do not wish to set a disk space limit.

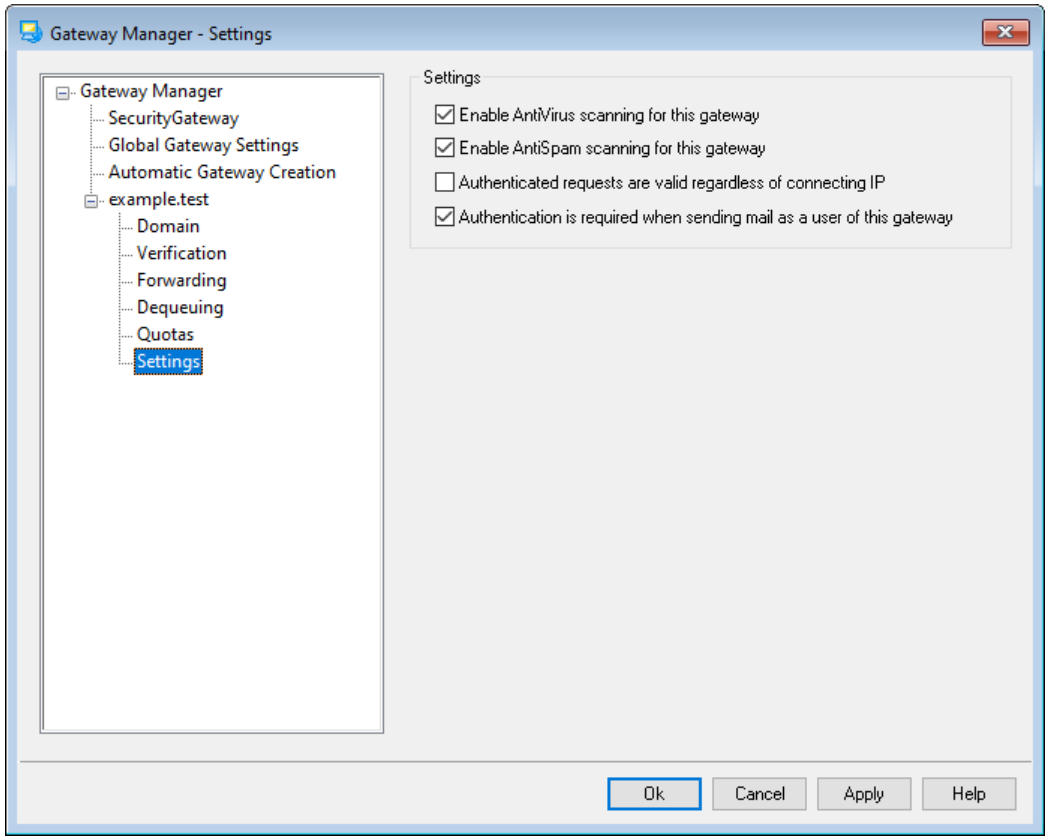
Place a warning message in gateway mail folder when over quota
If this option is enabled and a mail delivery to the domain is attempted that would exceed the maximum message or disk space limitations, an appropriate warning message will be placed in the domain gateway's mail folder. You can designate the warning message's "`From:`" and "`To:`" headers below.

Warning message is "From:"
Use this option to specify the "From:" address that will be used in the over-quota warning messages.

Warning message is "To:"
Use this option to specify the "To:" address that will be used in the over-quota warning messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.3.3.6 Settings



Settings

Enable AntiVirus scanning for this gateway
Click this option if you are utilizing the optional MDaemon AntiVirus 630 features and want this domain gateway's messages to be scanned. If you clear this option then AntiVirus will not scan this gateway's messages.

Enable AntiSpam scanning for this gateway
Click this option if you want to apply the Spam Filter settings to this domain gateway's messages. Otherwise, they will be excluded from Spam Filter scanning.

Authenticated requests are valid regardless of connecting IP
Enable this checkbox if you wish to honor authenticated requests regardless of the IP address from which they are coming. If this control is not enabled then only requests from those IP addresses specified in the Access section will be honored.

Authenticated is required when sending mail as a user of this gateway
Click this check box if you want all messages claiming to be from this domain to require authentication. If a message is purported to be from this domain then it must be using an authenticated connection (or connecting from a Trusted IP address) or it will be refused. This option is enabled by default.

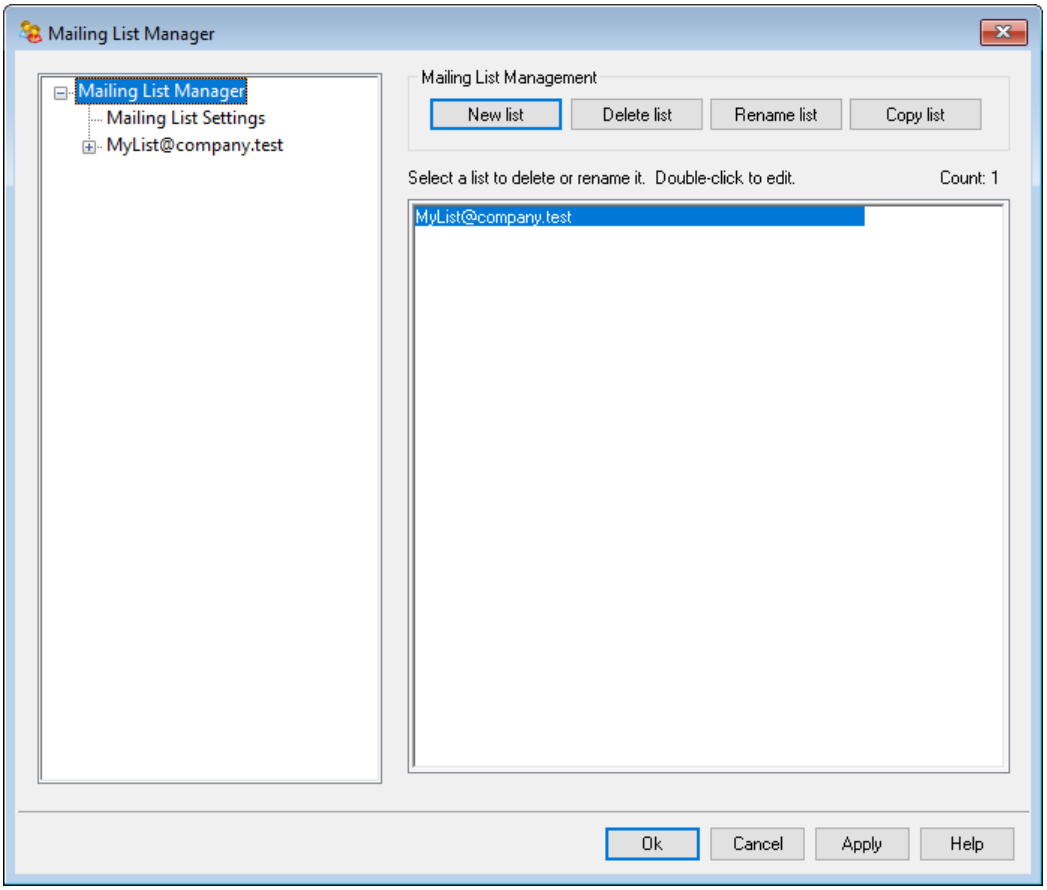
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

When new domain gateways are created, this option will be enabled by default. If you wish to change the default setting so that new gateways will have this option disabled, then edit the following key in the `MDaemon.ini` file:

```
[Special]
GatewaySendersMustAuth=No (default is Yes)
```

3.4 Mailing List Manager

Mailing Lists, sometimes called Email Groups or Distribution Lists, allow groups of users to be addressed as if they all shared a common mailbox. Copies of email messages sent to the list are distributed to each of the list's members. Lists may contain members with local and/or remote destination addresses, be public or private, moderated or open, be sent in digest 279 or normal message format, and more.



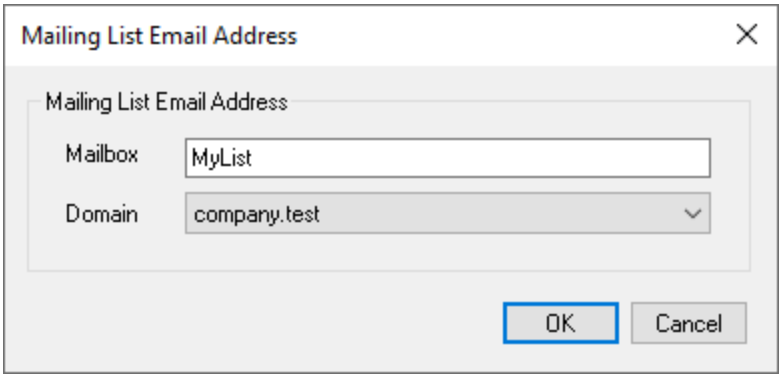
Located under the Setup » Mailing List Manager... menu selection, the Mailing List Manager is used to administer your lists.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailing List Management

The navigation pane on the left side of this dialog contains an entry for each of your mailing lists, with links to each screen used for configuring the various list-specific settings. It also provides access to the Mailing List Settings 262 screen, which is used for configuring several list-related global options. The options on the right side of this dialog are used for creating, deleting, and renaming your lists. You can double-click a mailing list to switch to the mailing list editor for configuring the list's settings.

New list
To create a new mailing list, click **New list** to open the Mailing List Email Address dialog. Create a mailbox name and select a domain, such as "MyList" and "example.com" respectively. This will be the mailing list's email address (i.e. MyList@example.com). Messages sent to this address will be distributed to members of the list, based on the list's particular settings. Click **OK** to create the list. After creating the list you can double-click its entry to configure its settings and add members. **Note:** List names cannot contain " ! " or " | "



Delete list
To delete a mailing list: select the list, click **Delete list**, and click **Yes** to confirm your decision.

Rename list
To rename a mailing list, select the list and then click **Rename list** to open the Mailing List Email Address dialog. Make your desired changes and click **OK**.

Copy list
If you wish to create a mailing list with the same settings and members as another list, select the list, click this button, and then specify a mailbox name and domain for the new list.

Modifying an Existing Mailing List

To configure a mailing list, double-click its entry on the Mailing List Manager. Then in the navigation pane on the left, click whichever screen you wish to edit:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Members 265
Settings 268
Headers 271
Subscription 274
Reminders 278
Moderation 283
Digest 279
Routing 285
Notifications 281
Support Files 287
Public Folder 289
Active Directory 290
ODBC 292

Mailing List Settings

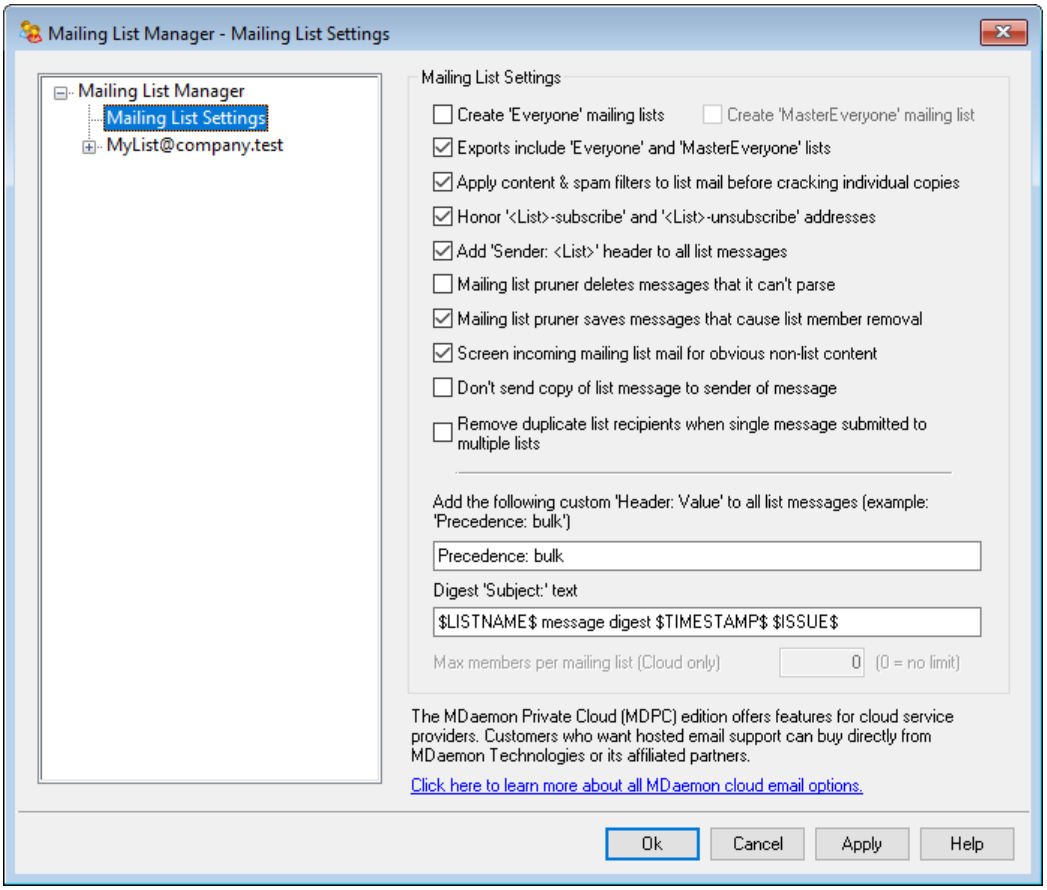
Click **Mailing List Settings** in the left pane to open the Mailing List Settings 262 screen, for configuring several global settings related to mailing lists.

See:

Mailing List Settings 262

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.1 Mailing List Settings



Mailing List Settings

Create "Everyone" mailing lists
Check this box if you wish to create and maintain "Everyone" mailing lists for all of your domains (e.g. "everyone@example.com"). A list will be created for each domain, which makes it possible for you to send a message to every user of a domain simply by addressing the message to "everyone@<domain>". Private accounts 744 are hidden from "Everyone" mailing lists. This option is disabled by default.

Create "MasterEveryone" list
Enable this option if you want there to be a "MasterEveryone" mailing list. Everyone on all of your domain-specific "everyone" lists will be included on this list. This option is disabled by default.

Exports include 'Everyone' and 'MasterEveryone' lists
By default, 'Everyone' and 'MasterEveryone' mailing lists are included when you use the "Accounts » Exporting..." options to export lists. Disable this option if you do not wish to include those lists in mailing list exports.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Apply content & spam filters to list mail before cracking individual copies
When the *Deliver list mail to each member individually* option is chosen on the Routing 285 screen of the mailing list editor, enabling this control will cause the content filter rules and spam filter to be applied to list messages before they are copied and distributed to list members.

Honor '<List>-subscribe' and '<List>-unsubscribe' addresses
Click this checkbox if you want MDaemon to recognize email addresses of this format as valid (as long as the list actually exists) in order to facilitate an easier method for users to join and leave your mailing lists. For example: suppose you have a list called `MyList@example.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@example.com` and `MyList-Unsubscribe@example.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

You can override this option for individual lists by specifying a value for the List-Subscribe and List-Unsubscribe headers in the **Mailing List URLs** options located on the Mailing List Editor's Moderation 283 screen.

Add 'Sender: <List>' header to all list messages
Enable this option if you wish to insert the `Sender` header into mailing list messages.

Mailing list pruner deletes messages that it can't parse
When this option is enabled, MDaemon will delete list messages that do not contain a parsable address.

Mailing list pruner saves messages that cause list member removal
When MDaemon scans returned list messages in an attempt to remove member addresses that cannot be reached, this control will cause messages that result in a list member's removal to be saved. For more information, see the *Remove undeliverable email addresses...* option on the Settings 268 screen.

Screen incoming mailing list mail for obvious non-list content
Check this box if you wish MDaemon to reject messages addressed to a mailing list when it determines that they should have been addressed to the system account instead. For example, a user may join or leave a list by placing the Subscribe or Unsubscribe command at the beginning of an email message and sending that message to the system address (e.g. "mdaemon@example.com"). Oftentimes users erroneously try to send those sorts of messages to the list itself. This option will prevent those messages from being posted to the list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not send copy of list message to sender of message
When this option is enabled and a list member sends a message to the list, the sender will not receive a copy of the message. This option is disabled by default.

Remove duplicate list recipients when single message submitted to multiple lists
When this option is enabled and a single message is addressed to multiple mailing lists, MDaemon will deliver only one copy of the message to any recipient who is a member[265] of more than one of the lists. For example, if `frank@example.net` is a member of `List-A@example.com` and `List-B@example.com` and an incoming message is addressed to both lists, Frank will receive only one copy of the message rather than two. This option only applies to lists, therefore in the above example if the message were addressed to Frank directly, plus the two lists, then Frank would receive two copies of the message rather than three. This option is disabled by default.

Using this option is not generally recommended. Mailing lists can be used and organized many different ways by users, and there is no way of knowing which list will receive the message when limiting duplicates in this way. Therefore using this option could cause unnecessary difficulties for some users, due to message threading preferences, using IMAP filters[720] to sort messages to specific folders, and so on.

Add the following custom 'Header: value' to all list messages
If you wish to add a static header/value combination (such as "Precedence: bulk") to all list messages, specify that text here.

Digest 'Subject:' text:
Use this option if you wish to customize the subject used when MDaemon sends mailing list digest[279] messages. The default is: "`$LISTNAME$ message digest $TIMESTAMP$ $ISSUE$`." The macros expand to the name of the mailing list, the time-stamp of the digest message creation, and the issue number.

Maximum members per mailing list [xx] (0=no limit)
Use this option if you wish to set a maximum number of members allowed per mailing list. You can set a per domain maximum on the Domain Manager's Settings[205] screen. This option is only available in MDaemon Private Cloud.

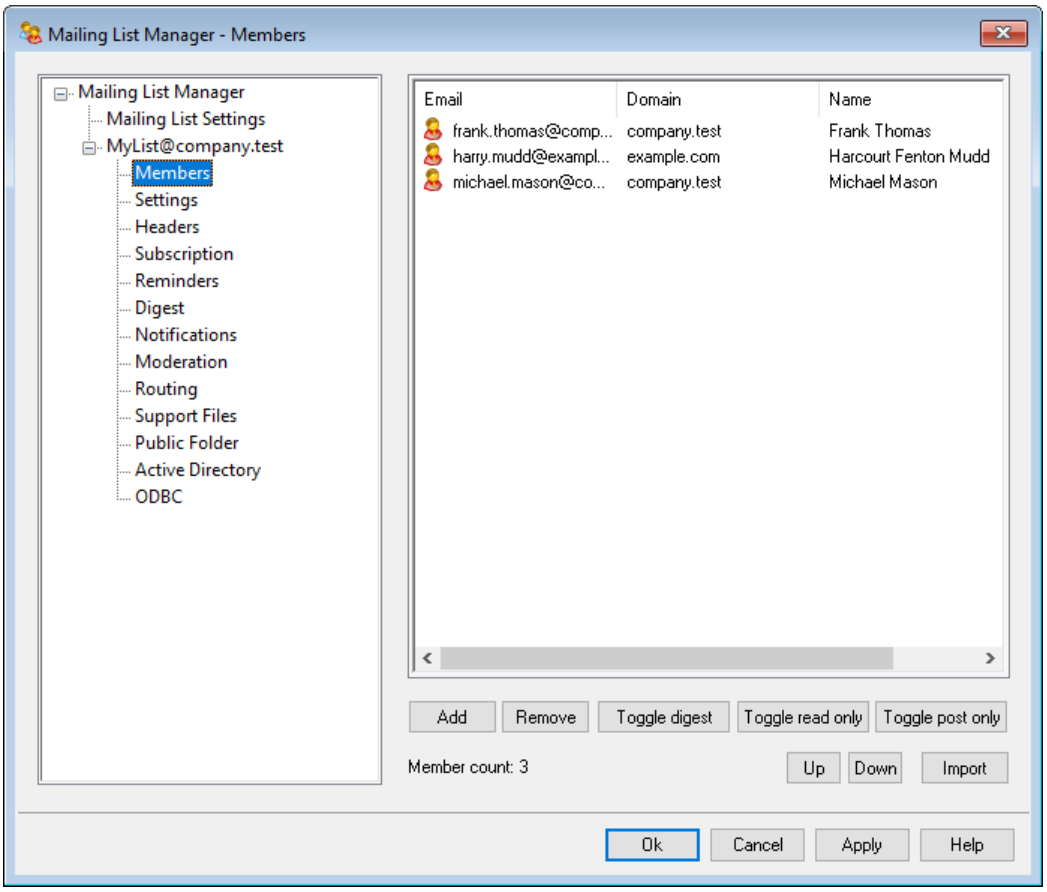
See:

Mailing List Manager[259]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2 Mailing List Editor

3.4.2.1 Members



This screen displays the email addresses and names of all members currently subscribed to the list. Each member's entry also states its "type" of membership: normal, digest, read only, or post only. To edit a member's settings, double-click the member's entry.

Add
This button opens the New List Member screen for adding new members 267.

Remove
To remove a member from the list, select its entry and then click this button.

Toggle digest
Select a member and then click this button to make it a Digest 279 membership. Click the button again to return the member to "normal" mode.

Toggle read only
Select a member's entry and then click this button to switch it to "Read Only" mode. The member will still receive messages from the list but will not be allowed to send them to it. Click the button again to return the member to "normal" mode.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Toggle post only
Clicking this button after selecting a member will set the membership to "Post Only." A Post Only member can send messages to the list but will not receive any. Click the button again to return the member to "normal" mode.

Up/Down
Select one or more members and then click these buttons to move them up or down in the list. You can also sort the list by clicking the heading of any column. **Note**: If you sort the list by a column heading it will override any manual sorting you have done using the Up/Down buttons.

Import
Click this button to import list members from a text file that has its fields separated by commas (i.e. a comma delimited file). Each entry must be on its own line and all of its fields must be separated by commas. Further, the first line of the file (the baseline) must list the names of the fields and the order in which they appear in the remaining lines. One of the fields must be called "**`Email`**" and contain email addresses. There are also two optional fields: "**`FullName`**" and "**`Type`**". `FullName` is for the list member's name. `Type` can have a value of: "`read only`", "`post only`", "`digest`", or "`normal`". All other fields will be ignored by the importer.

For example:

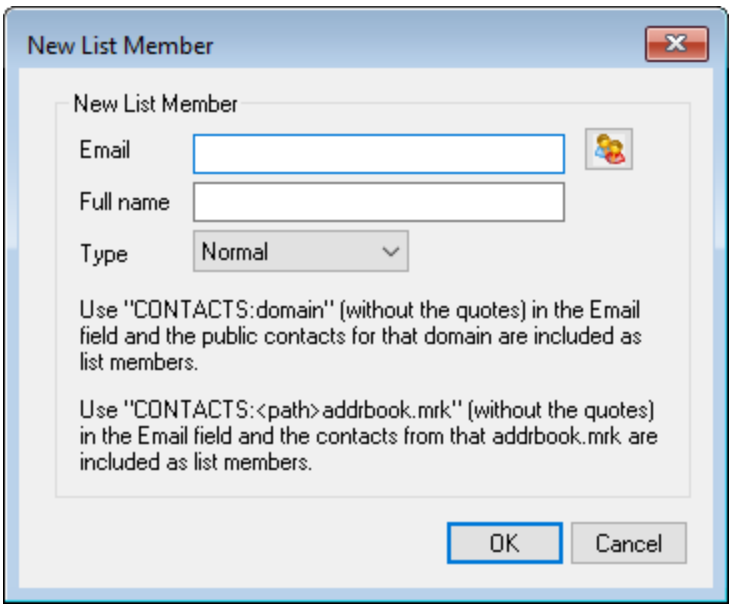
```
"Email", "FullName", "Type", "Address", "telephone"
"user01@altn.com", "Michael Mason", "Digest", "123 Street St",
"519.555.0100"
```

Imported members do not receive the list welcome packet (if any), and the importer will not check for member duplicates.

Member count:
The total number of members currently subscribed to the list is displayed at the bottom of the screen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Adding New Members



New List Member

Email
Enter the email address that you wish to add to the mailing list, or click the Account icon if you wish to browse MDaemon accounts and groups to add to the list. List member addresses cannot contain " ! " or "|".

If you wish to all users of one of your domains or all users belonging to a specific group, you can enter **ALL_USERS:<domain>** or **GROUP:<group-name>** respectively, instead of entering a specific email address. For example, adding `ALL_USERS:example.com` as a member of a list has the same effect as adding every `example.com` user account separately.

You can also use **CONTACTS:<domain>** to include a domain's public contacts 113 as list members. For example, `CONTACTS:example.com`.

Full name
Enter the member's name in this field. This name will appear in the "To:" header of list messages when the "*Replace 'TO:' header 'Display Name' with Member's name*" option is selected on the Headers 271 screen.

Type
Use the drop-down box to choose the type of membership for the user:

Normal—The member can send and receive list messages normally.

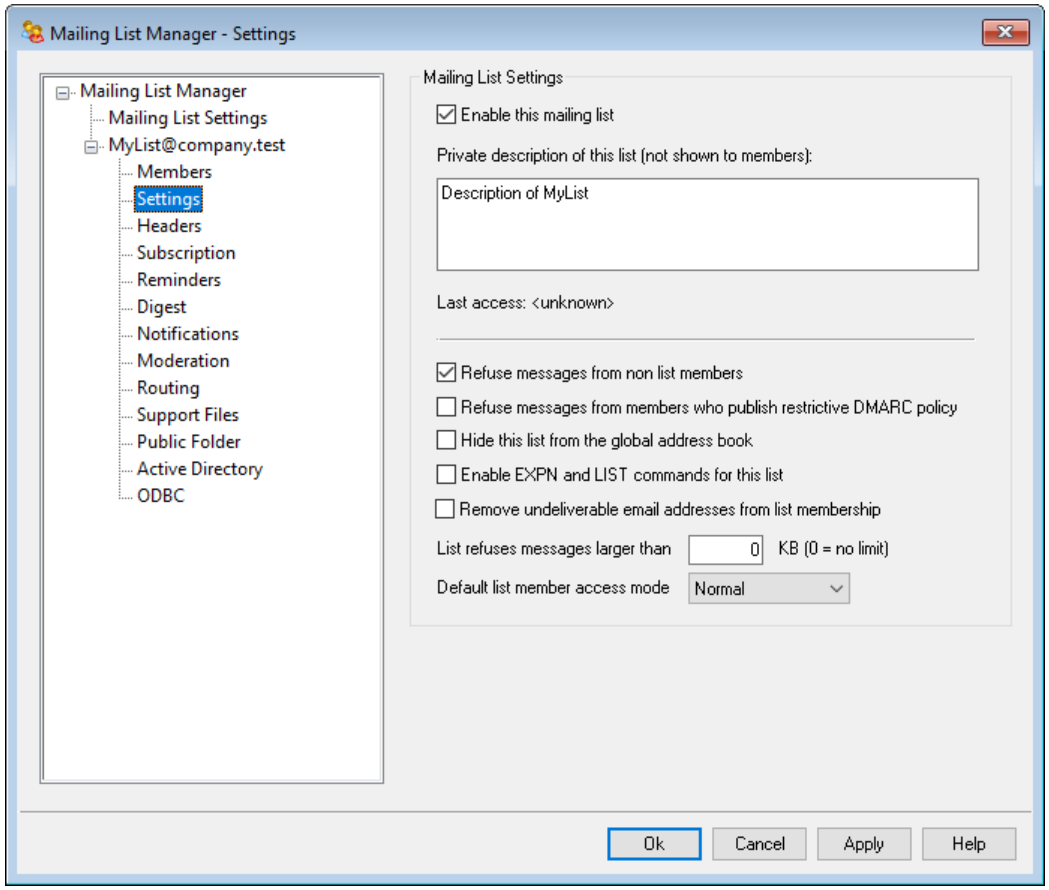
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Digest—The member can send and receive list messages, but received messages will be in digest format.

Read only—The member will receive messages from the list but cannot send messages to it.

Post only—The list member can send messages to the list but will not receive them.

3.4.2.2 Settings



Mailing List Settings

Enable this mailing list
Clear this checkbox if you wish to disable the mailing list temporarily. While the list is disabled, any message arriving via SMTP either to or from the list will generate a 451 temporary error and be refused.

Private description of this list (not shown to members)
You may enter a private description of the list here. This is for your own reference and it will not be displayed to any members or in any headers.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Last Access
Displays the time that someone last accessed this list. This can help you more easily identify lists that are rarely or no longer used.

Refuse messages from non list members
When this control is enabled, the list will be considered a "private" list, meaning that only list members can send messages to the list. Messages originating from non-members will be refused.

Refuse messages from domains with restrictive DMARC policies
Enable this option if you wish to reject any incoming message to the list that is sent by someone from a domain that publishes restrictive DMARC 523 policies (i.e. p=quarantine or p=reject). It is generally not necessary to enable this option if you are using the "*Replace 'From:' email address with list's email address if...*" option located on the Headers 271 screen.

If both this option and the "*Replace 'From:' email address with list's email address if...* 271" option are disabled then that would likely cause some list messages to be rejected by some receiving servers, and in some cases it could cause the recipient to be automatically removed from list membership 270. You should therefore take care to ensure that at least one of these options is enabled.

Hide this list from the global address book
Click this option to hide the mailing list from the Webmail and LDAP public address books.

Enable EXPN and LIST commands for this list
By default MDaemon will not honor EXPN and LIST commands for lists, in order to keep the membership private. If you enable this option then the membership of the list will be reported in response to an EXPN or LISTS command during a mail session.

Remove undeliverable email addresses from list membership
When this feature is enabled, MDaemon will automatically remove an address from the members list when it encounters a permanent fatal error while attempting delivery. An addresses is also removed when the message is moved to the Retry 856 system and subsequently expires from that system.

The *Remove undeliverable email addresses...* option is only designed to assist in situations where the remote mail server refuses to accept messages. This will only work when "*Deliver list mail to each member individually*" has been selected on the Routing screen 285. If you are instead routing list messages to a smart host then see Enhanced List Pruning 270 below for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

List refuses messages larger than [xx] KB
This control places an upper limit on the size of a message accepted for this mailing list. Messages larger than this limit are refused.

Default list member access mode
Use the drop-down list to set the default access mode to be used for for new members. You can change any existing member's access mode setting from the Members 265 screen. There are four membership modes:

Normal—The member can send and receive list messages normally.

Digest—The member can send and receive list messages, but received messages will be in digest format.

Read only—The member will receive messages from the list but cannot send messages to it.

Post only—The list member can send messages to the list but will not receive them.

Enhanced List Pruning

When the *Remove undeliverable email addresses from list membership* option is enabled and you have specified a local mailbox as the return path for the list's messages (see the *List's SMTP 'Bounce' address* option on Notifications 281), each day at midnight MDaemon will attempt to parse problem addresses from the returned mail and remove those members that couldn't be reached. This will aid in more efficiently pruning invalid addresses from mailing lists, especially when you are routing the list's messages to a smart host rather than delivering them directly.

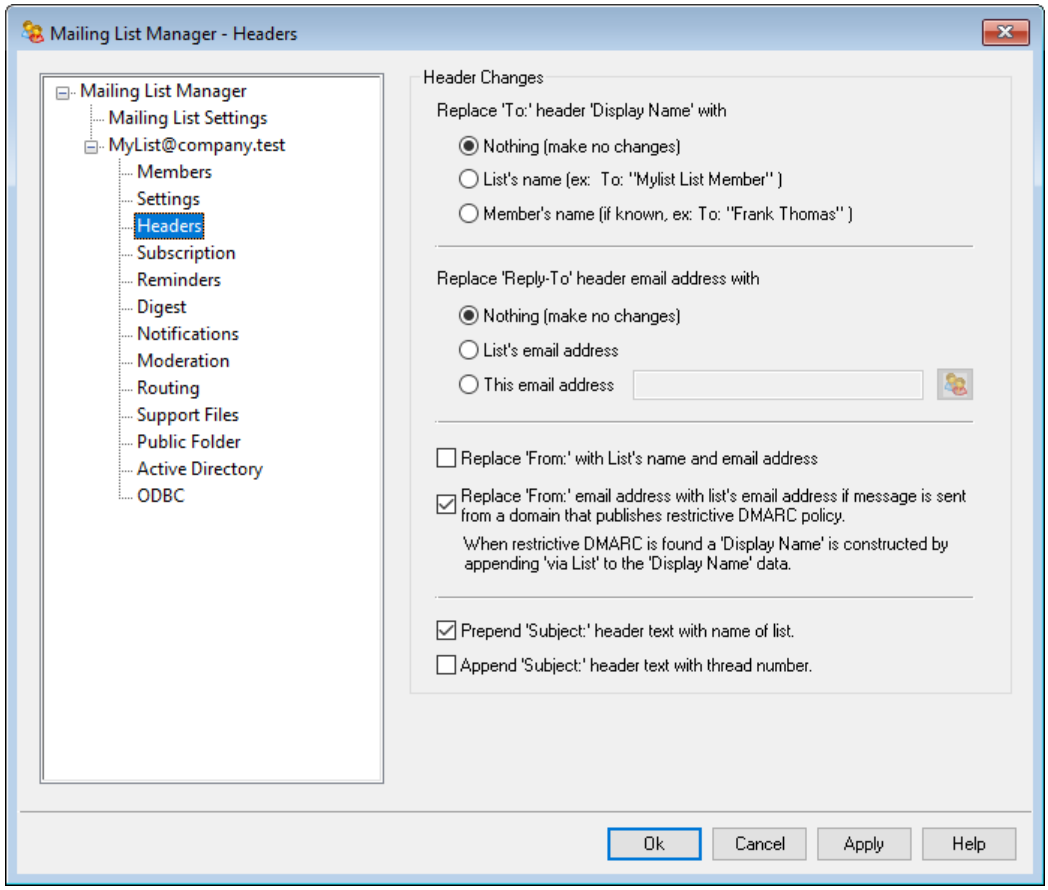
On Mailing List Settings 262 there are two options related to this feature. The *Mailing list pruner deletes messages that it can't parse* option will cause returned messages that do not contain a parsable address to be deleted, and the *Mailing list pruner saves messages that cause list member removal* option will cause all messages that result in a list member being deleted to be saved.

Setting the *List's SMTP 'Bounce' address* 281 to a local user's address could cause that user's email to be deleted as a result of the list pruner settings designated on Mailing List Settings 262.

When delivery to an address results in a 5xx error, the address will be appended to the `BadAddress.txt` file located in the logs folder. This can help you, for example, identify bad addresses in your mailing lists more quickly than searching the outgoing SMTP logs. This file is automatically removed at midnight each night to prevent it from growing too large.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.3 Headers



Header Changes

Replace 'TO:' header 'Display Name' with
Use this option to designate the text to display in the name portion of the TO: header whenever MDaemon receives a message directed to the list.

Nothing (make no changes) - When this options is selected MDaemon will make no changes. The display name and address contained in the TO: header will appear exactly as the sender of the message entered them.

List's name - This option replaces the displayed name with the name of the list plus "List Member". For example, for a mailing list named "My-Family" the display name portion of the To: header would say, "My-Family List Member".

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Member's name (if known) - When this option is selected, the TO: header will contain the name (if available) and address of the list member to whom the message is directed.

The *Member's name* option can only be chosen when "*Deliver list mail to each member individually*" has been selected on the Routing screen[285]. When "*Deliver list mail using individual RCPT commands for each member*" is selected, MDaemon will default to the *List's name* option.

Replace 'Reply-To:' header email address with
This option is for designating the email address that will appear in each list message's Reply-To: header.

Nothing (make no changes)
Choose this option if you wish to leave the Reply-To: header unchanged from whatever it is in the original message that will be distributed to the list. This is generally the option you should choose when you want replies to be directed back to whomever posted the message to the list, rather than to all of the list's members.

List's email address
Choose this option if you want replies to be directed to the list rather than to a specific person or address. This is the option you should choose if you wish to use the list as a group discussion tool, where replies are sent to all members.

This email address
If there is a specific email address to which you wish replies to be sent then type it here, or click the Account icon if you wish to browse for a specific MDaemon account to use. You could use this option, for example, for something like an email newsletter with a specific contact address for replies.

Replace 'From:' with List's name and email address
Check this box if you wish to replace the contents of the "From:" header with the mailing list's name and email address.

Replace 'From:' email address with list's email address if message is sent from a domain that publishes restrictive DMARC policy
By default, when an incoming message to the list is sent from a user at a domain that publishes a restrictive DMARC[523] policy (i.e. p=quarantine or p=reject), MDaemon will replace the user's email address in the From: header with the address of the list, before sending the message to the list. This is necessary to prevent the list message from being rejected by servers that honor restrictive DMARC policies. In addition to changing the From: header's email address, the displayed name will also be modified to add "via List Name," to show that it is a message sent by that mailing list on behalf of the named person. Further, any time the From: header is changed

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

by this feature the original From: header data will be moved into the Reply-To: header, but only if the message has no Reply-To: header to begin with and the list isn't configured to display a custom Reply-To: header.

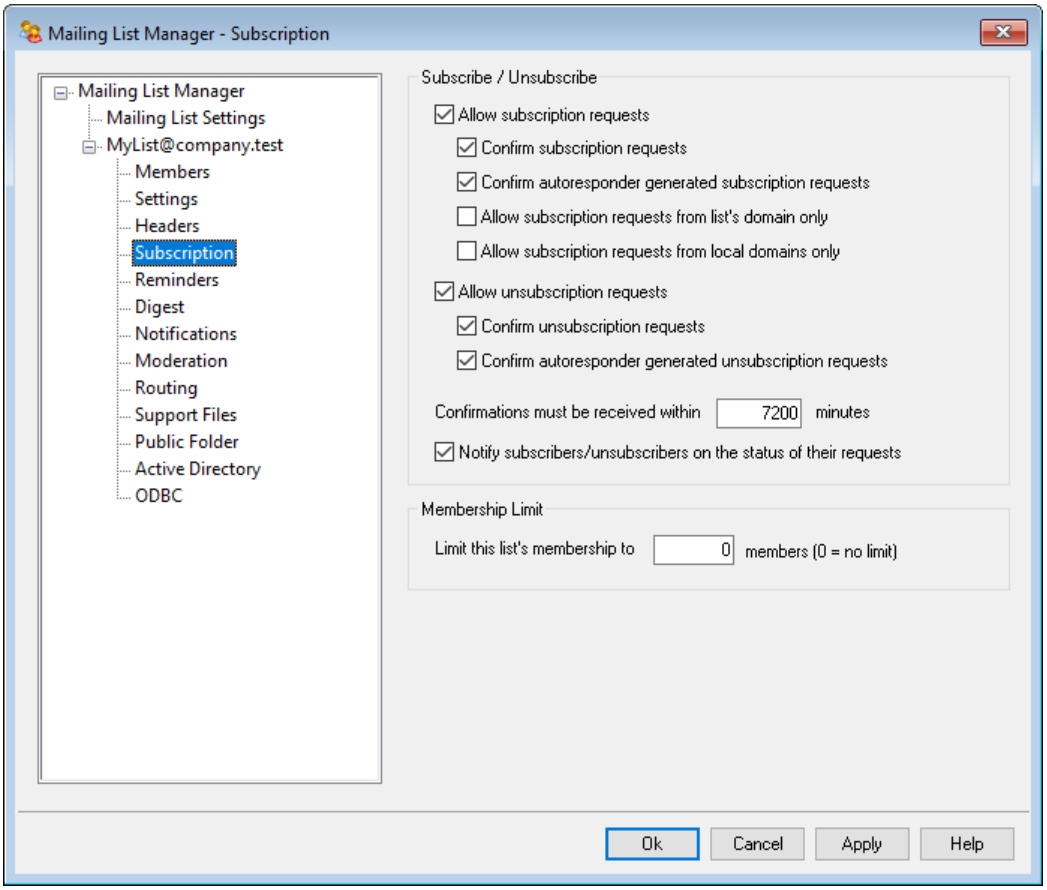
You should not disable this option unless you fully understand the ramifications of doing so and are certain that you need to disable it. Disabling this option would likely cause some list messages to be rejected by some receiving servers, and in some cases it could cause the recipient to be automatically removed from list membership 270. Alternatively, you could enable the *Refuse messages from domains with restrictive DMARC policies* 268 option instead, which causes incoming messages to the list to be refused when coming from a domain with a restrictive DMARC policy.

Prepend 'Subject:' header text with name of list
This setting causes MDaemon to enclose the name of the list in brackets (e.g. [ListName]) and add it to the beginning of the `Subject:` in all messages sent to the list. This is enabled by default.

Append 'Subject:' header text with thread number
This switch allows you to toggle whether thread numbers will be displayed in the `Subject:` header of list messages. They are appended to the end of the subject line in braces and used as a pseudo thread number. Sorting your Inbox by subject will align list mail in chronological order. This option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.4 Subscription



Subscribe/Unsubscribe

Allow subscription requests
This option controls whether or not the list will allow subscription requests, either through specially formatted email messages or through autoresponders. For more information, see: Subscribing to Mailing Lists 276.

Confirm subscription requests
When this box is checked, MDaemon will attempt to confirm subscription requests by generating a unique code and then sending it in a message to the address requesting to join the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below. **Note:** The contents of the confirmation message is contained in the `SubConf.dat` file, located in the "`MDaemon\app\`" folder.

Confirm autoresponder generated unsubscription requests
When this box is checked, MDaemon will attempt to confirm subscription requests that are generating automatically via the Autoresponder 708 option, "*Add sender to this mailing list*." As with the previous option, MDaemon will generate a unique code and then send it in a message to the address waiting to be added

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the list. If the person then replies to that confirmation message, MDaemon will automatically add the member to the list. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

Allow subscription requests from list's domain only
Choose this option if you wish to allow subscription requests only from users belonging to the list's domain. For example, for the list "MyList@example.com", only users "@example.com" would be allowed to subscribe to the list.

Allow subscription requests from local domains only
Choose this option if you wish to allow subscription requests only from users belonging one of the MDaemon server's local domains.

Unsubscribe

Allow unsubscription requests
This option controls whether or not the list will allow unsubscription requests, either through specially formatted email messages or through Autoresponders. For more information, see: Subscribing to Mailing Lists 276.

Confirm unsubscription requests
When this box is checked, MDaemon will attempt to confirm requests to remove a member from the list, by generating a unique code and then sending it in a message to the address requesting to unsubscribe from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member from the list. Confirmation messages are time-sensitive, meaning that the user must reply to the message within the number of minutes designated below. **Note:** The contents of the confirmation message is contained in the `UnSubConf.dat` file, located in the "`MDaemon\app\`" folder.

Confirm autoresponder generated unsubscription requests
When this box is checked, MDaemon will attempt to confirm unsubscription requests that are generating automatically via the Autoresponder 708 option, "*Remove sender from this mailing list*." As with the *Confirm unsubscription requests* option above, MDaemon will generate a unique code and then send it in a message to the address waiting to be removed from the list. If the person then replies to that confirmation message, MDaemon will automatically remove the member. These confirmation messages are also time-sensitive and therefore must replied to within the number of minutes designated below.

Confirmations must be received within [XX] minutes
This is the number of minutes that the recipient of a subscription or unsubscription confirmation message has before the message will expire. If this time limit is exceeded before MDaemon receives a reply to the message, then the address will not be added or removed from the list. The address would then need to submit a new request to join or leave the list. The default setting of this option is 7200 minutes (i.e. five days).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

This is a global value—it applies to all of your mailing lists rather than to the specific list you are editing.

Notify subscribers/unsubscribers on the status of their requests
When this checkbox is enabled, MDaemon will send a completion notification message to the user that has been subscribed/unsubscribed to the Mailing List.0

The content of a file called UnSubUser.dat (if it exists) will be appended to the email sent to users when they unsubscribe from lists.

Membership Limit

Limit this list's membership to [xx] members (0=no limit)
With this feature you can place an upper limit on the number of people who are allowed to subscribe to the Mailing List. Enter a zero into this field if you do not wish to limit list subscriptions.

This limit only applies to addresses subscribed via the email methods outlined in *Subscribing to Mailing Lists* 276. This limit does not apply to subscriptions entered manually on the Members 265 screen, nor to subscription requests sent via email when the List password 283 is included.

See:

Subscribing to Mailing Lists 276
Autoresponder 708

3.4.2.4.1 Subscribing to Mailing Lists

Subscribing/Unsubscribing via Email Commands

To subscribe to or unsubscribe from a mailing list, send an email message addressed to `MDaemon` (or any alias thereof) at the domain hosting the mailing list, and place the `Subscribe` or `Unsubscribe` command as the first line of the message body. For example, there is a mailing list called `MD-Support` being hosted by `mdaemon.com`. You can subscribe to the list by composing a message addressed to "`mdaemon@mdaemon.com`" and placing the value: `SUBSCRIBE MD-Support@mdaemon.com` as the first line of the message body. The message subject is irrelevant and can be left blank.

For complete details on how to form this and other control messages, see: Remote Server Control Via Email 880.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Occasionally, users will attempt to subscribe/unsubscribe to lists via email by sending the commands to the list itself rather than to the MDaemon system account. This results in the command being posted to the list rather than the user being subscribed or unsubscribed. To help prevent these sorts of messages from being posted to mailing lists, there is an option located at Setup » Preferences » System 480, called "*Screen incoming mailing list mail for obvious non-list content*." This option is enabled by default.

Subscribing/Unsubscribing via Email Addresses

The option, "*Honor '<List>-subscribe' and '<List>-unsubscribe' addresses*," located at Setup » Mailing List Manager » Mailing List Settings 262, makes it possible for users to join or quit mailing lists by sending a message to a special email address rather than requiring them to use the email commands described in *Subscribing/Unsubscribing via Email Commands* above. To use this method to join or quit a list, a user would simply send a message to the list's address, but with "`-subscribe`" or "`-unsubscribe`" appended to the mailbox portion of the address. For example, if the list's name is, "franks`-list@example.com`," then a user could subscribe to the list by sending a message to, "`franks-list-subscribe@example.com`." To unsubscribe from the list, the message would be sent to, "`franks-list-unsubscribe@example.com`." In both cases the content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@example.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

Subscribing/Unsubscribing via Autoresponders

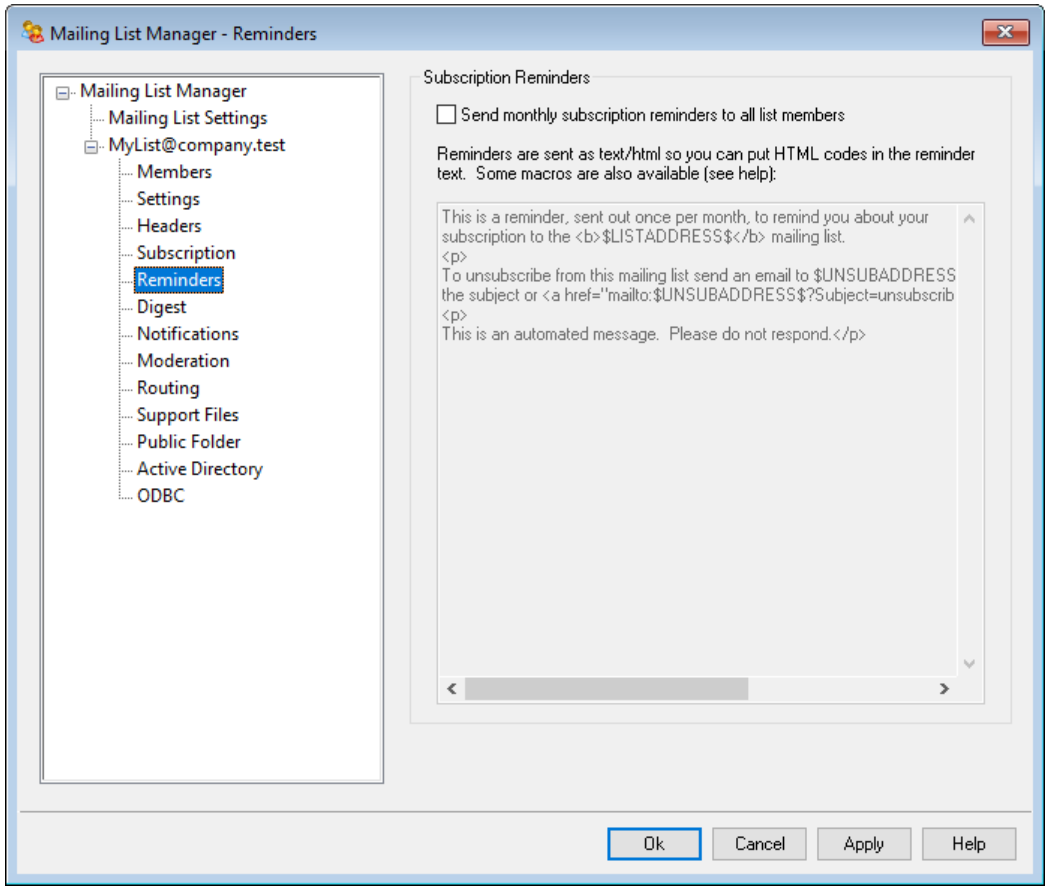
You can also utilize Autoresponders 708 to automatically add or remove list members. To do this you would create one or more MDaemon accounts whose sole purpose would typically be to automatically add or remove addresses who send messages to those accounts, via the Autoresponders configured for each account. For example, if you had a mailing list called, "`franks-list@example.com`," then you could create an MDaemon account with the address: "`join-franks-list@example.com`." You would then configure an autoresponder for that account to add to "`franks-list@example.com`" any addresses sending messages to it. Then, to join that list, all someone would have to do is send an email to "`join-franks-list@example.com`". This is a simple solution for users because it doesn't require them to remember any of the special email commands required by the *Subscribing/Unsubscribing via Email Commands* method outlined above.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Subscription 274
Remote Server Control via Email 880
Autoresponder 708
Preferences » System 480
Preferences » Miscellaneous 489

3.4.2.5 Reminders



Subscription Reminders

Send monthly subscription reminders to all list members
Enable this option if you wish to send the contents of the provided text box as a subscription reminder message to each list member on the first day of each month. The reminder message is sent as text/html so that you can use HTML code in the reminder text if you choose. The following macros are available for use within the reminder message:

$LISTADDRESS$ - expands to the mailing list's email address (e.g. MyList@example.com)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$LISTNAME$ - expands to the local-part of the mailing list's email address (e.g. MyList).

$UNSUBADDRESS$ - expands the list's unsubscribe address (the MDaemon system address, e.g. mdaemon@example.com)

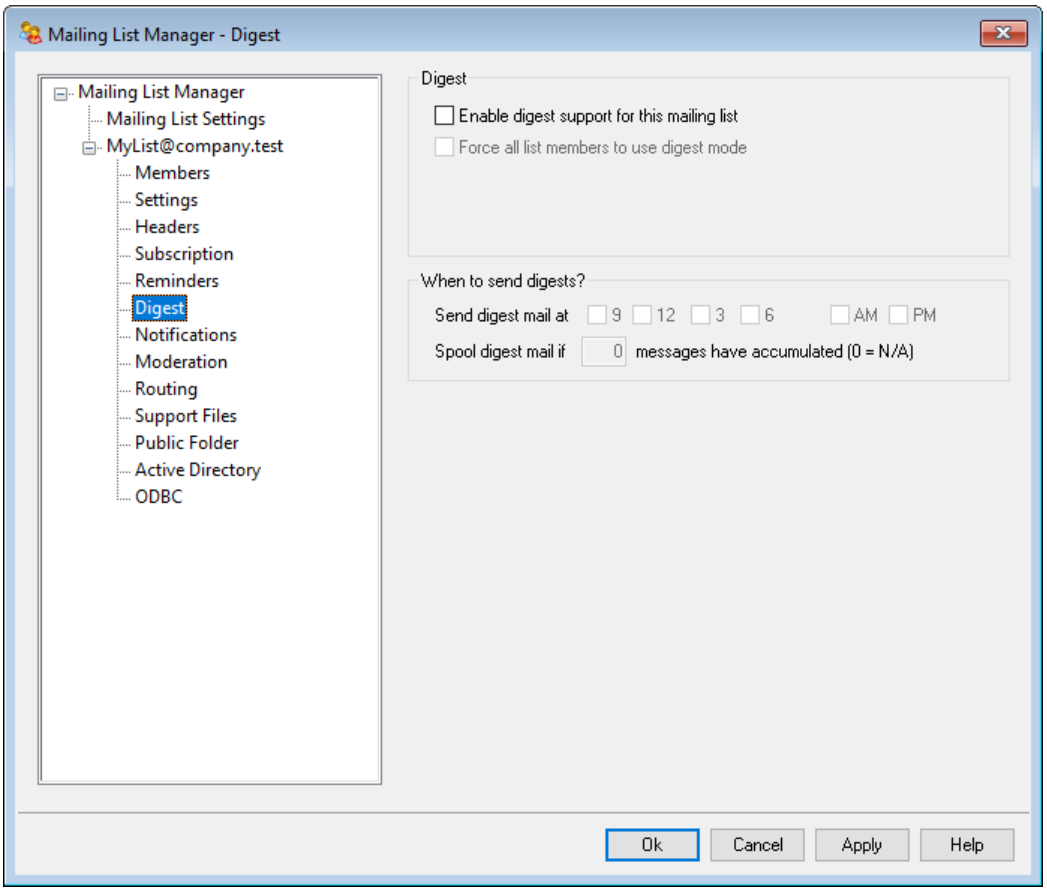
$MEMBERADDRESS$ - expands to the email address of the list member receiving the reminder (e.g. frank.thomas@example.com)

If you wish to send reminders on a different day of the month, you can do so by setting the following key in the MDaemon.ini file:

```
[Special]
ListReminderDay=X
```

Set "X" to a number from 1 to 28, representing that day of the month you wish to send reminders.

3.4.2.6 Digest



Digest

Enable digest support for this mailing list
Check this box if you wish to allow digest support for this mailing list. When digest support is enabled, a copy of each message sent to the mailing list will be archived

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

so that list members who have their membership type 265 set to *Digest* will periodically be sent batches of these archived messages in a compact and indexed format rather than receive them one at a time.

Force all list members to use digest mode
By default, list members can control whether they wish to receive list traffic in digest or normal format. Check this box if you wish to force all members to use digest mode, regardless of the mode they may have chosen for themselves.

When to send digests?

The following options determine how often and under what circumstances digests will be sent to those list members who are set to receive mail in digest format. All of the options operate independently of each other, meaning that any or all of them can cause a digest to be sent.

Send digest mail at 9, 12, 3, 6 AM, PM
Use this option to schedule how often this list's digests will be sent. If you check all of the boxes in this option then digests will be sent every three hours, in addition to any that may be triggered by the options below.

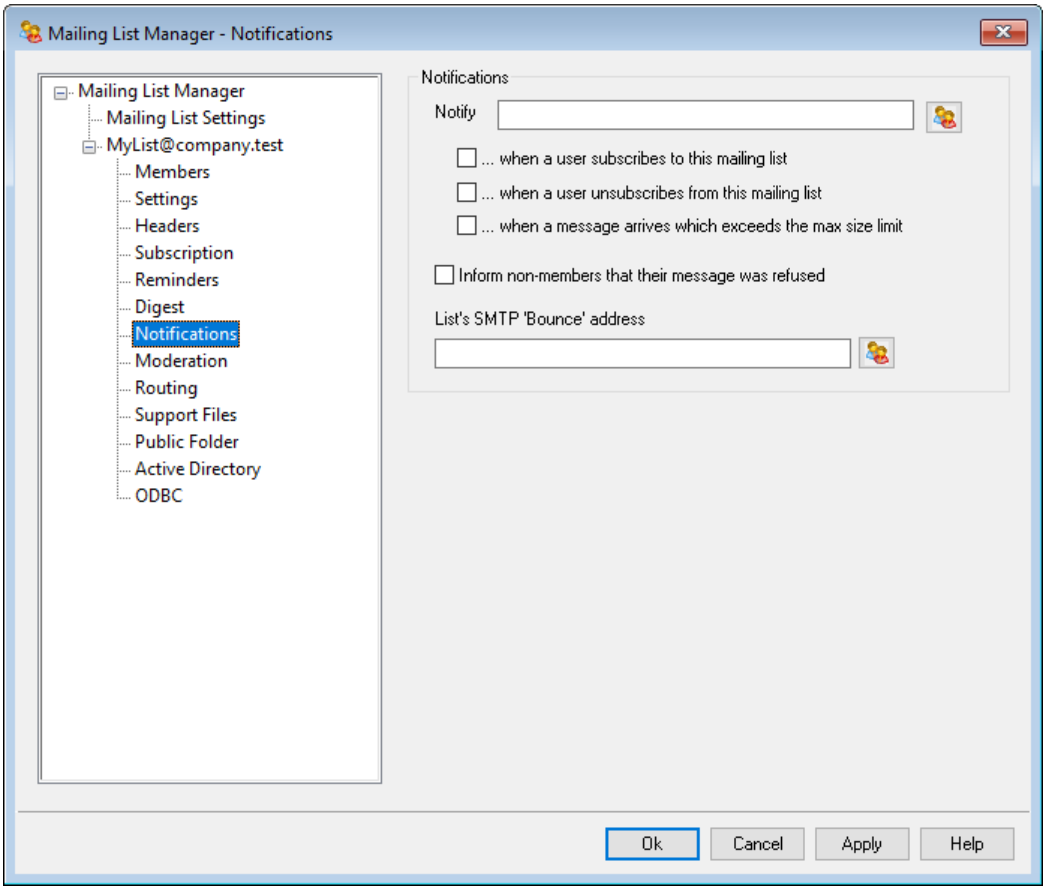
Spool digest mail if [xx] messages have accumulated (0 = n/a)
If you wish to send digests automatically whenever a certain number of messages have accumulated, specify that number here. Use "0" if you do not wish to use this option. "0" is the default setting.

See:

Members 265
Remote Server Control via Email 880

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.7 Notifications



Notifications

Notify
Use this option to list an address that will be notified when the selected events take place.

...when a user subscribes to this mailing list
Check this box if you wish to send a note to the designated address each time someone subscribes to the mailing list.

...when a user unsubscribes from this mailing list
Check this box if you wish to send a note to the designated address each time someone unsubscribes from the mailing list.

...when a message arrives which exceeds the max size limit
Check this box if you wish to send a note to the designated address each time someone sends a message to the mailing list that is larger than *List refuses messages larger than [xx] KB* limit designated on Settings 268.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Inform non-members that their message was refused
When this option is enabled and non-members of a private list send mail to the list, MDaemon will inform them that the list is private. They will also be given instructions on how to subscribe to list. Lists are designated as private by using the *Only list members can post to this list* option located on Settings 268.

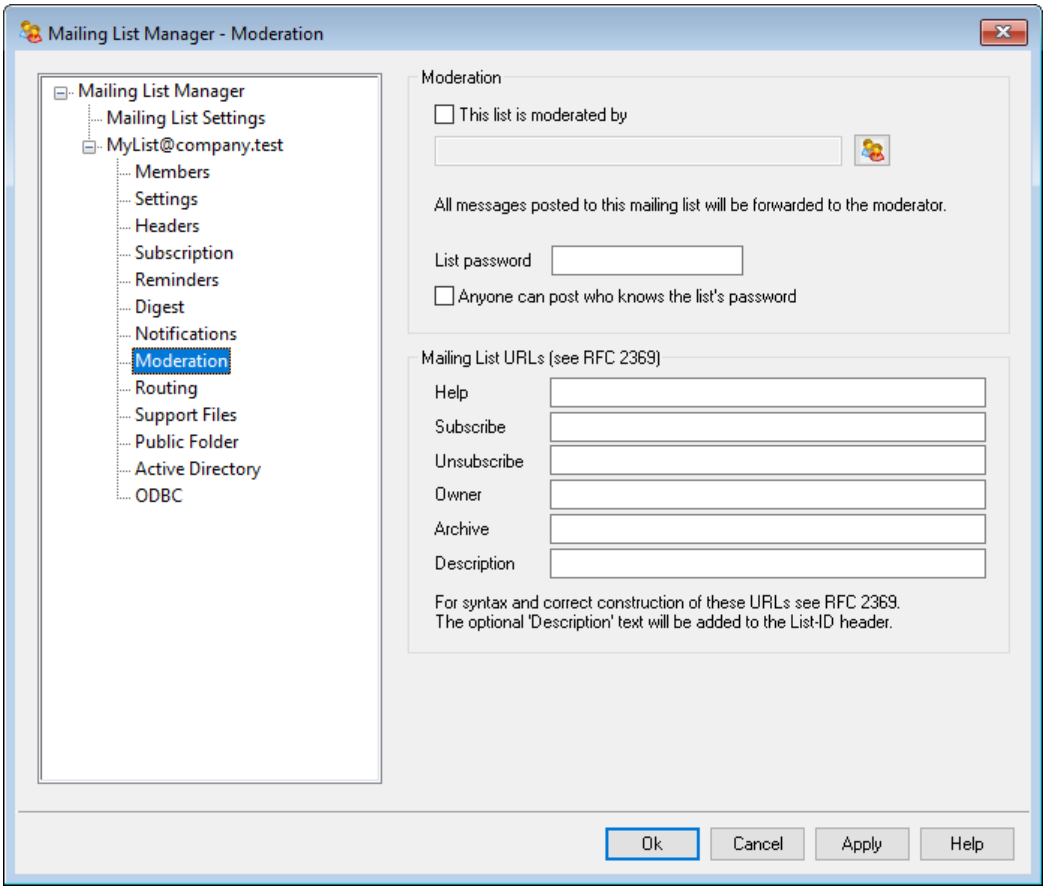
Returned Mail

List's SMTP 'Bounce' address
Use this option to specify the address that should receive any "bounced" mail or deliver status notification messages generated from list traffic. Any given message to a mailing list with 100 recipients might have, for example, ten undeliverable addresses due to address changes, down servers, or the like. The SMTP system will generate and return to the sender of the message a notification message concerning these undeliverable conditions. Using this option you can designate the address that should receive these messages for your mailing lists. You can also choose for no one to receive them, in which case MDaemon will place list mail into the mail stream in such a way that return mail will not be possible. This address should NOT be the mailing list's address.

Setting the *List's SMTP 'Bounce' address* to a local user's address could cause that user's email to be deleted as a result of the list pruner settings designated on Mailing List Settings 262. Use caution before setting this option to a local user's address. For more information, see Enhanced List Pruning 270.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.8 Moderation



Moderation

This list is moderated by
Check this box and specify an account if you wish the list to be moderated by the designated user. Moderated lists forward all posts to the moderator. The moderator alone may submit or forward messages to the list.

List password
If you wish to assign a password to this list, then enter it here. List passwords can be used with the *Anyone can post who knows the list's password* option below, and to override the *Membership Limit* option located on the Subscription screen 274. They also provide access to a number of features outlined in the *Remote Server Control via Email* 880 section.

Anyone can post who knows the list's password
If a password is assigned to the list, and this option is enabled, then anyone who includes the list's password at the beginning of a message's subject can post to the list, even if the list is moderated but the sender isn't the moderator.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailing List URLs (see RFC 2369)

MDaemon can add to mailing list messages any of the six header fields outlined in RFC 2369: *The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields*. The six headers are: **List-Help**, **List-Subscribe**, **List-Unsubscribe**, **List-Post**, **List-Owner**, and **List-Archive**. If you wish to use any of these headers to the list's messages, enter the desired header value into any of the fields below. The header values must be formatted according to the RFC 2369 specification (for example, `<mailto:list@example.com?subject=help>`). See the linked document for several examples of each header. MDaemon makes no changes to this data, therefore if the data is improperly formed it won't achieve any results.

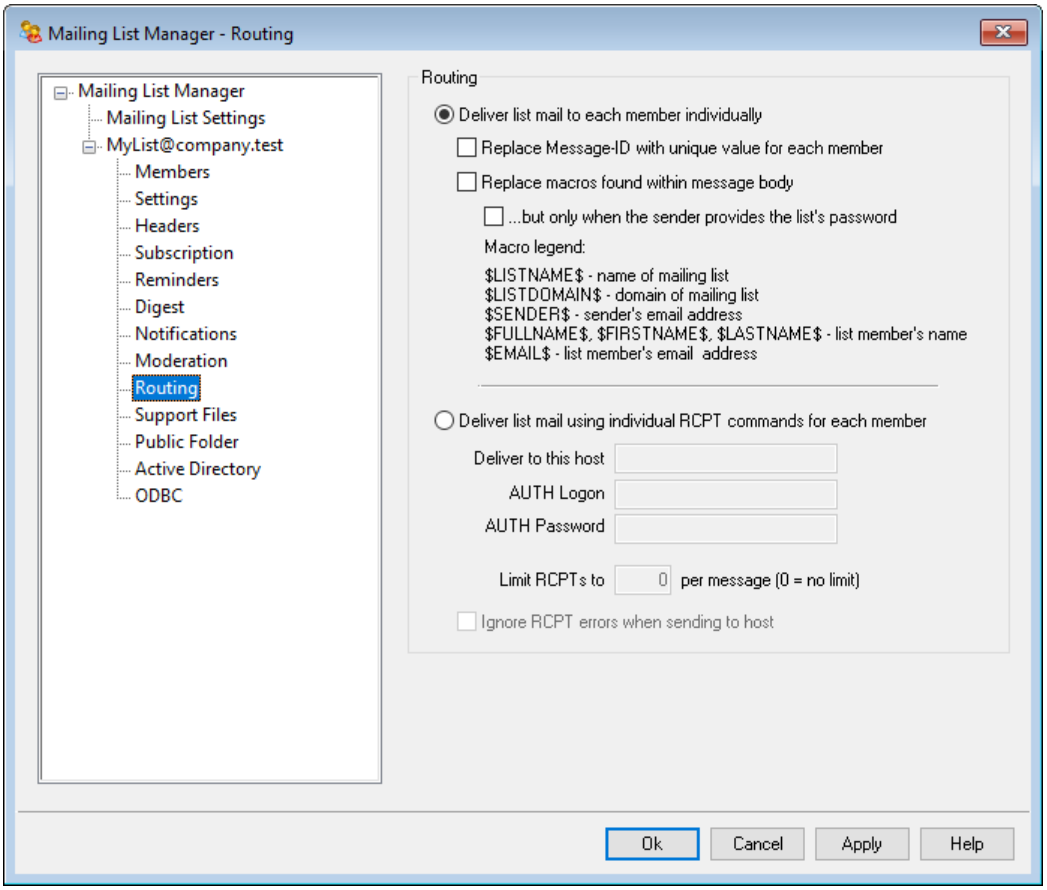
Description (used in List-ID: header)

Enter a short description of your mailing list here if you wish to add it to the `List-ID:` header included in messages that are sent to the list. The description and the list's identifier will be included in the header (e.g. `List-ID: "Frank's personal mailing list" <MyList.example.com>`) Note that the list's identifier is the mailing list's address with "." substituted for "@" in order to comply with the List-ID specification. If you leave the *Description* option blank then the List-ID: header will contain only the list identifier (e.g. `List-ID: <MyList.example.com>`). If an incoming message addressed to the list has a preexisting List-ID: header, MDaemon will replace the old header with the appropriate one for the list.

The List-Subscribe and List-Unsubscribe headers are included by default in all mailing list messages when the "*Honor '<List>-subscribe' and '<List>-unsubscribe' addresses*" option is enabled on the Preferences » Miscellaneous 489 screen. If you wish to override that option for this list, using different header values than those added automatically by that option, enter the desired values here. If that option is disabled then no List-Subscribe and List-Unsubscribe headers will be added to list messages unless you specify a value for them here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.9 Routing



Routing

Deliver list mail to each member individually
If selected, when messages are received for distribution to the list, a separate copy of each message will be created and dispatched to each list member. This will result in numerous individual messages being created which could affect the server's performance, depending on the size of the list and the load on the server. This option is selected by default.

Replace Message-ID with unique value for each member
When MDaemon is set to generate a separate copy of each message for each member, click this checkbox if wish each of those messages to have a unique Message-ID. This option is disabled by default and is not recommended unless you have special circumstances that require it.

Replace macros found within message body
Enable this option if you wish to allow the use of special macros in mailing list messages. When a macro is found, MDaemon will replace it with the corresponding value the macro represents, for each separate message before sending it to each list member.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...but only when the sender provides the list's password
When allowing macros within the message body, click this option if you wish to require the list's password[283] in order for someone to use macros in their message. When this option is disabled, anyone who can send a message to the list will be able to use macros.

Macros:

$LISTNAME$	The name of the list, or the "mailbox" portion of the list's address (e.g. "MyList" of MyList@example.com).
$LISTDOMAIN$	The list's domain (e.g. "example.com" of MyList@example.com).
$SENDER$	The message sender's email address.
$FULLNAME$ $FIRSTNAME$ $LASTNAME$	The list member's full name, first name, or last name, respectively (if available).
$EMAIL$	The list member's email address.

Deliver list mail using individual RCPT commands for each member
If selected, MDaemon will route a single copy of each list message to the specified smart host, rather then send individual messages to each member. This method employs multiple `RCPT To` statements during the SMTP session with the specified host.

Deliver to this host
Designate the smart host to which you wish to pass all of the list's messages for delivery, using RCPT To statements for each member.

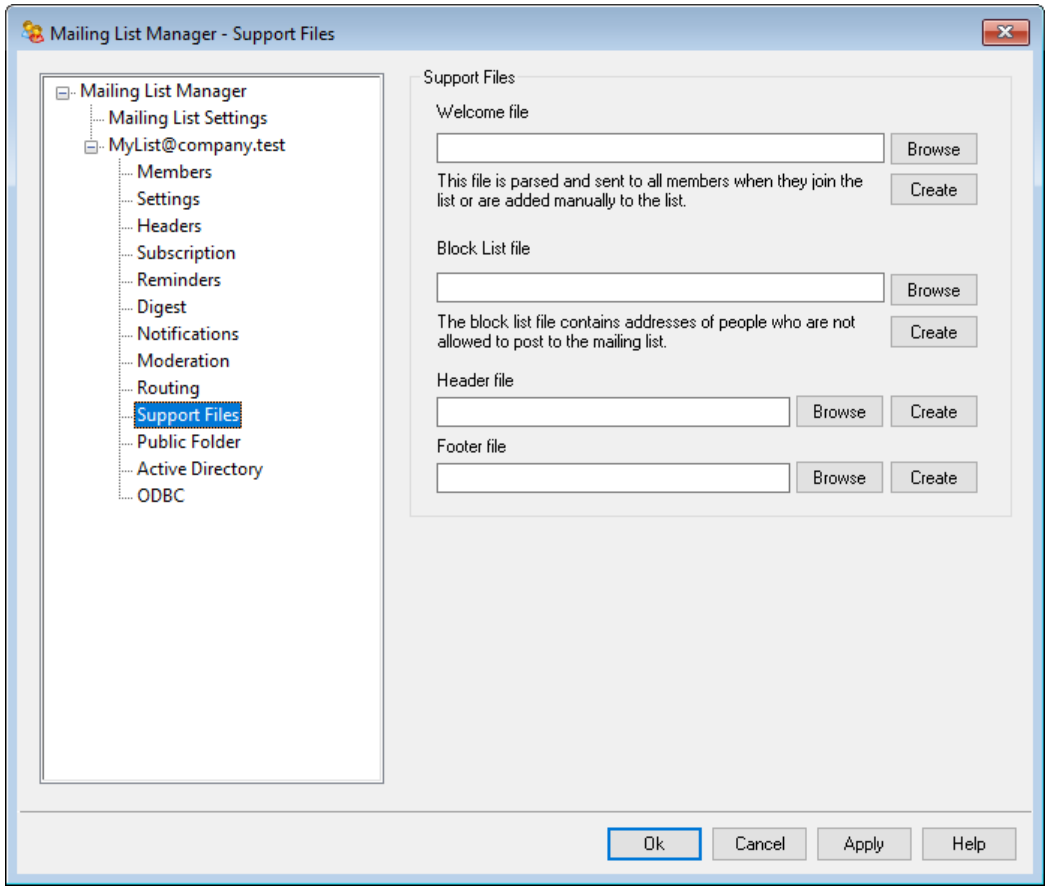
AUTH Logon/Password
Any logon credentials required by the host.

Limit RCPTs to [xx] per message (0=no limit)
Some hosts limit the number of `RCPT To` statements that they will accept when you are attempting to route a single copy of a message through them. If you specify the limit in this control then MDaemon will work around it by creating additional copies of the message and dividing the list into smaller groups. Then it will deliver the message to those groups thus avoiding the need to exceed the limitation. This is similar to the *Deliver list mail to each member individually* option above, but it generates less copies, sending each copy to groups of addresses rather than generating a separate copy for each member.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Ignore RCPT errors when sending to host
Since some smart hosts will refuse to queue or spool mail for certain domains, the routed approach to list delivery could cause numerous problems. An error code returned from the smart host as a result of this refusal would ordinarily cause MDaemon to abort the delivery attempt. Check this option if you want MDaemon to ignore error codes returned from the smart host during delivery of routed list mail, thus allowing those members that are accepted a chance to receive the message.

3.4.2.10 Support Files



Support Files

Welcome File
If specified, the file listed here will be processed and have its contents emailed to all new members just after they subscribe. You may use the following macros in a new member welcome file:

$PRIMARYDOMAIN$	This macro expands to MDaemon's Default Domain name, which is designated on the Domain Manager 174.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$PRIMARYIP$	This macro will return the IPv4 address associated with MDaemon's Default Domain 174.
$PRIMARYIP6$	This macro will return the IPv6 address associated with MDaemon's Default Domain 174.
$DOMAINIP$	This macro will return the IPv4 address associated with the domain.
$DOMAINIP6$	This macro will return the IPv6 address associated with the domain.
$MACHINENAME$	This macro returns the contents of the FQDN option designated on the Domain screen.
$LISTEMAIL$	Displays the list's email address. Example: `MyList@example.com`
$LISTNAME$	Displays the name of the mailing list. Example: `MyList`
$LISTDOMAIN$	This macro returns the mailing list's domain. Example: `example.com`
%SETSUBJECT%	Use this macro to designate an alternate subject for the Welcome message. The designated subject text can include other list macros such as `$LISTEMAIL$`. Example: `%SetSubject% =Welcome to the $LISTNAME$ list.`

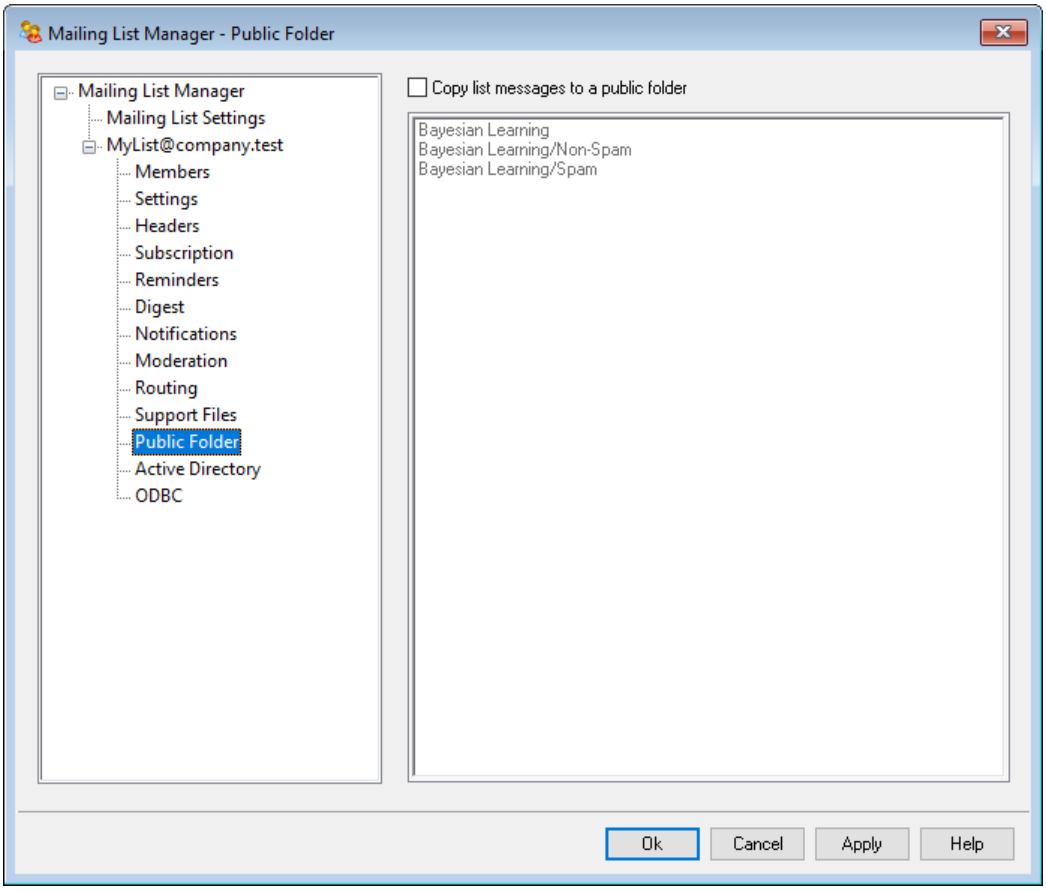
Block List File
If specified, the file listed here will be used to suppress messages sent from specified users.

Header/Footer File
The contents of the files specified here will be used as the header and/or footer file for list messages.

Create
To create a new file, click the *Create* button that corresponds to the file that you wish to create, specify a name, and then click *Open*. This will open the newly created file in Notepad for you to edit.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.11 Public Folder



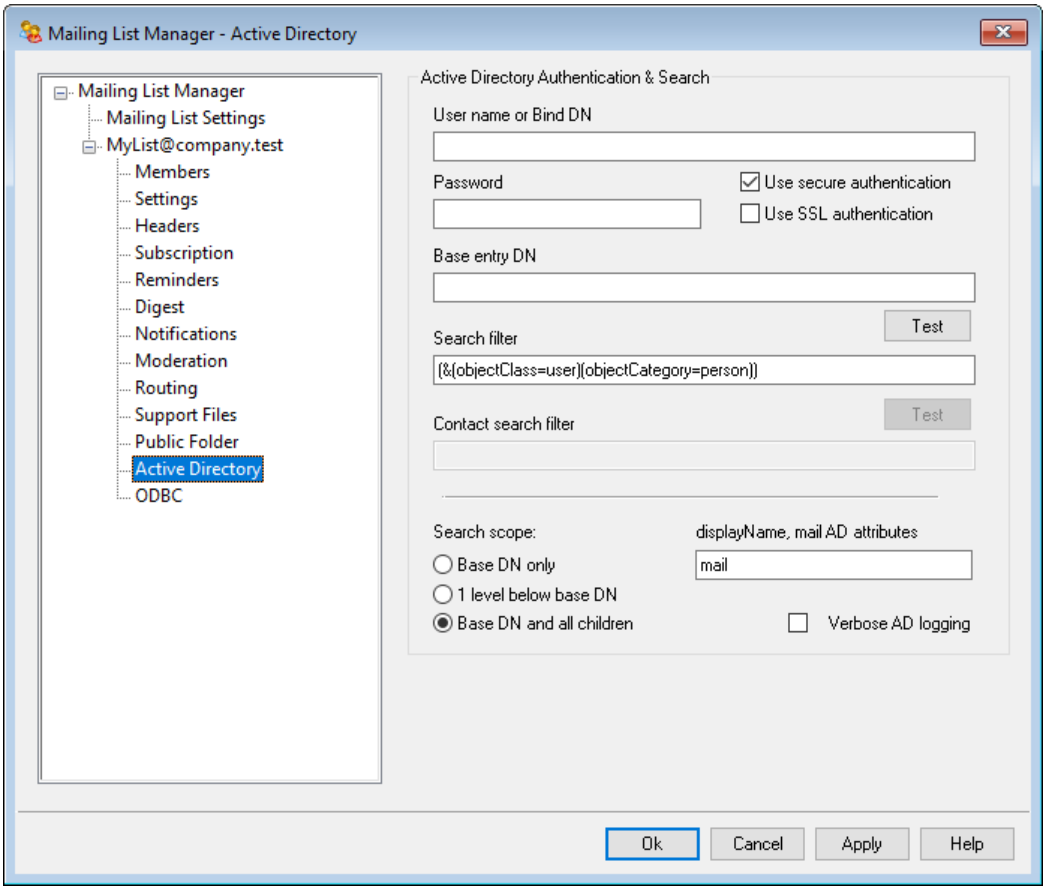
MDaemon supports using Public IMAP Folders 110 with mailing lists. Unlike personal IMAP folders, which are typically only accessible by a single user, Public folders are extra folders that are available to multiple IMAP users. The options on this screen are used to cause all messages destined for the Mailing List to be automatically copied to one of your public folders.

Copy list messages to a public folder
Enable this control if you want this list's messages to be copied to one of your Public Folders in addition to being delivered to the list.

Select a public folder
Click the Public Folder that you wish to associate with this list's messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.4.2.12 Active Directory



Use the options on this screen if you wish to pull some list member addresses from Active Directory.

Active Directory Authentication & Search

User name or Bind DN
This is the Windows account Logon or DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

Password
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use secure authentication
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

Use SSL authentication
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

Base entry DN
Specify the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search Active Directory for addresses. You can use "`LDAP://rootDSE`" in this option to begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts or desired group of addresses in your particular Active Directory tree can reduce the amount of time required to search the DIT. Leave this field blank if you do not wish to pull any list addresses from Active Directory.

Search filter
This is the LDAP search filter that will be used when for searching Active Directory. Use this filter to enable MDaemon to more precisely locate the desired user accounts or addresses that you wish to treat as list members.

Test
Use this button to test your search filter settings.

---

displayName, mail AD attributes
You must use this field to specify the attribute that will contain the email addresses used by this list. For example, if you used "`Mail`" in this field, then each Active Directory account that you wish to be treated as a list member must have the "`Mail`" attribute, and that attribute must contain an email address. You can additionally enter an Active Directory attribute for the full name field of list members before the email address attribute, separated by a comma. For example, you could enter: "`displayName, mail`" rather than just "`mail`" in this option. The first is the Active Directory attribute where the full name resides, and the second is the email attribute.

Search scope:

This is the scope or extent of your Active Directory searches.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

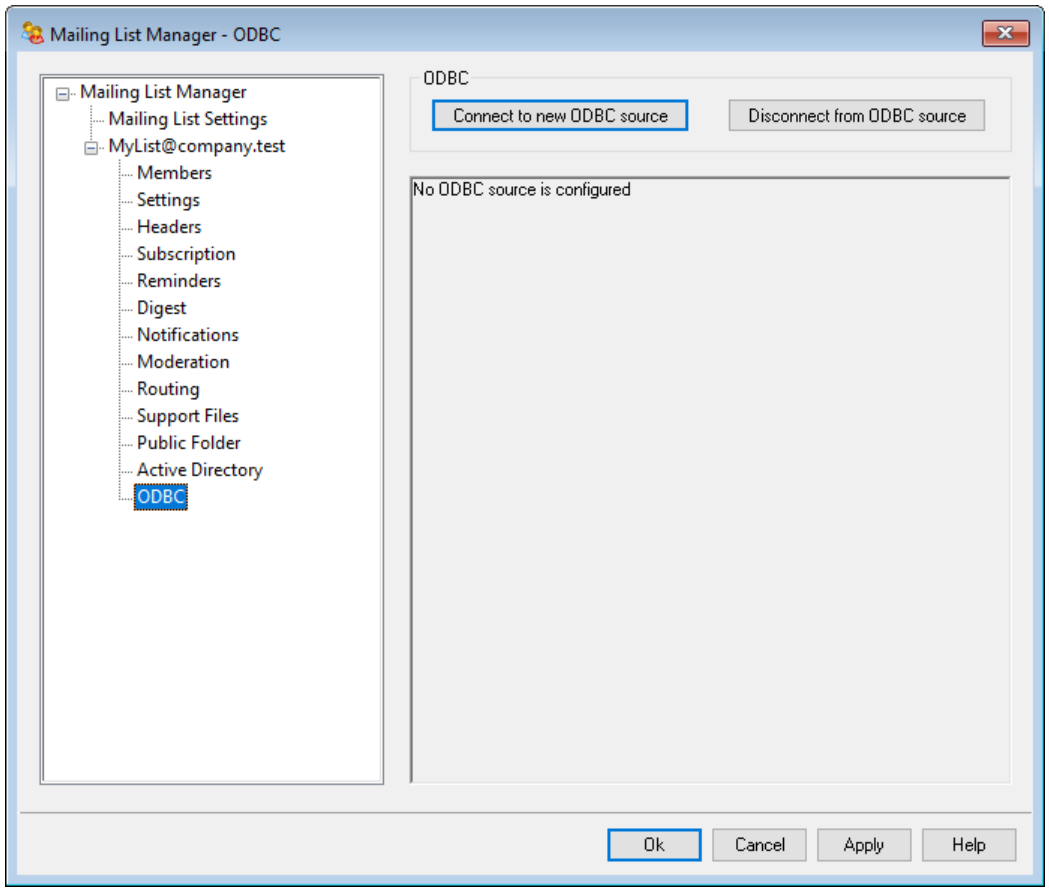
Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

1 level below base DN
Use this option if you wish extend your Active Directory search to one level below the supplied DN in your DIT.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT.

Verbose AD logging
By default MDaemon will use verbose logging for Active Directory. Clear this checkbox if you wish to use less extensive Active Directory logging.

3.4.2.13 ODBC



Using this feature you can maintain the list's membership list in an ODBC compliant database. The ODBC screen of the Mailing List editor is used to select a data source, table, and field mappings for MDaemon to link to the list. When messages arrive for

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

your list one or more SQL queries will be performed automatically and the resulting email addresses will be treated as part of the list's membership.

You can add, remove, and modify members of your list in the database using whatever ODBC compliant database application you choose.

ODBC

This section displays the current ODBC properties that you have set up for the mailing list. It displays the database's field mappings and the SQL queries that you have configured to designate each member's membership status (i.e. Normal, Post Only, Read Only, and/or Digest mode).

Connect to new ODBC source
Click this button to open the ODBC Selector Wizard for choosing the system data source that you wish to use for the mailing list.

Disconnect from ODBC source
Click this button to disconnect the list from the ODBC data source listed in the space above.

See:

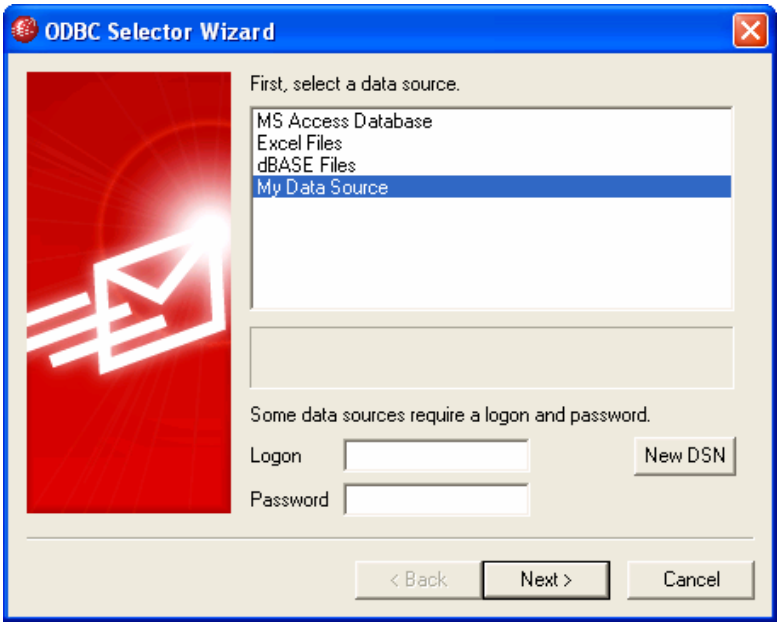
Configuring an ODBC System Data Source for a Mailing List 293
Creating a New System Data Source 296

3.4.2.13.1 Configuring an ODBC Data Source

To use an ODBC accessible database with a mailing list:

1. On the ODBC screen 292 of the Mailing List editor, click **Connect to new ODBC source** to open the ODBC Selector Wizard.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



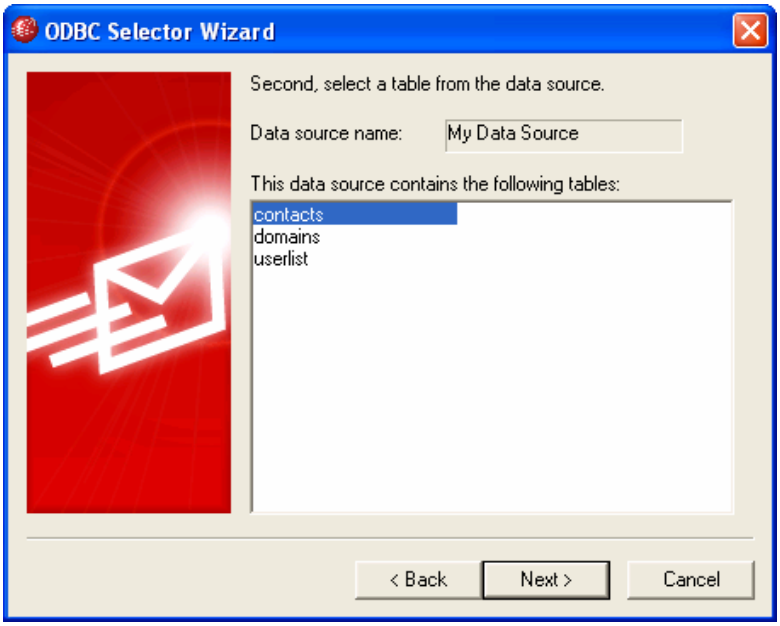
2. Select the **data source** that you wish to use for the list. If there is not a compatible data source listed, click **New DSN** and then follow the instructions listed under, **Creating a New ODBC Data Source** 296.

3. If required, enter the data source's **Logon** and **Password**.

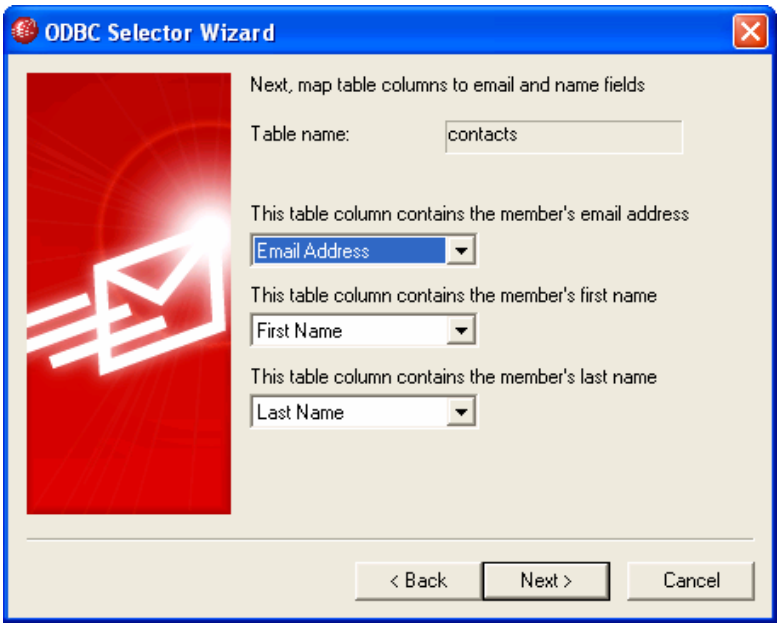
4. Click **Next**.

5. The data source must contain at least one table with fields for email addresses and names. If the data source contains one or more qualifying tables, choose the desired table and click **Next**. Otherwise, click **Cancel** to exit the ODBC Selector Wizard and then use your database application to add a table to the relevant database before continuing.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

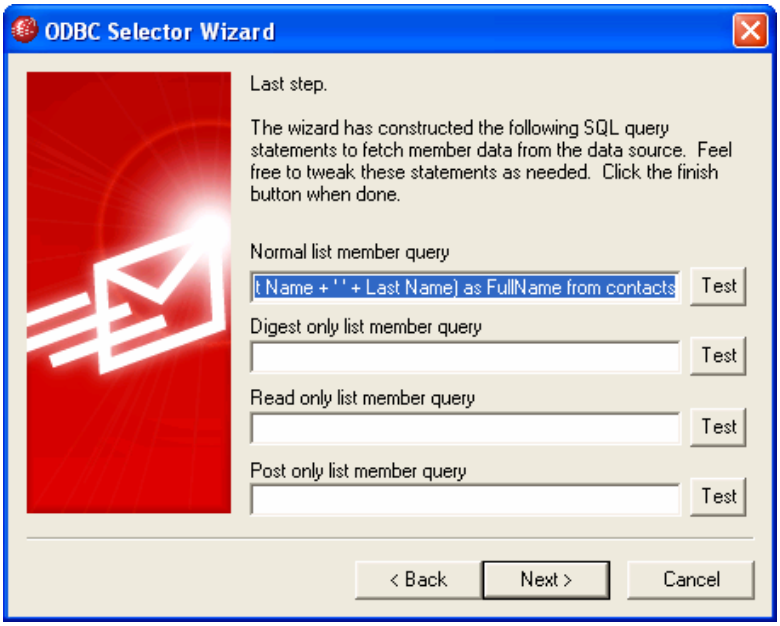


6. Use the drop-down list boxes to designate the table fields that will correspond to **email address**, **first name**, and **last name**. Click **Next**.



7. The ODBC Selector Wizard will construct an SQL query statement based on your selections in **Step 6**. MDaemon will use it to retrieve normal list member data from your database. You can edit this statement as desired, and include other query statements in the remaining controls to cause members to receive messages in Digest mode, and to designate members as Read Only or Post Only. A **Test** button is provided beside each control so that you can test your query statements to make sure they retrieve the proper data. When you are finished configuring your query statements, click **Next**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



8. Click **Finish**.

See:

Mailing List Editor » ODBC 292
Creating a New ODBC Data Source 296

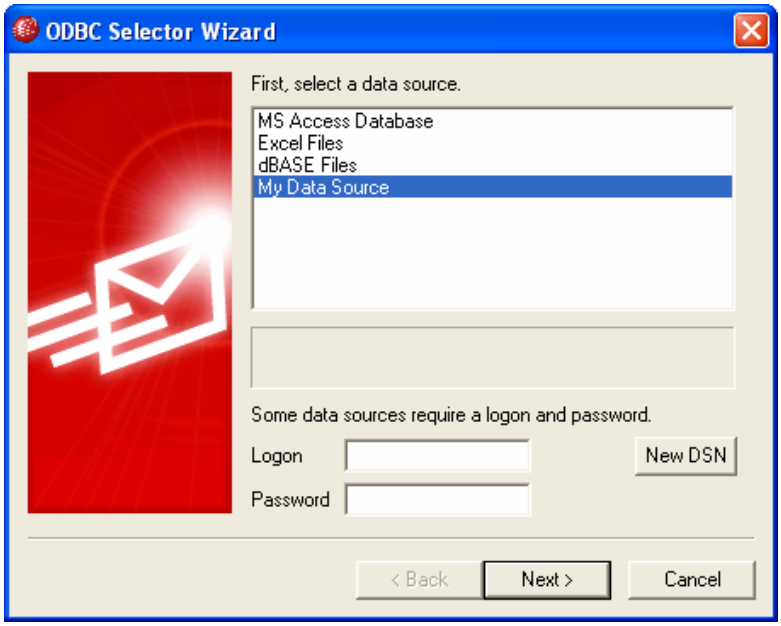
3.4.2.13.2 Creating a New ODBC Data Source

To create a new ODBC system data source for use by a mailing list:

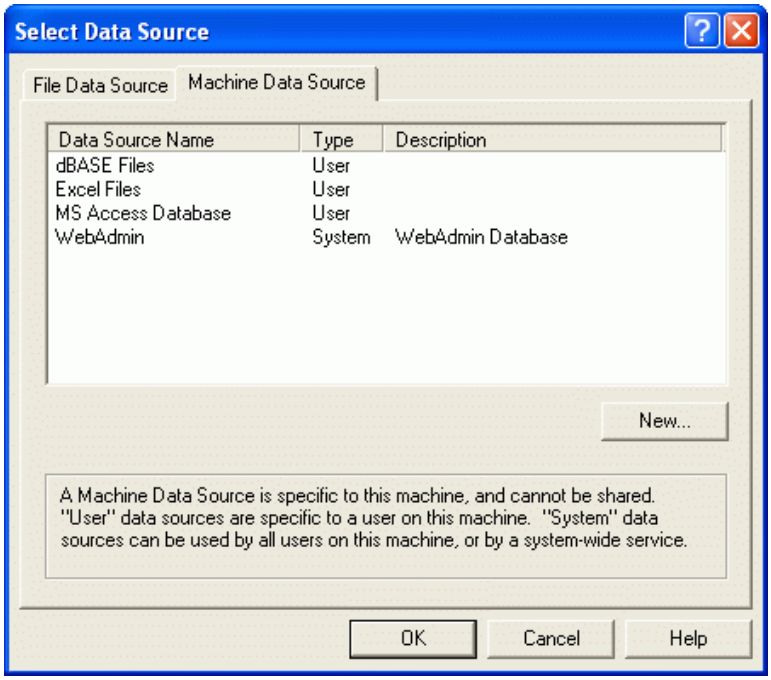
1. On the ODBC screen 292 of the Mailing List editor, click **Connect to new ODBC source** to open the ODBC Selector Wizard.

2. Click **New DSN** to open the Select Data Source dialog.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

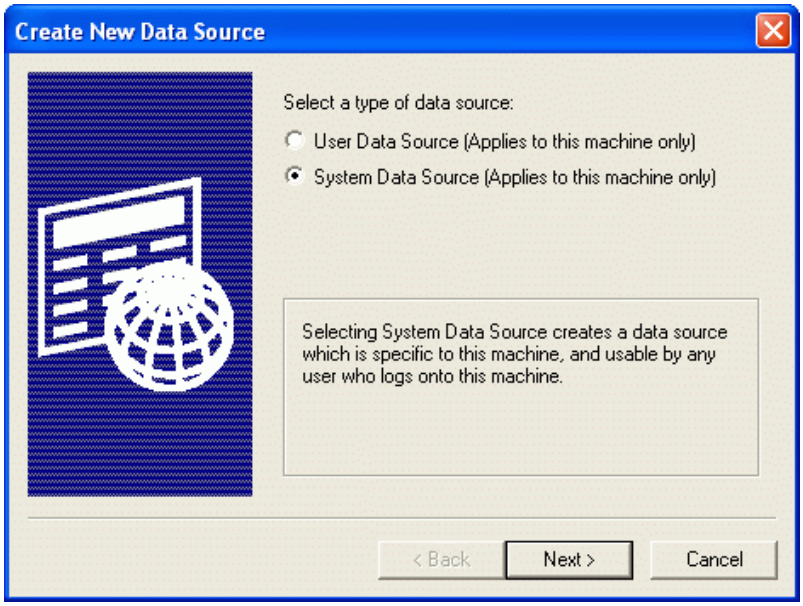


3. Switch to the **Machine Data Source** tab, and click **New...** to open the Create New Data Source dialog.

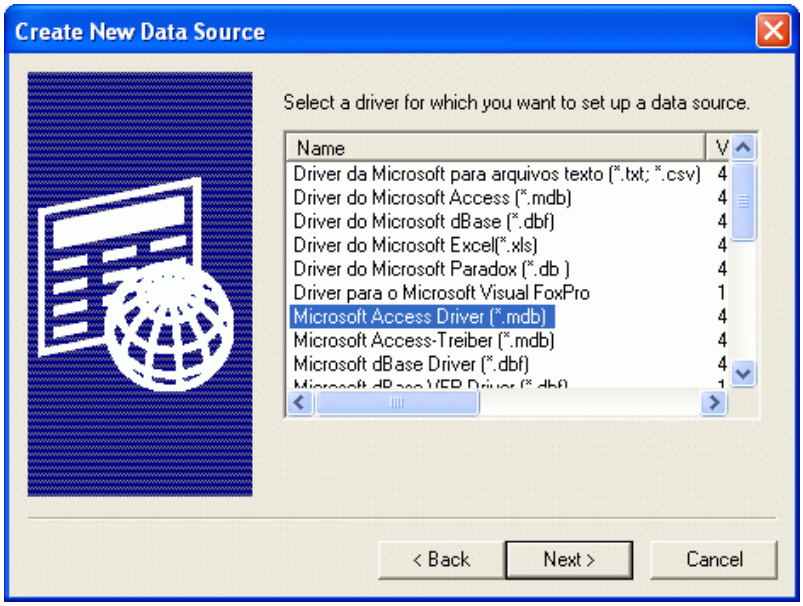


4. Select **System Data Source**, and click **Next**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

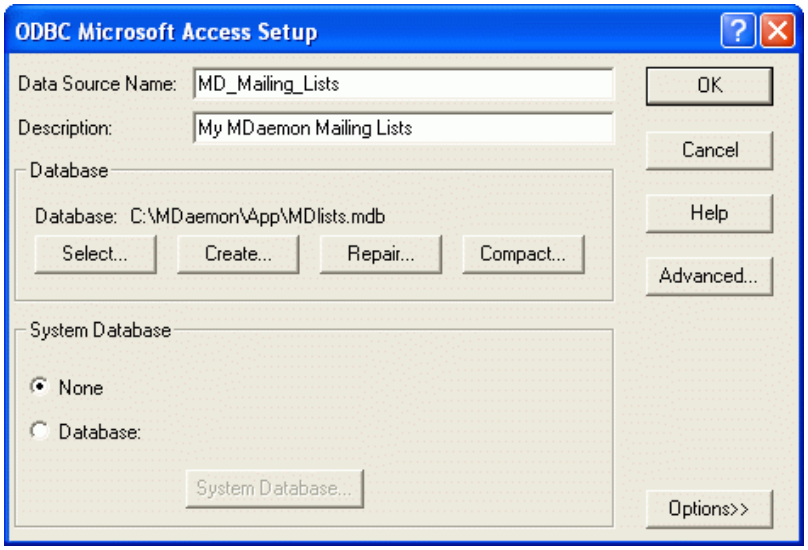


5. Select the **database driver** for which you wish to set up the data source, and click **Next**.



6. Click **Finish** to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



7. Designate a **Data Source Name** for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click **OK** to close the driver-specific dialog.

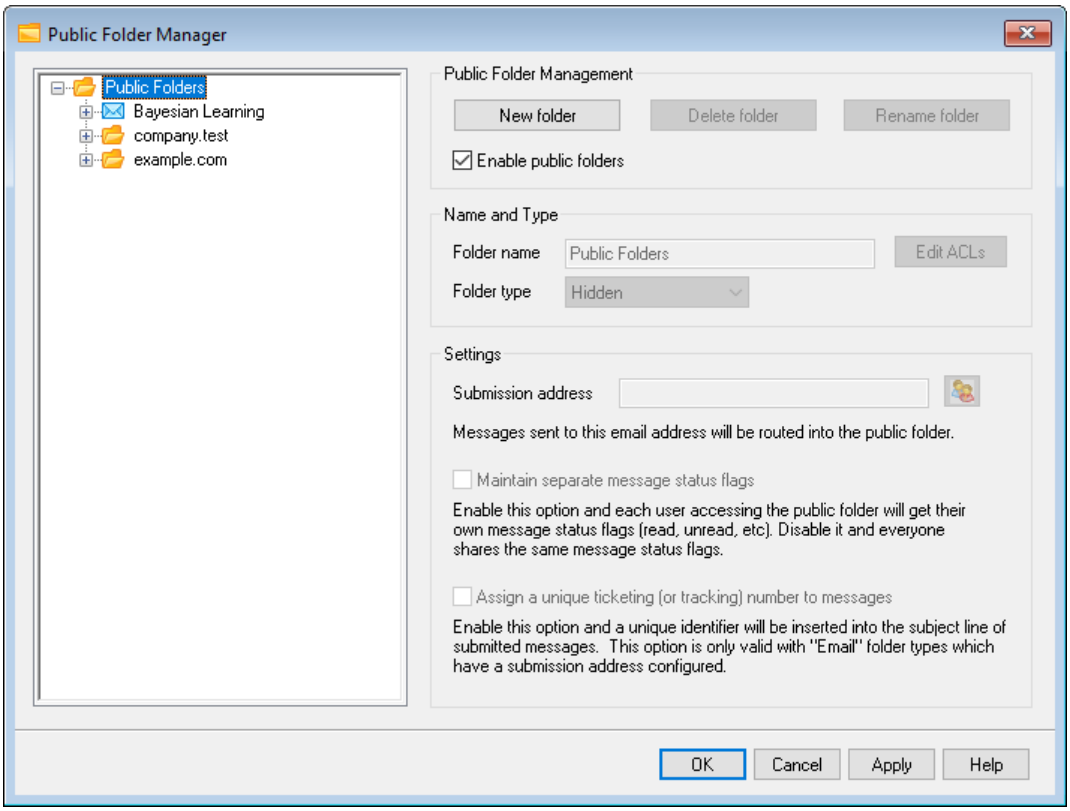
9. Click **OK** to close the Select Data Source dialog.

See:

ODBC - Mailing Lists 292
Configuring an ODBC System Data Source for a Mailing List 293

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.5 Public Folder Manager

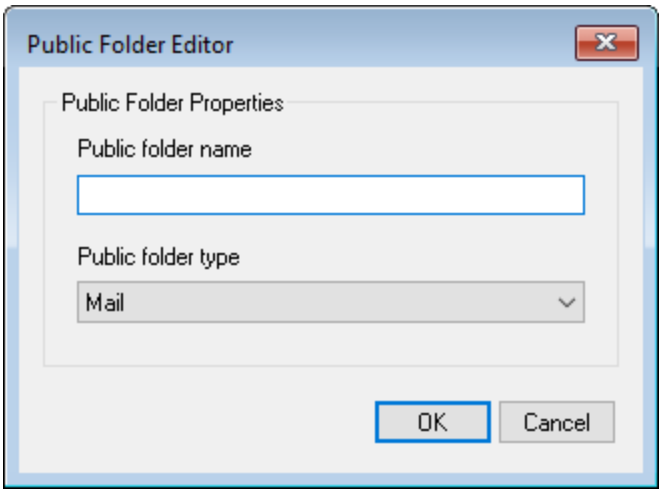


Use this screen to manager your public folders. To reach the Public Folder Manager, click "Setup » Public Folder Manager...".

Public Folder Management

New folder
To create a new public folder, select the folder in the list that you wish to be its parent folder, and click *New folder*. Enter a name for your folder, choose the folder type, and click *OK*.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Delete folder
To remove a public folder from the list, select the desired folder and then click the *Delete folder* button.

Rename folder
To rename a public folder, select a folder and click *Rename folder*. Type a new name and click *Ok*.

Enable public folders
Click this check box if you wish to allow users to gain access to public folders. The users that can access them and the level of access granted is controlled by selecting a folder and clicking the *Edit ACLs* button.

Name and Type

Folder name
This box displays the name of the folder you have selected in the list. The remaining options on this screen apply to the selected folder.

Folder type
Use the drop-down list to designate the type of folder: Mail, Contacts, Calendar, etc.

Edit ACLs
Choose a folder and then click this button to open the Access Control List 302 dialog for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

Settings

Submission address
Enter a local email address or choose a specific MDaemon account to associate with the shared folder, so that messages destined for that *Submission Address* will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Maintain separate message status flags
Click this check box if you want the folder's message flags (read, unread, replied to, forwarded, and so on) to be set on a per-user basis instead of globally. Each user will see the status of the messages in the shared folder displayed according to his or her personal interaction with them. A user who hasn't read a message will see it flagged as 'unread' while a user who has read it will see the status as 'read'. If this option is disabled then all users will see the same status. So, once any user has read a message then all users will see it marked as 'read'.

Assign a unique ticketing (or tracking) number to messages
Use this option if you wish to configure the public folder as a message ticketing public folder. MDaemon will add the *Folder name* and a unique identifier to the subject of messages sent to the public folder's *Submission address*. Any outbound messages having this specially formatted subject will have the From address changed to the submission address of the public folder and a copy of the outbound message will be placed into a child public folder named "Replied To". In addition, any inbound messages with this specially formatted subject will be automatically redirected to the public folder, regardless of the address the message was sent to.

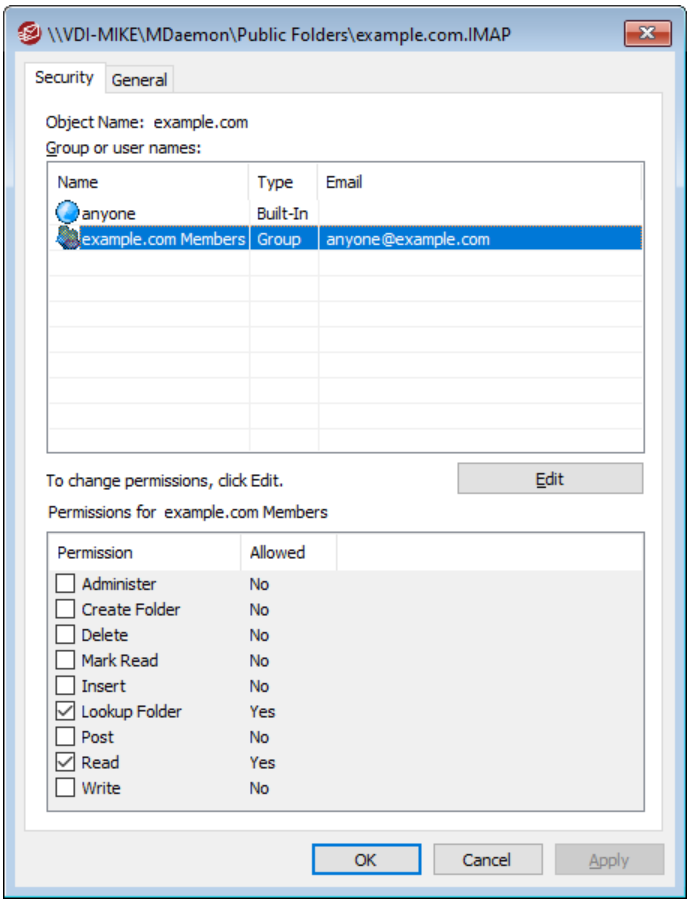
See:

Access Control List 302
Public Folders Overview 110
Public & Shared Folders 113
Account Editor » Shared Folders 726
Mailing List » Public Folders 289

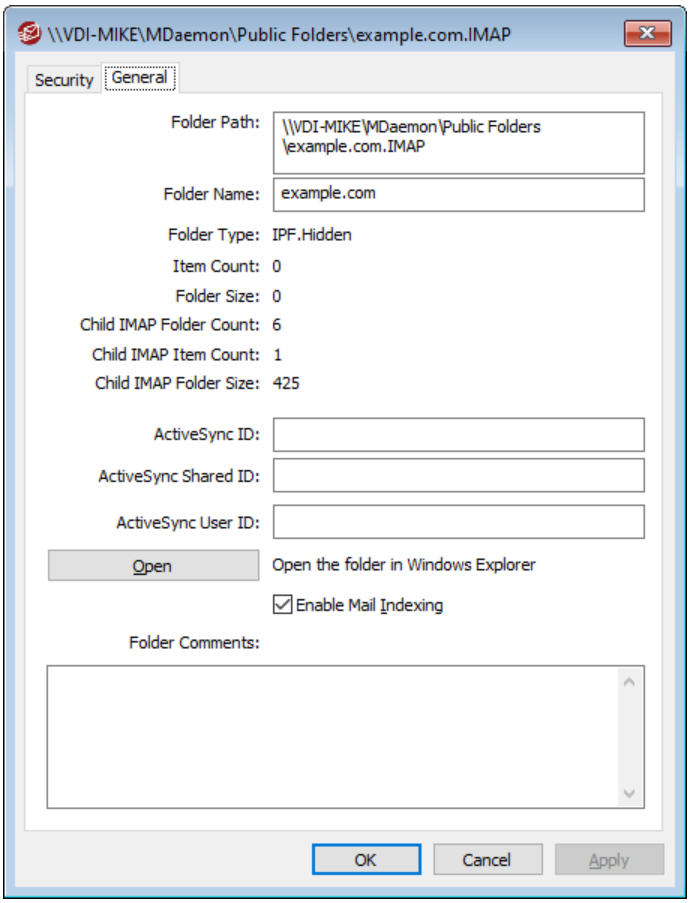
3.5.1 Access Control List

The Access Control List (ACL) is used for setting user or group access permissions for your public and shared folders 110. It is accessed from the *Edit ACLs* button on the Public Folder Manager 300 or the *Edit access control list* button on Account Editor's Shared Folders 726 screen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Security

This tab displays the list of groups or users associated with the folder and the specific access permissions granted to each. Select a group or user in the list to display its permissions[305] for review in the Permissions window below. To edit the permissions, click **Edit**[304].

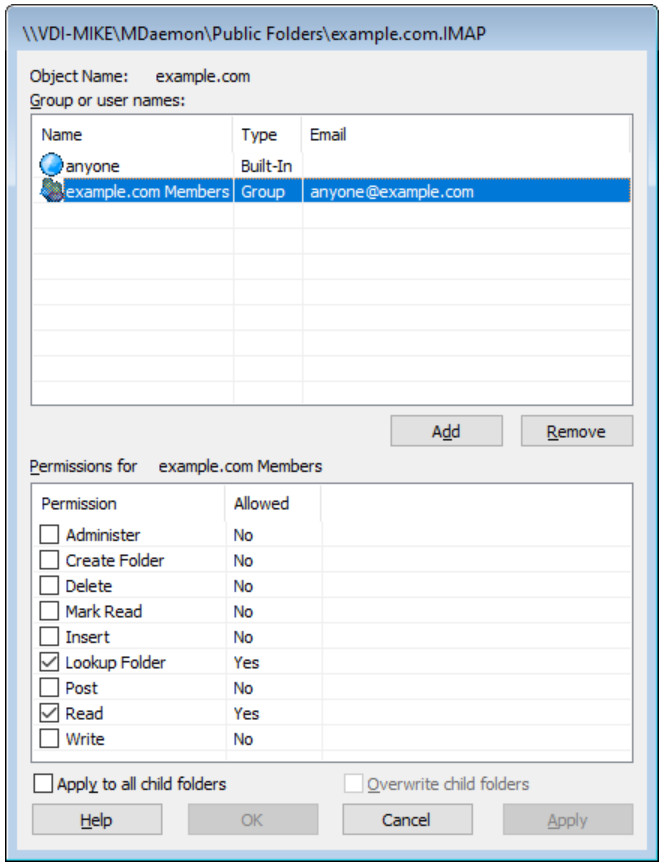
General

This tab displays the folder's properties, such as its path, name, type, size, and so on.

ACL Editor

Click **Edit** on the ACL's Security tab to open the ACL Editor for modifying access permissions.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Object Name
This is the name of the object or folder to which the ACL permissions will apply.

Group or user names
These are the groups or users to which some level of access permissions may have been granted. Select a group or user to display its permissions in the *Permissions for <group or user>* window below. Check the box next to any access permission that you wish to grant to the group or user.

Add
To grant access permissions to a group or user not listed above, click **Add** 306.

Remove
To remove a group or user, select its entry in the list above and click **Remove**.

Permissions for <group or user>
Check the box next to any access permission that you wish to grant to the group or user selected above.

You can grant the following access control permissions:

Administer – user can administer the ACL for this folder.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Create – user can create sub-folders within this folder.

Delete – user can delete items from this folder.

Mark Read – user can change the read/unread status of messages in this folder.

Insert – user can append and copy items into this folder.

Lookup Folder – user can see this folder in his personal list of IMAP folders.

Post – user can send mail directly to this folder (if folder allows).

Read – user can open this folder and view its contents.

Write – user can change flags on messages in this folder.

Apply to all child folders
Check this box if you wish to apply this folder's access control permissions to any sub-folders it currently contains. This will add the folder's user and group permissions to the child folders, replacing them when there are any conflicts. It will not, however, delete any other user or group permissions that currently have access to those folders.

Example,

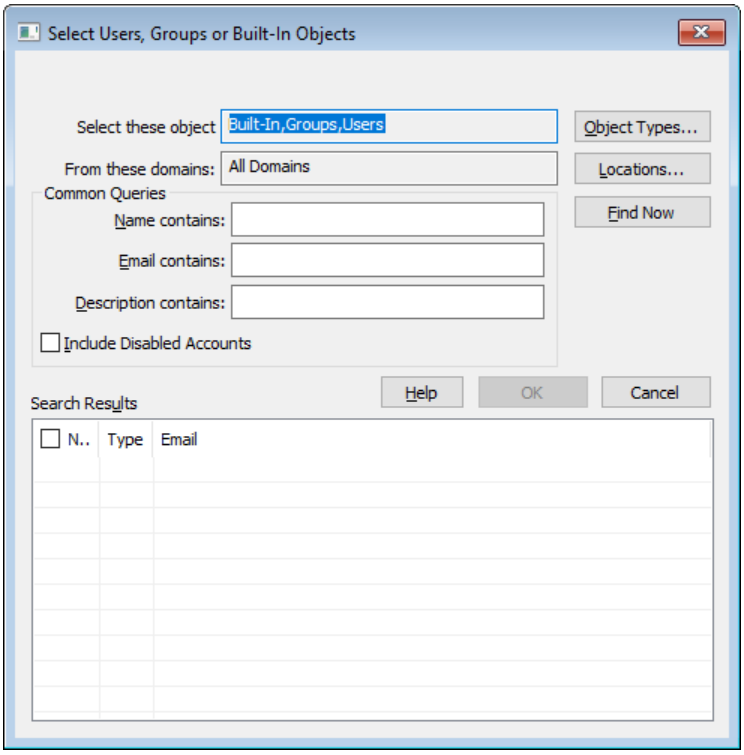
The parent folder grants certain permissions to `User_A` and `User_B`. The child folder grants permissions to `User_B` and `User_C`. This option will add `User_A` permissions to the child folder, replace the child folder's `User_B` permissions with those from the parent folder, and do nothing to the `User_C` permissions. Therefore the child folder will then have `User_A`, `User_B`, and `User_C` permissions.

Overwrite child folders
Check this box if you wish to replace all child folder access permissions with the parent folder's current permissions. The child folder permissions will then be identical to the parent folder.

Adding a Group or User

Click **Add** on the ACL Editor if you wish to add another group or user to the Access Control List. This opens the Add Group or User screen that you can use to search for them and then add them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Select these object types
Click **Object Types...** to select the object types that you wish to search for the groups or users you wish to add. You can select: Built-In, Groups, and Users.

From these locations
Click **Locations...** to select the domains that you wish to search. You can select all of your MDaemon domains or specific domains.

Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description 697. Leave these fields blank if you want the search results to contain every group and user that matches the Object Types and Locations specified above.

Include Disabled Accounts
Check this box if you wish to include disabled accounts 697 in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired groups or users in the Search Results and click **OK** to add them to the ACL.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting folder access rights to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at: http://www.rfc-editor.org/rfc/rfc2086.txt.

See:

Public Folder Manager 300
Public Folders Overview 110
Public & Shared Folders 113
Account Editor » Shared Folders 726
Mailing List » Public Folders 289

3.6 Web & IM Services

3.6.1 Webmail

3.6.1.1 Overview

MDaemon Webmail is a web-based email solution included in MDaemon and designed to offer users email client functionality using their favorite web browser. Webmail can easily hold its own against traditional mail clients while providing the added bonus of its ability to enable users to access their email from anywhere at anytime as long as they have an Internet or network connection. Further, because all of their email folders, contacts, calendars, and so on reside on the server instead of on their local computer, they can have access to everything as if they were at their desk.

MDaemon Webmail provides many benefits to email administrators. Since Webmail isn't workstation dependent you can configure everything from the server, unlike many client applications. This saves you from having to configure and maintain each individual email client. You can also customize the graphical images and HTML pages used in Webmail to suit your corporate needs, or the needs of your customer. Further, you can give your users the ability to maintain their own account settings thus saving you time — you can give as much or as little control to your users as you want.

Finally, in addition to the convenience of having a web-based client, there are many additional features that will benefit your users, such as: extensive email functionality, client-side interface available in almost 30 languages, personal and global address books, manageable mail folders and filters, send/receive file attachments, multiple visual "themes" for the interface, themes for mobile devices, calendar features, groupware features, an integrated instant messenger that can be downloaded to your desktop, and much more.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Calendar & Scheduling System

MDaemon is equipped with a complete collaboration system. From within Webmail you can easily create appointments, schedule meetings, and work with address books. Recurring appointments are fully supported, and appointments have many fields available to describe them. Further, contacts, calendars, and task data are stored as IMAP folders within each user's root mail directory. Through Webmail, your users can access these personal folders and control which other users have access to them. All Webmail themes have templates that present contact, calendar, notes, and task folders in a logical and attractive way.

Because the Calendar system is integrated with MDaemon, there is the added benefit of email notifications of appointments, whether scheduled by you or a third-party. Whenever someone other than yourself schedules an appointment for you, you will receive an email message summarizing the appointment. Each designated appointment attendee will receive an email message detailing the appointment's date, time, location, subject, and list of attendees. Further, any attendees who have calendar entries that conflict with the appointment's time slot will receive a message notifying them of the appointment and its conflict with their schedule. The person who scheduled the meeting will receive a summary message listing all of the meeting's details and invited attendees who did or did not have scheduling conflicts.

The Calendar System is also equipped with support for Internet Calendar (iCal) used by Microsoft Outlook and other iCalendar compliant email programs. The Calendar System can detect and process iCalendar information sent to your users and update their calendars accordingly. When a user opens an iCalendar attachment from within Webmail the information contained in the attachment will be reflected in the user's Webmail calendar. Also, when users create new meetings or appointments they can list one or more email addresses to which they wish an iCalendar email to be sent. This feature can be set by individual users in their Webmail options.

MDaemon Instant Messenger

MDaemon Instant Messenger (MDIM) is MDaemon's secure instant messaging client and tray applet that provides quick access to Webmail's email features. MDIM can be downloaded by each Webmail user and then installed on the individual's local computer. It is pre-configured for the specific user when downloaded, thus limiting the need to configure it manually.

MDIM runs in the background and checks your account for new mail by querying the Webmail server directly. This eliminates the need to open a browser or keep one open to check your email — MDIM checks for new mail and notifies you with a sound or visual alert when new mail arrives. MDIM also displays a list of your mail folders and the number and type of messages that each one contains (new, unread, and read). Furthermore, it can be used to launch your browser and move it immediately to a specific mail folder.

MDIM is also equipped with a complete instant messaging client. You can view your list of MDIM contacts and each one's online status (online, away, offline), start a conversation with any one or group of them, set your own online status, and view past conversations in a history folder.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

For specific instructions on how to use MDaemon Instant Messenger, see its online help system.

MDaemon Instant Messenger's Instant Messaging System

MDIM is equipped with an instant messaging (IM) client that utilizes MDaemon's XMPP 365 server. Using this feature you can add other users who share your domain (and optionally other domains hosted on your MDaemon server) to your MDIM contacts list and then communicate with them instantly. You can set your online status, view the status of your contacts, use emoticons, set text color, send files, set notification sounds and control other preferences. You can also start a group conversation involving several contacts at once. The IM features are available via the tray icon's shortcut menu, and from the MDIM window.

MDaemon Instant Messenger's IM system is also scriptable, which allows custom programs to interface with it. By creating semaphore (SEM) files in the \MDaemon\WorldClient\ folder, an external application can send instant messages to your MDIM users. The following is the format of the SEM file:

`To: user1@example.com`	Email address of MDIM user.
`From: user2@example.com`	Email address of instant message's sender.
`<blank line>`	
`Text of instant message.`	This is the text sent as an instant message.

The SEM file name must start with the characters "IM-" and be followed by a unique numerical value. For example, "IM-0001.SEM". Applications should also create a corresponding file called "IM-0001.LCK" to lock the SEM file. Once the SEM file is completed remove the LCK file and the SEM file will be processed. MDaemon uses this scripting method to send Instant Message reminders to you about upcoming appointments and meetings.

The Content Filter system is equipped with an Action that uses this scripting method to send instant messages. Further, rules utilizing this action can use the Content Filter macros in the IM. For example, you could create a rule to send an instant message rule containing lines like this:

```
You have received an email from $SENDER$.
Subject: $SUBJECT$
```

This rule would be an effective way to send new mail alerts through MDIM.

Because some administrators have reservations about using an Instant Messaging system in their company due to the inherent lack of centralized accountability and the inability to monitor IM traffic that is in traditional and well known IM clients, we have designed MDIM's instant messaging system to minimize those deficiencies. First of all, our system is not peer-to-peer — individual MDIM clients do not connect directly to each other for instant messaging. Further, because every instant message passes through the server, each message is logged in a central location accessible to the MDaemon administrator. Thus a record of all conversations can be maintained for the security of both your company and your employees or users. IM activity is logged in a file called XMPPServer-<date>.log located in the MDaemon\LOGS\ directory.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Instant Messaging is provided on a per-domain basis. The global control for activating instant messaging is located on the MDIM screen[320] of the Webmail dialog (Setup » Web & IM Services » Webmail » MDIM). There is a similar screen on the Domain Manager[183] for enabling or disabling it for specific domains.

MDaemon Instant Messenger Skins

MDIM's interface is compatible with *msstyles* skins, which are readily available on the internet. Several styles are included, but to install a new style, download the `*.msstyles` file and place it under MDIM's `\Styles\` folder in a subfolder with the same name as the file. For example, if the file was called `Red.msstyles` then the path for the file would be: "`\.\Styles\Red\Red.msstyles`"

Dropbox Integration

A new screen has been added to Ctrl+W|Webmail|Dropbox. Here you will find controls where you can enter your Dropbox "app key", "app secret", and privacy policy text. All are needed in order to enable the integrated service and they are all obtained when you register your MDaemon Webmail as a Dropbox "app" by visiting the Dropbox website. We cannot do this for you but it only needs doing once. Please see Knowledge Base article 1166 for complete instructions on how to register your Webmail as an app with Dropbox.

Once the "app key" and "app secret" are configured Webmail will be able to connect their accounts to a Dropbox account. The first time a user logs into the WorldClient theme or LookOut theme, the user will be presented with a dropdown at the top of the page. The user has three options, view the dropdown on next login, never show it again, or go to the new Options | Cloud Apps view. On the Options | Cloud Apps view, the user can click the Setup Dropbox button. Doing so will open an OAuth 2.0 popup. The popup details what the user is connecting to, and what authorizations Webmail is requesting. There is also a link to the privacy policy, and "Connect to Dropbox" button. Once the user clicks the "Connect to Dropbox" button, the page will navigate to Dropbox. If the user is not logged into Dropbox, Dropbox will present a site for them to either login or create an account. Once this step is completed, the user will be presented with another Dropbox page that asks if the user would like to allow Webmail to have full access to his/her account. Clicking "Allow", will take the user back to Webmail and tell the user whether or not the authorization was a success. This authorization is good for one week after which time the same screen is presented again and another access token is obtained and used for a subsequent week. Once authorization is completed, the user will be presented with a Dropbox icon next to each message attachment. Clicking the icon will result in the attachment being saved to the user's Dropbox account under the /WorldClient_Attachments folder.

In the Compose view for WorldClient and LookOut themes, users will be able to choose files from their Dropbox accounts by clicking the Dropbox icon in the HTML editor's toolbar (top left). This feature does not require the users to setup access to their accounts via the Options | Cloud Apps view and OAuth 2.0. It only requires the "app key" and "app secret".

Dropbox support is disabled by default, but can be enabled on the Dropbox[325] screen in MDaemon. If you wish to enable or disable Dropbox on a per user basis, you can do so by adding "DropboxAccessEnabled=Yes" to the User.ini.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Using Webmail

Starting Webmail

There are three ways to start/stop the Webmail server:

1. In the Stats pane on the left-hand side of the MDaemon GUI, right-click on the Webmail entry and choose the *Toggle Active/Inactive* selection on the shortcut menu.
2. Click "File » Enable Webmail" server on the main interface.
3. Click "Setup » Web & IM Services" on the main interface, and then click *Webmail runs using built-in web server* on the Web Server screen.

Logging in to Webmail

1. Point your web-browser to `http://example.com:WebmailPortNumber`. This port is designated on the Web Server 313 screen of the Webmail section. If you configure Webmail to listen to the default web port (port 80) then you do not need to denote the port number in the login URL (e.g. `www.example.com` instead of `www.example.com:3000`).
2. Type your MDaemon account's user name and password.
3. Click Sign-in.

Changing Webmail's Port Setting

1. Click "Setup » Web & IM Services" on the menu bar.
2. Type the desired port number in the control labeled *Run Webmail Server using this TCP Port.*
3. Click OK.

Client-side Help

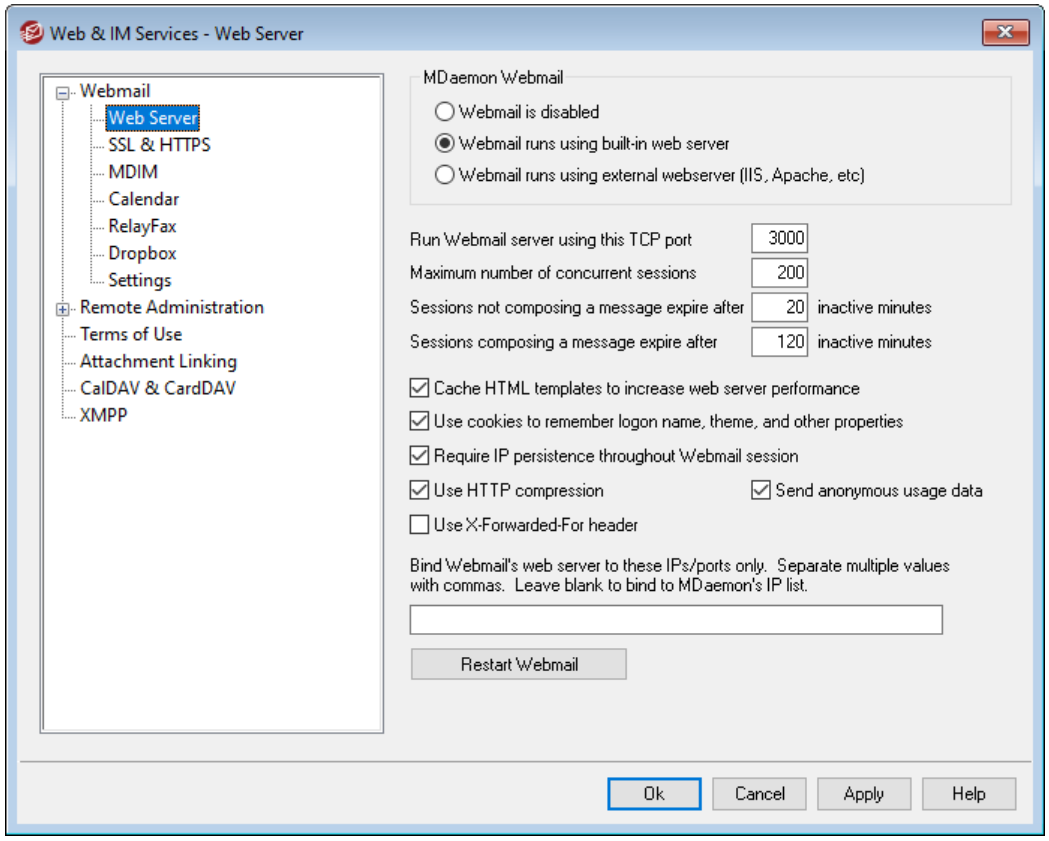
Webmail is equipped with extensive client-side help for your users. See the online help system within Webmail for information on the client features and functions.

For more Address Book options, see:

Webmail » MDIM 320
LDAP 815

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.1.2 Web Server



This screen contains various global, server level settings that govern Webmail's configuration and behavior regardless of the users or domains to which they belong.

MDaemon Webmail

Webmail is disabled
Choose this option to disable Webmail. You can also toggle Webmail active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Webmail must be active when using the Attachment Linking 357 feature.

Webmail runs using built-in web server
Choose this option to run Webmail using MDaemon's built-in web server. You can also toggle Webmail active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Webmail runs using external web server (IIS, Apache, etc)
Choose this option when you wish to run Webmail under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see the MDaemon Technologies knowledge base article: How to setup Webmail, ActiveSync, CalDav, CardDav, and AutoDiscover services in IIS

Run Webmail server using this TCP port
This is the port on which Webmail will listen for connections from your users' web browsers.

Maximum number of concurrent sessions
This is the maximum number of sessions that may be connected to Webmail at the same time.

Sessions not composing a message expire after xx inactive minutes
When a user is logged in to Webmail but is not composing a message, this is the amount of time that their session will remain inactive before Webmail will close it.

Sessions composing a message expire after xx inactive minutes
This timer governs how long a user's session will be kept open while they are composing a message and the session remains inactive. It is a good idea to set this timer higher than the *Sessions not composing a message...* timer, since inactivity time is typically greater while a user is composing a message. This is because composing a message requires no communication with the server until the message is sent.

Cache HTML templates to increase web server performance
Click this box to cause Webmail to cache templates in memory rather than read them each time they need to be accessed. This can dramatically increase server performance but Webmail will have to be restarted if you ever make a change to one of the template files.

Use cookies to remember logon name, theme, and other properties
Click this option if you want Webmail to store each user's logon name, theme, and certain other properties in a cookie on his or her local computer. Using this feature gives your users a more "customized" login experience but requires that they have support for cookies enabled in their browsers.

Require IP persistence throughout Webmail session
As an added security measure you can click this checkbox to cause Webmail to restrict each user session to the IP address from which the user connected when the session began. Thus, no one can "steal" the user's session since IP persistence is required. This configuration is more secure but could cause problems for users who may be using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

Use X-Forwarded-For header
Click this checkbox to enable the use of the `X-Forwarded-For` header, which is sometimes added by proxy servers. This option is disabled by default. Enable it only if your proxy server inserts this header.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use HTTP Compression
Click this check box if you want to use HTTP compression in your Webmail sessions.

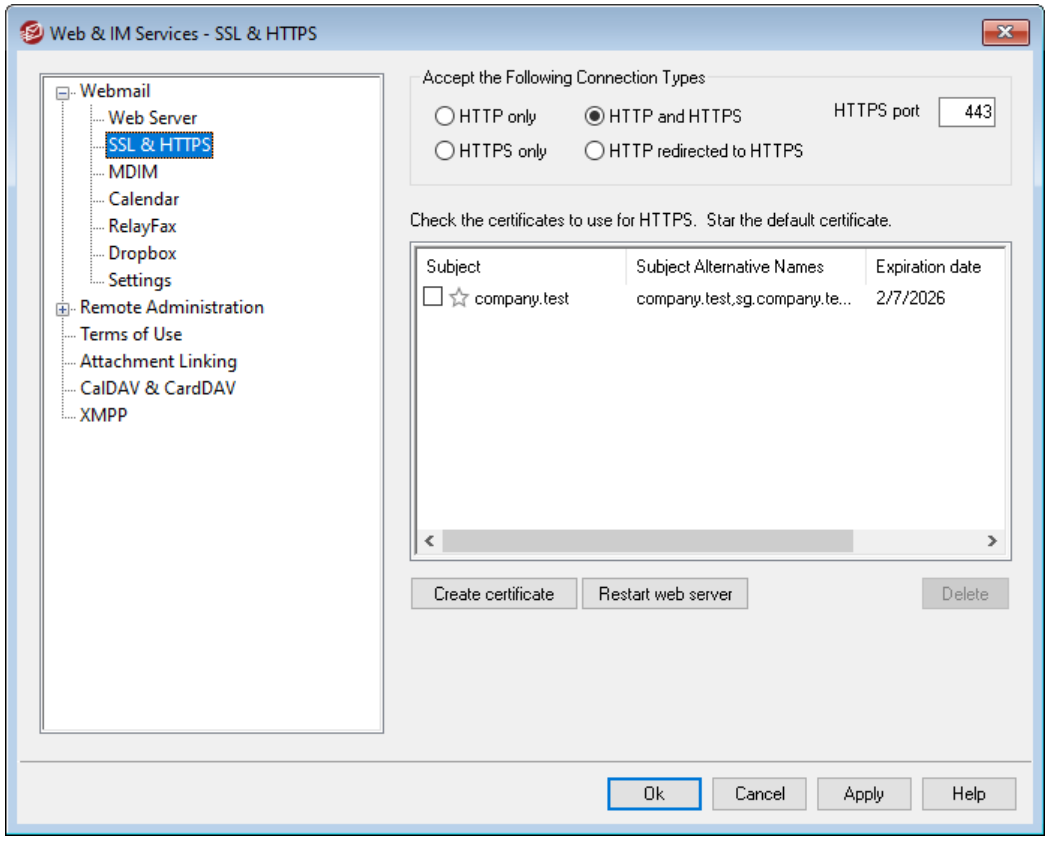
Send anonymous usage data
By default Webmail sends anonymous, benign usage data such as: the OS used, browser version used, language, and the like. This data is used by MDaemon Technologies to help us improve Webmail. Disable this option if you do not wish to send anonymous usage data.

Bind Webmail's web server to these IPs/ports only
If you wish to restrict the Webmail server to only certain IP addresses or ports then specify those IPs and ports here separated by commas. Use the format: "`IP_address:Port`" to designate a port (for example, `192.0.2.0:80`). If you do not include a port, then the default TCP port specified above and the default HTTPS port specified on the SSL & HTTPS 316 screen will be used. Use "`*`" if you want Webmail to listen on all ports. For example, "`*,*:80`" would cause Webmail to listen on all IP addresses, on the default ports specified (3000 and 443), and it would also listen on all IP addresses on port 80. If you leave this field blank then Webmail will monitor all IP addresses designated for your Domains 174.

Restart Webmail (required when port or IIS value changes)
Click this button if you wish to restart the Webmail server. Note: when changing Webmail's port setting you must restart Webmail in order for the new setting to be recognized.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.1.3 SSL & HTTPS



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Webmail to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Webmail". For your convenience, however, these options are also mirrored under "Security » Security Manager » SSL & TLS » Webmail".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 561

This screen only applies to Webmail when using MDaemon's built-in web server. If you configure Webmail to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Accept the Following Connection Types

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Webmail. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Webmail, but do not wish to force your Webmail users to use HTTPS. Webmail will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Webmail TCP port designated on the Web Server 313 screen of Webmail.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Webmail. Webmail will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Webmail will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in Webmail's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the Webmail port that is designated on the Web Server 313 screen of Webmail. If you are still allowing HTTP connections to Webmail then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Check the box next to any certificates you wish to be active. Click the star next to the one that you wish to set as the default certificate. MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used. Double-click a certificate to open it in Windows' Certificate dialog for review (only available in the application interface, not in the browser-based remote administration).

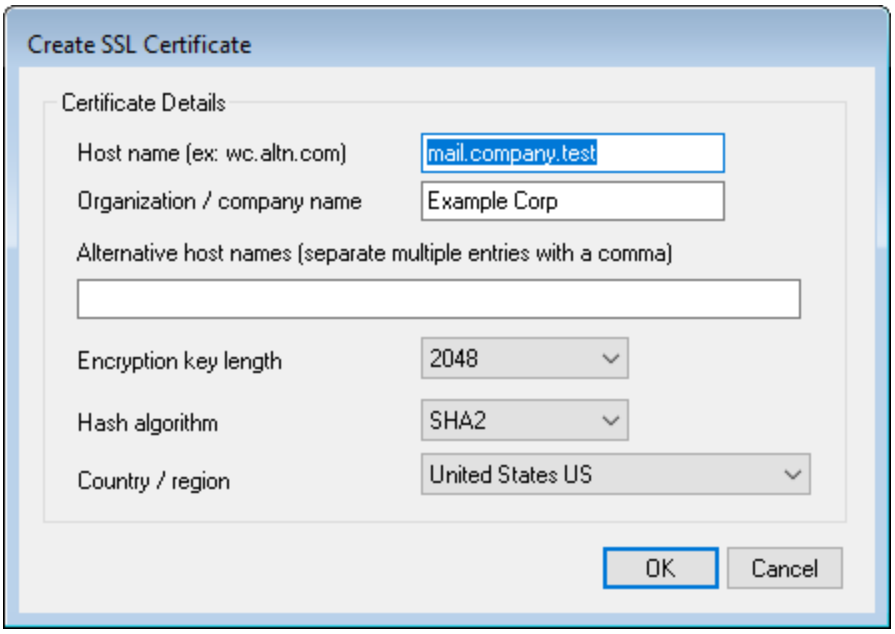
Delete
Select a certificate in the list and then click this button to delete it. A confirmation

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Certificate Details

Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field. If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

Using Let's Encrypt to Manage Your Certificate

Let's Encrypt is a Certificate Authority (CA) that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

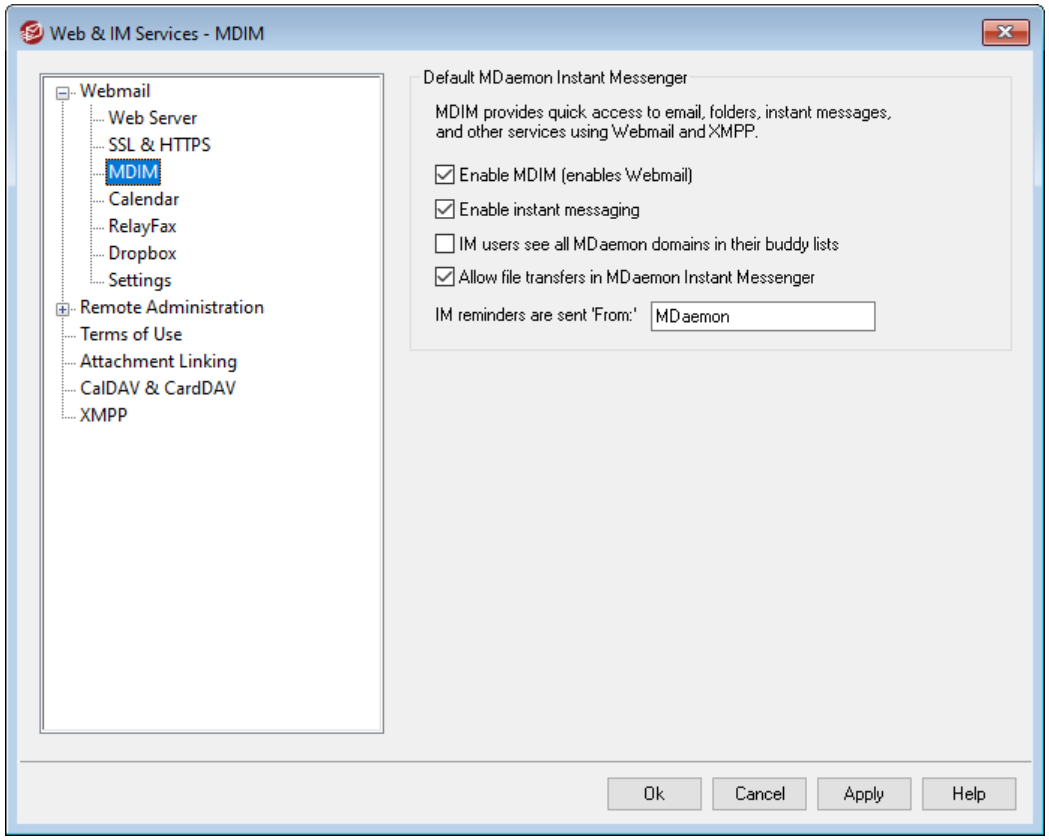
To support using Let's Encrypt's automated process to manage a certificate, the Let's Encrypt 580 screen is provided to help you easily configure and run the PowerShell script included in the "`MDaemon\LetsEncrypt`" folder. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*. See the Let's Encrypt 580 topic for more information.

See:

SSL & Certificates 561
Creating and Using SSL Certificates 896

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.1.4 MDIM



This screen controls the default MDaemon Instant Messenger (MDIM) 309 settings for new domains. Settings for specific domains can be modified via the Domain Manager's MDIM screen 183. MDaemon Instant Messenger services can be enabled or disabled for specific accounts or groups via the Web Services 703 and Group Properties 766 screens respectively.

Default MDaemon Instant Messenger

Enable MDIM (enables Webmail)
Enable this option if you wish to make MDaemon Instant Messenger available for download from within Webmail by default. Users can download it from the *Options » MDaemon Instant Messenger* page. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier. This option also makes it possible for MDIM to use the My Mail Folders features, allowing users to check for new email and open Webmail directly from the MDIM shortcut menu. MDIM is enabled by default.

Enable instant messaging
By default, accounts can use MDIM and third-party XMPP 365 clients to instant message other members of their domain. Clear this checkbox if you do not wish to allow instant messaging by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

IM users see all MDaemon domains in their buddy lists
Click this option if you want your users by default to be able to add contacts to their buddy list from all of your MDaemon domains. When this option is disabled, contacts must be on the same domain. For example, if your MDaemon is hosting mail for example.com and example.org, activating this option allows users to add instant messaging contacts from both domains. Disabling it means that example.com users can only add other example.com users, and example.org can only add example.org. This option is disabled by default. There is an equivalent option on the Domain Manager 183 for enabling or disabling this feature for specific domains.

Allow file transfers in MDaemon Instant Messenger
By default, MDIM users can transfer files to their MDIM contacts. Clear this checkbox if you do not wish to allow MDIM to be used to transfer files.

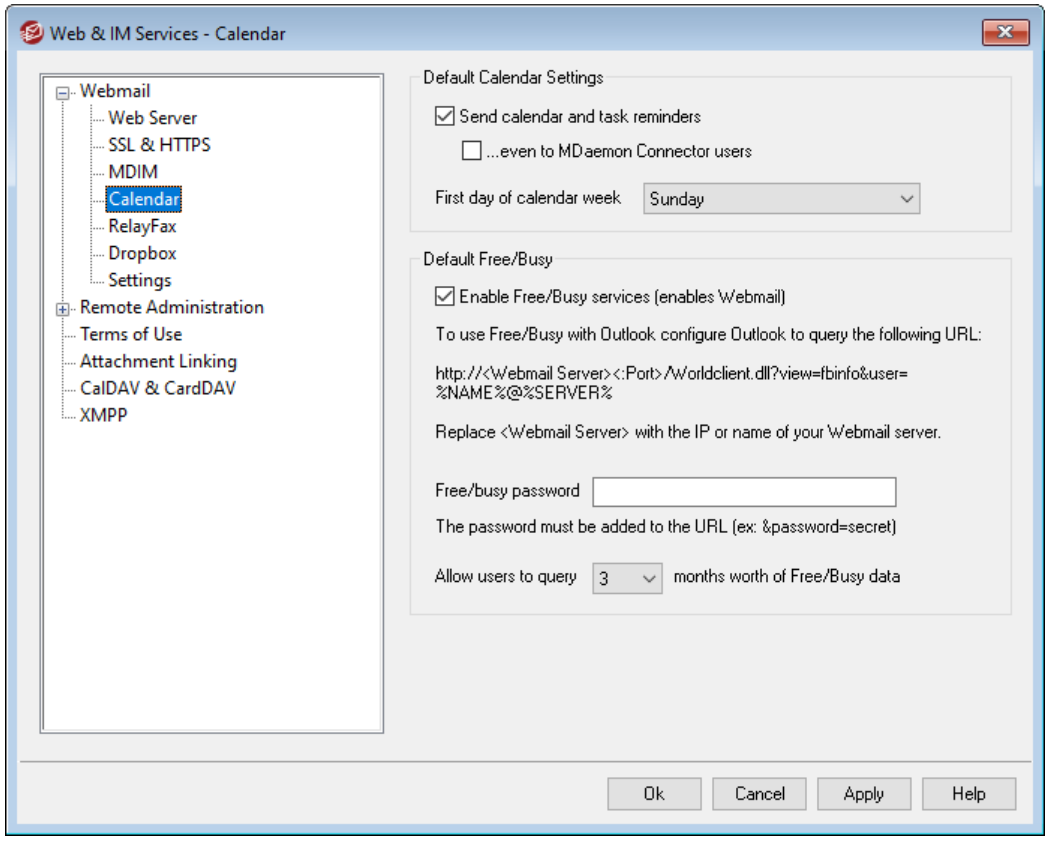
IM reminders are sent 'From:'
When an appointment is scheduled on a user's Webmail calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message to the user. Use this text box to specify the name that you wish the message to appear to be '`From:`'. This is the default setting for new domains. You can change it for specific domains via the Domain Manager's MDaemon Instant Messenger 183 screen.

See:

Domain Manager » MDaemon Instant Messenger 183
Account Editor » Web Services 703
Group Properties 766

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.1.5 Calendar



This screen controls the default settings for MDaemon's Calendar features. Settings for specific domains can be controlled via the Domain Manager's Calendar[185] screen.

Default Calendar Settings

Send calendar and task reminders
Click this checkbox if you wish to allow Webmail's calendar and task reminders to be sent to your users via email and MDaemon Instant Messenger.

...even to MDaemon Connector users
If you have enabled the "*Send calendar and task reminders*" option above, click this option if you also wish to enable reminders for MDaemon Connector[379] users.

First day of week
Choose a day from the drop-down list. The selected day will appear in the calendars as the first day of the week.

Default Free/Busy

MDaemon includes a Free/Busy server, which makes it possible for a meeting planner to view the availability of potential meeting attendees. To access this feature, click Scheduling within Webmail when creating a new appointment. This opens a Scheduling window containing the list of attendees and a color-coded calendar grid

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

with a row for each one. Each attendee's row is color-coded to indicate the times at which he or she might be available for a meeting. There are colors for Busy, Tentative, Out of Office, and No information. There is also an Auto-Pick Next button that makes it possible for you to query the server for the next time slot at which all attendees may be available. When you have finished creating the appointment it will send an invitation to all of the attendees, who can then accept or decline.

Webmail's Free/Busy server is also compatible with Microsoft Outlook. To use it, configure Outlook to query the URL listed below for Free/Busy data. In Outlook 2002, for example, the Free/Busy options are located under "Tools » Options » Calendar Options... » Free/Busy Options..."

Free/Busy server URL for Outlook:

```
http://<Webmail><:Port>/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Replace "<Webmail>" with the IP address or domain name of your Webmail server, and "<:Port>" with the port number (if you aren't using the default web port). For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

For more on how to use Webmail's Free/Busy features to schedule your appointments, see the online Help system within Webmail.

Enable Free/Busy services
Click this option if you wish to provide access to the Free/Busy server features to users.

Free/Busy password
If you wish to require a password when users attempt to access the Free/Busy server features via Outlook, include the password here. This password must be appended to the URL listed above (in the form: "&password=FBServerPass") when the users configure their Free/Busy settings within Outlook. For example:

```
http://example.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%&password=MyFBServerPassword
```

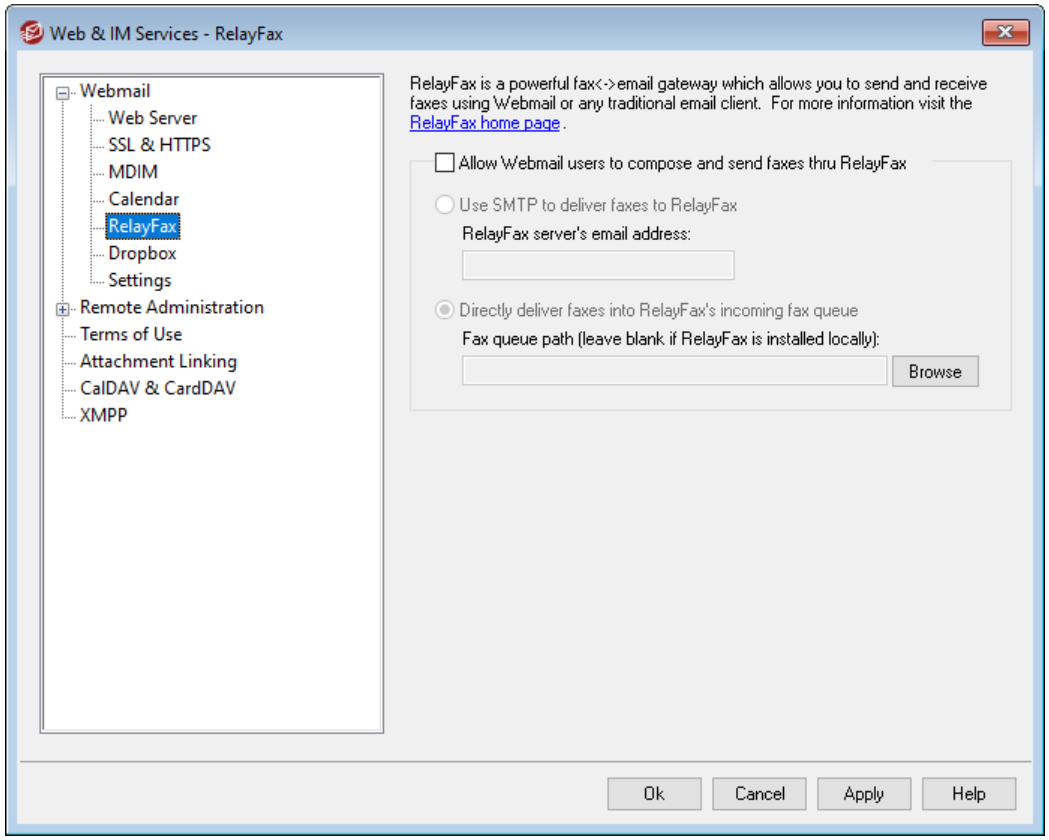
Allow users to query X months worth of Free/Busy data
Use this option to designate how many months worth of Free/Busy data your users may query.

See:

Domain Manager » Calendar 185

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.1.6 RelayFax



MDaemon Technologies' RelayFax Server is an email to fax and fax to email gateway that can be seamlessly integrated with Webmail in order to provide its services to your users. When this functionality is enabled, Webmail users will be given access to various features that will enable them to compose and send faxes via the Webmail client pages. For more information, visit the RelayFax section of www.mdaemon.com.

RelayFax Integration Options

Allow Webmail users to compose and send faxes thru RelayFax
Click this option to integrate RelayFax with Webmail. When active it will cause a "Compose Fax" control and other fax related features to appear on the Webmail pages.

Use SMTP to deliver faxes to RelayFax
RelayFax monitors a specific mailbox for incoming messages that are to be faxed. Click this option and MDaemon will use the normal SMTP email delivery process to send these messages to that mailbox's address. This option is useful when RelayFax is monitoring a mailbox located somewhere other than your local network. If RelayFax resides on your network you may choose to have MDaemon deliver the messages directly to RelayFax's message queue and thus bypass the SMTP delivery process altogether. For more information on this method, see *Directly deliver faxes into RelayFax's incoming fax queue* below.

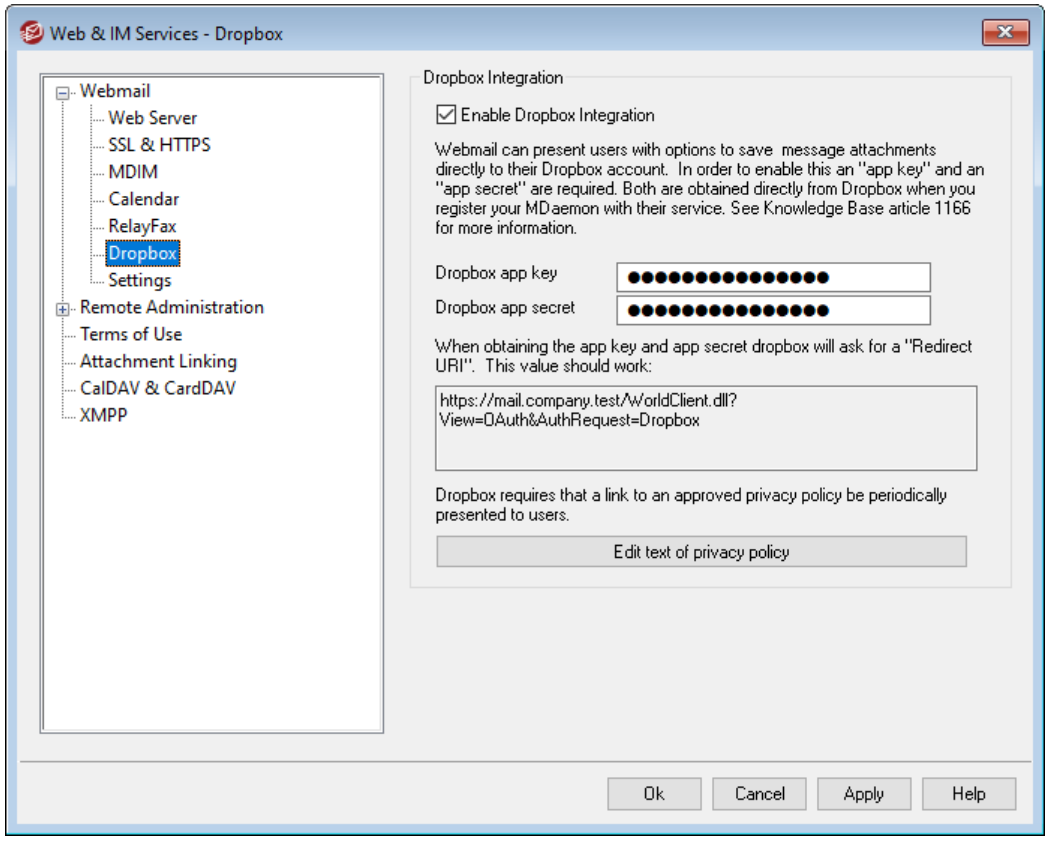
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

RelayFax server's email address
Specify the email address to which you want messages intended for faxing to be delivered. This value must match the address that you have configured RelayFax to monitor for these messages.

Directly deliver faxes into RelayFax's incoming fax queue
If RelayFax resides on your LAN you may choose this method rather than SMTP for distributing messages for faxing. When MDaemon receives a message intended for RelayFax it will be placed directly into RelayFax's incoming queue rather than delivered using SMTP.

Fax queue path
If RelayFax resides on the same machine on which MDaemon is running, you may leave this file path blank. Otherwise, you must specify the network path to RelayFax's \app\ folder.

3.6.1.7 Dropbox



Webmail is equipped with direct support for Dropbox, which allows your users to save file attachments to their Dropbox accounts, and to insert direct links to Dropbox files in outgoing messages. To provide this feature to your Webmail users, you must set up your Webmail as a Dropbox app on the Dropbox Platform. This is a simple process, requiring you only to sign in to a Dropbox account, create a unique name for an app

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

with Full Dropbox access, specify the Redirect URI to Webmail, and change one default setting. Then, you will copy and paste the Dropbox App Key and App Secret from there to the options on this screen in MDaemon. After that your users will be able to link their Dropbox accounts to Webmail when they next sign in to Webmail. For step-by-step instructions on how to create your Dropbox app and link it to Webmail, see: Creating and Linking Your Dropbox App 327 below.

When you create your Dropbox app it will initially have "Development" status. This allows up to 500 of your Webmail users to link their Dropbox accounts to the app. According to Dropbox, however, "once your app links 50 Dropbox users, you will have two weeks to apply for and receive Production status approval before your app's ability to link additional Dropbox users will be frozen, regardless of how many users between 0 and 500 your app has linked." This means that until you receive production approval, Dropbox integration will continue to work but no additional users will be able to link their accounts. Obtaining production approval is a straightforward process to ensure that your app complies with Dropbox's guidelines and terms of service. For more information, see the Production Approval section of the Dropbox Platform developer guide.

Once your Webmail app is created and configured properly, each Webmail user will be given the option to connect their account to their Dropbox account when they sign in to Webmail. The user is required to log in to Dropbox and grant permission for the app to access the Dropbox account. Then the user will be redirected back to Webmail using a URI that was passed to Dropbox during the authentication process. For security that URI must match one of the Redirect URIs (see below) you specified on your app's info page at Dropbox.com. Finally, Webmail and Dropbox will exchange an access code and access token, which will allow Webmail to connect to the user's Dropbox account so that the user can save attachments there. The exchanged access token expires every seven days, meaning that periodically the user must reauthorize the account to use Dropbox. Users can also manually disconnect their account from Dropbox, or reauthorize it when necessary, from the Cloud Apps options screen within Webmail.

Dropbox Integration

Enable Dropbox Integration

Once you have created your Dropbox app and linked it to Webmail, click this checkbox to allow your Webmail users to link to their Dropbox accounts. If you wish to enable or disable Dropbox on a per user basis, you can do so by adding "`DropboxAccessEnabled=Yes` (or `No`)" to the `User.ini`.

Dropbox app key and app secret

The App key and App secret are located on your app's info page at Dropbox.com. Enter them here to link Webmail to your Dropbox app.

Redirect URI

You must specify a Redirect URI on your app's info page at Dropbox.com. MDaemon automatically displays a URI here that you should be able to use there. You can, however, add multiple Redirect URIs. Therefore you could add a URI for each of your domains and even one for localhost, which might be used if signing in to Webmail from the machine on which the server is running.

For example:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
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 requires your Redirect URIs to be secure, therefore HTTPS 316 must be enabled for Webmail.

Edit text of privacy policy
Click this button to edit the text file containing your Webmail App's privacy policy. Because Dropbox requires that an approved privacy policy be periodically presented to your users, a "Privacy Policy" link to the contents of this file is provided on the **Connect to Dropbox** page displayed to your users. That link opens a small window containing the text and a Download button that users can click to download the file. Use HTML code in the file if you wish to format the text or want it to contain any links.

Creating and Linking Your Dropbox App

Step-by-step instructions for creating your Dropbox app and linking it to Webmail.

1. In your browser navigate to Dropbox Platform
2. Sign in to your Dropbox account
3. Choose **Dropbox API**
4. Choose **Full Dropbox**
5. Give your app a unique name
6. Click **Create App**
7. Click **Enable additional users**, and click **Okay**
8. Change **Allow implicit grant** to **Disallow**
9. Enter one or more Redirect URIs, clicking **Add** after each one. They must be secure URLs to your Webmail (HTTPS must be enabled in Webmail).

   For example:

   https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=Dropbox

   https://localhost/WorldClient.dll?View=OAuth&AuthRequest=Dropbox
10. Leaving your browser open to your app info page, open the MDaemon GUI
11. Click **Setup**
12. Click **Web & IM Services**
13. Click **Dropbox** under **Webmail**
14. Copy/Paste the **App key** and **App secret** from your browser to the **Dropbox** screen in MDaemon.
15. Click **Apply**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

16. Click **OK**

For instructions on linking a Webmail user account to the user's Dropbox account, see the online help system within Webmail, or see Knowledge Base article 1166.

3.6.1.8 Google Drive

This page is only available in the MDaemon Remote Administration 341 (MDRA) web-interface.

Google Drive Integration

MDaemon Webmail can present users with options to save message attachments directly to their Google Drive account, and to edit and work with documents stored there. In order to enable this, an **API Key**, **Client ID**, and **Client Secret** are required. All are obtained directly from Google by creating an App using the Google API Console and registering your MDaemon with their service. An OAuth 2.0 authentication component is part of this app, which allows your Webmail users to sign-in to Webmail and then authorize access to their Google Drive account through MDaemon. Once authorized, users can view their folders and files that are in Google Drive. Further, they can upload, download, move, copy, rename, and delete files, as well as copy/move files to and from the local document folders. If the user wants to edit a document, clicking the option to view the file in Google Drive will allow the user to make edits to it in accordance with their permissions set in Google Drive. The Google Drive setup process is similar to MDaemon's Dropbox Integration 325 and MultiPOP OAuth Integration 137 features.

Enable Google Drive Integration
Click this checkbox to enable Google Drive Integration. See: **Setting up Google Drive Integration** below.

Google Drive API Key:
This is your unique API key that will be generated for you in the Google Drive API console while you are creating your app. copy and paste the key here.

Client Drive Client ID
This is the unique Client ID assigned to your Google Drive app when you create it in the Google API Console. After you create your app, copy its Client ID and paste it here.

Google Drive Client Secret
This is the unique Client Secret assigned to your Google Drive app when you create it in the Google API Console. After you create your app, copy its Client Secret and paste it here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Redirect URI
You must specify one or more Redirect URIs when creating your Google Drive app. The sample Redirect URI is built from your Default Domain's 174 SMTP host name 177, which should work for that domain's users when signing in to Webmail. You should add additional Redirect URIs to your app for any additional MDaemon domains your users go to when signing in to Webmail. For example, "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" would work for any of your users who go to `mail.example.com` when signing in to Webmail. See: **Creating and Linking Your Google Drive App** below for more information.

Edit text of privacy policy
Google Drive integration requires that you periodically present a link to your users to an approved privacy policy. Click this button to edit your privacy policy.

Creating and Linking Your Google Drive App

Step-by-step instructions for creating your Google Drive app.

Follow the steps below to create a Google application to allow users to access their Google Drive within Webmail on the **Documents** page.

1. Sign in to MDaemon Remote Administration 341 and go to the Google Drive page (located under Main » Webmail Settings), and turn on the **Enable Google Drive Integration** option.
2. In a separate browser tab, sign in to your Google Account and go to the Google API console.
3. If on the Project List, click **NEW PROJECT**, or if on the Manage Resources page, click **(+) CREATE PROJECT**.
4. Type a **Project name,** such as "Google Drive for MDaemon," then click **Edit** if you wish to edit the Project ID, or leave it set to the default value. **Note:** the Project ID cannot be changed after the project is created.
5. If you have an Organization Resource, choose it in **Location**. Otherwise, leave it set to "No organization."
6. Once loaded, click **+ ENABLE APIS AND SERVICES**.
7. In the search field, type "Google Drive", select **Google Drive API**, and click **Enable**.
8. In the left pane, under **APIs & Services**, click **Credentials**.
9. Click **+ Create Credentials** at the top of the page, and select **API Key** in the drop-down menu.
10. Copy **Your API key** (there is a Copy to Clipboard icon beside it).
11. Switch to your browser's MDaemon tab and paste it into the **Google Drive API Key** field on the Google Drive page in MDaemon (or save it somewhere else if you wish to do that later).
12. In the left pane, under **APIs & Services,** click **OAuth consent screen**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

13. Under User Type, select **External**, and click **Create**. **Note:** if you have an Organization Resource, or depending on your app's Publishing Status, choosing Internal might be a better choice. See the Publishing Status[331] note below for more information.
14. Enter the **App name** (e.g. Google Drive for Webmail), a **Support email address** for users to contact, and a **Developer email address** for Google to contact about changes to your project. That is all that's required on this page for setup, but depending on your particular organization or verification requirements, you can also enter your company logo and links to your Terms of Service[356] and Privacy Policy (see above). The **Authorized domains** fields will be filled in for you automatically when you add the *Redirect URIs* in a later step below. **Note:** This info is used for the Consent screen that will be presented to users for authorizing Webmail to access the user's Google Drive.
15. Click **Save and Continue**.
16. Click **ADD OR REMOVE SCOPES**, and copy/paste the URIs below (you can copy/paste them all at once) into the box under "Manually add scopes." Then click **ADD TO TABLE**.

```
https://www.googleapis.com/auth/userinfo.email
https://www.googleapis.com/auth/drive.file
https://www.googleapis.com/auth/documents
https://www.googleapis.com/auth/drive
https://www.googleapis.com/auth/drive.readonly
https://www.googleapis.com/auth/drive.metadata
https://www.googleapis.com/auth/drive.photos.readonly
https://www.googleapis.com/auth/drive.activity.readonly
https://www.googleapis.com/auth/spreadsheets
```

17. Click **Save and Continue**.
18. Under Test Users, click **ADD USERS**, enter each Google account whose Google Drive MDaemon will be accessing through this app, and click **ADD** (see the note below about your app's Publishing Status[331]).
19. Click **Save and Continue**.
20. On Summary, click **BACK TO DASHBOARD** at the bottom of the page.
21. Click **Credentials** in the left pane, click **(+) Create Credentials**, and select **OAuth client ID**.
22. In the "Application type" drop-down box, select **Web application**, and under "Authorized redirect URIs", click **+ ADD URIs**. Enter the Redirect URI. The Redirect URI displayed on the Google Drive page in MDaemon is an example built from your Default Domain's[174] SMTP host name[177], which should work for that domain's users when signing in to Webmail. You should add additional Redirect URIs to your app for any additional MDaemon domains your users go to when signing in to Webmail. For example, "`https://mail.example.com/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive`" would work for any of your users who go to `mail.example.com` when signing in to Webmail. If you also host a domain called, "`mail.company.test`", then you would also need to enter a Redirect URI for that domain, i.e.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

"https://mail.company.test/WorldClient.dll?View=OAuth&AuthRequest=GoogleDrive".

23. Click **CREATE**.
24. Copy the values in **Your Client ID** and **Your Client Secret** to the *Google Drive Client ID* and *Google Drive Client Secret* boxes on the Google Drive page in MDaemon. You can also enter your Google Drive API Key if you didn't do that earlier.

Publishing Status — These instructions are for creating a Google app with the Publishing Status set to "**Testing**". This requires you to add each specific Google account that will be using the app to access their Google Drive, and it is limited to 100 users. Further, in Webmail when your users are asked to authorize MDaemon to access Google, a warning message will be displayed "to confirm the user has test access to your project but should consider the risks associated with granting access to their data to an unverified app." Also, authorization expires after seven days, therefore each user would be required to reauthorize Google access every week.

If you wish to remove these requirements and limitations then you must change your status to "**In Production**", which may or may not require you change your User Type from external to internal, to go through an app verification process, or both. For more information on app verification and publishing status, see the following Google articles: Setting up your OAuth consent screen and OAuth API verification FAQs.

Authorizing Google Drive in Webmail

Once you have created your Google Drive app and configured MDaemon's Google Drive page according to the instructions above, each user who wishes to access their Google Drive in Webmail must first authorize access to do so. To do this, each user should:

1. Sign in to Webmail.
2. Click the **Options icon** in the top right corner, and click **Cloud Apps**.
3. Click **Setup Google Drive** (this will open an **OAuth 2.0** page).
4. Click **Connect to Google Drive**.
5. If not signed in, Google Drive will ask them for sign-in information or to choose an account.
6. They may be presented with a warning message that says, "Google hasn't verified this app. You've been given access to an app that's currently being tested. You should only continue if you know the developer that invited you." Click **Continue**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

7. Select which Google Drive features Webmail will be able to access, click **Continue**.
8. A final page will display stating that MDaemon is now connected to Google Drive. They can then close this window.
9. They can then access Google Drive from their **Documents** page in Webmail.

See:

MultiPOP OAuth 137
Dropbox Integration 325

3.6.1.9 Categories

The Categories options are located in MDaemon's Remote Administration interface, at: **Main » Webmail Settings » Categories**.

Webmail supports categories for email, events, notes, and tasks in the LookOut and WorldClient themes. Users can add the Categories column to the message list by going to "**Options » Columns**" and checking "**Categories**" in the Message List section.

To set categories for one or more messages in the message list, select the messages and right-click one of them. Use the context menu to set the category. Alternatively, you can open a message and set a category using the option on the toolbar.

Categories

On the Categories page in MDaemon's Remote Administration interface, you can set the Domain Categories, which is a fixed list of categories that users will see in Webmail but cannot edit or delete. You can also create the default list of Personal Categories that will be displayed to new users.

Domain Categories

Domain Categories are fixed categories that cannot be reordered, edited, or deleted by your users. When the *Enable Domain Categories* option is enabled, the list will appear at the top of your user's list of categories in Webmail. You can reorder, edit, delete, or create new Domain Categories using the options provided.

Personal Categories

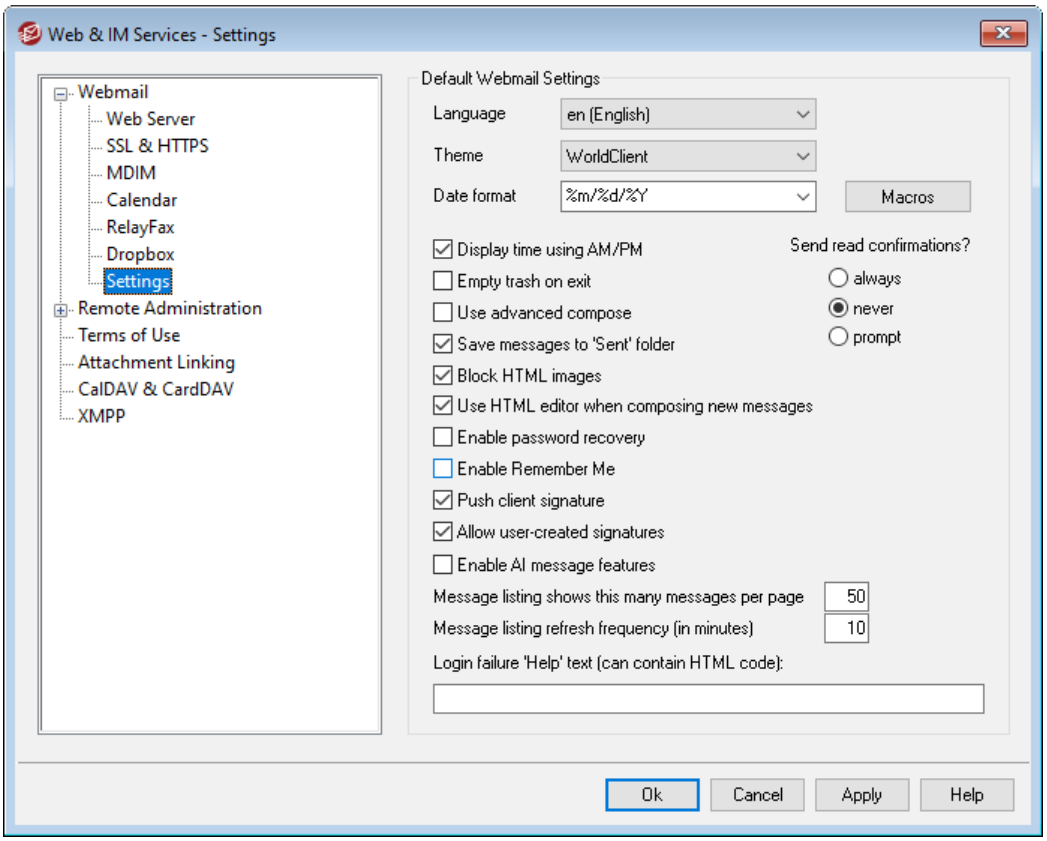
This is the default list of categories that will be copied to new Webmail users' accounts. Users have complete control over their list of personal categories. They can reorder, edit, or delete them, and they can create new ones. If, however, you are also using Domain Categories then those categories will be listed at the top for each user and cannot be edited or duplicated by them. Any personal category with a name that matches a domain category will be hidden. If you do not wish to allow personal categories then uncheck **Users can edit personal categories**. In that case only

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

domain categories will be displayed. If the Domain Categories option is also disabled then no Categories options will be available to the users.

For more detailed information relating to the MDaemon files in which categories and category translations are managed, see: `MDaemon\WorldClient\CustomCategories.txt`.

3.6.1.10 Settings



This screen designates the default settings for the Domain Manager's Webmail Settings 187 screen. When a user signs in to Webmail, these options govern how various Webmail features initially work for that user. Many of these settings can then be customized by the user via the Options pages within Webmail.

Default Webmail Settings

Language
Use the drop-down list box to choose the default language in which the Webmail interface will appear when your users first sign in to the selected domain. Users can

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

change their personal language setting on the Webmail Sign-in page, and through an option in Options » Personalize within Webmail.

Theme
Use this drop-down list box to designate the default Webmail theme to used for users whenever they sign in for the first time. The users can personalize the theme setting from Options » Personalize within Webmail.

Date format
Use this text box to designate how dates will be formatted within Webmail. Click the *Macros* button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

%A — Full weekday name

%B — Full month name

%d — Day of month (displays as "01-31")

%m — Month (displays as "01-12")

%y — 2-digit year

%Y — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in Webmail as "`12/25/2011`".

Macros
Click this button to display the list of macro codes that can be used in the *Date format*.

Send read confirmations?
This option governs how Webmail will respond to incoming messages that contain a request for read confirmation.

always
If this option is selected, MDaemon will send a notification to the sender indicating that the message was read. The Webmail user who received the message will not see any indication that the read confirmation was requested or responded to.

never
Choose this option if you want Webmail to ignore read confirmation requests.

prompt
Select this option if you wish to ask Webmail users whether or not to send a read confirmation each time a message is opened that requests it.

Display time using AM/PM
Click this option if you want a 12-hour clock with AM/PM to be used within Webmail for times displayed. Clear the check box if you want to use a 24-hour clock. Individual users can modify this setting via the "*Display my hours in an AM/PM format*" option located on the Options » Calendar page within Webmail.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Empty trash on exit
This option causes the user's trash to be emptied when he or she signs out from Webmail. Individual users can modify this setting from the Options » Personalize page within Webmail.

Use advanced compose
Check this box if you want users to see the Advanced Compose screen in Webmail rather than the normal Compose screen by default. Individual users can modify this setting from Options » Compose within Webmail.

Save messages to 'Sent' folder
Click this option if you want a copy of each message that you send to be saved in your mailbox's *Sent* folder. Individual users can modify this setting from the Options » Compose page within Webmail.

Block HTML images
Enable this check box if you wish to prevent remote images from being displayed automatically when viewing HTML email messages in Webmail. In order to view the images the user must click the bar that appears above the message in the browser window. This is a spam prevention feature, because many spam messages contain images with special URLs that identify the email address of the user who viewed the images, thus confirming to the spammer that it is a valid, working address. This option is enabled by default.

Use HTML editor when composing new messages
Check this box if you want users to see the HTML compose editor by default in Webmail. They can control this setting for themselves from Options » Compose within Webmail.

Enable password recovery
If enabled, users who have permission to edit their password 703 will be able to enter an alternate email address in Webmail, which can be sent a link to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in Webmail on the Options » Security page. Once set, if the user attempts to log in to Webmail with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page. This feature is disabled by default.

You can enable or disable this option on a per-user basis by adding the following key to a Webmail user's `user.ini` file (e.g. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (or "=No" to disable the option for the
user)
```

Allow Two Factor Authentication Remember Me (also applies to Remote Admin)
When someone uses Two-Factor Authentication (2FA) when signing in to Webmail or Remote Admin, there is ordinarily a Remember Me option available to the user on the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

2FA authentication page, which will prevent the server from requiring 2FA again from that user for a set number of days (see the "*Enable Remember Me*" option below). Clear this checkbox if you do not wish to display the 2FA Remember Me option, which means all users with 2FA enabled will have to enter a 2FA code every time they sign in. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Enable Remember Me
Check this box if you want there to be a *Remember Me* checkbox on the MDaemon Webmail sign-in page when users connect via the https 316 port. If users check this box at sign-in, their credentials will be remembered for that device. Then any time they use that device to connect to Webmail in the future they will be signed in automatically, until such time that they manually sign out of their account or their Remember Me token expires.

By default, user credentials are remembered for a maximum of 30 days before the user is forced to sign in again. If you wish to increase the expiration time then you can do so by changing the value of the *Expire Remember Me tokens after this many days* option in the MDaemon Remote Administration (MDRA) 341 web-interface. You can also change it by editing the `RememberUserExpiration=30` key in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. The expiration value can be set to a maximum of 365 days. **Note:** Two-Factor Authentication 703 (2FA) has its own Remember Me expiration key (`TwoFactorAuthRememberUserExpiration=30`), located in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. Therefore 2FA will again be required at sign-in when the 2FA Remember Me token expires, even if the regular token is still valid.

The *Remember Me* option is disabled by default and applies to all of your domains. If you wish to override this setting for specific domains then use the *Remember Me* setting located on the Domain Manager's Webmail 187 screen.

Because *Remember Me* allows users to have a persistent login on multiple devices, users should be discouraged from using it on public networks. Further, if you ever suspect that an account may have had a security breach, in MDRA there is a *Reset Remember Me* button that you can use to reset Remember Me tokens for all users. This will require all users to sign-in again.

Push client signature
Check this box if you wish to push the Default Client Signature 132 to Webmail users. In Webmail, this will create a signature called "System" under the signature options at: **Options » Compose**. Users can then choose to have this signature automatically inserted into the compose view when composing a new message. If you wish to customize or enable/disable the client signature for specific domains, use the Domain Manager's Client Signatures 200 and Webmail 187 options.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow user-created signatures
Check this box if you wish to allow users to create their own custom signatures in Webmail. Users can then choose which signature they wish to insert into the compose view automatically when composing messages. When you do not allow user-created signatures, but the *Push client signature* option above is enabled, only the Client Signature 132 (i.e. the "System" signature in Webmail) can be inserted automatically. In Webmail, the signature options are located at: **Options » Compose**.

Allow users to edit their alias display names
Check this box if you wish to allow users to edit the display name of any alias associated with their account. They can do this by using the *Edit Alias Display Names* option, located in Webmail's Pro Theme, under Settings » Compose. This option is disabled by default. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Enable AI message features
Check this box if you wish to enable support for MDaemon's AI Message Features in MDaemon Webmail for all of your domains. You can override this setting for specific domains using the option of the same name located on the Domain Manager's Webmail Settings 187 screen. **Note:** enabling AI Message Features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services 703 screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features. See: "Webmail's AI Message Features 339" below for important information and cautions about using these features.

Message listing shows this many messages per page
This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from Options » Personalize within WorldClient.

Message listing refresh frequency (in minutes)
This is the number of minutes that Webmail will wait before automatically refreshing the Message Listing. Individual users can modify this setting from Options » Personalize within Webmail.

Login failure 'Help' text (can contain HTML code)
You can use this option to specify a sentence of text (either plain text or HTML) to display on the Webmail sign-in page when a user encounters a problem signing in. The text is displayed below the following default text: "*Incorrect Logon, please try again. If you need assistance please contact your email administrator.*" This text could be used to direct users to a page or contact info for help regarding signing in to Webmail.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Security Settings (**Note:** The options in this section are only available in the MDaemon Remote Administration (MDRA) 341 web-interface.)

Allow WebAuthn at Sign-In
Check this box if you wish to allow MDaemon Webmail users to sign in utilizing the Web Authentication API (also known as WebAuthn), which gives them a secure, passwordless sign-in experience, by allowing them to use biometrics, USB security keys, Bluetooth, and more for authentication. WebAuthn is allowed by default.

Prompt users to register the current device on first sign-in
Check this box if you wish to prompt users to register their current device (phone, biometrics, etc.) for passwordless sign-in when they first sign in to their account.

Visit: **webauthn.guide**, for more information on WebAuthn and how it works.

Enable password recovery
If enabled, users who have permission to edit their password 703 will be able to enter an alternate email address in Webmail, to which a link can be sent to reset their password if they forget it. To set up this feature, users must enter both the password recovery email address and their current password in Webmail on the Options » Security page. Once set, if the user attempts to log in to Webmail with an incorrect password a "forgot password?" link will appear. This link takes them to a page that asks them to confirm their password recovery email address. If entered correctly, an email will be sent with a link to a change password page. This feature is disabled by default.

You can enable or disable this option on a per-user basis by adding the following key to a Webmail user's `user.ini` file (e.g. `\Users\example.com\frank\WC\user.ini`):

```
[User]
EnablePasswordRecovery=Yes (or "=No" to disable the option for the
user)
```

Allow Active Directory users to change their passwords through Webmail
When this box is checked/enabled, users whose accounts are set to use Active Directory authentication can use Webmail's "Change Password" option. When this option is disabled, only users whose passwords are set in MDaemon instead of Active Directory can change their password from within Webmail. The Domain Manager has an option of the same name 187 that you can use to override this setting for specific domains.

Allow users to view passwords being typed
When this option is turned on, the password field on the Webmail sign-in page has an icon that the user can click to make the typed password visible. Clear this checkbox if you do not wish to allow the password to be seen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow users to receive Two Factor Authentication verification codes over email
By default, users are allowed to enter an alternative email address into Webmail when setting up Two Factor authentication, so that they can receive verification codes via email rather than having to use the Google authenticator app. Turn off this option if you do not wish to allow verification codes via email. You can override this option separately for each of your domains by using the option of the same name on the Domain Manager's Webmail Settings 187 page.

Two Factor Authentication verification code sent over email expires after: [xx] minutes
When receiving Two Factor authentication codes via email, this is how long the user will have to enter the code before it expires. By default this is set to **10** minutes.

Allow WebAuthn for Two Factor Authentication
Check this box if you wish to allow MDaemon Webmail users to utilize the Web Authentication API (also known as WebAuthn) for two factor authentication. WebAuthn allows users to use biometrics, USB security keys, Bluetooth, and more for authentication. WebAuthn is allowed by default for two-factor authentication.

For security, you cannot use the same authentication method for both passwordless sign-in and two factor authentication. Therefore if you wish to use both passwordless authentication and two factor authentication, choose a different authentication method for each.

Visit: **webauthn.guide**, for more information on WebAuthn and how it works.

Allow Two Factor Authentication Remember Me (also applies to Remote Admin)
When someone uses Two-Factor Authentication (2FA) when signing in to Webmail or Remote Admin, there is ordinarily a Remember Me option available to the user on the 2FA authentication page, which will prevent the server from requiring 2FA again from that user for a set number of days (see the "*Expire Remember Me tokens after this many days*" option below). Clear this checkbox if you do not wish to display the 2FA Remember Me option, which means all users with 2FA enabled will have to enter a 2FA code every time they sign in.

Webmail's AI Message Features

As of MDaemon 23.5.0, the Pro theme in MDaemon's Webmail client includes various Artificial Intelligence (AI) features to help assist your users in managing their email and increasing productivity. These features are optional and disabled by default, but can be enabled for any user you choose.

With these features, in MDaemon Webmail you can use AI to:

- Give you a summary of the contents of an email message.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- Suggest a reply to the message, according to several guidelines that you can instruct the AI to use. You can set the *Tone* of the reply to be professional, respectful or casual. The *Position*, or stance, to take in the reply can be set to interested or not interested, agree or disagree, or skeptical. The *Attitude* the reply should convey can be set to confident, excited, calm, or apologetic. Last, you can designate the *Length* of the reply, ranging from very brief to detailed.
- Assist you in composing a new email message, based on some text you have already included. As with the *Suggest a Reply* option above, you can also designate the Tone, Position, Attitude, and Length for the AI to use when composing the message.

The *Enable AI message features* option on the main Webmail Settings 333 dialog controls whether or not support for the AI features is enabled by default for your domains. There is an option of the same name located on the Domain Manager's Webmail 187 dialog that can be used to override that main setting for specific domains. **Note:** enabling AI Message Features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services 703 screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features.

Enabling accounts to use MDaemon's AI message features allows them to submit and receive information to and from third-party generative AI services, specifically ChatGPT by OpenAI. Administrators and users should therefore be aware that this introduces several potential privacy concerns due to the feature's ability to process personal data and generate potentially sensitive information. To address privacy concerns, it's vital for organizations to train their employees to use AI responsibly. **Note:** Data submitted to/from Open AI is not stored on the local server or on our network.

You can find MDaemon Technologies' AI Usage Policy at our Artifical Intelligence (AI) Information Page. On that same page there is also a link to OpenAI's Terms of Use.

Customizing Allowed Senders and Blocked Senders Folders

There are various standard Webmail features that you can customize by editing certain files in the `MDaemon\WorldClient\` folder:

You can hide the Allowed Senders and Blocked Senders folders for Webmail users by default. To do so, open `MDaemon\WorldClient\Domains.ini`, and under `[Default:UserDefaults]` change the value of "`HideWhiteListFolder=`" or "`HideBlackListFolder=`" from "`No`" to "`Yes`". You can hide or show these folders for specific users by editing those same keys in the `User.ini` file under the `[User]` section.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Domain Manager » Webmail Settings 187

3.6.1.11 Branding

If you wish to customize the Webmail banner images that appear on the login page and in the navigation sidebar, you can do so from the Branding page in MDaemon's Remote Administration 341 web interface.

To use your own custom images:

1. Click **Use custom images** in the Customization section.
2. In the Login Page Image section, use the **Choose File** or **Browse** option (depending on your browser) to select the file you wish to upload. This section also lists the default dimension size for the login page image.
3. Click **Upload Custom Image**.
4. Repeat steps 2 and 3 for the Navigation Sidebar Image and Inverted Navigation Sidebar Image.

The uploaded images will appear in their corresponding boxes and now be used instead of Webmail's default images.

3.6.2 Remote Administration

MDaemon's Remote Administration (MDRA) web interface is designed to make it possible for you to administer MDaemon remotely using a web browser. It is a server application designed to run in the background on the same computer as MDaemon. To access Remote Administration, open your browser to the URL and port number on which the remote administration server resides (e.g. `www.example.com:1000`). After providing your login credentials, you will be given access to various controls and settings within MDaemon. The type and number of settings to which you will have access is dependent upon the level of access given. There are three levels of access that can be provided to remote administration users: Global, Domain, and User.

Global Administrators — Global administrators are users who have global access permission enabled under their account settings within MDaemon. Global access means that the user can see and configure every setting and control that is accessible via Remote Administration. Global administrators can add, edit, and delete users, domains, and mailing lists. They can edit product INI files, designate other users as Domain administrators, manage passwords, and do many other things; they have complete administrative control.

Domain Administrators — Similar to Global administrators, Domain administrators also have control over the users and settings accessible via Remote Administration. Their administrative control, however, is limited to the domain or domains to which they have been given access and the permissions designated on the Web Services 703 screen. Domain administrators and the domains over which they have control are designated from within Remote Administration by a

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Global administrator, or by another Domain administrator with access to those domains.

Users — The lowest possible level of Remote Administration access is User access. MDaemon users can sign in to the remote administration interface and, for example, view their individual account settings as well as edit their MultiPOP entries, mail filters, Autoresponders, and so on. The type and number of settings that can be edited depends on the permissions given in each user's account settings

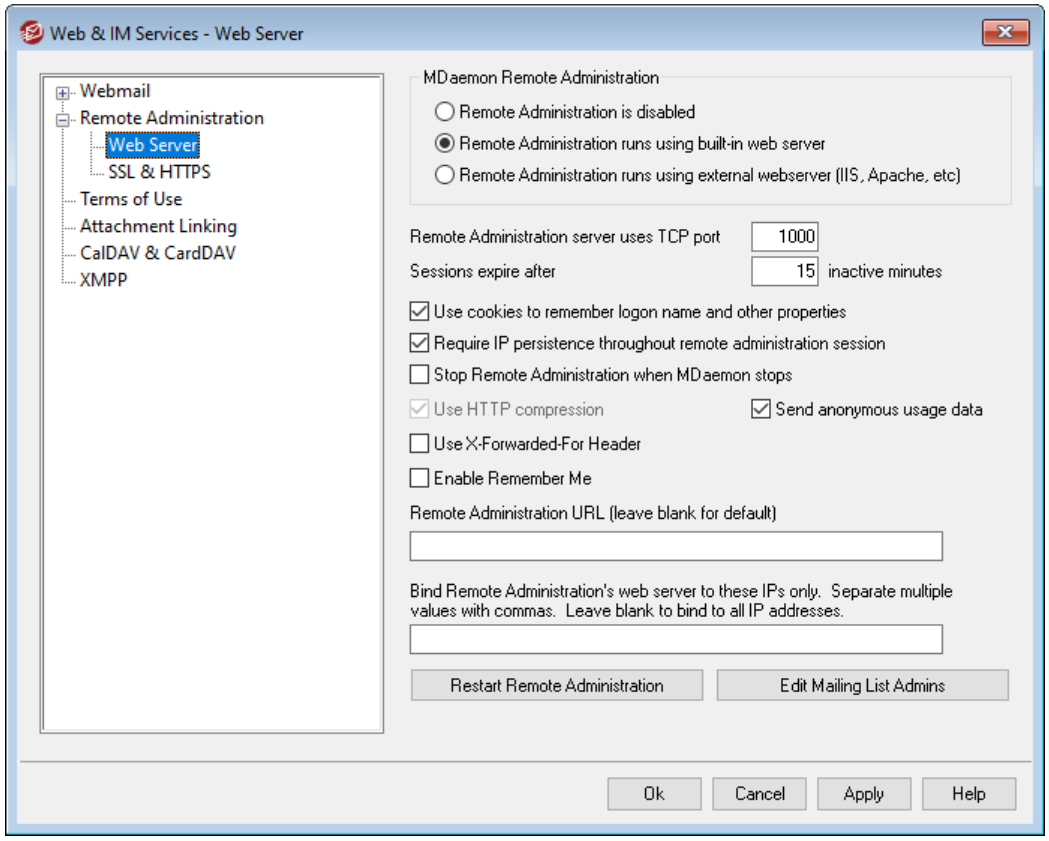
Everyone who has permission to access both Webmail and Remote Administration can access Remote Administration from within Webmail, rather than having to sign in to both separately. Remote Administration is opened in a separate browser window from within Webmail by clicking the "Advanced Settings" link under "Options".

See:

Remote Administration » Web Server 343
Remote Administration » HTTPS 348
Template Manager » Web Services 782
Account Editor » Web Services 703
Running Remote Administration under IIS 352

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.2.1 Web Server



MDaemon Remote Administration

Remote Administration is disabled
Choose this option to disable Remote Administration. You can also toggle Remote Administration active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Remote Administration runs using built-in web server
Choose this option to run Remote Administration using MDaemon's built-in web server. You can also toggle Remote Administration active/inactive from the File menu, or from the Servers section of the Stats frame on the main MDaemon GUI.

Remote Administration runs using external web server (IIS, Apache, etc)
Choose this option when you wish to run Remote Administration under Internet Information Server (IIS) or some other web server instead of MDaemon's built-in server. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with your alternate server.

For more information, see Running Remote Administration under IIS 352.

Remote Administration server uses TCP port
This is the port on which Remote Administration will listen for connections from your web browser. The default port is 1000.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Sessions expire after xx inactive minutes
When you are logged in to Remote Administration, this is the amount of time that your session is allowed to be inactive before Remote Administration will close it. The default is 15 minutes.

Security Settings

Note: The options in this section are available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Use Cross-Site-Request-Forgery tokens
By default, Cross-Site-Request-Forgery (CSRF) tokens are used for more secure transactions, to prevent CSRF attacks.

Allow users to view passwords being typed
By default, users can click an icon to view the password characters they are typing when signing in to the remote administration web interface. Clear this checkbox if you do not wish to allow that.

Allow WebAuthn at Sign-In
Check this box if you wish to allow MDRA users to sign in utilizing the Web Authentication API (also known as WebAuthn), which gives them a secure, passwordless sign-in experience, by allowing them to use biometrics, USB security keys, Bluetooth, and more for authentication. WebAuthn is allowed by default.

Allow WebAuthn for Two Factor Authentication
Check this box if you wish to allow MDRA users to utilize the Web Authentication API (also known as WebAuthn) for two factor authentication. WebAuthn allows users to use biometrics, USB security keys, Bluetooth, and more for authentication. WebAuthn is allowed by default for two-factor authentication.

For security, you cannot use the same authentication method for both passwordless sign-in and two factor authentication. Therefore if you wish to use both passwordless authentication and two factor authentication, choose a different authentication method for each.

Visit: **webauthn.guide**, for more information on WebAuthn and how it works.

Enable Remember Me
Check this box if you want there to be a *Remember Me* checkbox on the MDaemon Remote Administration (MDRA) sign-in page when users connect via the https 348 port. If users check this box at sign-in, their credentials will be remembered for that device. Then any time they use that device to connect to MDRA in the future they will be signed in automatically, until such time that they manually sign out of their account or their Remember Me token expires. The *Remember Me* option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Expire Remember Me tokens after this many days
Use this option to designate the number of days that your users' credentials will be remembered. By default credentials are remembered for a maximum of 30 days before a user is forced to sign in again. This option can be set to a maximum of 365 days. **Note:** Two-Factor Authentication 703 (2FA) has its own Remember Me expiration key (`TwoFactorAuthRememberUserExpiration=30`), located in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. Therefore 2FA will again be required at sign-in when the 2FA Remember Me token expires, even if the regular token is still valid.

Reset Remember Me
Click this button if you suspect that an account may have had a security breach. This will reset the Remember Me tokens for all users, causing them to have to sign-in again.

Because *Remember Me* allows users to have a persistent login on multiple devices, users should be discouraged from using it on public networks.

Miscellaneous Settings

Use cookies to remember logon name and other properties
By default the Remote Administration interface uses cookies so that the user's browser can remember the user's login name and other properties. Disable this checkbox if you do not wish to use cookies. Using this feature gives users a more customized login experience but requires that they have support for cookies enabled in their browser.

Require IP persistence throughout remote administration session
As an added security measure you can click this checkbox to cause Remote Administration to restrict each session to the IP address from which you connected when the session began. Thus, no one can "steal" the session since IP persistence is required. This configuration is more secure but could cause problems if you are using a proxy server or Internet connection that dynamically assigns and changes IP addresses.

Stop Remote Administration when MDaemon stops
Click this option if you want Remote Administration to be shut down whenever MDaemon is shut down. Otherwise, Remote Administration will continue to run in the background.

Use HTTP Compression
Click this check box if you want to use HTTP compression in your Remote Administration sessions.

Notify of new releases on Logon page
By default you will be notified on the Sign-in page when a new MDaemon release is available. Uncheck this box if you do not wish to be notified there. **Note:** This option is available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send anonymous usage data
By default MDaemon's Remote Administration web client sends anonymous, benign usage data such as: the OS used, browser version used, language, and the like. This data is used by MDaemon Technologies to help us improve Remote Administration. Disable this option if you do not wish to send anonymous usage data.

X-Forwarded-For header
Click this checkbox to enable the use of the `X-Forwarded-For` header, which is sometimes added by proxy servers. This option is disabled by default. Enable it only if your proxy server inserts this header.

Enable Remember Me
Check this box if you want there to be a *Remember Me* checkbox on the Remote Administration sign-in page when users connect via the https 348 port. If users check this box at sign-in, their credentials will be remembered for that device. Then any time they use that device to connect in the future they will be signed in automatically, until such time that they manually sign out of their account or their Remember Me token expires.

By default, user credentials are remembered for a maximum of 30 days before the user is forced to sign in again. If you wish to increase the expiration time then you can do so by changing the value of the *Expire Remember Me tokens after this many days* option in the MDaemon Remote Administration (MDRA) web-interface. You can also change it by editing the `RememberUserExpiration=30` key in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. The expiration value can be set to a maximum of 365 days. **Note:** Two-Factor Authentication 703 (2FA) has its own Remember Me expiration key (`TwoFactorAuthRememberUserExpiration=30`), located in the `[Default:Settings]` section of the `Domains.ini` file, located in the `\MDaemon\WorldClient\` folder. Therefore 2FA will again be required at sign-in when the 2FA Remember Me token expires, even if the regular token is still valid.

The *Remember Me* option is disabled by default.

Because *Remember Me* allows users to have a persistent login on multiple devices, users should be discouraged from using it on public networks. Further, if you ever suspect that an account may have had a security breach, in MDRA there is a *Reset Remember Me* button that you can use to reset Remember Me tokens for all users. This will require all users to sign-in again.

Remote Administration URL
This is the URL that Webmail will use internally when users click the Advanced Settings link to edit their account settings via Remote Administration. If you are running Remote Administration with the built-in web server, then leave this field blank. If you are using an alternate web server such as IIS, and you have configured Remote Administration to run at an alternate URL or IP address, then specify that URL here.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Bind Remote Administration's web server to these IPs only
If you wish to restrict the remote administration server to only certain IP addresses, specify those addresses here separated by commas. If you leave this field blank then Remote Administration will monitor all IP Addresses that you have designated for your Domains 174.

Restart Remote Administration (required when port or IIS value changes)
Click this button if you wish to restart the remote administration server. Note: when changing the port setting you must restart Remote Administration in order for the new setting to be recognized.

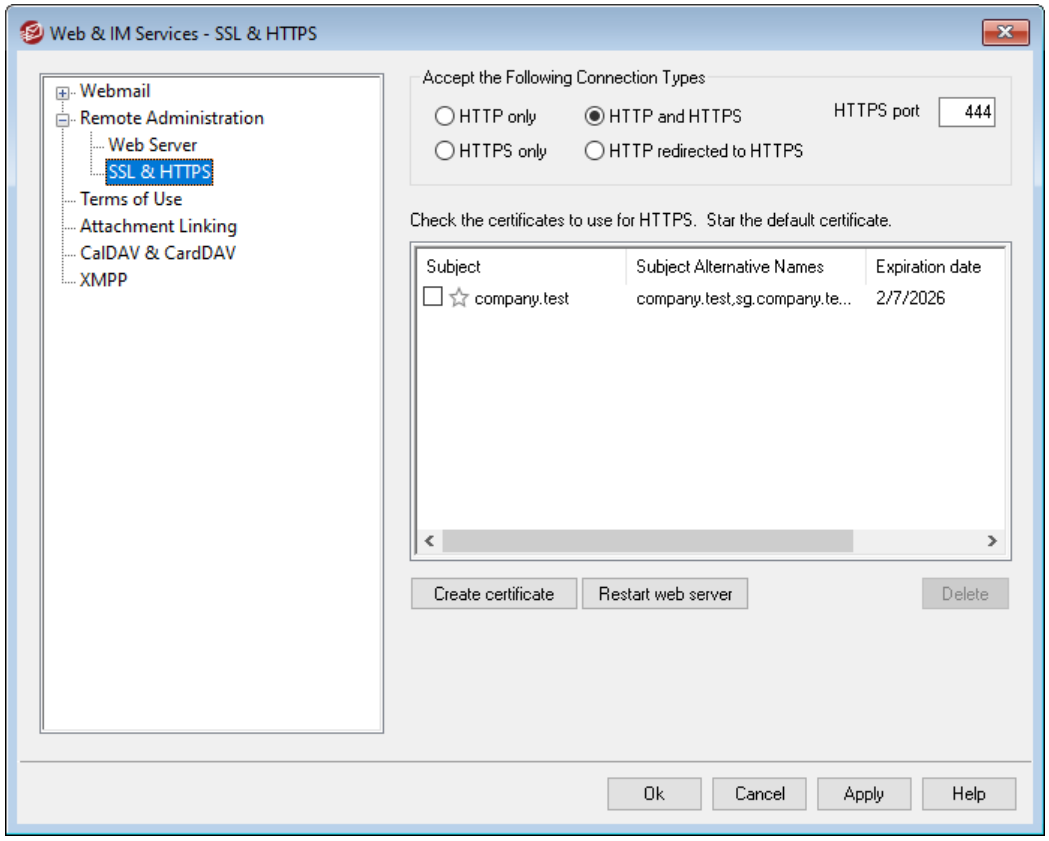
Edit Mailing List Admins
Click this button if you wish to open the mailing list administrators file to view or edit it.

See:

Remote Administration 341
Remote Administration » HTTPS 348
Running Remote Administration under IIS 352
Template Manager » Web Services 782
Account Editor » Web Services 703

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.2.2 SSL & HTTPS



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Remote Administration to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Remote Administration". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » Remote Administration".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 561

This screen only applies to Remote Administration when using MDaemon's built-in web server. If you configure Remote Administration to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Accept the Following Connection Types

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Remote Administration. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Remote Administration, but do not wish to force your Remote Administration users to use HTTPS. Remote Administration will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Remote Administration TCP port designated on the Web Server 343 screen.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Remote Administration. Remote Administration will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Remote Administration will listen to for SSL connections. The default SSL port is 444. If the default SSL port is used, you will not have to include the port number in Remote Administration's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:444").

This is not the same as the Remote Administration port that is designated on the Web Server 343 screen. If you are still allowing HTTP connections to Remote Administration then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Check the box next to any certificates you wish to be active. Click the star next to the one that you wish to set as the default certificate. MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used. Double-click a certificate to open it in Windows' Certificate dialog for review (only available in the application interface, not in the browser-based remote administration).

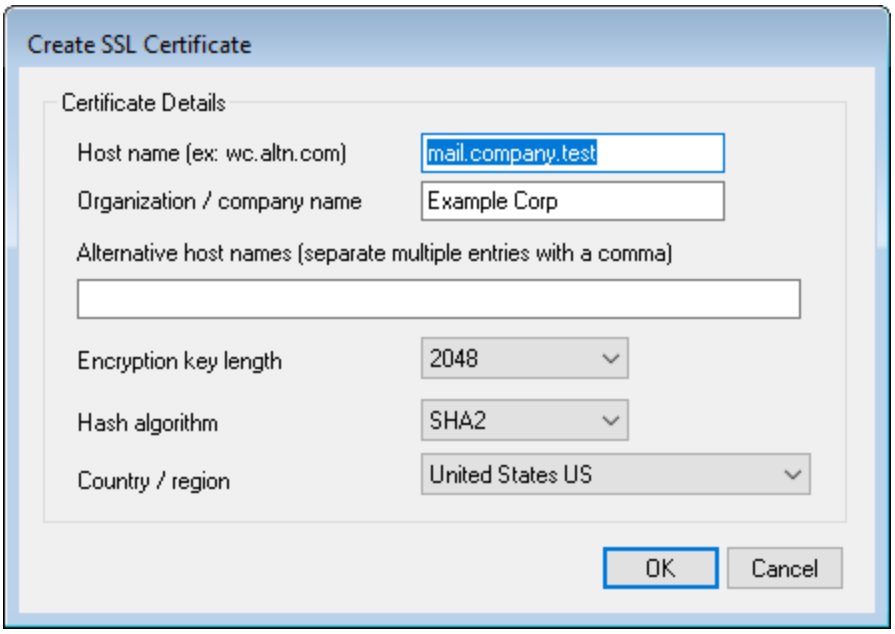
Delete
Select a certificate in the list and then click this button to delete it. A confirmation

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Certificate Details

Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field. If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

Using Let's Encrypt to Manage Your Certificate

Let's Encrypt is a Certificate Authority (CA) that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

To support using Let's Encrypt's automated process to manage a certificate, the Let's Encrypt 580 screen is provided to help you easily configure and run the PowerShell script included in the "`MDaemon\LetsEncrypt`" folder. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*. See the Let's Encrypt 580 topic for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

For more information on SSL and Certificates, see:

Running Remote Administration under IIS 352
SSL and Certificates 561
Creating and Using SSL Certificates 896

For more information on Remote Administration, see:

Remote Configuration 341
Remote Administration » Web Server 343
Web Access Defaults 782
Account Editor » Web 703

3.6.2.3 Running Remote Administration under IIS

MDaemon is equipped with a built-in web server, which means that Remote Administration doesn't require Internet Information Server (IIS) to operate. However, it does support IIS, and can therefore function as an ISAPI DLL.

To configure to operate under IIS 5:

1. Stop Remote Administration from running. You can do this by right-clicking on the Remote Administration entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.

2. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools→Internet Services Manager**).

3. Right-click **Default Website** and then select **New→Virtual Directory**.

4. Follow the Wizard as it takes you through the steps of creating a Virtual Directory. The following are suggested names and locations for data to be typed into the Wizard, but will vary depending on your installation of MDaemon and the location of MDaemon's Remote Administration component.

   a. Alias: "`WebAdmin`". Click **Next**.
   b. Directory: "`c:\mdaemon\webadmin\templates`". Click **Next**.
   c. Click **Next**.
   d. Click **Finish**.

5. Set the Execute Permissions to **Scripts Only**.

6. Set the Application Protection to **Low (IIS Process)**.

7. Click the **Configuration** button in the Application Settings section of the Virtual Directory tab.

8. On the **Mappings** tab click the **Add**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

9. In the **Executable** field enter "`c:\mdaemon\webadmin\templates\WebAdmin.dll`". Note: This field cannot contain any spaces. If the path contains a space it must be converted to 8.3 format. The `dir /x` command will show the 8.3 name for a file or directory.
10. In the **Extension** field enter "`.wdm`" and select the radio button for **All Verbs**.
11. Click the **Script Engine** box.
12. Click **OK**.
13. All other mappings can be removed if you choose, then click the **OK**.
14. On the **Documents** tab add `login.wdm` as a Default Document and remove all other entries from the list.
15. In MDaemon, go to **Setup→Web & IM Services→Remote Administration** and click **Remote Administration runs using external webserver**.
16. In **Remote Administration URL** type "`/WebAdmin/login.wdm`".
17. Click **OK**.

To configure to operate under IIS 6:

Create a new application pool for Remote Administration:

1. Stop Remote Administration from running. You can do this by right-clicking on the Remote Administration entry under *Servers* in the left pane of the MDaemon GUI, and then clicking **Toggle Active/Inactive**.
2. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools→Internet Services Manager**).
3. Right-click **Application Pools**.
4. Click **New→Application Pool**.
5. In the Application pool ID field type "`Alt-N`" and click **OK**.
6. Right-click **Alt-N**
7. Click **Properties**.
8. Click **Performance** tab.
9. Clear "**Shutdown worker processes after being idle for**" and "**Limit the kernel request queue**".
10. Click **Identity** tab.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

11. In the drop-down for Predefined, choose **Local System**.
12. Click **OK**.

Create a virtual directory for Remote Administration:

1. Open the IIS management program (**Start→Settings→Control Panel→Administrative Tools (Internet Services Manager)**).
2. Right-click your web site and then select New (Virtual Directory).
3. Specify an alias for the virtual directory (for example, "`WebAdmin`").
4. In the Path field, type the path to the Remote Administration Templates directory — for example, "`C:\Program Files\Alt-N Technologies\WebAdmin\Templates`".
5. Leave the **Read** and **Run Scripts** options checked.
6. Finish the wizard and right-click on the Virtual Directory that was created.
7. Select **Properties**.
8. On the Home Directory tab change the application pool to "Alt-N".
9. Click the Configuration button.
10. Click **Add** to add an ISAPI extension mapping.
11. In the Executable field enter the path to the `WebAdmin.dll` file. For example, "`C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`".
12. In the Extension field enter "`.wdm`"
13. Click the boxes for **Script Engine** and **Verify the file exists**.
14. Click **OK**.
15. All other mappings can be removed if you choose, then click the **OK**.
16. Select the **Documents** tab.
17. Ensure that **Enable default content page** is checked.
18. Ensure that only "`login.wdm`" exists in the list.
19. Click the **Ok** and exit the virtual directory properties dialog.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add `.WDM` to list of allowed web extensions:

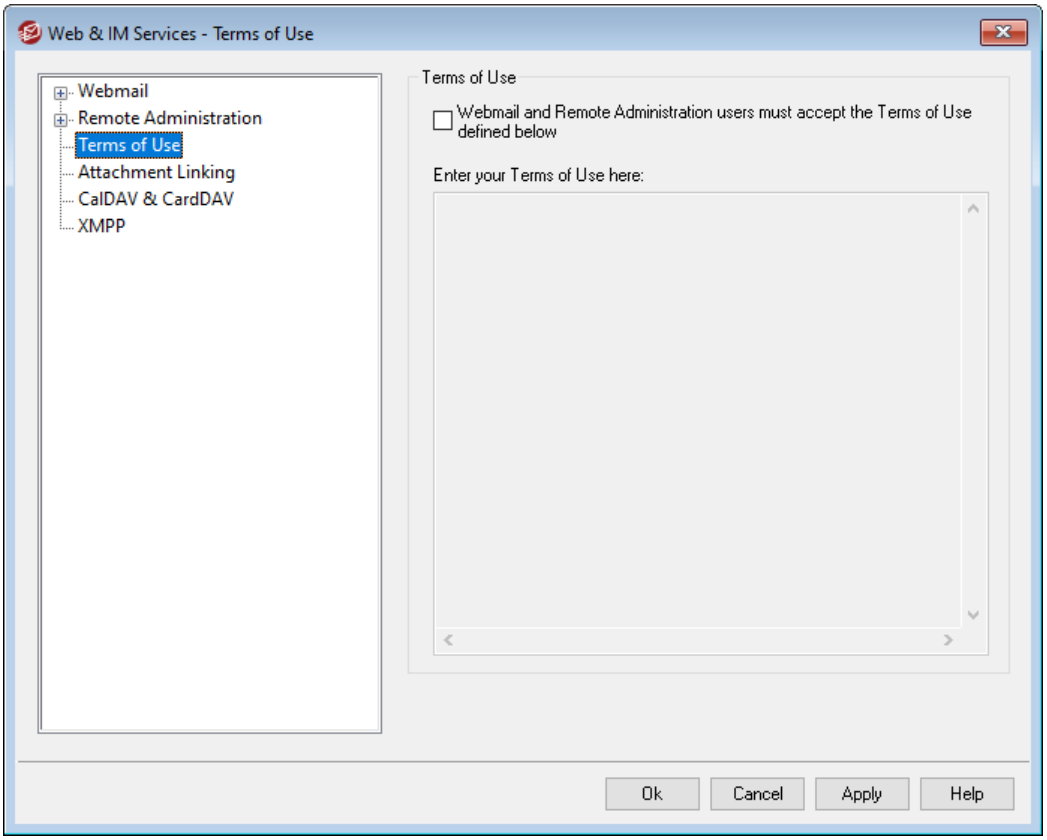
1. Click on the **Web Service Extensions** folder (in the IIS MMC).
2. Click **Add new web service extension**.
3. In the Extension name field enter "`WebAdmin`".
4. Click **Add** and then browse to the WebAdmin ISAPI extension. For example: `C:\Program Files\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`.
5. Check **Set extension status to allowed**.
6. Click **OK**.
7. In MDaemon, go to **Setup→Web & IM Services→Remote Administration** and click **Remote Administration runs using external web server**.
8. In **Remote Administration URL** type "`/WebAdmin/login.wdm`".
9. Click **OK**.

For more information on Remote Administration, see:

Remote Administration 341
Remote Administration » Web Server 343
Remote Administration » SSL & HTTPS 348
Template Manager » Web Services 782
Account Editor » Web Services 703

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.3 Terms of Use

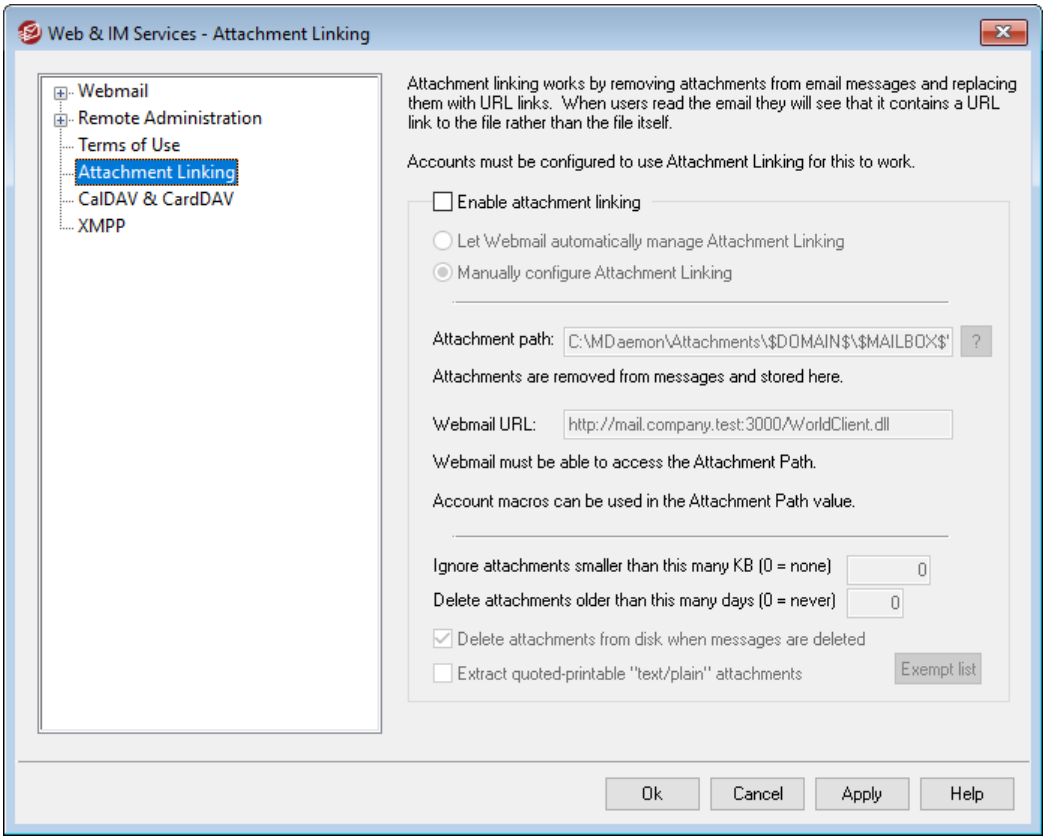


Webmail and Remote Administrations users must accept the Terms of Use defined below

Check this box and enter your Terms of Use statement in the space provided if you wish to require Webmail and Remote Administration users to accept the Terms of Use statement each time they sign in.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.4 Attachment Linking



Attachment Linking (`Setup » Web & IM Services » Attachment Linking`) is a feature that makes it possible for MDaemon to remove all attachments from incoming email messages, store them in a designated location, and then place URL links to the files in each message from which they are extracted. The recipients can then click those links to download the files. This can greatly speed up mail processing when your users retrieve their messages or synchronize their mail folders, since the messages will be devoid of large attachments. It can also provide increased security and an increased level of protection for your users, because attachments can be stored in a central location for monitoring by the administrator and will not be downloaded automatically to mail clients where they might be executed automatically. Further, if you choose the "*Let Webmail automatically manage Attachment Linking*" option, management of the file locations and the Webmail URL is handled automatically. If you choose to manage Attachment Linking manually, you can specify the location where the files will be stored, and you can use special macros to make the location dynamic. In order for Attachment Linking to work, it must be enabled globally using the option on this screen, and each Account that you wish to use it must be configured specifically to do so on the Attachments 718 screen of the Account Editor. On that same screen there is also an option for applying Attachment Linking to outbound messages as well; the account's outbound messages will have attachments extracted and replaced with a link to the stored files. Finally, the links to the attachments that MDaemon will place in messages do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Attachment Linking will try to use the file name provided in the MIME headers (if present). If the file name is longer than 50 characters then only the last 50 characters will be used. If the file name is missing an extension, ".att" will be appended.

By default, the Attachment Linking feature places the text, "MDaemon replaced the following files with these links:" into certain emails. If you wish to change that text, add the following key to your MDaemon.ini file, located in the \app\ folder, then restart MDaemon:

```
[AttachmentLinking]
HeaderText=This Is My Text.
```

Enable attachment linking
Click this checkbox to enable Attachment Linking for all accounts that are specifically configured to use it on the Attachments 718 screen of the Account Editor. When you enable this global option you will be asked if you also wish to enable the account specific option for all MDaemon accounts. If you choose "Yes" then Attachment Linking will be enabled for all accounts, and the corresponding option on the New Accounts 799 template will also be enabled. If you choose "No" then the Attachment Linking feature will be enabled but the account specific option will not—you must manually activate it for each account that you wish to use it. When Attachment Linking is enabled, the Webmail server must remain active.

Let Webmail automatically manage Attachment Linking
This is the default option when Attachment Linking is enabled. Use this option if you wish to let Webmail handle Attachment Linking automatically. Extracted files will be stored at: "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\".

Manually configure Attachment Linking
Choose this option if you wish to designate the folder in which extracted file attachments will be stored. You must designate both the attachment path and the Webmail URL when you choose this option.

Attachment path
Use this text box to designate the folder in which to store extracted file attachments. You can set a static file path or use template 778 and script 828 macros to make the path dynamic. For example, "$ROOTDIR$\Attachments\$DOMAIN$\" will group all attachments into a subfolder named for the domain to which the user belongs, which is under another subfolder called "Attachments" contained in MDaemon's root folder (usually C:\MDaemon\). So, for "user1@example.com" the above example would cause the extracted attachments to be placed in the subfolder, "C:\MDaemon\Attachments\example.com\." You could further subdivide attachment storage by appending the "$MAILBOX$" template macro to the above example. This would cause user1's files to be stored in a subfolder beneath "\example.com\" called "user1." Therefore the new file path would be: "C:\MDaemon\Attachments\example.com\user1\."

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Webmail URL
Enter Webmail's URL here (e.g. "`http://mail.example.com:3000/WorldClient.dll`"). MDaemon will use this URL when inserting the links to extracted attachments in messages.

Ignore attachments smaller than this many KB (0 = none)
This is the minimum size required before an attachment will be extracted from a message. Use this option if you do not wish to extract smaller attachments. If set to "0" then Attachment Linking will extract all attachments, no matter how small.

Delete attachments older than this many days (0 = never)
Use this option if you wish to set a limit on the number of days that attachments will be stored. As part of the daily cleanup event MDaemon will remove any stored attachments that are older than the designated limit, if those attachments are contained within the default attachment folder or one of its subfolders. The default folder is: "`<MDaemonRoot>\Attachments\...`". Attachments will not be removed if you customize the attachment folder to point elsewhere. This option is disabled by default (set to "0").

Delete attachments from disk when messages are deleted
Click this option if you want to delete extracted attachments from the server whenever the messages to which they are linked are deleted.

When this option is enabled and a user collects his email via a POP3 client that is not configured to leave messages on the server, then all of his extracted attachments will be irretrievably lost. If this option is not enabled then no attachments will be lost, but a great deal of your hard drive space could eventually be taken up by outdated and useless files that their original recipient no longer wants or needs. Virtually all POP clients have the ability to leave messages on the server.

Extract quoted printable “text/plain” attachments
By default, quoted printable `text/plain` attachments will not be extracted. Click this checkbox if you wish to include them in automatic extraction.

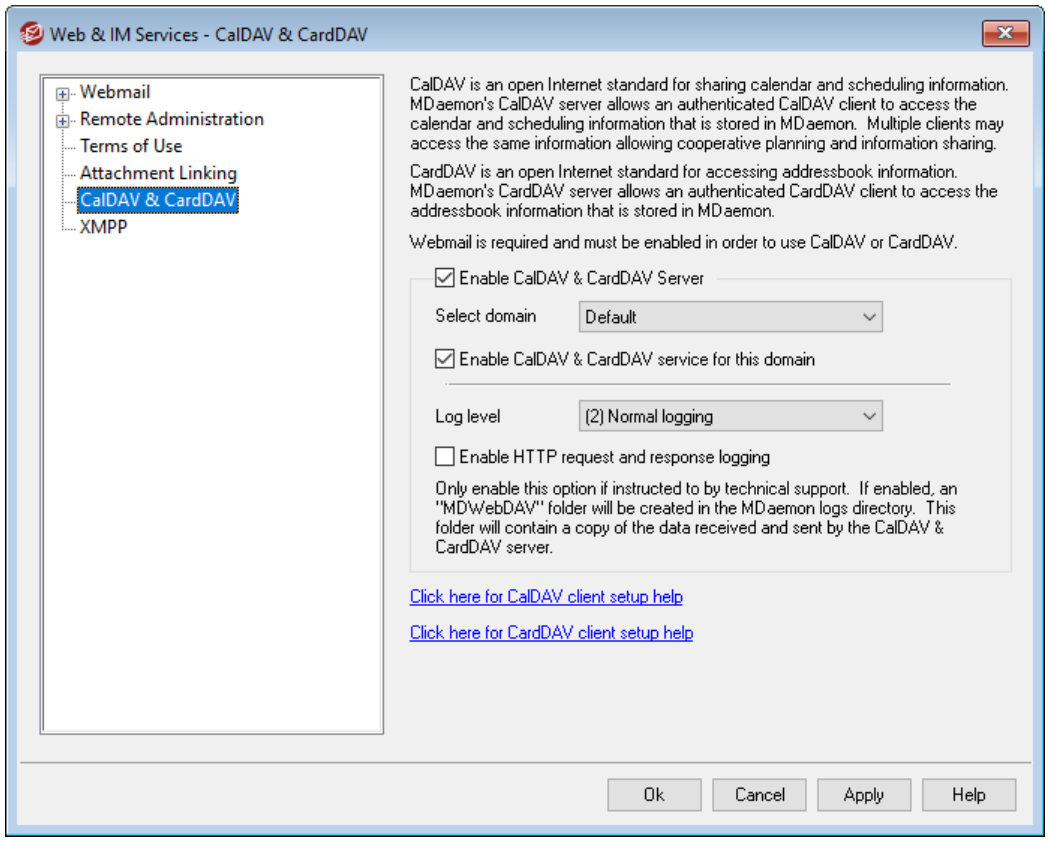
Exempt List
Click this button to open the Attachment Linking exempt list. Include any file names that you do not wish to extract from messages. `Winmail.dat` is included on this list by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

New Accounts Template 776
Account Editor » Attachments 718
Template Macros 778
Script Macros 828

3.6.5 CalDAV & CardDAV



CalDAV is an Internet standard for managing and sharing calendars and scheduling information. MDaemon's CalDAV support makes it possible for your accounts to use any client that supports CalDAV to access and manage their personal calendars and tasks. They can also access any public 300 or shared 726 calendars or tasks according to their access rights 302. CardDAV is a standard for accessing contacts/address book information. MDaemon's CardDAV server allows an authenticated CardDAV client to access the contact information that is stored in MDaemon.

Enable CalDAV & CardDAV Server
CalDAV/CardDAV support is enabled by default. However, Webmail is required and therefore must be enabled 313 in order to use it. Disable this option if you do not wish

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

to support CalDAV or CardDAV. To enabled/disable it for individual domains, use the options below.

Changing the Default CalDAV/CardDAV Setting for Domains
Initially, all of MDaemon's domains will have CalDAV/CardDAV enabled or disabled based the *Default* selection in the *Select domain* drop-down list. To change the default setting:

1. In the *Select domain* drop-down list, choose **Default**.
2. Check the box next to **Enable CalDAV & CardDAV service for this domain** if you want CalDAV/CardDAV to be enabled for all domains by default, or clear the box if you want it to be disabled by default.
3. Click **Ok**.

Enabling/Disabling CalDAV/CardDAV for Specific Domains
To override the *Default* CalDAV/CardDAV setting for individual domains:

1. In the *Select domain* drop-down list, choose a specific domain.
2. Check the box next to **Enable CalDAV & CardDAV service for this domain** if you want CalDAV/CardDAV to be enabled for the domain, or clear the box if you want it to be disabled.
3. Click **OK**.

Logging

Log level
Use this drop-down list to designate the degree to which CalDAV/CardDAV activities will be logged. There are six possible levels of logging: 1-Debug logging, 2-Normal logging (default), 3-Warnings and errors only, 4-Errors only, 5-Critical errors only, and 6-No logging. This is a global setting—it cannot be applied to specific domains

Enable HTTP request and response logging
If enabled, this will create an `MDWebDAV` folder in MDaemon's logs folder. All data sent and received by the CalDAV/CardDAV server will be logged to that folder. Ordinarily this option would only be used for diagnostics and shouldn't be enabled unless you are instructed by Technical Support to do so.

Configuring CalDAV Clients

To configure clients that support RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV)), only the server, user name, and password should be required. You can setup your DNS records to point the client to the correct URL. When a DNS record has not been configured, the user can enter a special "well-known URL" in the client: "hostname/.well-known/caldav". For example: `http://example.com:3000/.well-known/caldav` . Webmail's built-in web server support the well-known URL.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Clients that do not support automatically locating the CalDAV service, such as Mozilla Thunderbird via the Lightning plugin, will require a full URL for each Calendar and Task list. MDaemon's CalDAV URLs are constructed like this:

Calendars and Tasks
User's default calendar or task list:

`http://[host]/webdav/calendar`
(e.g. `http://example.com:3000/webdav/calendar`)

`http://[host]/webdav/tasklist`
(e.g. `http://example.com/webdav/tasklist`)

User's custom calendar or task list:

`http://[host]/webdav/calendar/[calendar-name]`
(e.g. `http://example.com/webdav/calendar/personal`)

`http://[host]/webdav/tasklist/[tasklist-name]`
(e.g. `http://example.com/webdav/tasklist/todo`)

User's custom calendar or task list in a subfolder:

http://[host]/webdav/calendar/[folder]/[calendar-name]
(e.g. `http://example.com/webdav/calendar/my-stuff/personal`)

http://[host]/webdav/tasklist/[folder]/[tasklist-name]
(e.g. `http://example.com/webdav/tasklist/my-stuff/todo`)

Shared Calendars and Tasks
Another user's default calendar or task list:

`http://[host]/webdav/calendars/[domain]/[user]`
(e.g. `http://example.com/webdav/calendars/example.net/frank`)

`http://[host]/webdav/tasks/[domain]/[user]`
(e.g. `http://example.com/webdav/tasks/example.net/frank`)

Another user's custom calendar or task list:

`http://[host]/webdav/calendars/[domain]/[user]/[calendar-name]`
(e.g. `http://example.com/webdav/calendars/example.net/frank/personal`)

`http://[host]/webdav/tasks/[domain]/[user]/[tasklist-name]`
(e.g. `http://example.com/webdav/tasks/example.net/frank/todo`)

Public Calendars and Tasks
Domain's default calendar or task list:

`http://[host]/webdav/public-calendars/[domain]`
(e.g. `http://example.com/webdav/public-calendars/example.com`)

`http://[host]/webdav/public-tasks/[domain]`
(e.g. `http://example.com/webdav/public-tasks/example.com`)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Calendar or task list in the root of the Public Folder hierarchy:

`http://[host]/webdav/public-calendars/[calendar-name]`
(e.g. `http://example.com/webdav/public-calendars/holidays`)

`http://[host]/webdav/public-tasks/[tasklist-name]`
(e.g. `http://example.com/webdav/public-tasks/projects`)

Special care should be taken if testing the OutlookDAV client. If multiple MAPI profiles exist we've seen the client issue delete commands to the server for all of the calendar items returned by the server. OutlookDAV only supports the default MAPI profile.

For more information on setting up CalDAV clients, search "CalDav" at the MDaemon Knowledge Base.

Configuring CardDAV Clients

To configure clients that support RFC 6764 (Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV)), only the server address, username, and password should be required. Apple Address Book and iOS support this standard. DNS records can be setup that point the client to the correct URL. When a DNS record has not been configured, clients query a "well-known URL," which in the case of CardDAV is `/.well-known/carddav`. Webmail's built-in web server supports this well-known URL. Clients that do not support automatically locating the CardDAV service will require a full URL.

Notable CardDAV clients are Apple Contacts (included with Mac OS X), Apple iOS (iPhone), and Mozilla Thunderbird via the SOGO plugin.

As of OS X 10.11 (EL Capitan), the Apple Contacts application only supports a single collection/folder. When the CardDAV server detects the Apple Contacts application, it will only return the authenticated user's default contacts folder. In addition, OS X 10.11 (EL Capitan) has a known issue that prevents a CardDAV account from being added using the "Advanced" view of the dialog.

Accessing address books

The "addressbook" path is a shortcut to your own default addressbook.

`http://[host]/webdav/addressbook` - your default contacts folder.

`http://[host]/webdav/addressbook/friends` - your "friends" contacts folder.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

`http://[host]/webdav/addressbook/myfolder/personal` - your "personal" contacts folder in a subfolder called "myfolder".

Accessing shared folders of another user to which you have access
The "contacts" path is a shortcut to shared contact folders.

`http://[host]/webdav/contacts/example.com/user2` - user2@example.com's default contact folder

`http://[host]/webdav/contacts/example.com/user2/myfolder` - user2@example.com's "myfolder" contact folder

Access public folders, to which you have access
The "public-contacts" path is a shortcut to public contact folders.

`http://[host]/webdav/public-contacts/example.com` - example.com's default contact folder

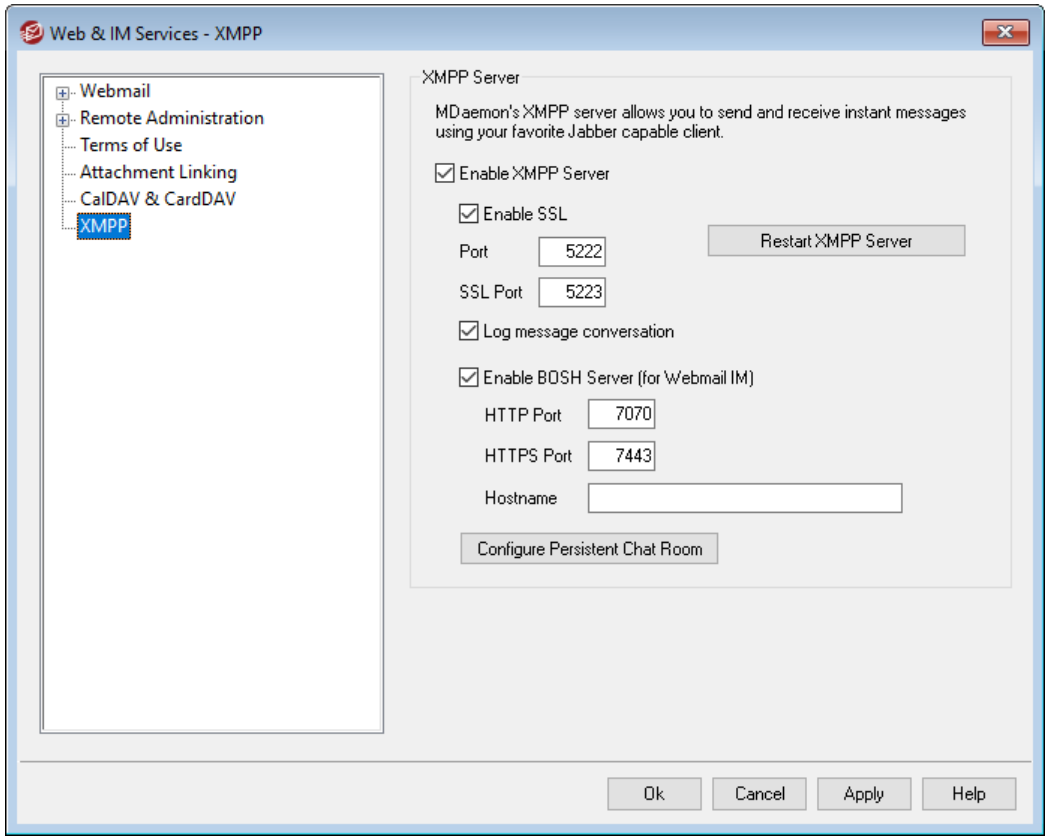
`http://[host]/webdav/public-contacts/foldername` - "foldername" contact folder in the root of the public folder hierarchy

Special care should be taken if testing the OutlookDAV client. OutlookDAV only supports the default MAPI profile. If multiple MAPI profiles exist, the client may issue delete commands to the server for all of the items that were returned by the server.

For more information on setting up CardDAV clients, search "CardDav" at the MDaemon Knowledge Base.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.6.6 XMPP



MDaemon is equipped with an Extensible Messaging and Presence Protocol (XMPP) server, sometimes called a Jabber server. This allows your users to send and receive instant messages using MDaemon Instant Messenger 309 and third-party XMPP clients, such as Pidgin, Gajim, Swift and many others. Clients are available for most operating systems and mobile device platforms.

The XMPP server is installed as a Windows service, and the default server ports are 5222 (SSL via STARTTLS) and 5223 (dedicated SSL). The XMPP server will use MDaemon's SSL configuration if it is enabled in MDaemon. Also, some XMPP clients use DNS SRV records for auto-discover of host names. Please refer to http://wiki.xmpp.org/web/SRV_Records for more information.

Users sign-in through their chosen XMPP client using their email address and password. Some clients, however, require the email address to be split into separate components for signing in. For example, instead of "`frank@example.com`," some clients require you to use "`frank`" as the Login/Username and "`example.com`" as the Domain.

For multi-user/group chat service, clients typically display this as "rooms" or "conferences." When you want to start a group chat session, create a room/conference (giving it a name) and then invite the other users to that room. Most clients don't require you to enter a server location for the conference; you only need to enter a name for it. When you are required to do so, however, use "`conference.<your domain>`" as the location (e.g. `conference.example.com`). A few

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

clients require you to enter the name and location together in the form: "room@conference.<your domain>" (e.g. Room01@conference.example.com).

Some clients (such as Pidgin), support the user search service, allowing you to search the server for users by name or email address, which makes adding contacts much easier. Usually you will not have to provide a search location, but if asked to do so, use "search.<your domain>" (e.g. search.example.com). When searching, the % symbol can be used as a wildcard. Therefore you could use "%@example.com" in the email address field to display a list of all users with an email address ending in "@example.com."

XMPP Server

Enable XMPP Server
Click this option to enable the XMPP server. To allow instant messaging, you must also ensure that the **Enable instant messaging** option is enabled on the MDIM 320 screen.

Enable SSL
Click this option if you wish to support SSL for the XMPP Server, using the *SSL Port* specified below. **Note:** This also applies to the BOSH server *HTTPS Port* option below.

Port
The default port for XMPP is 5222, which supports SSL via STARTTLS.

SSL Port
XMPP's dedicated SSL port is 5223.

Restart XMPP Server
Click this button to restart the XMPP server.

Log message conversation
By default all instant message conversations are logged in a file called XMPPServer-<date>.log, located in the MDaemon\Logs\ folder. Clear this checkbox if you do not wish to log conversations.

Enable BOSH Server (for Webmail IM)
Click this option to enable the BOSH server, allowing instant messaging within MDaemon Webmail.

HTTP Port
By default the BOSH server uses HTTP port 7070.

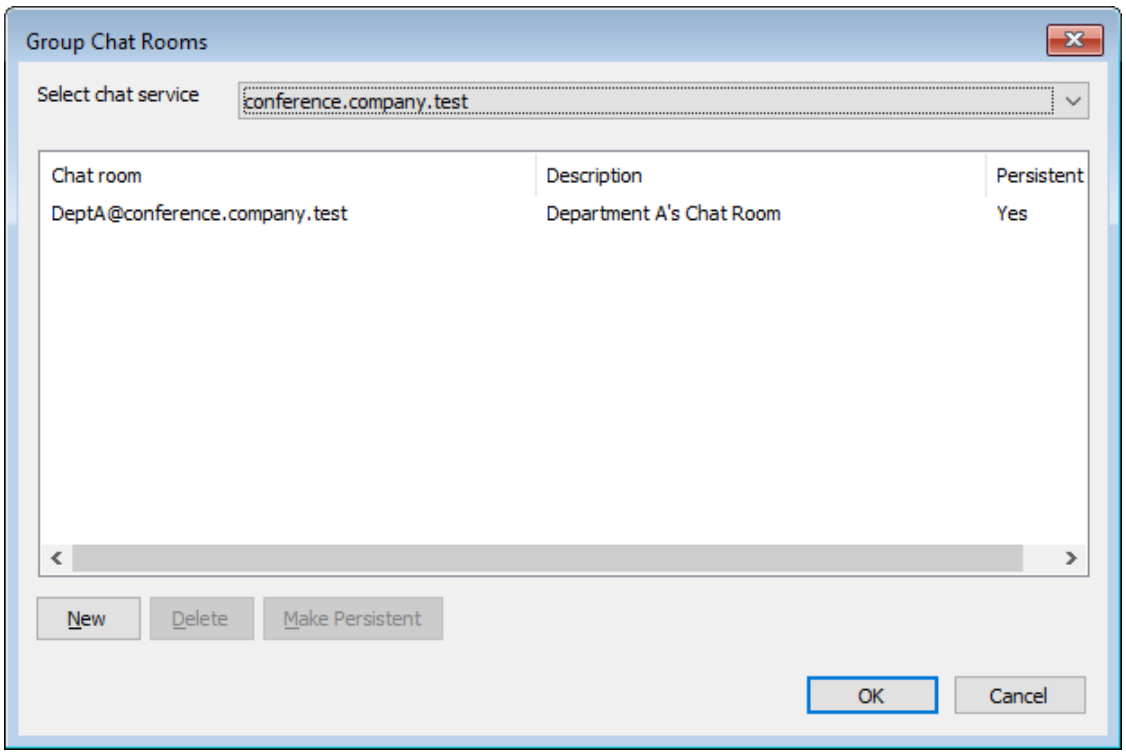
HTTPS Port
The BOSH server uses this HTTPS port when the *Enable SSL* option above is activated. The default port is 7443.

Hostname
Use this option to specify a Hostname if necessary.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

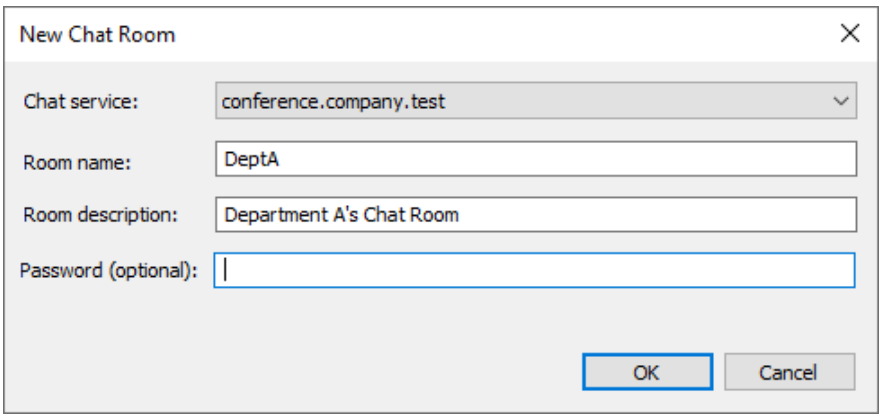
Configure Persistent Chat Rooms

Click this button to open the Group Chat Rooms dialog. Ordinarily, when a user creates a chat room it will disappear when the last person leaves the room, but you can use these options to create persistent chat rooms that will remain when empty. You can also delete rooms and convert existing, temporary rooms to persistent ones.



Select chat service
Select the chat service to display that domain's chat rooms.

New
Click this button to add a persistent chat room.



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Select chat service
Select the chat service for the room.

Room name
Type a name for the chat room, without any spaces.

Room description
Include a description of the room here. Users will see this when selecting a room to join.

Password (optional)
If you wish to require a password in order to join the chat, enter the password here.

Delete
If you wish to remove a room, select the room and click this button to delete it.

Make Persistent
When a temporary chat room is in the list, select the room and click this button if you wish to make it persistent.

See:

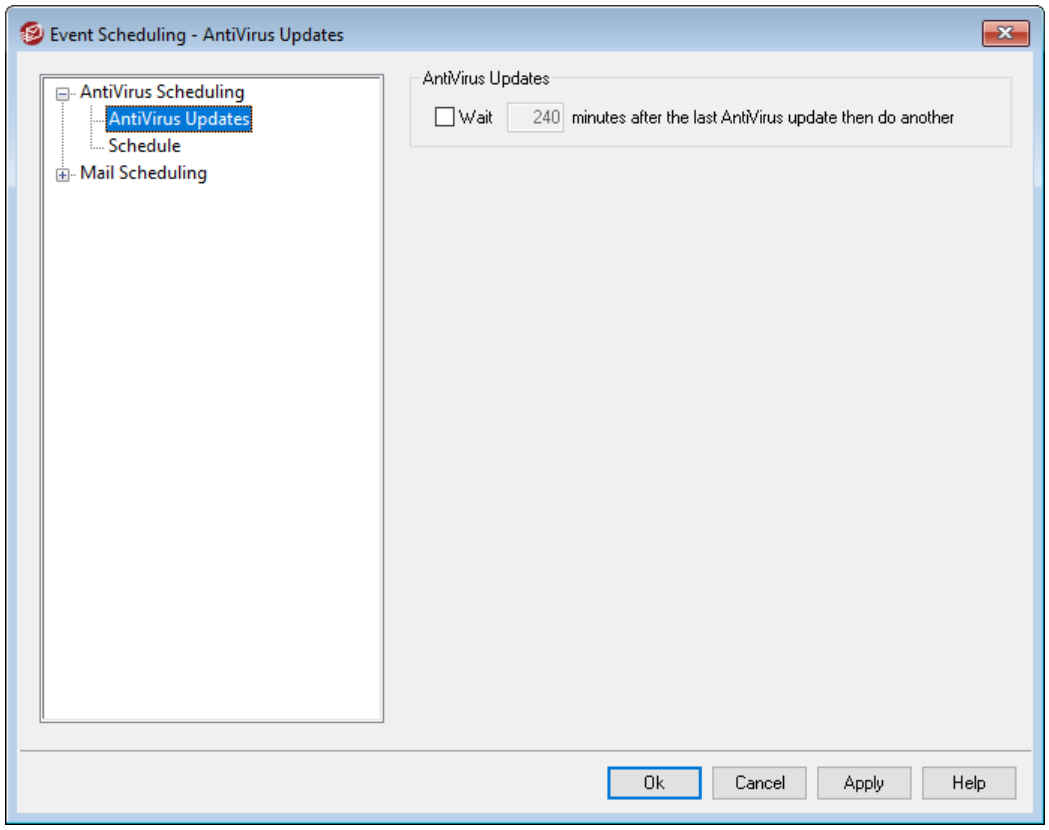
Webmail » MDIM 320

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.7 Event Scheduling

3.7.1 AntiVirus Scheduling

3.7.1.1 AntiVirus Updates



AntiVirus Updates

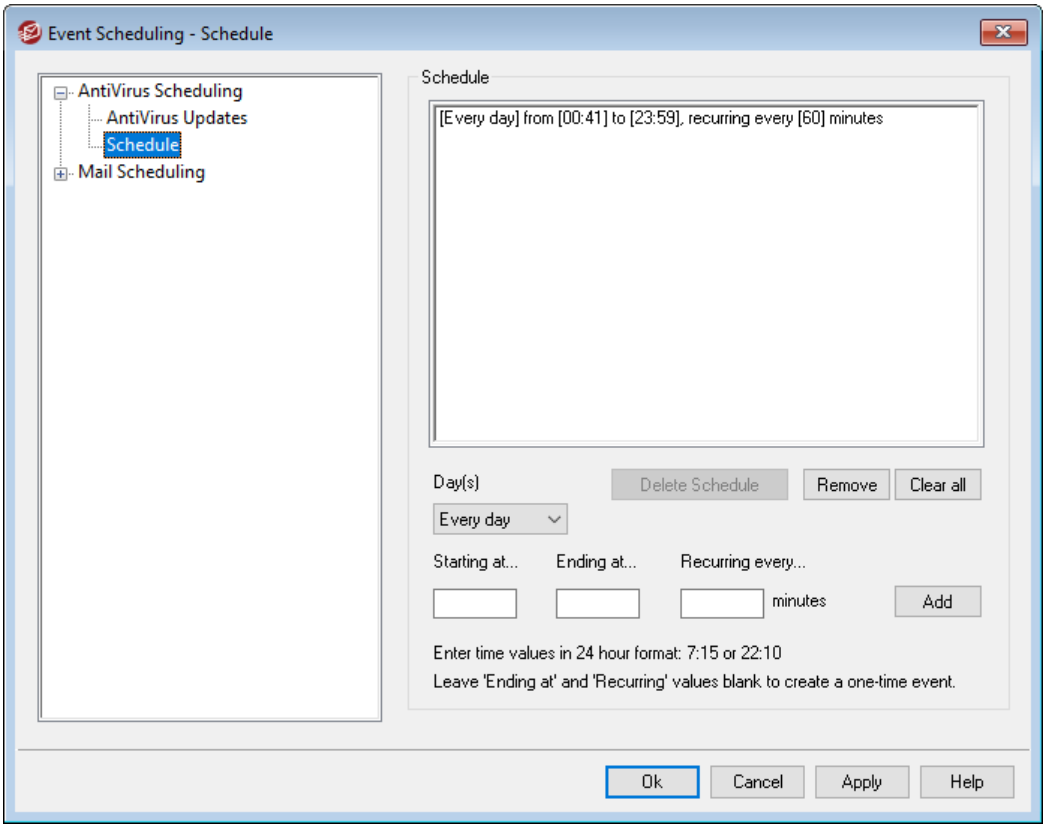
Wait XX minutes after the last AntiVirus update then do another
Click this checkbox and specify the number of minutes that you want AntiVirus to wait before checking for new virus signature updates. Note, this is actually the number of minutes that AntiVirus will *attempt* to wait after the last time you checked for an update, whether the update was triggered by the scheduler or manually. The scheduler and manually triggered updates are given precedence over this setting and will therefore reset this counter if an AntiVirus update event is triggered by one of those other methods. Thus, for example, if you have this option set to check for updates every 240 minutes and you manually check for an update after 100 minutes, this counter will be reset to 240.

See:

AntiVirus Update Schedule 370
AntiVirus 653
AntiVirus Updater 657

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.7.1.2 Schedule



Use the AntiVirus Update Schedule to designate specific times to check for AntiVirus updates. The schedule is located at: Setup » Event Scheduling » AntiVirus Updates » Schedule.

Schedule

Remove
To remove an event from the list, select the entry and then click this button.

Clear all
This button removes all entries from the schedule.

Creating Schedule Events

Day(s)
When creating a new event for the schedule, first select the day or days on which this scheduled update check event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Starting at...
Enter the time that you wish the update check to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending at...* and *Recurring every...* options blank).

Ending at...
Enter the time that you wish the update check event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

Recurring every [xx] minutes
This is the time interval at which AntiVirus will check for updates between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

Add
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

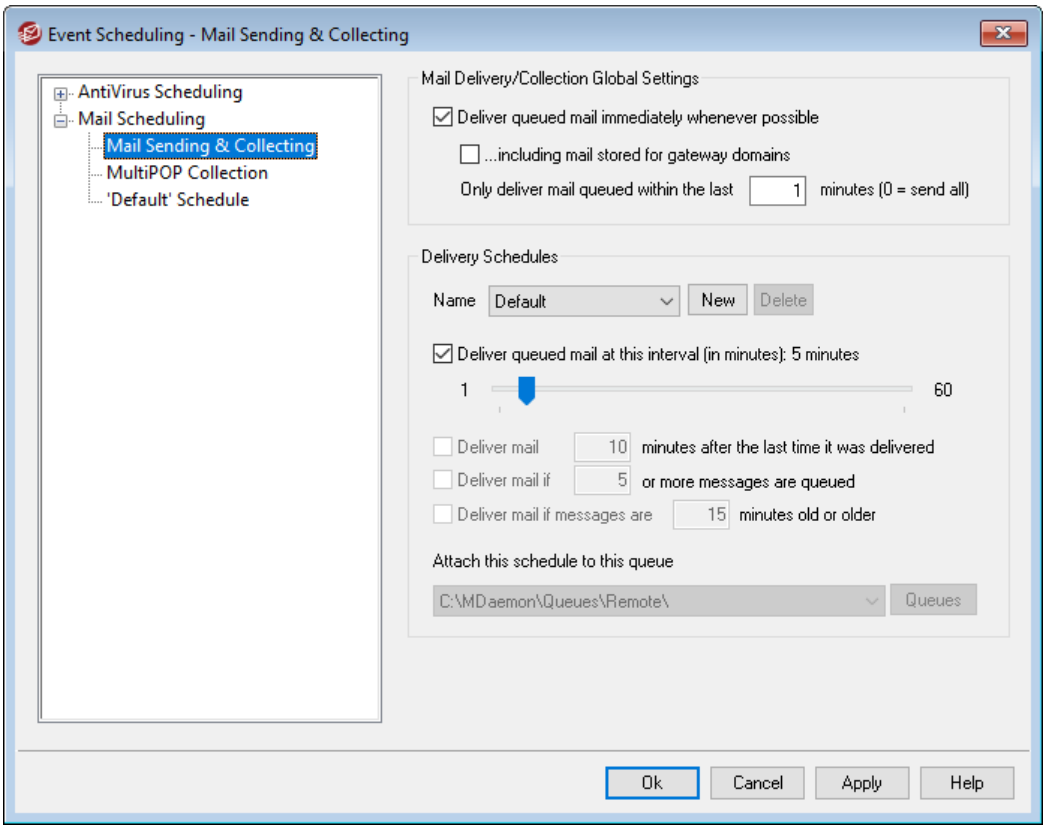
See:

AntiVirus Updates
AntiVirus 653
AntiVirus Updater 657

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.7.2 Mail Scheduling

3.7.2.1 Mail Sending & Collecting



Click Setup » Event Scheduling to open MDaemon's Event Scheduler. Using this screen you can schedule MDaemon's Remote mail processing events as extensively or as simply as you prefer. You can use a counter to process mail at regular intervals, or you can schedule exact times for mail delivery and collection using the Mail Schedule 377 screens. You can also set conditions that will trigger mail processing at unscheduled times such as when a certain number of messages are waiting to be delivered, or when a message has been waiting a specified amount of time. Further, you can create custom schedules that you can assign to custom remote mail queues. Custom schedules make it possible for you to set different schedules for different types of messages. For example, you could create schedules for large messages, mailing list messages, certain domains, and so on.

Use the AntiVirus Updates 369 section of the Event Scheduler to schedule how often MDaemon will check for AntiVirus 630 updates.

Mail Delivery/Collection Global Settings

Deliver queued mail immediately whenever possible
When this option is enabled and a message arrives and is queued for remote delivery, rather than waiting for the next scheduled processing interval or some

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

other event to trigger mail processing, MDaemon will immediately process and deliver all remote mail that has been queued within the number of minutes designated in the *Only deliver mail queued within the last [xx] minutes* option below.

...including mail stored for gateway domains
Click this check box if you also want messages for Domain Gateways to be delivered immediately. However, this only applies to gateways with the *Deliver stored messages each time MDaemon processes remote mail* option enabled on the Gateway 247 screen of the Gateway Editor.

Only deliver mail queued within the last [xx] minutes (0=send all)
This option governs how recently messages must have been queued before the *Deliver queued mail immediately whenever possible* option above will spool them for delivery. When that option triggers remote mail processing, instead of attempting to deliver everything in the queue, MDaemon will process only those messages that were queued within the designated number of minutes. The entire queue will still be processed, however, when the *Process...queue* toolbar button is pressed or when any other normal scheduling event triggers remote mail processing. By default, this option is set to one minute. You can set it to "0" if you wish to process the entire queue every time remote mail processing is triggered, but that is not recommended since it is much less efficient.

The above options only apply to the Default schedule. They are unavailable for custom schedules (see the *Name...* option below).

Delivery Schedules

Name...
Use this drop-down list box to select a schedule to edit. The Default schedule will always be used for the regular, remote mail queue and for DomainPOP and MultiPOP collected mail. For configurations using dialup services, the Default schedule will also be used for LAN Domains, which are remote domains that you have designated as residing on your local area network and therefore do not require RAS dialup. Other schedules can be assigned to custom remote mail queues, and messages can be routed to those custom queues 861 automatically by using the Content Filter 631. When you are finished editing a schedule's options, click OK or select another schedule for editing. If you make changes to a schedule and then select another schedule, a confirmation box will open asking you whether you wish to save or discard the currently selected schedule's changes before switching to the other schedule.

New
Click this option to create a new schedule. A box will open so that you can designate a name for it. After the schedule's name is designated, a corresponding Mail Schedule 377 screen will be created for it in the menu on the left. Use that screen to assign times to that schedule.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete
To delete a custom schedule, first select it in the *Name...* drop-down list and then click *Delete*. A confirmation box will open asking you if you are sure you wish to delete it. Deleting a custom schedule will not delete any custom remote queue or content filter rules associated with it. However, if you delete a custom queue then any schedules associated with that queue will also be deleted, and all associated content filter rules as well.

Deliver queued mail at this interval (in minutes)
Click the check box and slide this bar left or right to specify the time interval between mail processing sessions. It can be configured to count down from a range of 1 to 60 minutes. After that amount of time, MDaemon will process remote mail before beginning the countdown again. When this check box is cleared, *Remote Mail* processing intervals will be determined by the other scheduling options.

Deliver mail [xx] minutes after the last time it was delivered
Use this option when you want a remote mail processing session to occur at a regular time interval after the last session occurred, regardless of the trigger that initiated the session. Unlike the rigidly fixed intervals used when setting up specific times or when using the *Deliver queued mail at this interval* slide bar, this option's time interval will reset each time mail is processed.

Deliver mail if [xx] or more messages are queued
When this option is enabled, MDaemon will trigger a mail session whenever the number of messages waiting in the remote queue meets or exceeds the number that you specify here. These mail sessions are in addition to any other normally scheduled sessions.

Deliver mail if messages are [xx] minutes old or older
When this box is checked, MDaemon will trigger a mail session whenever a message has been waiting in the queue for the number of minutes specified. These sessions are in addition to any other normally scheduled sessions.

Queues

Attach this schedule to this queue
Use this option to associate the selected schedule with a specific custom remote mail queue. You can then use the content filter to create rules that will place certain messages in that queue. For example, if wanted to schedule mailing list messages destined for remote addresses to be delivered at some specific time, then you could create a custom queue for those messages, create a rule to put all of them into your custom queue, and then create a custom schedule and assign it to that queue.

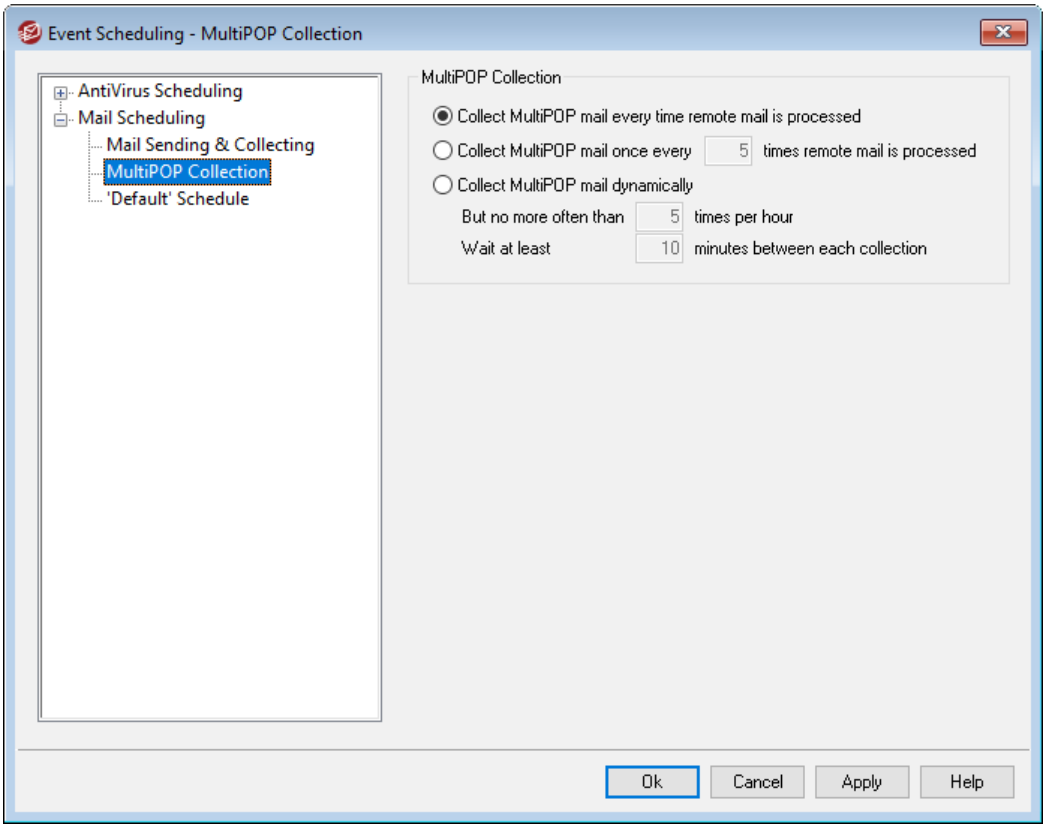
Queues
Click the button to open the Custom Queues 861 screen, on which you can create custom remote queues to use with the Event Scheduler.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Mail Schedule 377
AntiVirus Updates 369

3.7.2.2 MultiPOP Collection



MultiPOP Collection

Collect MultiPOP mail every time remote mail is processed
Choose this option if you want MDaemon to collect all MultiPOP 723 mail every time that remote mail is processed.

Collect MultiPOP mail once every XX times remote mail is processed
Choose this option and specify a numeral in the box if you want MultiPOP mail to be collected less often than remote mail is processed. The numeral denotes how many times remote mail will be processed before MultiPOP mail will be collected.

Collect MultiPOP mail dynamically
Choose this option if you wish to collect MultiPOP messages dynamically. Ordinarily, MultiPOP is collected for all users at the same time at each remote mail processing interval, or at every *x* number of intervals. When collected dynamically, MultiPOP messages are collected for each individual user when that user checks his or her

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

local mail via POP, IMAP, or Webmail rather than for all users at once. However, because MultiPOP collection is triggered by a user checking his email, any new MultiPOP messages collected will not be visible to the user until he checks his mail *again*. Thus, he would need to check his mail twice in order to see new MultiPOP messages. The first time to trigger MultiPOP and a second time to see the mail that was collected.

But no more often than XX times per hour
In order to reduce the load that extensive use of MultiPOP can potentially place on your MDaemon, you can use this control to specify a maximum number of times per hour that MultiPOP can be collected for each user.

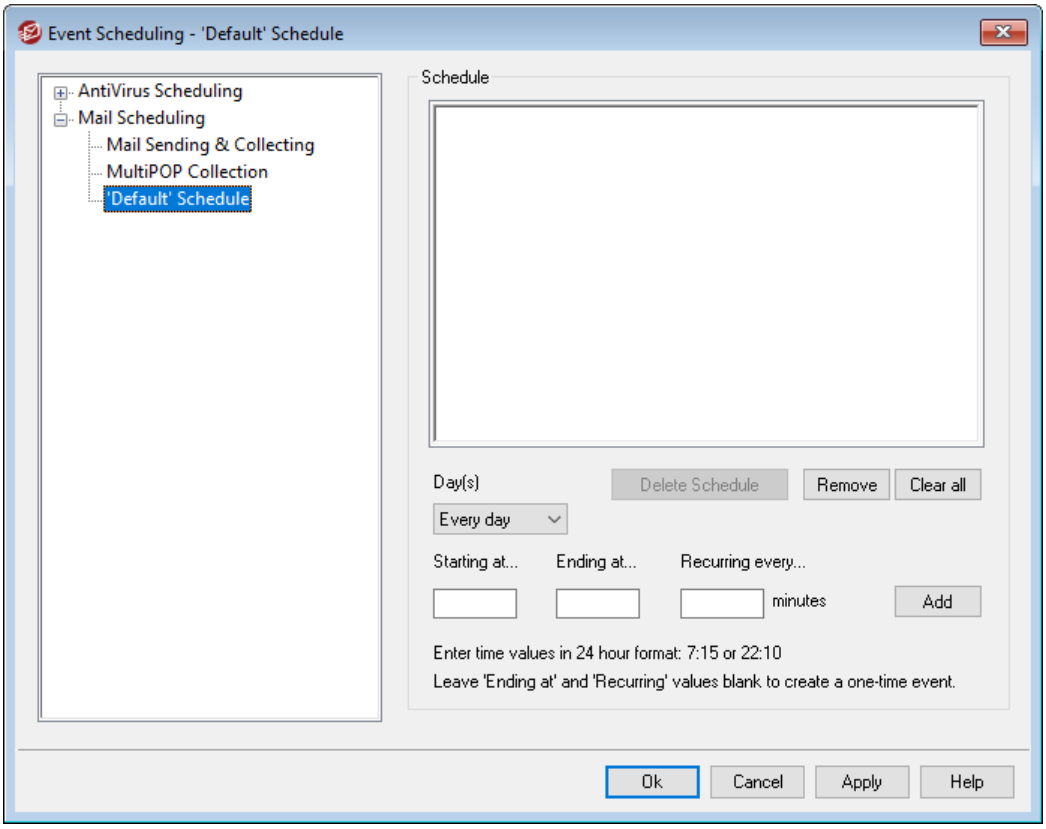
Wait at least XX minutes between each collection
This option can help to reduce the load on the mail server by limiting how frequently MultiPOP messages can be collected by each user. It will restrict MultiPOP mail collection to once every so many minutes per user. Specify the number of minutes that you wish to require the user to wait before being allowed to check MultiPOP again.

See:

MultiPOP 137
Account Editor | MultiPOP 723

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.7.2.3 Mail Schedule



Each Mail Schedule corresponds to the schedule of the same name listed in the *Name* drop-down list on the Mail Sending & Collecting 372 screen. Use each Mail Schedule to designate the specific times that remote mail processing will occur for that schedule. Mail Schedules are located at: Setup » Event Scheduling » Mail Scheduling » 'ScheduleName' Schedule.

Schedule

Delete Schedule
This button will delete the custom Mail Schedule. The schedule will be deleted and its entry will be removed from the *Name* drop-down list on the Mail Sending & Collecting 372 screen. After you click this button, a confirmation box will open asking if you are sure you want to delete the schedule. This option is only available for custom schedules — the Default Schedule cannot be deleted.

Remove

To remove an entry from the list, select the entry and then click this button.

Clear all
This button removes all entries from the schedule.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Creating Schedule Events

Day(s)
When creating a new event for the schedule, first select the day or days on which this scheduling event will occur. You can select: every day, weekdays (Monday thru Friday), weekends (Saturday and Sunday), or specific days of the week.

Starting at...
Enter the time that you wish the event to start. The time value must be in 24 hour format, from 00:00 to 23:59. If you wish this to be a single event rather than recurring event, this is the only time value that you will enter (leave the *Ending at...* and *Recurring every...* options blank).

Ending at...
Enter the time that you wish the event to end. The time value must be in 24 hour format, from 00:01 to 23:59, and it must be greater than the *Starting at...* value. For example, if the *Starting at...* value were "10:00" then this value could be from "10:01" to "23:59". Leave this option blank if you wish it to be a single event rather than recurring event.

Recurring every [xx] minutes
This is the time interval at which mail will be processed between the designated *Starting at...* and *Ending at...* times. Leave this option blank if you wish it to be a single event rather than recurring event.

Add
Once you have designated the *Day(s)* and *Starting at...* time, and the optional *Ending at...* time and *Recurring every...* value, click this button to add the event to the schedule.

Depending on your needs, it may be sufficient to use the simple scheduling options on the Mail Sending & Collecting 372 screen to control mail processing intervals. For example, it is pointless to make a specific schedule with events for every minute of every day when you can simply set the slider bar on Mail Sending & Collecting to one minute intervals and accomplish the same thing. On the other hand, if you want the processing intervals to be more than an hour apart, or only on certain days, then you can use some combination of the scheduling options and specific times.

See:

Mail Sending & Collecting 372
AntiVirus Updates 369
AntiSpam Updates 679

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8 MDaemon Connector

Support for *MDaemon Connector* (MC) is a licensed feature available from MDaemon Technologies. MC makes it possible for any of your users who wish to use Microsoft Outlook as their preferred email client to do so when MC is installed on their computer. It provides groupware and collaboration functionality by connecting a user's Outlook client to the MDaemon server, to use Outlook's email, calendar with free/busy scheduling, address book, distribution lists, tasks, and notes.

When you have activated support for MC, the MDaemon Connector screens will be available from MDaemon's menu bar, located at: `Setup » MDaemon Connector`. This dialog is used for enabling and configuring MC and for authorizing specific accounts to use it.

For more information, or to acquire the MDaemon Connector feature, visit the MDaemon Connector page at www.mdaemon.com.

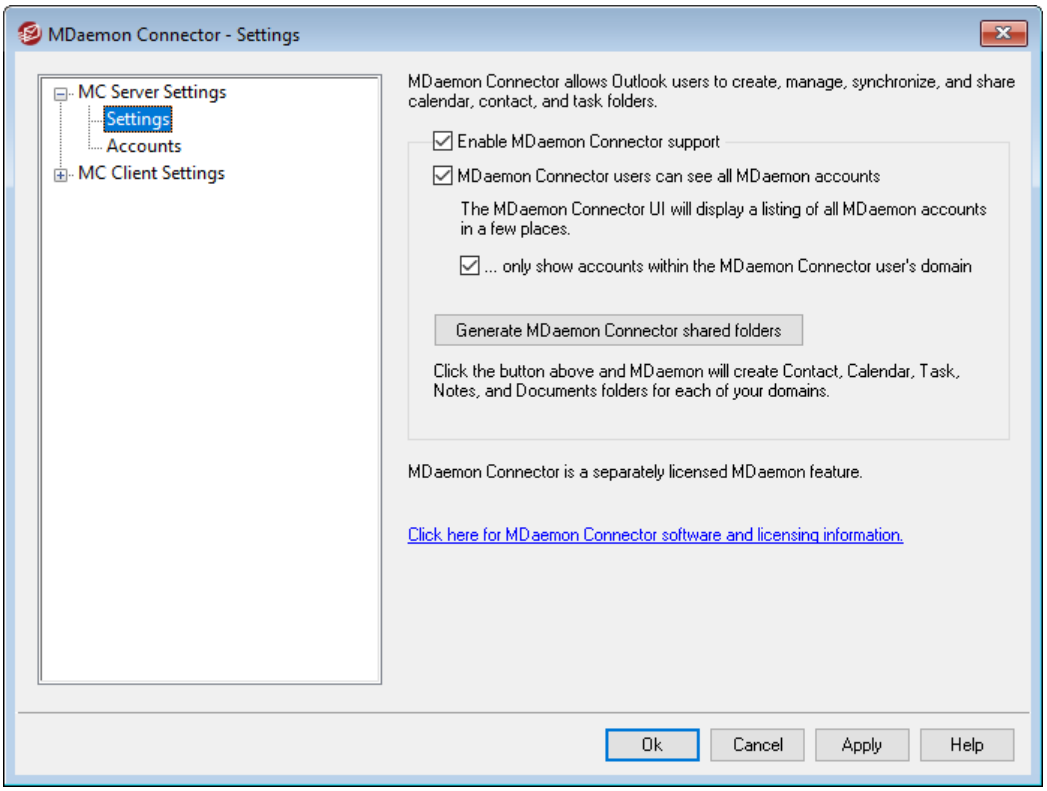
See:

MC Server Settings » Settings 380
MC Server Settings » Accounts 381
MC Client Settings 382

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.1 MC Server Settings

3.8.1.1 Settings



MDaemon Connector

Enable MDaemon Connector support
Click this checkbox to enable support for MDaemon Connector (MC). Your users will not be able to utilize MC's features unless this option is enabled.

MDaemon Connector users can see all MDaemon accounts
Click this option if you want all MDaemon accounts that have been authorized to connect via MC to be visible on the *Permissions* list that appears in MDaemon Connector on the users' clients. From that list, MC users can choose the accounts to which they wish to grant permission to share their Outlook items. When this option in disabled, MDaemon Connector's *Permissions* list will be blank and the users will have to enter email addresses manually. Only addresses belonging to accounts authorized to connect via MC will be able to share the Outlook items. If a user enters an address that is not authorized then the items will simply not be shared with that address unless it is authorized to connect via MC at some later time.

...only show accounts within the MDaemon Connector user's domain
This option is only available when the *MDaemon Connector users can see all MDaemon accounts* option above is enabled. Click this checkbox if you want only users who are authorized to connect via MC, and who belong to same domain, to appear on the *Permissions* list in MDaemon Connector. Accounts belonging to

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

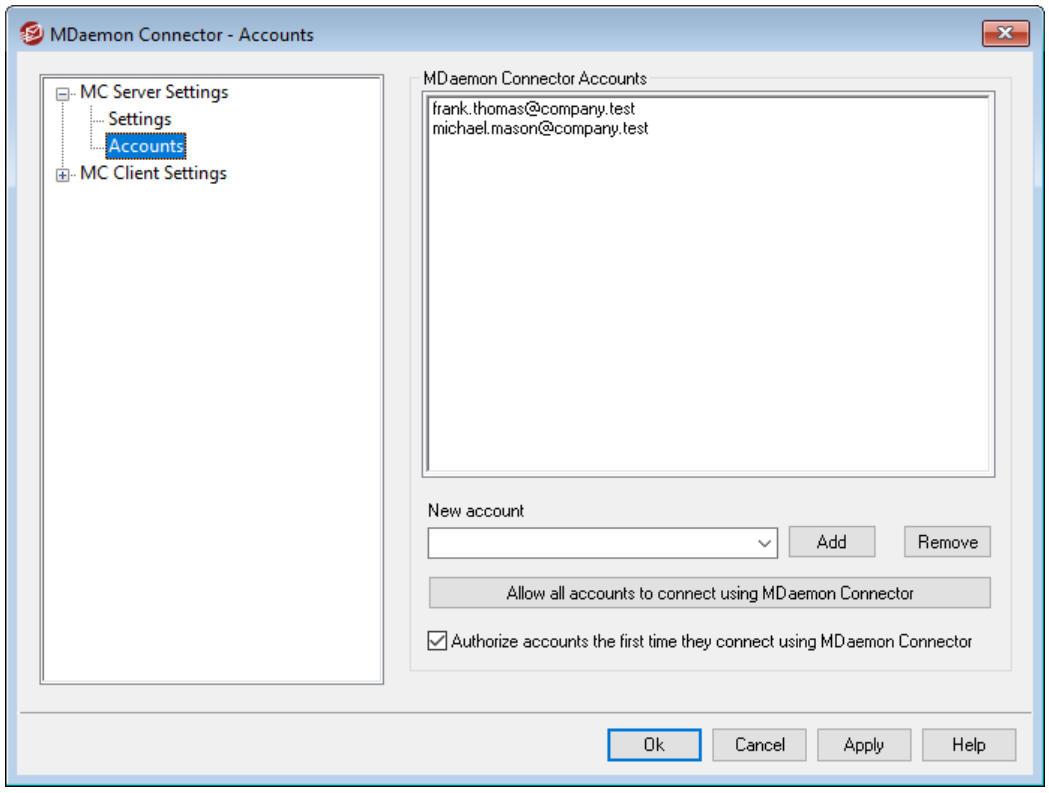
different domains will not be listed even if they are authorized to connect via MC.

Generate MDaemon Connector shared folders
Click this button to generate a set of MC folders for each domain. It will generate the following folders: Contacts, Appointment, Journal, Tasks, and Notes.

See:

MC Server Settings » Accounts 381
MC Client Settings 382

3.8.1.2 Accounts



MDaemon Connector Accounts

This is the list of MDaemon accounts who are authorized to share their Outlook folders, Calendars, Contacts, Notes, and so on via MDaemon Connector. You can add accounts to the list by using the options outlined below.

New account
To add an MDaemon account to the list of authorized MDaemon Connector Accounts, select the desired account from this drop-down list and then click *Add*. To remove an account, select the account and then click *Remove*.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

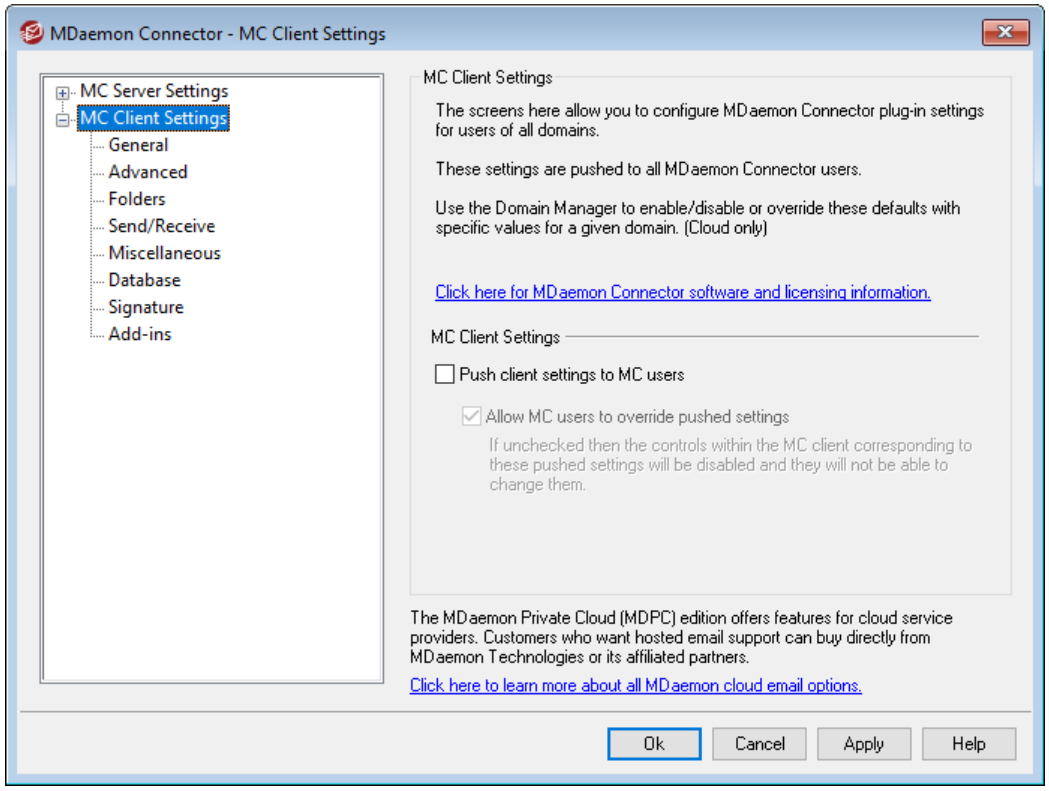
Allow all accounts to connect using MDaemon Connector
To instantly authorize all MDaemon accounts to connect via MDaemon Connector, click this button and all MDaemon accounts will be added to the *MDaemon Connector Users* list.

Authorize accounts the first time they connect using MDaemon Connector
Click this checkbox if you want individual accounts to be added to the *MDaemon Connector Accounts* list the first time each connects using MDaemon Connector. **Note:** if you enable this option then you have in effect authorized all MDaemon accounts to use MDaemon Connector. The accounts simply will not be added to the list until the first time each one uses it.

See:

MC Server Settings » Settings 380
MC Client Settings 382

3.8.2 MC Client Settings



Use the MC Client Settings dialog to centrally manage the client settings of your MDaemon Connector (MC) users. Configure each screen with your desired client settings and MDaemon will push those settings to the corresponding client screens as necessary, each time an MC user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

connected and received them. If the option below to "*Allow MC users to override pushed settings*" is enabled, users can override any pushed settings on their individual clients. If that option is disabled, then all of the client screens are locked; MC users can make no changes.

To allow for certain settings that must be different for each user or domain, MC Client Settings supports macros such as `$USERNAME$`, `$EMAIL$`, and `$DOMAIN$`. These macros will be converted to data specific to the user or domain when pushing settings to a client. Take care not to place any static values in any fields that should use a macro, such as putting something like "Frank Thomas" in the Your Name field. To do so would cause every MC user who connects to MDaemon to have his or her name set to "Frank Thomas." For your convenience there is a Macro Reference button on the General 384 screen, which displays a simple list of the supported macros.

For those using MDaemon Private Cloud (MDPC), there is another MC Client Settings dialog on the Domain Manager 174, for controlling the MDaemon Connector client settings on a per domain basis.

This feature is disabled by default and is only supported in MDaemon Connector client version 4.0.0 or higher.

MC Client Settings

Push client settings to MC users
Enable this option if you wish to push the preconfigured settings on the MC Client Settings screens to your MC users whenever they connect. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them. This option is disabled by default.

Allow MC users to override pushed settings
If this option is enabled, users can override any of the pushed settings on their individual clients. If it is disabled, all of the client screens are locked; MDaemon Connector users can make no changes.

Allowing users to override pushed settings will not prevent the server from pushing future changes to the clients. For example, if a user changes one of his MDaemon Connector settings and then the administrator makes some change to one of the MC Client Settings screens on the server, all of the MC Client Settings will be pushed to that user's client the next time it connects to the server. Therefore even the setting that the user had previously overridden will be changed to match the settings on the server.

Automatically Discovering MC Settings

When first configuring MDaemon Connector on the client, users can click the "*Test & Get Account Settings*" button on the General screen after entering their *User Name* and *Password*. This causes MDaemon Connector to attempt to validate the credentials and automatically retrieve the Server Information for the account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

To connect to the server, first the client will try common FQDN values. For IMAP, it tries to authenticate to `mail.<domain>` (e.g. `mail.example.com`) using the dedicated SSL port, then the non-SSL port with TLS. If that doesn't succeed then it will repeat the same process for `imap.<domain>`, then `<domain>`, and finally, `imap.mail.<domain>`. If all attempts fail then unencrypted sign-in is attempted for those same locations.

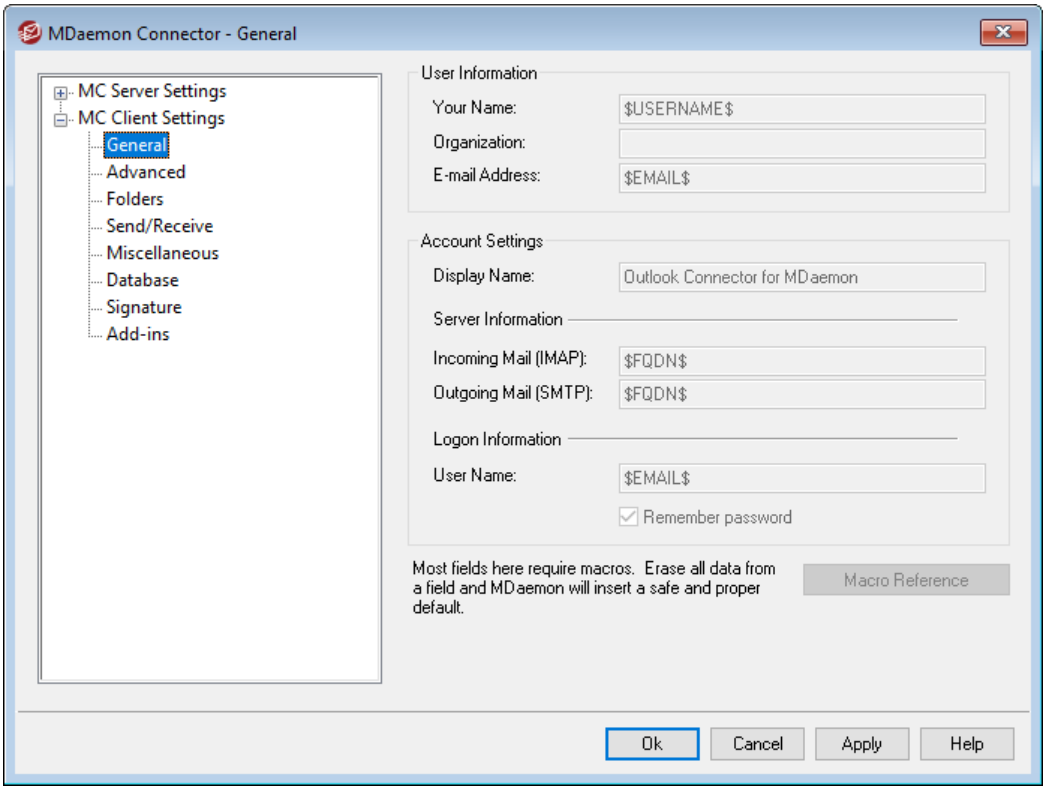
For SMTP, it tries `mail.<domain>` using port 587, 25, and then 465, first using SSL and then TLS. This is repeated for `smtp.<domain>`, `<domain>`, and then `smtp.mail.<domain>`. If all attempts fail then unencrypted sign-in is attempted for those same locations.

If MDaemon Connector is able to successfully authenticate then the incoming and outgoing server information along with the SSL/TLS information is configured automatically.

See:

MC Server Settings » Settings 380
MC Server Settings » Accounts 381
MC Client Settings » General 384

3.8.2.1 General



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them. Most of the fields on this screen should contain macros rather than static values. See Macro Reference 386 below.

User Information

Your Name
By default this option uses the $USERNAME$ macro, which inserts the user's first and last name. This appears in the From header of the user's messages.

Organization
This is an optional space for your business or organization name.

E-mail Address
By default this option uses the $EMAIL$ macro, which inserts the user's email address. This appears in the From header of the user's messages.

Account Settings

Display Name
This name is displayed in Outlook so that the user can identify which account he is using. This is useful for users who have multiple accounts in their profile. Only the user sees this information. This is set to "MDaemon Connector" by default.

Server Information

Incoming Mail (IMAP)
This is the server the MC clients will access to collect and manage each user's email. This set to $FQDN$ by default.

Outgoing Mail (SMTP)
This is the server to which the MC clients will connect to send your users' outgoing messages. Frequently this is the same as the Incoming Mail (IMAP) server above. This set to $FQDN$ by default.

Logon Information

User Name
This is the user name needed to access and manage each user's MDaemon email account. This is typically the same is the *E-mail Address* above. By default this is set to $EMAIL$.

Remember password
By default MDaemon Connector clients are set to save the user password, so that when Outlook is started it will automatically sign in to the email account without asking for credentials. Disable this option if you wish to require users to enter their password when starting Outlook.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Macro Reference

To allow for certain settings that must be different for each user or domain, MC Client Settings supports macros such as $USERNAME$, $EMAIL$, and $DOMAIN$. These macros will be converted to data specific to the user or domain when pushing settings to a client. Take care not to place any static values in any fields that should use a macro, such as putting something like "Frank Thomas" in the *Your Name* field. To do so would cause every MC user who connects to MDaemon, to have his or her name set to "Frank Thomas." Click the Macro Reference button to view the list of available macros:

$USERNAME$	This macro inserts the value of the "*First and last name*" option under the user's Account Details 697 screen. It is equivalent to: "$USERFIRSTNAME$ $USERLASTNAME$"
$EMAIL$	Inserts the user's email address. This is equivalent to: $MAILBOX$@$DOMAIN$.
$MAILBOX$	This macro inserts the account's Mailbox name 697.
$USERFIRSTNAME$	This macro resolves to the first name of the account holder.
$USERFIRSTNAMELC$	This macro resolves to the first name of the account holder, in lower case letters.
$USERLASTNAME$	This macro resolves to the last name of the account holder.
$USERLASTNAMELC$	This macro resolves to the last name of the account holder, in lower case letters.
$USERFIRSTINITIAL$	This macro resolves to the first letter of the account holder's first name.
$USERFIRSTINITIALLC$	This macro resolves to the first letter of the account holder's first name, in lower case.
$USERLASTINITIAL$	This macro resolves to the first letter of the account holder's last name.
$USERLASTINITIALLC$	This macro resolves to the first letter of the account holder's last name, in lower case.
$MAILBOXFIRSTCHARSn$	Where "n" is a number between 1 and 10. This will expand to the first "n" characters of the mailbox name.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

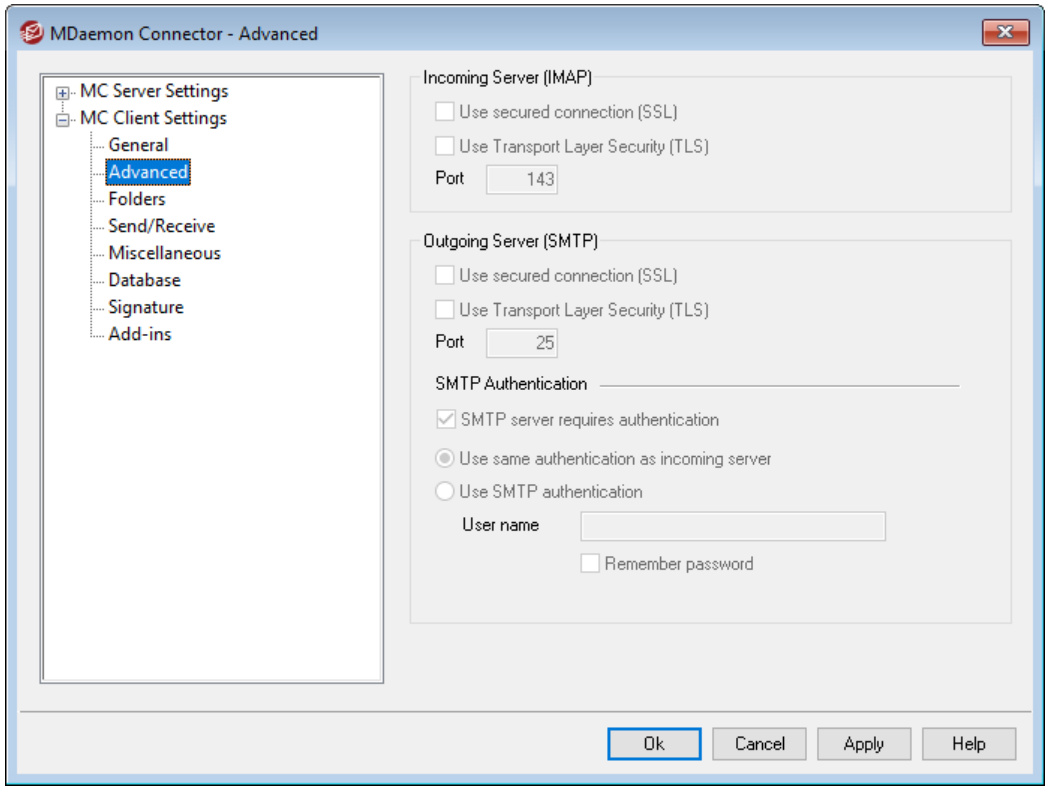
$DOMAIN$	Inserts the account's Mailbox domain 697.
$DOMAINIP$	This macro resolves to the IPv4 address 177 associated with the domain to which the account belongs.
$DOMAINIP6$	This macro resolves to the IPv6 address 177 associated with the domain to which the account belongs.
$FQDN$	Inserts the fully qualified domain name, or SMTP host name 177, of the domain to which the account belongs.
$PRIMARYDOMAIN$	This macro resolves to MDaemon's default domain 174 name.
$PRIMARYIP$	This macro resolves to the IPv4 address 177 associated with MDaemon's default domain 174.
$PRIMARYIP6$	This macro resolves to the IPv6 address 177 associated with MDaemon's default domain 174.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.2.2 Advanced



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them.

Incoming Server (IMAP)

Use secured connection (SSL)
Check this box if you want clients to use a secure SSL connection when connecting to the Incoming Mail (IMAP) server. Enabling this option will automatically change the Port setting to "993," which is the default SSL port.

Use Transport Layer Security (TLS)
Check this box if you want clients to use a secure TLS connection when connecting to the Incoming Mail (IMAP) server.

Port
This is the port on which the MC clients will connect to your Incoming Mail (IMAP) server. By default this is set to 143 for IMAP connections or 993 for SSL encrypted IMAP connections.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Outgoing Server (SMTP)

Use secured connection (SSL)
Check this box if you want MC clients to use a secure SSL connection when connecting to the Outgoing Mail (SMTP) server. Enabling this option will automatically change the Port setting to "465," which is the default SSL port.

Use Transport Layer Security (TLS)
Check this box if you want MC clients to use a secure TLS connection when connecting to the Outgoing Mail (SMTP) server.

Port
This is the port on which the MC clients will connect to your Outgoing Mail (SMTP) server. By default this is set to 25 for SMTP connections or 465 for SSL encrypted SMTP connections.

SMTP Authentication

SMTP server requires authentication
By default users must use valid login credentials to authenticate themselves when connecting to the Outgoing Server (SMTP) to send an email message.

Use Same Authentication as Incoming Server
By default MC clients will authenticate themselves using the same login credentials for the Outgoing Mail (SMTP) server that they use for the Incoming Mail (IMAP) server.

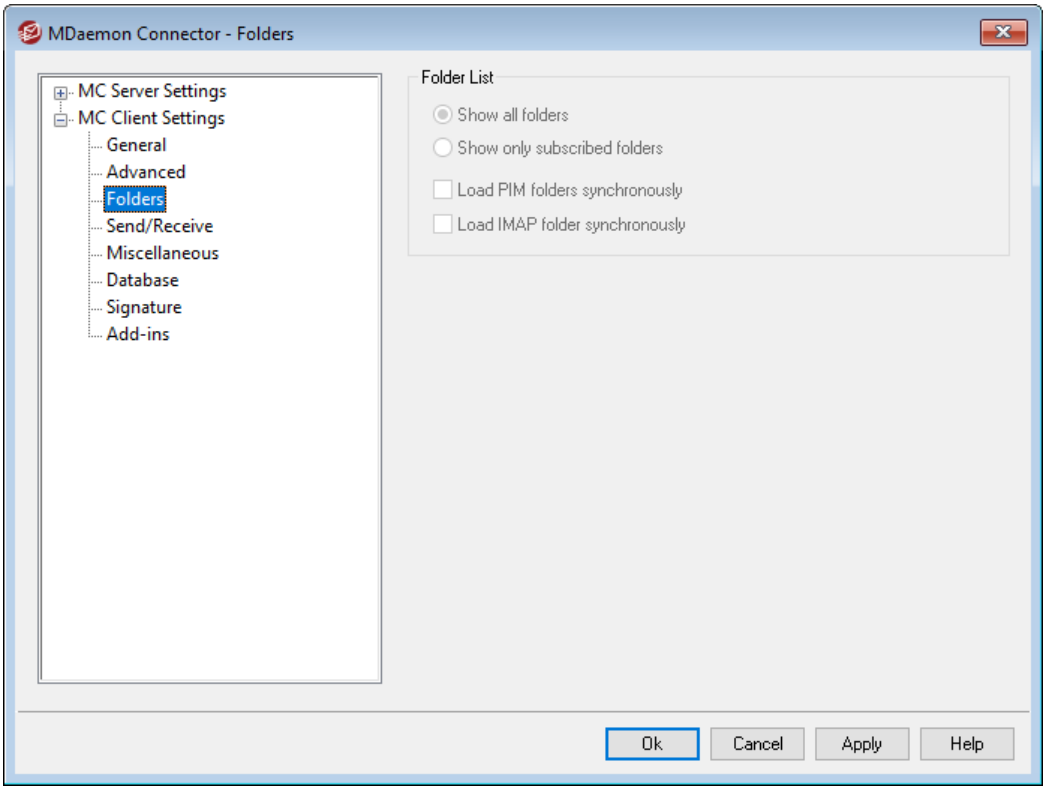
Use SMTP Authentication
Use this option if you wish to require your MC users to use different authentication credentials when sending messages, such as may be necessary when using a different email server for outgoing mail.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.2.3 Folders



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them.

Folder List

Show All Folders
By default the folder list in Outlook will display all of the folders to which the MDaemon Connector user has access on the mail server.

Show Only Subscribed Folders
Select this option if you want the Outlook folder list to display only those folders to which the user has subscribed.

Load PIM Folders Synchronously
In most cases this option should be left unchecked, which means that an MDaemon Connector user can continue to use Outlook while MDaemon Connector loads the contents of PIM folders (i.e. non-mail folders, such as: Contacts, Calendars, and Tasks). If you check this box then Outlook will effectively be blocked from use until all of the data has been loaded. Ordinarily this option may only be needed when the user has 3rd party applications attempting to access PIM folder contents.

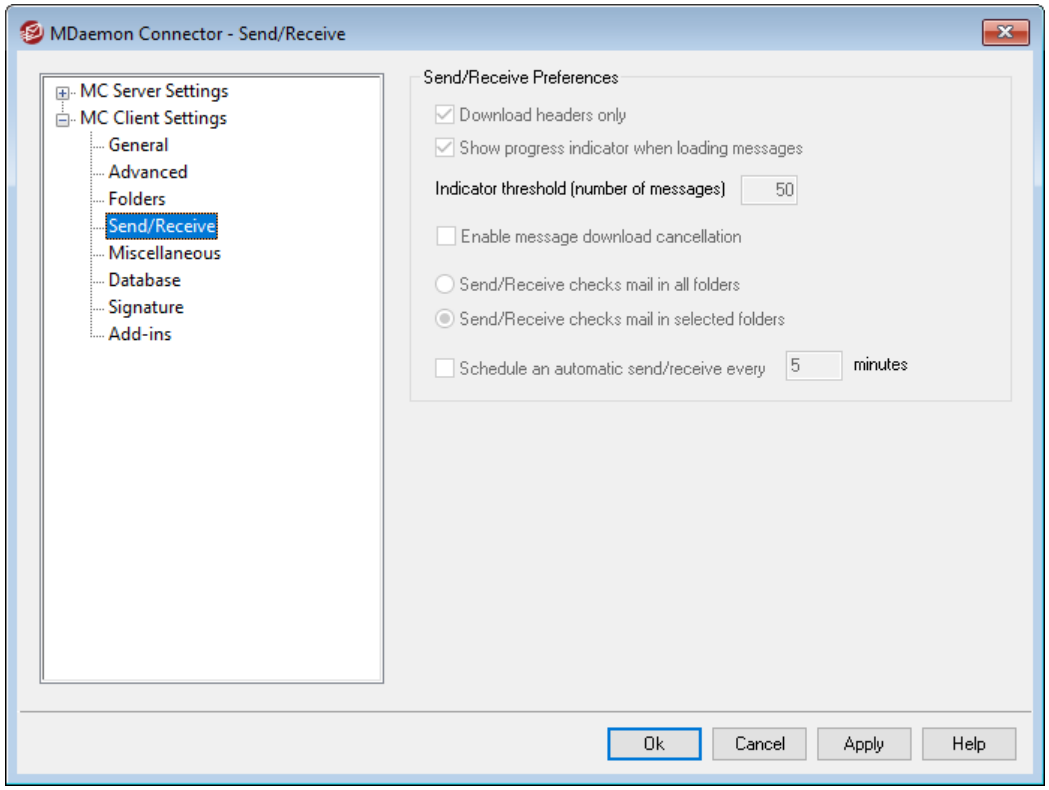
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Load IMAP Folders Synchronously
In most cases this option should be left unchecked, which means that an MDaemon Connector user can continue to use Outlook while MDaemon Connector loads the contents of the user's IMAP mail folders. If you check this box then Outlook will effectively be blocked from use until all of the data has been loaded. Ordinarily this option may only be needed when the user has 3rd party applications attempting to access mail folder contents.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

3.8.2.4 Send/Receive



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send/Receive Preferences

Download Headers Only
By default when MDaemon Connector does a Send/Receive and finds new messages, it will only download the message headers (i.e. To, From, Subject, and the like) for display in the message list. The full message isn't downloaded until it is viewed.

Show progress indicator when loading messages
MDaemon Connector displays a progress indicator when downloading a large number of messages. Clear this checkbox if you do not wish to display the progress indicator.

Indicator threshold (number of messages)
When the *Show progress indicator...* option is enabled, the Progress Indicator is displayed when downloading this number of messages or more.

Enable message download cancellation
Check this box if you want your MDaemon Connector users to be able to cancel the download while MDaemon Connector is downloading a large message.

Send/Receive checks mail in all folders
Select this option if you want MDaemon Connector to check every mail folder for new messages when it performs a Send/Receive action for the user's account.

Send/Receive checks mail in selected folders
Select this option if you want MDaemon Connector to check the user's specified folders for new messages when performing a Send/Receive action on the account.

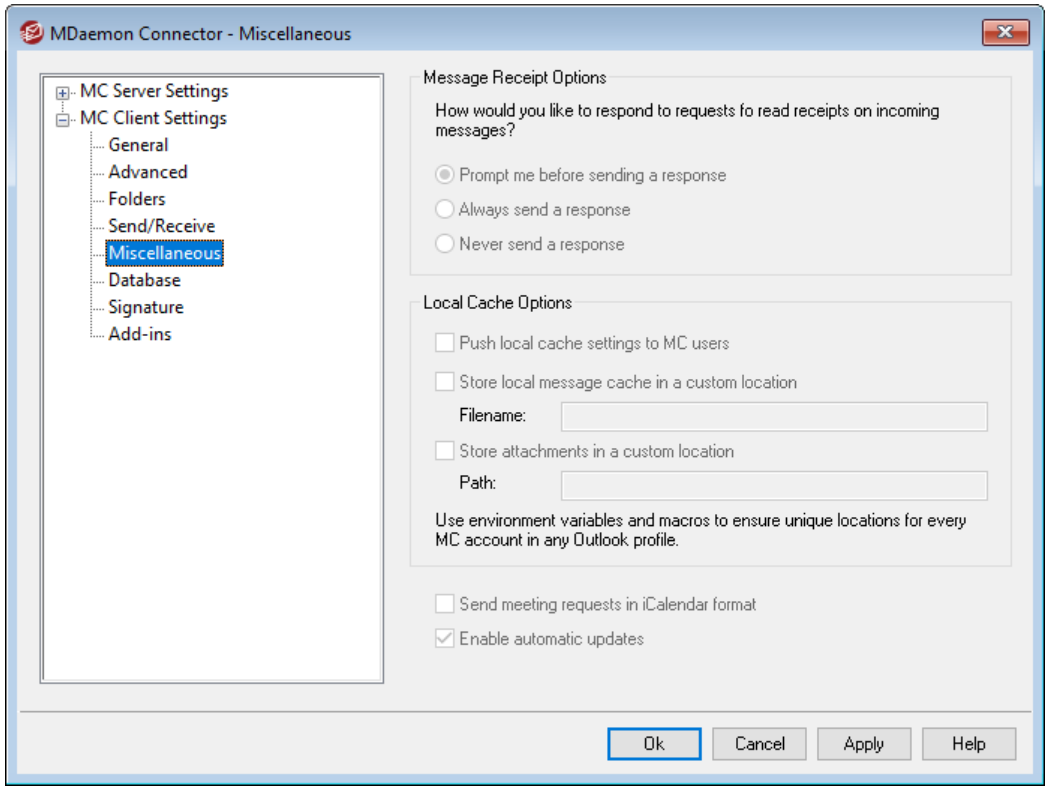
Schedule an automatic send/receive every [xx] minutes
Use this option if you wish to do a send/receive at a designated interval.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.2.5 Miscellaneous



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them.

Manage Receipt Options

Sometimes incoming messages contain a special header for requesting that an automated message be sent back to the sender to let him or her know when you read the message. Set this option to specify how you want MDaemon Connector to handle messages that ask for read confirmations.

Prompt me before sending a response
Choose this option if you want users to be asked whether or not to send the read confirmation message whenever they open a message that requests it.

Always send a response
Select this option if you wish to send a read confirmation message automatically whenever a user opens a message that requests it.

Never send a response
Choose this option if you do not want MDaemon Connector to respond to read confirmation requests.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Local Cache Options

The options in this section govern the specific location of the MDaemon Connector user's local message cache and where attachments are saved.

These options require the user's MDaemon Connector to be version 4.5.0 or newer.

Push local cache settings to MC users
By default MDaemon does not push these settings to the MDaemon Connector client. Check this box if you do wish to push them there. The MC client will move the local files from their current location to the default location, or to a custom location if you specify one in the custom options below.

Store local message cache in a custom location | Filename
Specify a local path and filename for the cache if you want the MC client to move the local files to a custom location. Environment variables and macros should be used to ensure a unique location for each user. For example:

```
%APPDATA%\Alt-N\Outlook Connector 2.0\Accounts\%OUTLOOKPROFILE%\%
  OUTLOOKEMAIL%\LocalCache.db
```

Store attachments in a custom location | Path
If you wish to customize the location of the folder in which the MC client stores file attachments, specify a path here. Environment variables and macros should be used to ensure a unique location for each user.

Send meeting requests in iCalendar format
Check this box if you want MC to send meeting requests in iCalendar (iCal) meeting format.

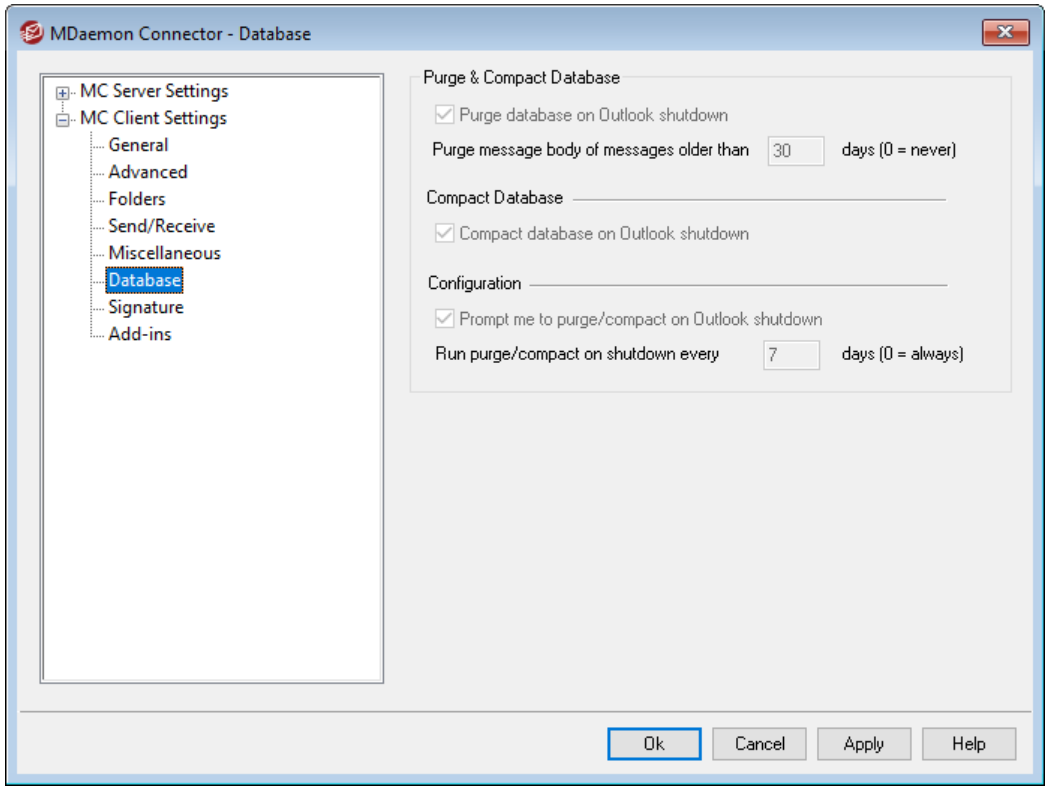
Enable automatic updates
By default MC will be updated automatically whenever a new version is available. Clear this checkbox if you do not wish to update automatically.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.2.6 Database



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the settings on this screen will be pushed to the corresponding screen in the MDaemon Connector client whenever an MDaemon Connector user connects to the server. The MC Client Settings are only sent to clients when one of the settings has changed since the last time the client connected and received them.

Purge & Compact Database

Purge database on Outlook shutdown
To conserve disk space and improve performance, by default MDaemon Connector is set to purge/delete the message body of old messages when you shut down Outlook. This does not remove the message headers nor does it affect the original messages stored on the server; it simply removes the locally cached body of old messages. Whenever you open an old message that has been purged in the past, the message body will be downloaded again to your computer. Further, only email message bodies are purged; this doesn't affect Contacts, Calendars, Tasks, Journals, or Notes. Disable this option if you do not wish to purge the database at shutdown.

Purge message body of messages older than XX days (0=never)
Use this option to designate how old a message must be for its message body to be purged at Outlook shutdown. By default a message must be more than 30 day old for it to be purged. Its age is based on the message modified date. Use "0" in this option if you never wish them to be purged.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Compact Database

Compact database on Outlook shutdown
To conserve disk space and improve performance, by default MDaemon Connector is set to compact and defragment the locally cached messages database file when the user shuts down Outlook. Outlook must shutdown cleanly, however, for the compact action to occur; if Outlook crashes or you use the Task Manager to "End Task" then the database will not be compacted. You can use the options in the Configuration section below to designate how often this will occur and whether or not you will be prompted before it does.

Configuration

Prompt me to Purge/Compact on Outlook shutdown
Use this option if you want users to be prompted before MDaemon Connector will purge or compact the database file at shutdown. If the user clicks **Yes** then it will perform the compact or purge actions, displaying a progress indicator as it does so. Clear this checkbox if you do not want users to be prompted; at shutdown MDaemon Connector will begin purging or compacting the database automatically, displaying a progress indicator when doing so.

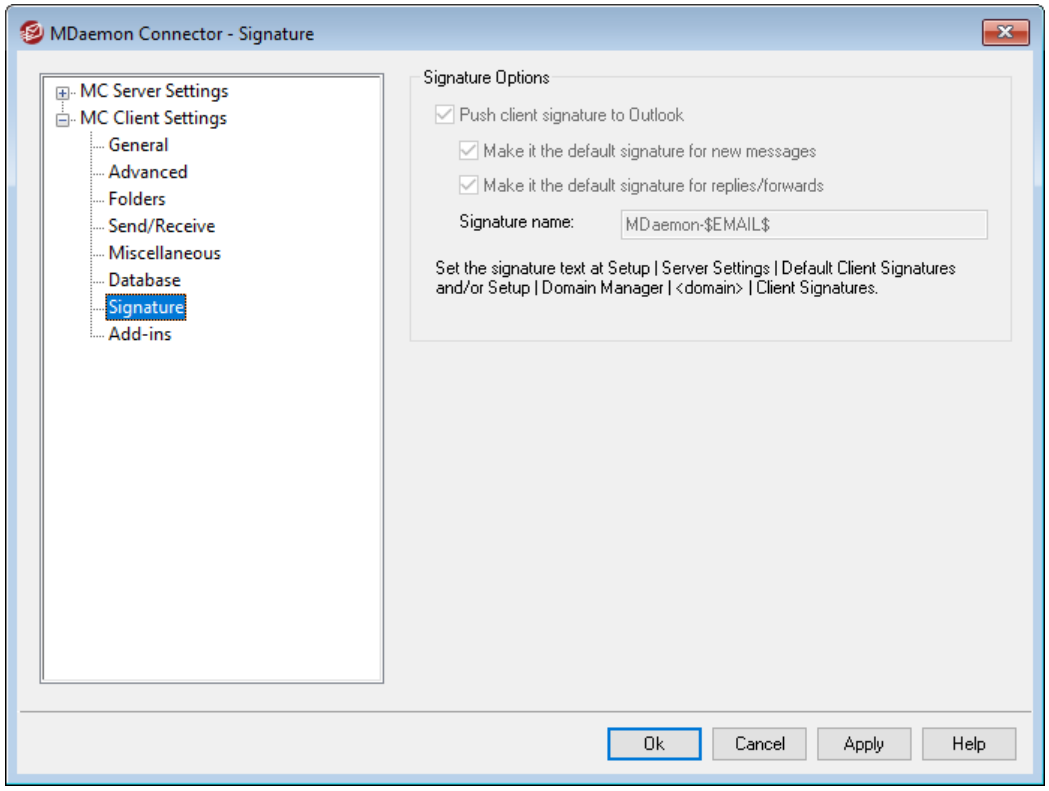
Run Purge/Compact on shutdown every XX days (0=always)
This option controls how often MDaemon Connector will purge or compact the database at shutdown. By default this option is set to 7 days, meaning that it will run the Purge/Compact process at shutdown once every seven days. Set this option to "0" if you wish to purge/compact the database every time a user shuts down Outlook.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.8.2.7 Signature



When you have enabled the "*Push client settings to MC users*" option on the MC Client Settings 382 screen, the selected settings on this screen will be pushed to the Signatures screen (located in Outlook under **File » Options » Mail » Signatures**) whenever an MDaemon Connector user connects to the server. This feature requires MDaemon Connector 6.5.0 or newer.

Signature Options

Push client signature to Outlook
Enable this option if you wish to push the default client signature 132 (or domain-specific client signature 200, if one has been created) to your MDaemon Connector users. Designate a name for the signature in the *Signature name* option below.

Make it the default signature for new messages
Check this box if you wish to make the client signature the default signature used for new messages.

Make it the default signature for replies/forwards
Check this box if you wish to make the client signature the default signature used when replying to messages and forwarding messages.

Signature name:
This is the name given to the signature pushed to the MDaemon Connector user's email account in Outlook. By default the signature's name is set to:

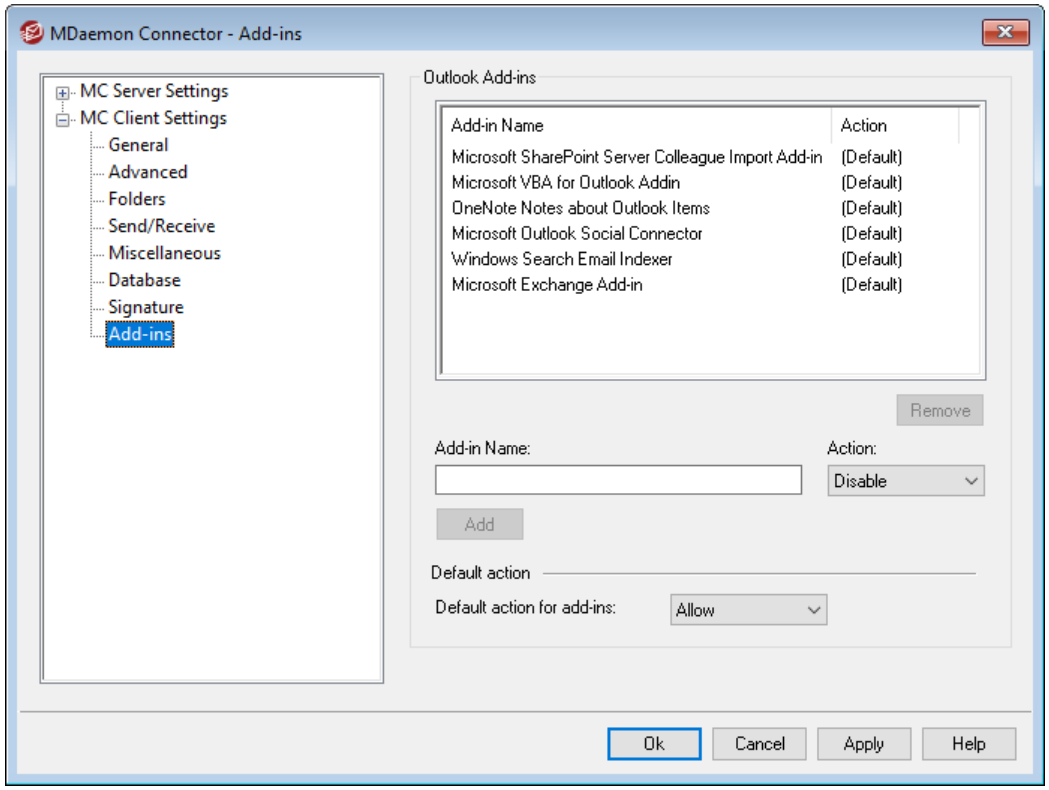
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

"MDaemon-$EMAIL$". The $EMAIL$ macro will be converted to the user's email address. For example, "MDaemon-Frank.Thomas@company.test"

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381
Default Client Signatures 132
Domain Manager » Client Signatures 200

3.8.2.8 Add-ins



Using the Add-ins screen you can manage the state of the Outlook Add-ins used by your MDaemon Connector (MC) users. You can allow any or all of the add-ins to be used normally, or you can disable any that you choose. This feature can be especially useful in cases where you know of a specific add-in that conflicts with MDaemon Connector, allowing you to disable that add-in to avoid problems. The Add-ins feature requires MDaemon Connector 5.0 or newer.

Outlook Add-ins

This box contains the list of your users' Outlook Add-ins and the Action assigned to each one: *Disable*, *Allow*, or *Default*. When an MC user starts Outlook, the MC Client

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

sends the list of the user's add-ins to MDaemon and then disables any that have been set to *Disabled.* Any set to *Allow* will not be changed. Those set to *Default* will use the *Default action for add-ins* assigned below.

MDaemon Connector can only manage the Outlook Add-ins for users who have set their MDaemon Connector account as the default account in Microsoft Outlook.

Adding, Removing, and Modifying Add-ins

Adding an Add-in

To add an add-in to the list, type the *Add-in Name* as it appears in Outlook, set the *Action*, and click **Add**. This option is useful if you know of an add-in that you wish to manage but no user has yet connected who has that add-in installed.

Removing an Add-in

To remove an add-in from the list, select it and click *Remove*.

Setting an Add-in's Action

To modify an add-in, select it, use the drop-down list to set its *Action*, and click **Add**.

Default Action

Default action for add-ins

Set this option to *Allow* or *Disable*. When set to *Allow*, by default MDaemon Connector will only disable add-ins that you have specifically set to "*Disable.*" All other add-ins will be left alone. When set to *Disable*, MDaemon Connector will automatically disable all add-ins except those that you have specifically set to "*Allow*." This option is set to *Allow* by default.

See:

MC Client Settings 382
MC Server Settings » Settings 380
MC Server Settings » Accounts 381

3.9 Cluster Service

MDaemon's Cluster Service is designed to share your configuration between two or more MDaemon servers on your network. This makes it possible for you to use load balancing hardware or software to distribute your email load across multiple MDaemon servers, which can improve speed and efficiency by reducing network congestion and overload and by maximizing your email resources. It also helps to ensure redundancy in your email systems should one of your servers suffer a hardware or software failure.

Here are a number of things to consider when deciding whether or not to set up an MDaemon cluster on your network:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Nodes

An MDaemon cluster will have a primary node and secondary nodes. One MDaemon server will be designated as Primary and all the others will be Secondary.

- The MDaemon server acting as the primary node has its configuration replicated on all other nodes. Thus the primary node is the only node that can be used to make configuration changes; if you access a secondary node and make configuration changes, those changes will be overwritten. Consequently, most configuration options aren't accessible in the user interface on secondary nodes.
- The cluster service does not replicate mailbox folders or public folders across nodes; all nodes share the same set of message folders. User mail folders and public folders must be at a location on your network that is accessible to all nodes.
- Any changes to email that happen on a secondary node are sent to the primary node and then all other nodes are notified of the change.
- The XML-API on secondary nodes is read only.
- Each node in the cluster should be on the same network. We do not recommend using the cluster service to cluster servers that are in different locations.
- Each node in the cluster needs to be running the same version of MDaemon.
- Each node in the cluster requires its own MDaemon key.

Routing

MDaemon does not handle the routing of any traffic to or from specific nodes. We recommend that you use a third-party load balancer to handle the routing of traffic.

Sticky sessions in your load balancer is required so that all traffic from the same IP is routed to the same host. Sticky sessions is most important for MDRA, Webmail, and XMPP traffic as they are not yet cluster aware, which means session information is not passed between the nodes. To deal with this limitation:

- All MDRA connections must be routed to the primary node.
- When someone logs in to Webmail on a specific server, all traffic for that session must be routed to that same server.
- Webmail and XMPP traffic needs to be routed to the same server in order for Webmail's built-in chat features to work.
- All XMPP traffic must be routed to the same node, otherwise users connecting to different servers would not be able to chat with each other.
- Considering the above points, we recommend that all HTTP and XMPP traffic be routed to the primary node, as that is the easiest configuration and least likely to cause any problems. If you are not using some of these features, however, you could alter your configuration (although sticky sessions are still required).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailboxes and Folders

Mailboxes, Public folders, and some other folders must be stored in a shared path that is accessible by each node in the cluster. Remember if you are using a UNC path you will need to run the MDaemon service as a user that has access to the network location.

- You must manually update your mailbox and folder paths and move the contents of the folders to the cluster accessible location. This is not an automated function that MDaemon can perform for you when setting up clustering. The cluster service will update the MDaemon.ini file with the network folder paths for Mailboxes and Public Folders that you provide in your cluster service configuration.
- The Lockfiles directory must to be moved to a shared location. You can allow the Clustering Service to do this automatically, or you can do it manually by editing the `LockFiles` key in the `[Directories]` section of the `MDaemon.ini` file. If you allow the clustering service to do it for you, the LockFiles directory will be located under the Network Mailbox path.
- The PEM directory also must be moved to a shared location. To do this, copy the `MDaemon\PEM\` folder to the new shared location, edit the `PEM` key in the `[Directories]` section of the `MDaemon.ini` file and restart MDaemon..
- The new account template will be updated with the mailbox path provided in the cluster service configuration.

Dynamic Screening

- Dynamic screening 596 sends all requests to the primary server node, and the data from the primary node is replicated to secondary nodes.
- If the primary node is offline, secondary nodes use their own dynamic screening configuration, which should be identical to the configuration on the primary node at the time it went offline. When the primary comes online, any changes to Dynamic screening made by the secondary servers will be overwritten.

Certificates

- SSL Certificates are automatically replicated from the Primary to Secondary nodes.
- MDaemon also replicates its certificate settings 563, so each node/server in the cluster will attempt to use the same certificate. If a node does not have the correct certificate all SSL/TLS/HTTPS traffic will fail on that node.
- MDaemon's LetsEncrypt options do not support secondary nodes at this time.

Other

- Attachment Linking 357 cannot be used in a cluster and is therefore disabled when you enable clustering.
- Automatic Update Installation 487 must be disabled.
- Domain name to IP address binding 177 must be disabled.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- All nodes in a cluster should be set to the same time zone, and set to the exact same time. If the time zone is not the same, or if the times are off by more than 1 second, a warning will be logged in the Cluster log.

Configuring the Cluster Service

Follow these steps to set up your cluster service:

1. Make sure that you have updated all mailbox paths and adjusted the public folder paths. The primary server should be using a network storage location for this data and should be able to access the data without any issues prior to proceeding.
2. All the appropriate certificates should be installed on each node.
3. Install MDaemon on a secondary node using a unique key.
4. On the primary node, go to **Setup » Cluster Service**.
5. Right-click the list of Registered Servers, and click **Add new MDaemon server to cluster** (this may be slow because it is searching the network for available servers).
6. In *Server Name*, enter the NETBIOS name, IP address, or DNS name of the secondary node MDaemon is installed on, or select the server from the drop-down list—there may be a delay as it is searches the network for available servers.
7. Click **Ok**.
8. Check the Plugins / Cluster log to ensure the two servers were connected and that replication is occurring.
9. Go to **Setup » Cluster Service** on the secondary node to confirm that it now also lists the primary and secondary nodes under Registered Servers.
10. Configure your load balancing hardware or software to route traffic to the cluster as discussed above.

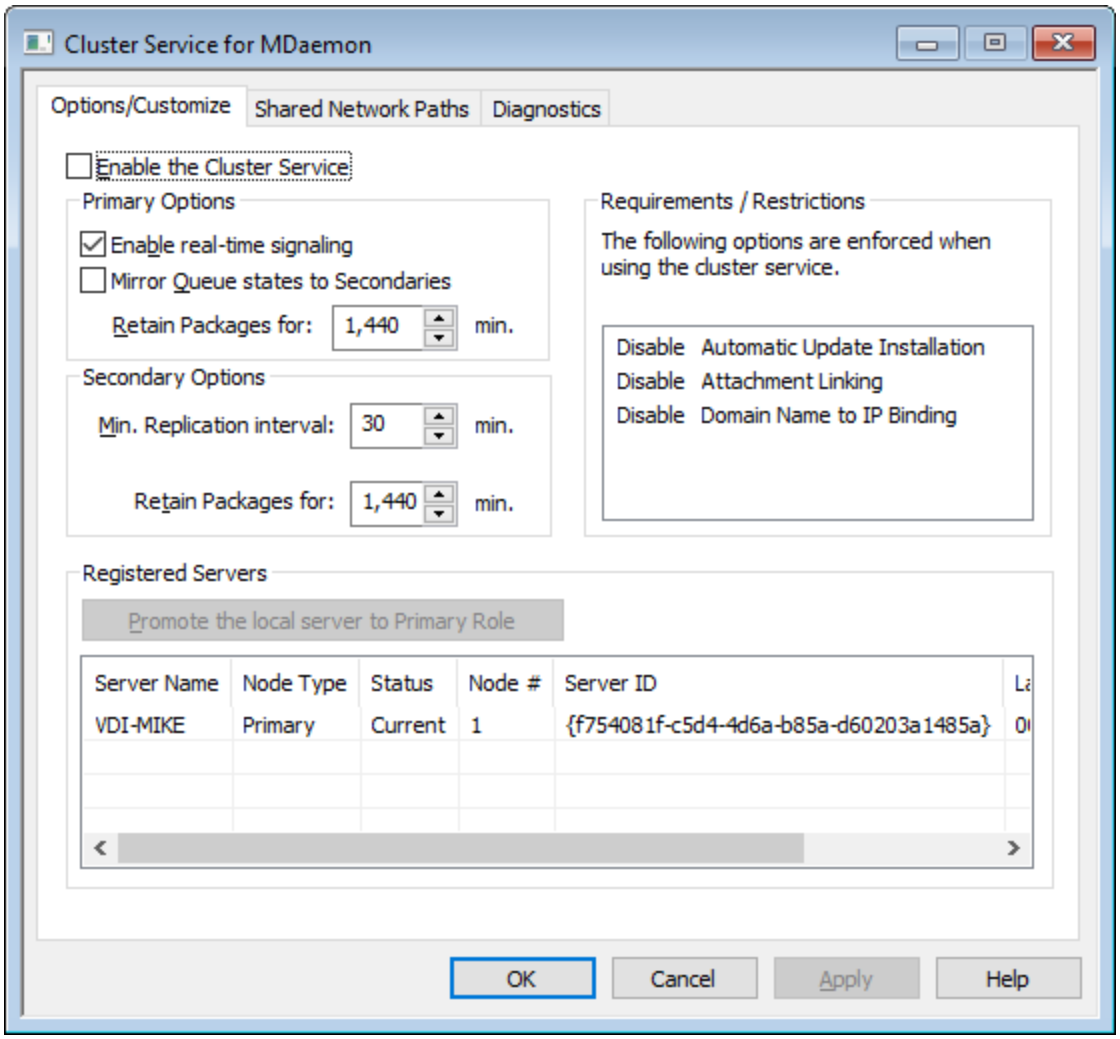
See:

Cluster Service | Options/Customize 402
Cluster Service | Shared Network Paths 404
Cluster Service | Diagnostics 406

3.9.1 Options/Customize

Options/Customize

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Enable the Cluster Service

Click to enable the Cluster Service.

Primary Options

Enable real-time signaling

By default, whenever a change occurs on the Primary node, it sends a replication signal to the Secondary nodes, to notify them that they need to make a replication request to sync the settings between the nodes.

Mirror Queue states to Secondaries

Check this box if you wish to ensure that if you change a mail queue's state (i.e. frozen or thawed) on the Primary node, that state will be changed on the Secondary nodes also.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Secondary Options

Replication interval [xx] minutes
This option determines how long a Secondary node will wait for a replication signal from the Primary node before making a replication request anyway. By default this is set to 30 minutes.

Registered Servers

This displays all the nodes in your MDaemon server cluster.

Promote the local server to Primary Role
To change a Secondary node to the Primary node, on the Secondary that you wish to promote, select the node in the list and click **Promote**. The new Primary should then inform the old Primary to rejoin the cluster as a secondary. For setups with multiple secondary nodes, the additional secondary nodes will need to be removed and re-added to the cluster.

Add new MDaemon server to cluster
To add a new MDaemon server to the cluster, right-click the list of servers and click **Add new MDaemon server to cluster**. On the screen that opens, enter the NETBIOS name, IP address, or DNS name of the server on which MDaemon is installed, or select it from the drop-down list. There may be a delay as it is searches the network for available servers.

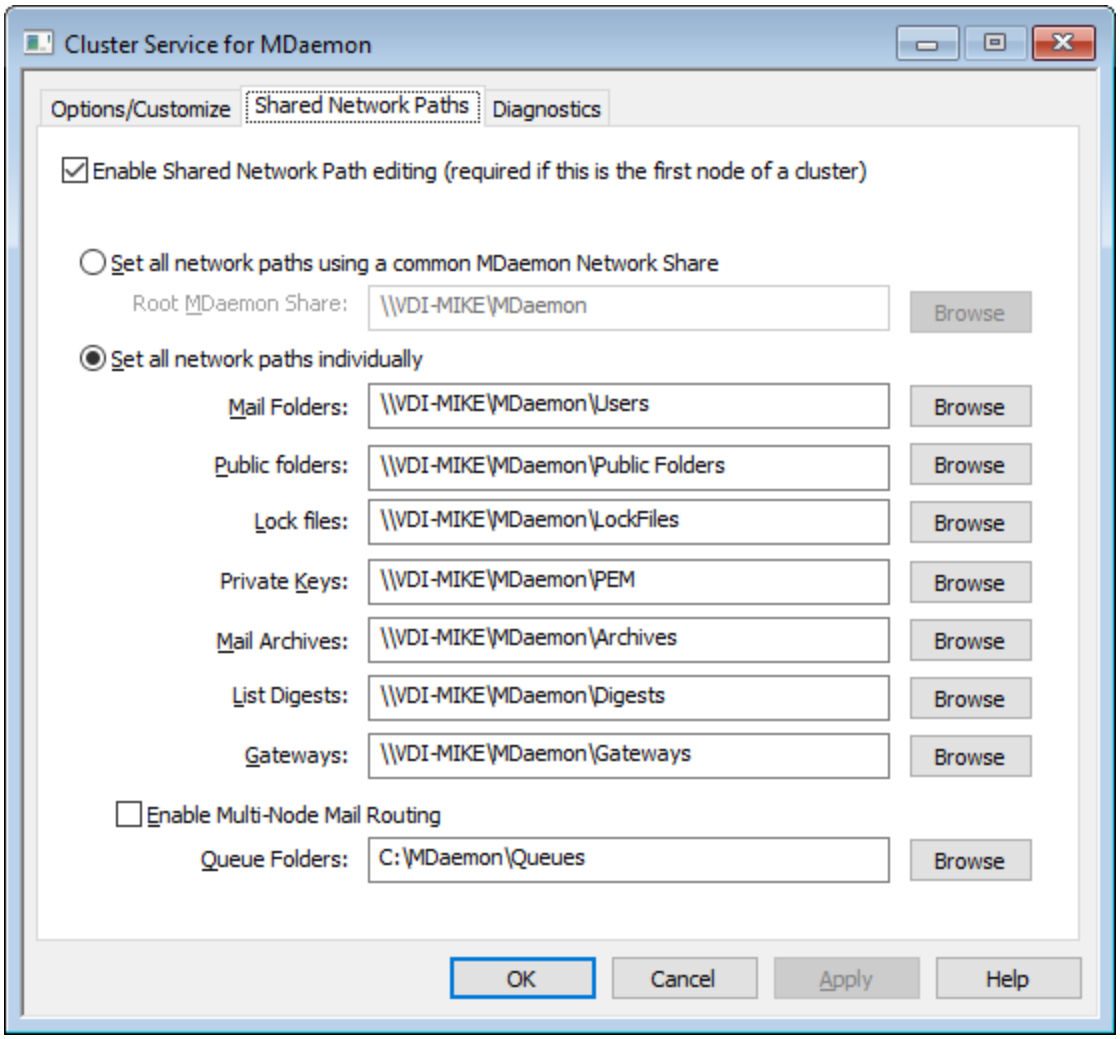
See:

Cluster Service 399
Cluster Service | Shared Network Paths 404
Cluster Service | Diagnostics 406

3.9.2 Shared Network Paths

Shared Network Paths

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Enable Shared Network Path editing (required if this is the first node of a cluster)

Use the options on this screen to set the shared network paths that will be used by the MDaemon cluster. This is required on the first node of the cluster so that the shared network paths can be replicated on the other nodes.

Set all network paths using a common MDaemon Network Share
Choose this option if you wish to locate all of the shared network paths under a single, common network share. This option results in all of the paths being set to the default values, and all path controls will be read-only.

Set all network paths individually
Choose this option if you wish to set each shared network path individually. Such as, for example, if you wish to store mail folders and mail archives at different network locations.

Enable Multi-Node Mail Routing
Use Multi-Node Mail Routing if you wish to share mail queues between the cluster nodes. Having multiple servers process and deliver the messages allows them to split

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

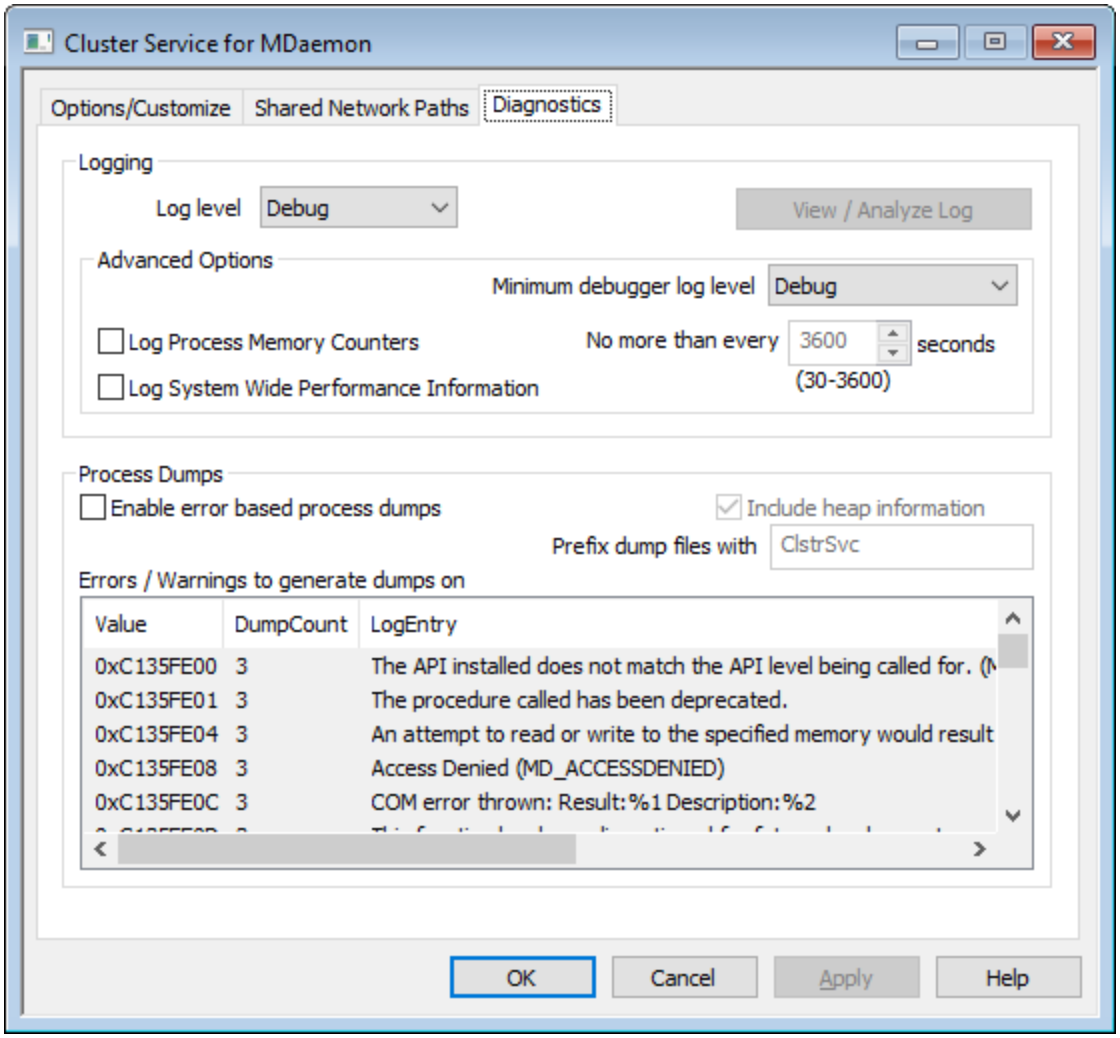
the work more evenly and prevents messages from being stuck in the queues of any servers that are down.

See:

Cluster Service 399
Cluster Service | Options/Customize 402
Cluster Service | Diagnostics 406

3.9.3 Diagnostics

Diagnostics



Logging

Log level
Six levels of logging are supported, from the highest to lowest amount of data

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem, or when the administrator wants detailed information.

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

View/Analyze Log
Click this button to open the MDaemon Advanced System Log Viewer. By default the logs are stored in: "..\MDaemon\Logs\"

Advanced Options

Minimum debugger log level
This is the minimum level of logging to emit to the debugger. The available log levels are the same as those outlined above.

Log process memory counters
Check this box to log process-specific Memory, Handle, and Thread information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

Log system wide performance information
Check this box if you with to log system-wide performance information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

No more than every [xx] seconds
Use this option to set the limit on how often the process and performance information will be logged.

Process Dumps

Enable error based process dumps
Enable this option if you want to generate process dumps whenever a specific warning or error occurs that you have designated below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Include heap information in dumps
By default, heap information is included in the process dumps. Clear this checkbox if you do not wish to include it.

Prefix dump files with
Process dump filenames will begin with this text.

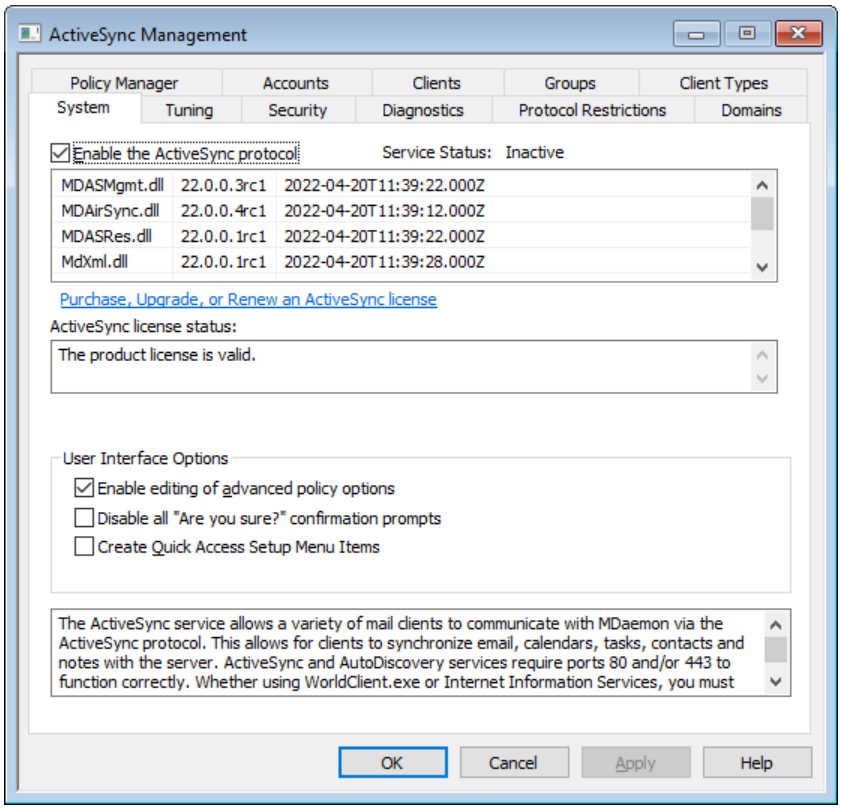
Errors/Warnings to generate dumps on
Right-click this area and use the *Add/Edit/Delete Entry...* options to manage the list of errors or warnings that will trigger process dumps. For each entry you can specify the number of process dumps allowed before it will be deactivated.

See:

Cluster Service 399
Cluster Service | Options/Customize 402
Cluster Service | Shared Network Paths 404

3.10 ActiveSync

3.10.1 System



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon includes support for "ActiveSync for MDaemon," which is a separately licensed over-the-air (OTA) ActiveSync server. This server is capable of synchronizing a user's Email and PIM data (i.e. Contacts, Calendars, and Tasks) between his MDaemon/Webmail account and an ActiveSync capable device.

If you enable ActiveSync for MDaemon the first time using a trial key, it will operate for 30 days. After that, if you wish to continue using it you can acquire a license key from www.mdaemon.com or your local distributor/reseller.

ActiveSync is a web-service extension that only works on ports **80** (for http) and **443** (for https). This is an ActiveSync implementation requirement. If ActiveSync is enabled and you are using Webmail's built-in web server, but it is not running on port 80 or 443, then it will automatically begin running on port 80 in addition to whatever other ports you have configured on the Web Server 313 and SSL & HTTPS 316 screens. If you are using another server for Webmail such as IIS then you must manually configure it to use port 80 or 443.

If you intend to run ActiveSync under IIS you must call the ActiveSync DLL (`MDAirSync.dll`) when "`/Microsoft-Server-ActiveSync`" is requested. This is the request that all the ActiveSync clients will use. Some versions of IIS do not have this capability without downloading, installing, and configuring third party software.

All first time syncs with ActiveSync are a one way sync from the server to the device. You will lose related data on the device when you sync with ActiveSync for the first time. This is an ActiveSync implementation requirement. You should therefore backup your device data before using ActiveSync for the first time. Most devices that support ActiveSync warn the user that "**device data will be lost**," but some do not.

Enabling/Disabling ActiveSync

Click *Enable the ActiveSync protocol* to turn on ActiveSync for MDaemon. Then you can use the Domains 426 options to control whether or not it is available to all or some of your domains.

User Interface Options

Enable editing of advanced policy options
Enable this option if you want the Advanced Settings tab to be visible on the ActiveSync Policy Editor 435. It contains various advanced policy settings that in most cases will not need to be changed. This option is disabled by default.

Disable all "Are you sure?" confirmation prompts
By default when you change certain ActiveSync settings you are presented with a prompt asking you if you are sure that you wish to make the change. Click this checkbox if you wish to disable those prompts.

Create quick access Setup menu items
If you enable this option, the Setup » ActiveSync menu in MDaemon's application interface will be changed, adding links to the ActiveSync Connections monitor and the Log Viewer/Analyzer. **Note:** when this option is disabled, those tools can still be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

reached by right-clicking **ActiveSync** under Servers in the Stats pane of the application interface.

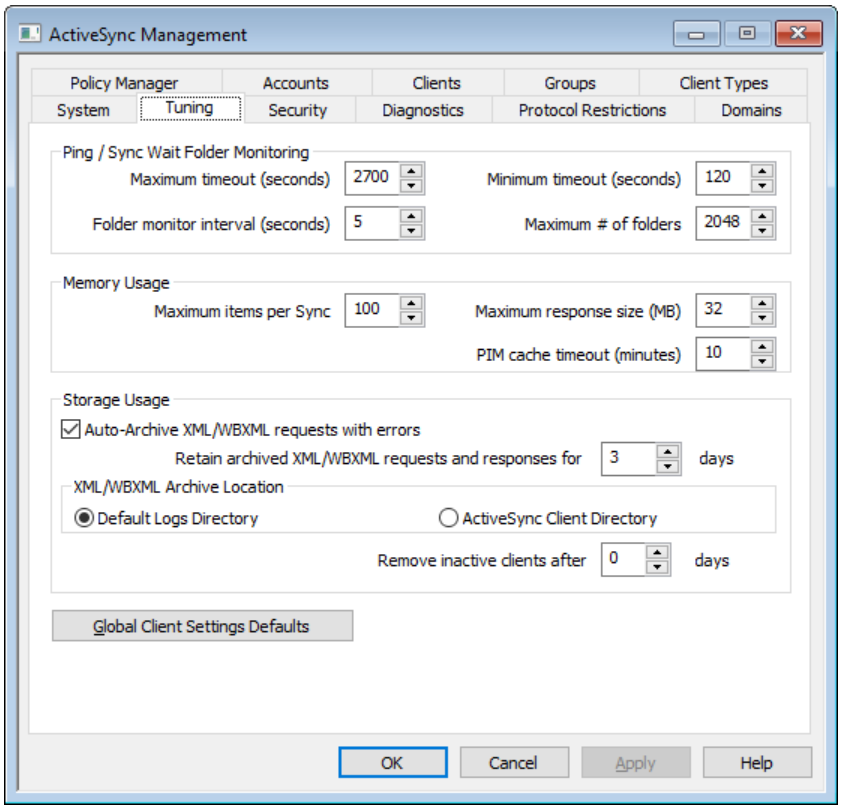
AutoDiscovery Service 73

MDaemon supports the AutoDiscovery Service 73, which allows users to set up an ActiveSync account with just their email address and password, without needing to know the host name of the ActiveSync server. AutoDiscovery requires HTTPS 316 to be enabled.

See:

Account Editor » ActiveSync 747
ActiveSync » Domains 426
SSL & HTTPS 316
Web Server 313

3.10.2 Tuning



This screen contains advanced options, which in most cases will not need to be adjusted, and it contains a button to open the Global Client Settings Defaults 413 dialog, to adjust the default settings used for ActiveSync clients.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Ping/Sync Wait Folder Monitoring

Maximum timeout (1200-7200 seconds)
This is the maximum amount of time that MDaemon ActiveSync Service (MDAS) will wait while monitoring a folder before returning a response to the client. The default value is 2700 seconds (i.e. 45 minutes).

Minimum timeout (120-480 seconds)
This is the minimum amount of time that MDAS will wait while monitoring a folder before returning a response to the client. The default value is 120 seconds. If necessary you can reduce the number of connections that are made to the server by raising this value, since it would cause the client to connect less often due to the wait time involved being longer.

Folder monitor interval (3-50 seconds)
This is the number of seconds that the ActiveSync service will wait between folder monitoring occurrences. This is set to 5 seconds by default.

Maximum # of folders
This is the maximum number of folders that each ActiveSync client is allowed to monitor for changes. The default is 2048.

Memory Usage

Maximum items per Sync
This is the maximum number of items that the ActiveSync service will return to the client in response to a Sync request. Using a lower value in this option can reduce memory usage on a busy server, but it will require more connections and bandwidth. It can also decrease battery life because devices may need to make more requests to get all changes during a sync. Higher values in this option increase memory usage and are more susceptible to communication errors. The default value of 100 is generally a good compromise. It is worth noting, however, that clients will specify the value that they prefer, which could effectively lower this value for some clients. If a client requests a value greater than the maximum, then the maximum will be used.

Maximum response size (MB)
This is the maximum allowable size of a response to a Sync request from a client. Prior to processing a given item for server-to-client synchronization, the current size of the response is checked and if it is greater than or equal to this value, the collection is flagged that there are more changes available, and no more item will be added to the response. This is useful with servers that regularly contain a lot of large attachments in their email.

PIM cache timeout (5-60 minutes)
Since Contacts, Documents, Events, and other PIM data is often static, getting only occasional updates from clients, MDAS caches this data to reduce disk activity. It is, however, automatically reloaded whenever the data changes on disk. This value controls how long to cache the user's data since the last time it was accessed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Storage Usage

Auto-Archive XML/WBXML requests with errors
In the event that you have turned off the options to *Archive [XML | WBXML] requests and responses* on the Client Settings 413 screen, this option will still archive problematic XML or WBXML requests. Only requests that cause errors will be archived. This option is enabled by default.

Retain archived XML/WBXML requests and responses for this [xx] days
This is the number of days that the auto-archived responses will be saved. They are kept for 3 days by default.

XML/WBXML Archive Location

Default Logs Directory
The auto-archived XML/WBXML requests and errors files will be stored in MDaemon's logs directory by default.

ActiveSync Client Directory
Choose this option if you wish to store the files in the user's ActiveSync Client Debug directory instead.

Remove inactive clients after [xx] days
This is the number of days that an ActiveSync device 451 can go without connecting to MDAS before it will be removed. When the device is removed, its configuration and access settings are discarded. If the device ever connects again, MDaemon will respond as if it is a new device that has never been used on the server. It will be forced to reprovision if a policy is in place for the domain 426 or account 442, perform an initial folder sync, and re-sync all subscribed folders. This option can help keep your server free from maintaining information for old and unused devices. The option is set to 31 days by default. When set to "0", devices will not be removed, regardless of how long they have been inactive.

Global Client Settings Defaults

Click this button to open the Global ActiveSync Client Settings 413 dialog, for configuring the default settings to be used for ActiveSync clients.

ActiveSync Notifications

Sync Rollback Notifications

The ActiveSync Service can notify the administrators if a client is repeatedly/frequently sending expired Sync Keys in Sync operations.

These merely inform the admin that the server issued a rollback for a given collection because a client made a sync request with the most recently expired Sync Key. The subject states "ActiveSync Client Using expired Sync Key". This could occur because of a network issue or something about the content previously sent to the client in that collection. In some cases, the item ID will be there, it

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

merely depends upon whether or not the previous sync on that collection sent any items.

Rollback warnings do not mean the client is out of Sync, it means that the client has the potential to go out of Sync and our internal system detected it. Rollback warnings are issued for a collection no more than once per 24 hour period. The following keys can be edited under the [System] header in the `\MDaemon\Data\AirSync.ini` file:

- [System] SendRollbackNotifications=[0|1|Yes|No|True|False] (Default is disabled)
- [System] RollbackNotificationThreshhold=[1-254] : The number of rollbacks that must occur on a given collection prior to a notification being sent to the admin. We recommend a value of at least 5 here, since Network hiccups play a part in this. (Default is 10)
- [System] RollbackNotificationCCUser=[0|1|Yes|No|True|False] : Whether or not to CC the user whose client sent that expired Sync Key. (Default is disabled)

ActiveSync Corrupt Message Notifications

The ActiveSync Service can notify the administrators if a particular message cannot be processed. These are sent in real time to inform the admin of a mail item that could not be parsed and that further action on this item is not possible. The subject states "Corrupt message notification". These items, in previous versions, could lead to a crash. In most cases, the content of the msg file will not be MIME data. If it is MIME data, it is likely corrupt. You can choose to CC the affected user of these notifications with the CMNCCUser key so that they are aware that an email has arrived in their mailbox that is un-readable. The appropriate action for these is to move the designated msg file from the user's mailbox and analyze it to determine both why it is not able to be parsed and how it came to exist in the state that it is in. The following keys can be edited under the [System] header in the `\MDaemon\Data\AirSync.ini` file:

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

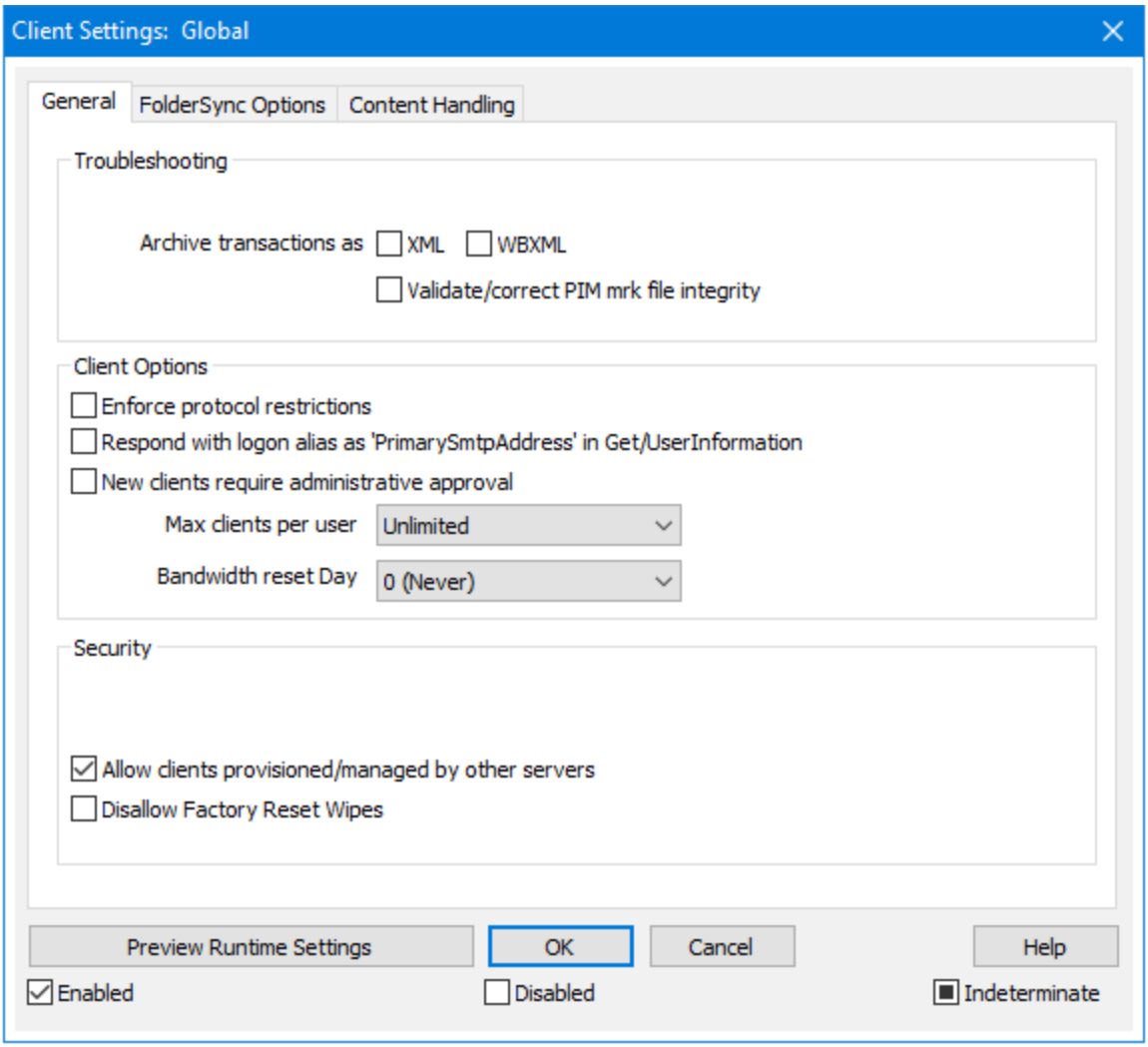
See:

ActiveSync » Diagnostics 422

3.10.2.1 Client Settings

The Client Settings page lists the default ActiveSync settings profiles that have been configured for ActiveSync. You can create and edit client settings profiles for: Global, Domains 200, Groups 460, Accounts 442, Client-Types 466, and Clients 451 (i.e. devices) on their respective dialogs.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



This screen contains the global settings for managing ActiveSync clients. There are corresponding client settings under ActiveSync's other pages, such as Domains 426, Accounts 442, and Clients 451, for setting these options per domain, per account, and per client respectively. The global settings are set to specific values, but the domain, account, client, and other settings are by default set to *Inherit* their settings from their respective parent options. Therefore changing any setting on this screen will effectively change the same setting on all child screens, allowing you by default to manage all clients on the server by changing only the settings on this one screen. Conversely, changing a setting on a child screen will override its parent setting, allowing you to alter the settings at the domain, account, or other level if necessary.

Similar to Policies 434, which are assigned to the device and generally govern what the device can do, Client Settings govern what the server will do with regards to various client-related options, such as: governing how many separate ActiveSync clients an account can use, whether or not Public Folders will be synced to a device along with the account's personal folders, whether or not to include the user's allowed senders folder, and so on.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]

Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity

This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions

Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders 113 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders 726 to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients 451 and client types 466 that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

added to the Exchange ActiveSync (EAS) protocol 424 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias 818 for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

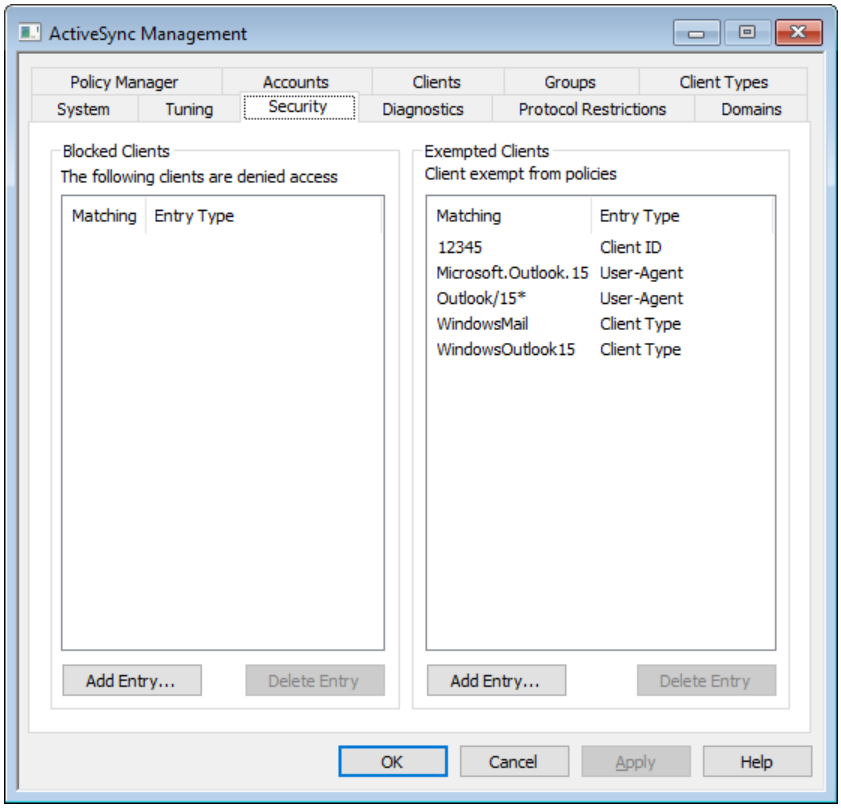
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Domains 426
ActiveSync » Accounts 442
ActiveSync » Clients 451

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.10.3 Security

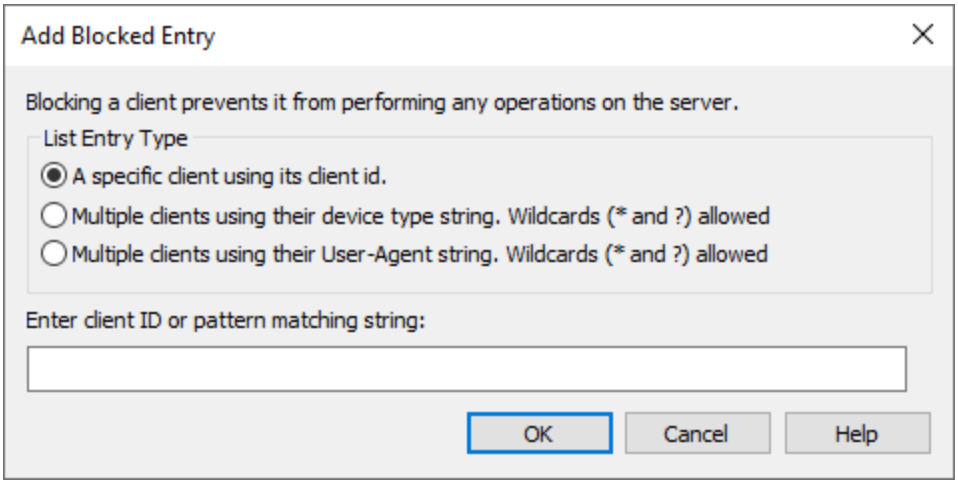


Blocked Clients

Use this option to prevent a specific Device Type, Client ID, or User Agent from accessing MDaemon's ActiveSync server.

Adding a Blocked Entry

To add an entry to the list, click **Add Entry**, specify the device info, and click **Ok**. You can obtain the device info from the device itself or from the ActiveSync log files if the device has connected to MDaemon's ActiveSync server.



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

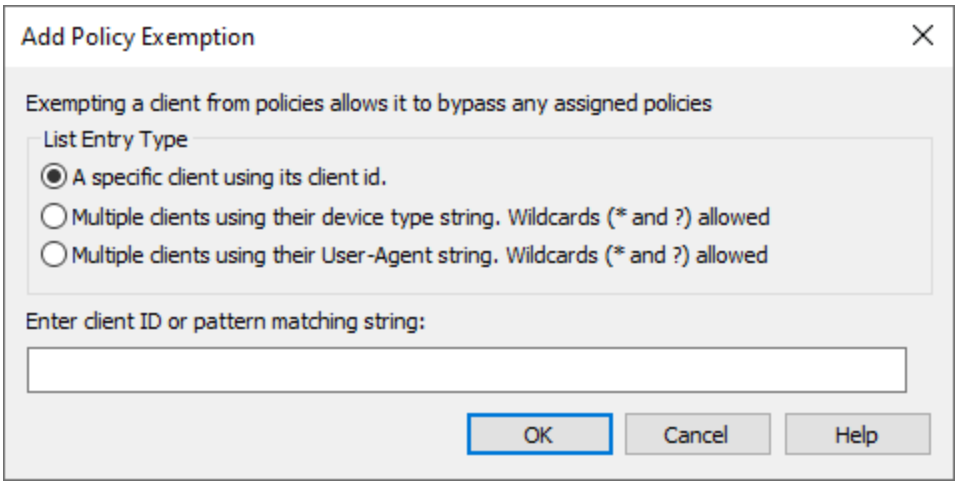
You can block a device easily from the Clients 451 dialog. Right-click a client in the list, and click **Block this client**.

Deleting a Blocked Entry
To delete entries, select one or more entries from the list and click **Delete Entry**. You will be asked to confirm the action before they are deleted.

Exempted Clients

Use this option to exempt a specific Device Type, Client ID, or User Agent from provisioning or policy 434 restrictions.

Adding an Exempted Client
To add an entry to the list, click **Add Entry**, specify the device info, and click **Ok**. You can obtain the device info from the device itself or from the ActiveSync log files if the device has connected to MDaemon's ActiveSync server.



You can exempt a device easily from the Clients 451 dialog. Right-click a client in the list, and click **Exempt this client from policies**.

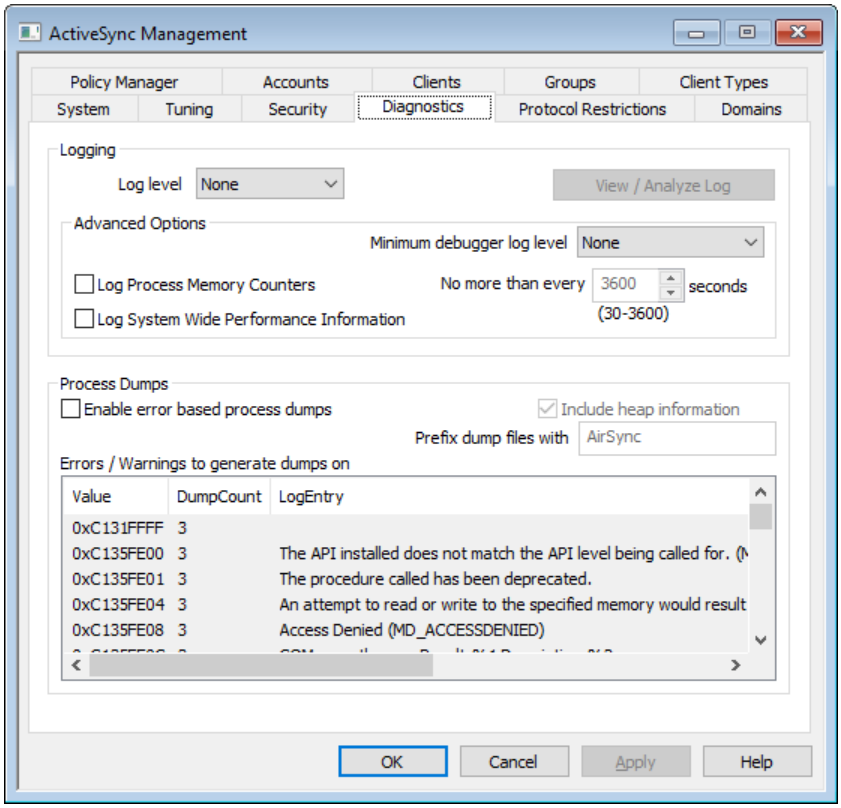
Deleting an Exempted Entry
To delete entries, select one or more entries from the list and click **Delete Entry**. You will be asked to confirm the action before they are deleted.

See:

ActiveSync » Clients 451

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.10.4 Diagnostics



This screen contains advanced options that in most cases will not need to be used unless you are attempting to diagnose a problem or are dealing with technical support.

Logging and Archiving

This section contains ActiveSync's global Log Level setting. Domain Client Settings[208] with the Log Level set to "Use inherited or default," will inherit that setting from here.

Log level
Six levels of logging are supported, from the highest to lowest amount of data logged:

Debug	This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem, or when the administrator wants detailed information.
Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

View/Analyze Log
Click this button to open the MDaemon Advanced System Log Viewer. By default the logs are stored in: "..\MDaemon\Logs\"

Advanced Options

Minimum debugger log level
This is the minimum level of logging to emit to the debugger. The available log levels are the same as those outlined above.

Log process memory counters
Check this box to log process-specific Memory, Handle, and Thread information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

Log system wide performance information
Check this box if you with to log system-wide performance information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

No more than every [xx] seconds
Use this option to set the limit on how often the process and performance information will be logged.

Process Dumps

Enable error based process dumps
Enable this option if you want to generate process dumps whenever a specific warning or error occurs that you have designated below.

Include heap information in dumps
By default, heap information is included in the process dumps. Clear this checkbox if you do not wish to include it.

Prefix dump files with
Process dump filenames will begin with this text.

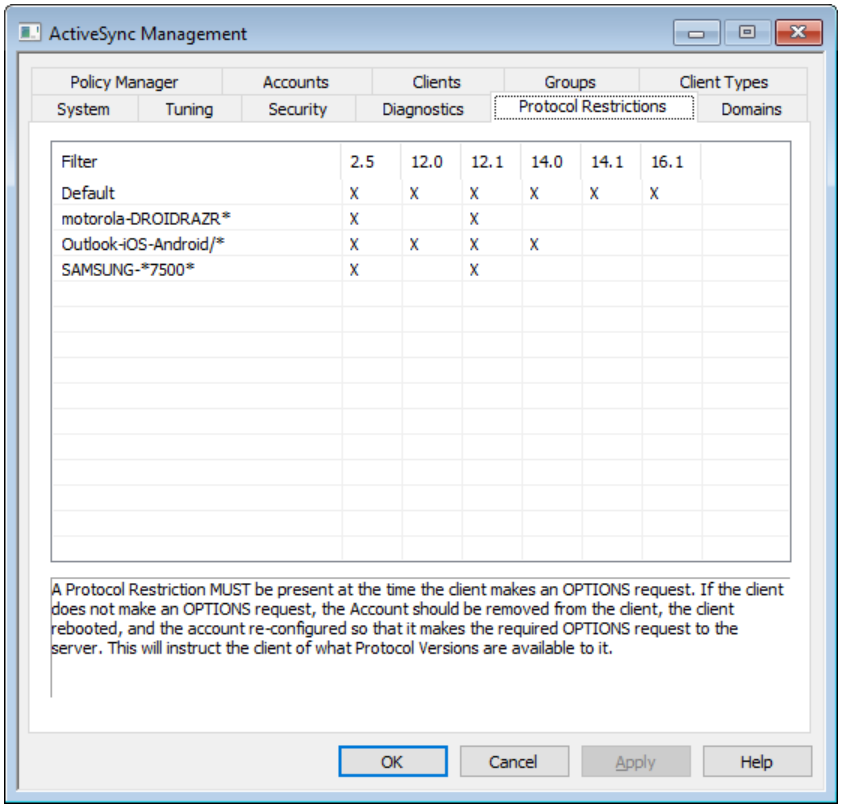
Errors/Warnings to generate dumps on
Right-click this area and use the *Add/Edit/Delete Entry...* options to manage the list of errors or warnings that will trigger process dumps. For each entry you can specify the number of process dumps allowed before it will be deactivated.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

ActiveSync » Tuning 410

3.10.5 Protocol Restrictions



Device Protocol Restrictions

Use the options located under "ActiveSync » Protocol Restrictions" to tell certain clients and devices that they are restricted to specific ActiveSync protocols. This is useful when, for example, a certain type of device is found to have unreliable support for one protocol but reliable support for another. Using the Add/Edit Protocol Restriction 425 dialog, you can define restrictions based on User Agent or Device Type, and restrict the devices to any of the following ActiveSync protocol versions: 2.5, 12.0, 12.1, 14.0, 14.1, and 16.1.

By default, protocol restrictions do not prevent a client from attempting to use a different protocol; they tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. If you wish to deny connections that attempt to use restricted protocols, use the *Enforce protocol restrictions* option on the Client Settings 413 dialogs.

Right-click an entry in the list to open a shortcut menu with the following options:

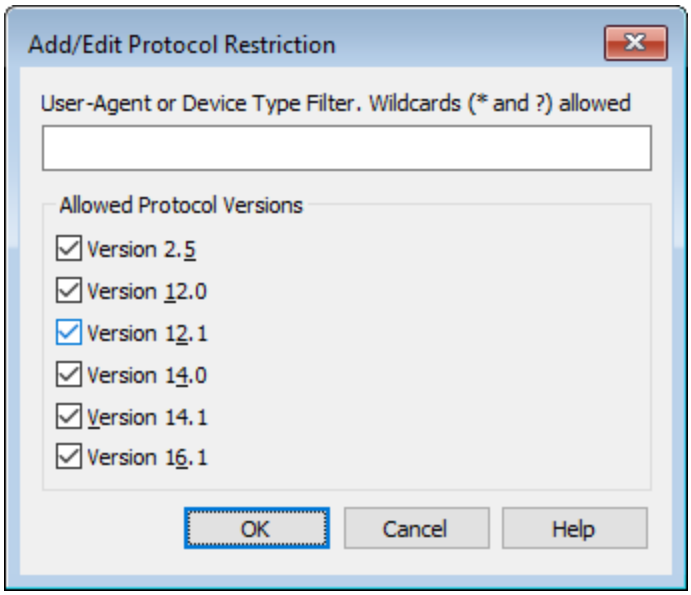
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Create Protocol Restriction
Click this option to open the Add/Edit Protocol Restriction 425 dialog (see below), used for adding your protocol restrictions.

Edit Protocol Restriction
To edit a protocol restriction, double-click an entry in the list (or right-click and choose **Edit Protocol Restriction**). After making your desired changes in the restriction editor, click **OK**.

Delete Protocol Restriction
To delete a protocol restriction, double-click an entry in the list (or right-click and choose **Delete Protocol Restriction**). Click **Yes** to confirm your decision to delete the restriction.

Add/Edit Protocol Restriction

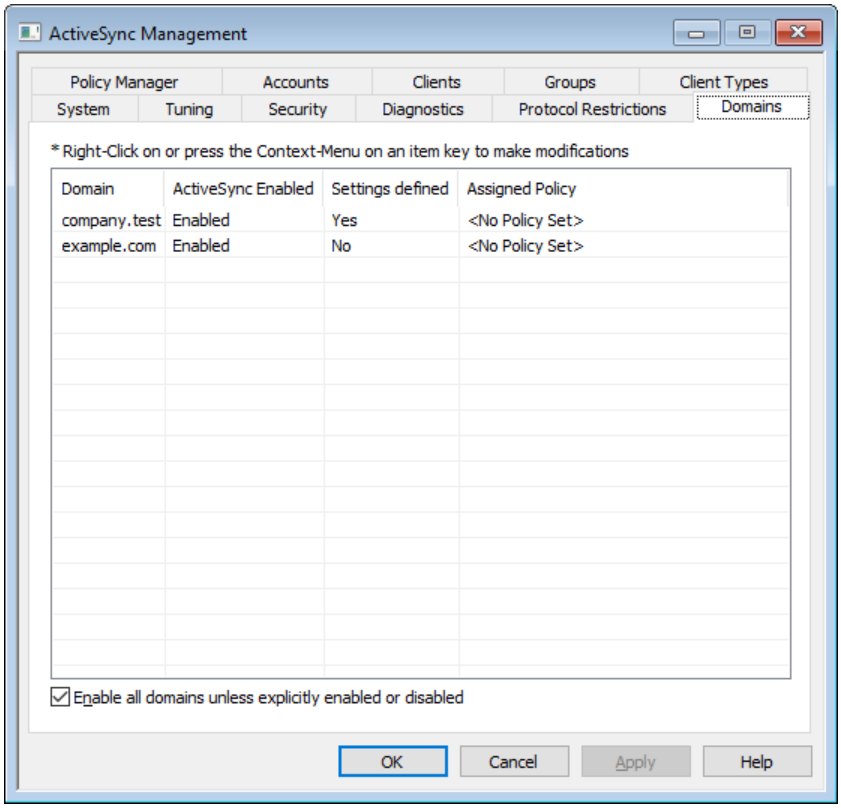


User-Agent or Device Type Filter
Enter the User Agent or Device Type to which the restriction will apply. When identifying the agent, MDaemon uses up to and including the first "/" character in the string, if one is present. If not, then the entire string is used. If you do not know the exact name of the User Agent or Device Type, once the client has connected to MDaemon ActiveSync (MDAS) you can go to the Clients 451 screen, select the client from the list, and click Details. You can also find this info by examining the MDAS log file directly.

Allowed Protocol Versions
Click each protocol that you wish to support for the device or agent. When the specified client connects to MDaemon it will be told to use only the protocols that you have selected.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.10.6 Domains



Use this screen to manage the ActiveSync settings for your domains[174]. You can enable or disable ActiveSync for each domain, assign a default ActiveSync policy[434], manage the default client settings, and manage devices associated with the domain.

Enabling/Disabling ActiveSync for Specific Domains

To set the ActiveSync state for a specific domain:

1. Right-click a domain in the list.
2. Click **Enable**, **Disable**, or **Default**. If you choose "*Default*" then the option below to "*Enable all domains unless explicitly enabled or disabled*" will determine whether or not ActiveSync is active for the domain.

In order to use ActiveSync you will need to properly configure an ActiveSync client on the user's device. For instructions on how to do this, follow the *Purchase, Upgrade, or Review ActiveSync for MDaemon* link on the ActiveSync for MDaemon[408] screen and scroll down to the device setup instructions.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Setting the Default ActiveSync State

Domains with the *ActiveSync Enabled* column set to **Enabled/Disabled (Default)** get their ActiveSync setting from state of the option: **Enable all domains unless explicitly enabled or disabled**. When that option is enabled, all domains will have ActiveSync enabled by default. When it is disabled, ActiveSync will be disabled by default. Setting a domain specifically to **Enabled** or **Disabled** will override the default setting.

If you change a domain's *ActiveSync Enabled* setting to **Disabled**, a confirmation box will open to ask if you wish to revoke ActiveSync access for all of that domain's users. Choose **No** if you wish to allow any of the domain's users who currently use ActiveSync to continue using it. If you choose **Yes**, then ActiveSync will be disabled for all of that domain's users.

Changing a Domain's Client Settings

Right-click a domain to manage the Client Settings for the domain. By default these settings are inherited from the global Client Settings 413 screen. See Managing a Domain's Client Settings 427 below.

Assigning a Default ActiveSync Policy

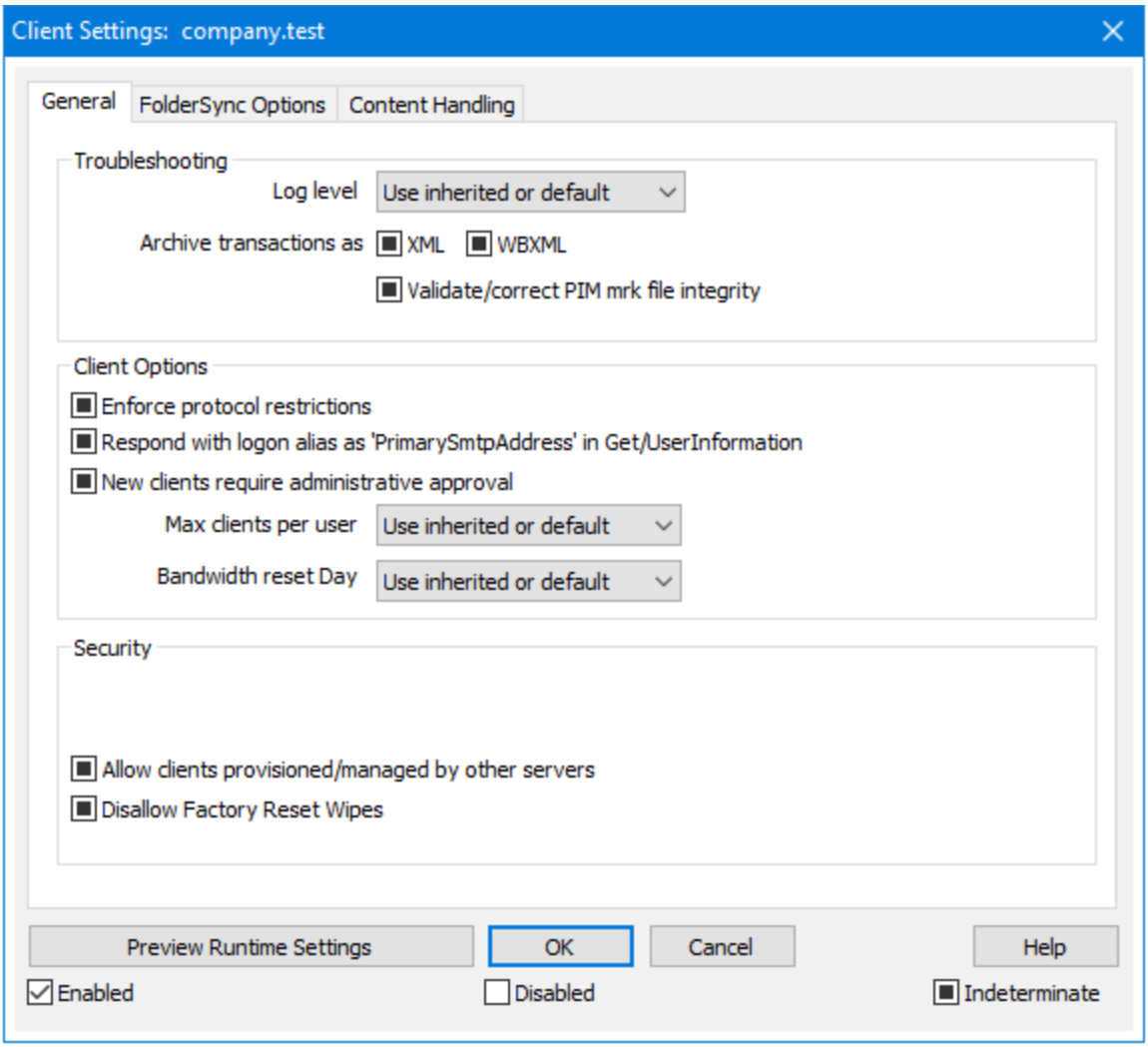
To assign a default ActiveSync policy to a domain:

1. Right-click a domain in the list.
2. Click **Apply Policy**.
3. Under "Policy to Assign" select the desired policy in the drop-down list (to manage your available policies, see the Policy Manager 434).
4. Click **OK**.

Managing a Domain's Client Settings

The domain's Client Settings screen allows you to manage the default settings for accounts and clients associated with the domain.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the global Client Settings 413 screen. Similarly, the client settings screens for this domain's Accounts 442 will inherit their settings from this screen, since the domain's Client Settings screen is their parent screen. Any changes made to the options on this screen will be reflected on those screens. Below that, Client Types have settings screens that inherit their settings from the account-level settings, and finally individual clients 451 also have their own settings. This configuration makes it possible for you to make changes to all of a domain's accounts and clients simply by making changes to this one screen, while also making it possible for you to override those settings for any account or client as needed.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

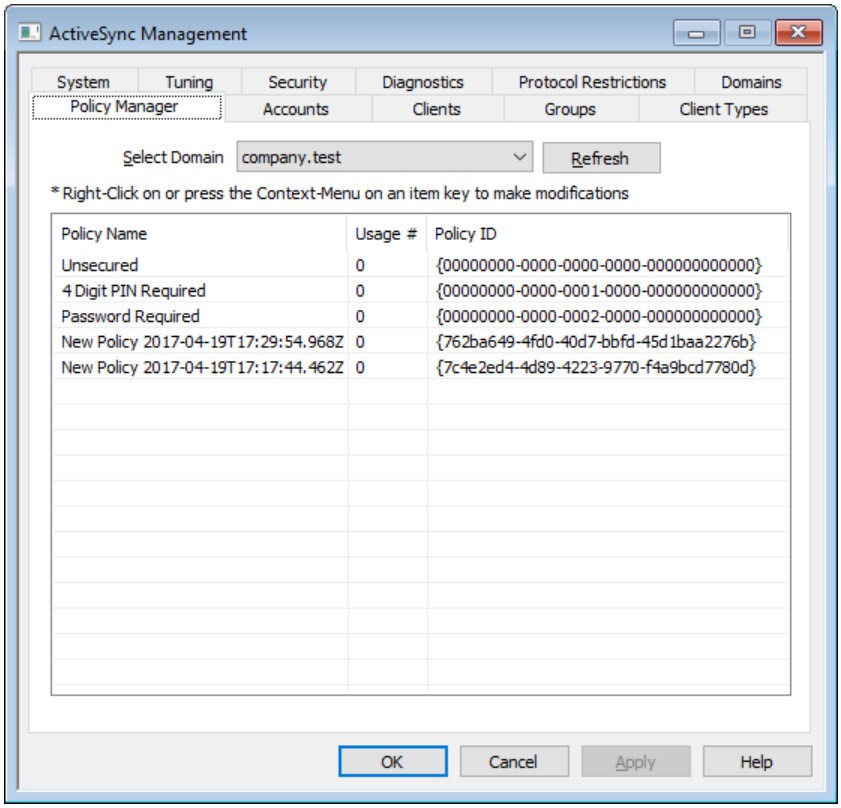
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

Domain Manager » ActiveSync Client Settings 208
Domain Manager » ActiveSync Clients 232
ActiveSync » Policy Manager 434

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.10.7 Policy Manager



Use this screen to manage the ActiveSync Policies that can be assigned to user devices to govern various options. Predefined policies are provided, and you can create, edit and delete your own. Default policies can be assigned per domain[426] and per per account[442], and policies can be assigned to specific clients[232].

Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy to a device, it will not be applied to the device until the next time it connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

ActiveSync Policies

Right-click the list to open the shortcut menu with the following options:

Create Policy
Click this option to open the ActiveSync Policy Editor[435], used for creating and editing your policies.

Delete
To delete a policy, select a custom policy from the list and then click **Delete**. Click

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Yes to confirm the action. The predefined policies cannot be deleted.

Edit Policy
To edit a policy, right-click a custom policy from the list and then click **Edit Policy**. After making your desired changes in the policy editor, click **OK**. The predefined policies cannot be edited.

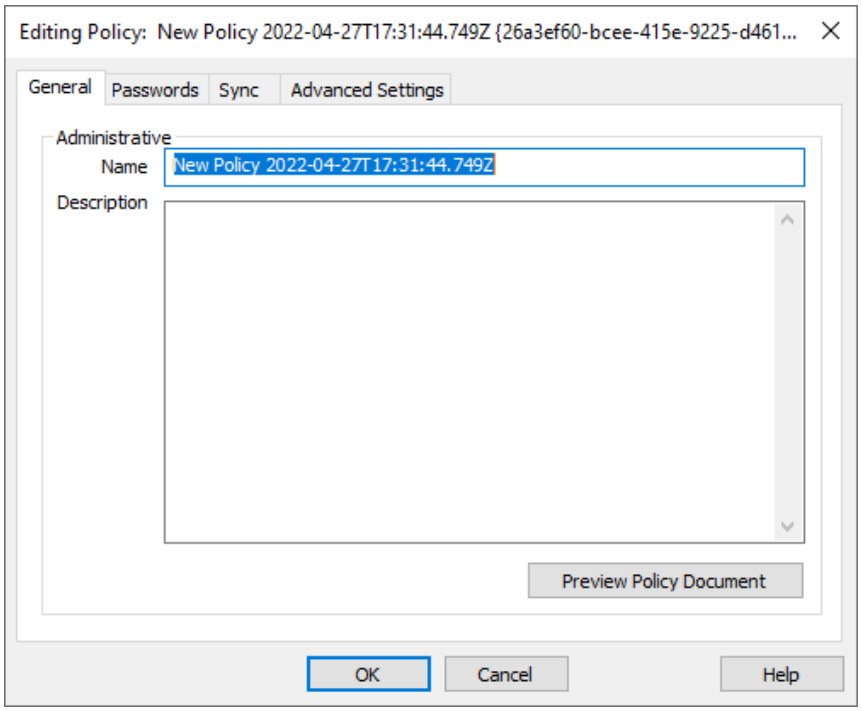
View Policy Usage
Right-click a policy and then choose this option to view a list of all domains, accounts, and clients that are set to use this policy.

ActiveSync Policy Editor

The ActiveSync Policy Editor has four tabs: General, Passwords, Sync, and Advanced Settings. The Advanced Settings tab is hidden unless you activate *Enable editing of advanced policy options* 408, located on the ActiveSync System screen.

General

Use this screen to designate a name and description for your policy. You can also preview the XML policy document.



Administrative

Name
Specify a name for your custom policy here.

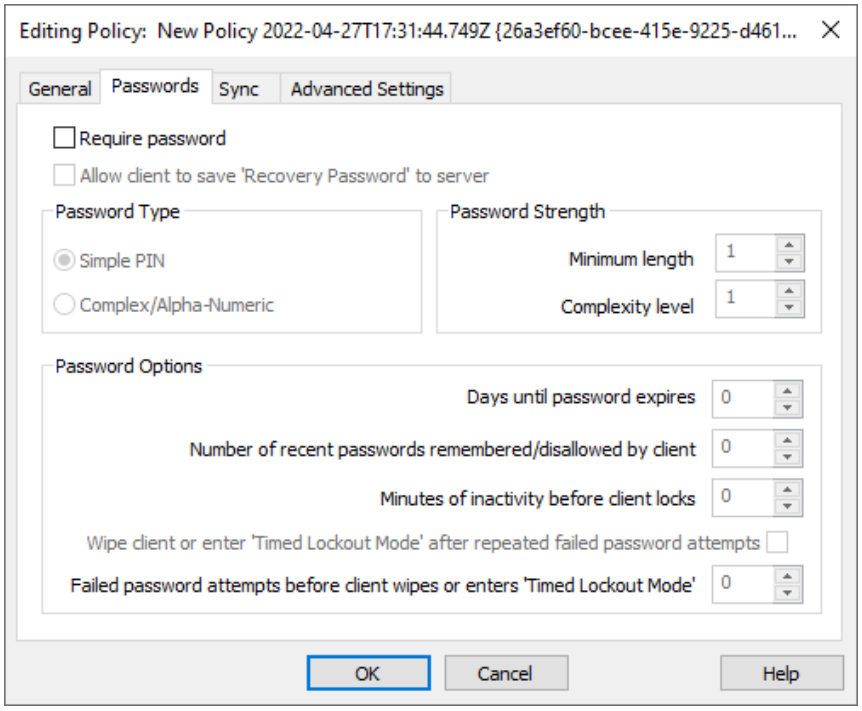
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Description
Use this area to describe your custom policy. This description appears on the Apply Policy dialog when selecting a policy to apply to a domain, account, or client.

Preview Policy Document
Click this button to preview the XML policy document for this policy.

Passwords

Password options and requirements for the policy are designated on this tab.



Require password
Check this box if you wish to require a password on the device. It is disabled by default.

Allow device to save 'Recovery Password' to server
Enable this option if you wish to allow clients to use ActiveSync's Recovery Password option, which allows a device to save a temporary recovery password to the server to unlock the device if the password is forgotten. The administrator can find this recover password under the client's Details[451]. Most devices do not support this feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Password Type

Simple PIN
How this option is implemented is largely dependent on the device, but selecting *Simple PIN* as the password type generally means that no restrictions or complexity requirements are placed on the device password, other than the *Minimum password length* option below. This allows simple passwords such as: "111," "aaa," "1234," "ABCD" and the like.

Complex/Alpha-Numeric
Use this policy option if you wish to require more complex and secure device passwords than the *Simple PIN* option. Use the *Complexity level* option below to define exactly how complex the password must be. This is the default selection when a password is required by the policy.

Password Strength

Minimum length
Use this option to set the minimum number of characters that the device password must contain, from 1-16. This option is set to "1" by default.

Complexity level
Use this option to set the complexity level requirement for *Complex/Alpha-numeric* device passwords. The level is the number of different types of characters that the password must contain: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters (such as punctuation or special characters). You can require from 1-4 character types. For example, if this option were set to "2", then the password must contain at least two of the four character types: uppercase and numbers, uppercase and lowercase, numbers and symbols, and so on. This option is set to "1" by default.

Password Options

Days until password expires (0=never)
This is the number of days allowed before the device's password must be changed. This option is disabled by default (set to "0").

Number of recent passwords remembered/disallowed by device (0=none)
Use this option if you wish to prevent the device from reusing a specified number of old passwords. For example, if this option is set to "2" and you change your device password, you will not be able to change it to either of the last two passwords that were used. The option is disabled by default (set to "0").

Minutes of inactivity before device locks (0=never)
This is the number of minutes that a device can go without any user input before it will lock itself. This password option is disabled by default (set to "0").

Wipe device or enter 'Timed Lockout Mode' after repeated failed password attempts
When this option is enabled and the user fails the designated number of

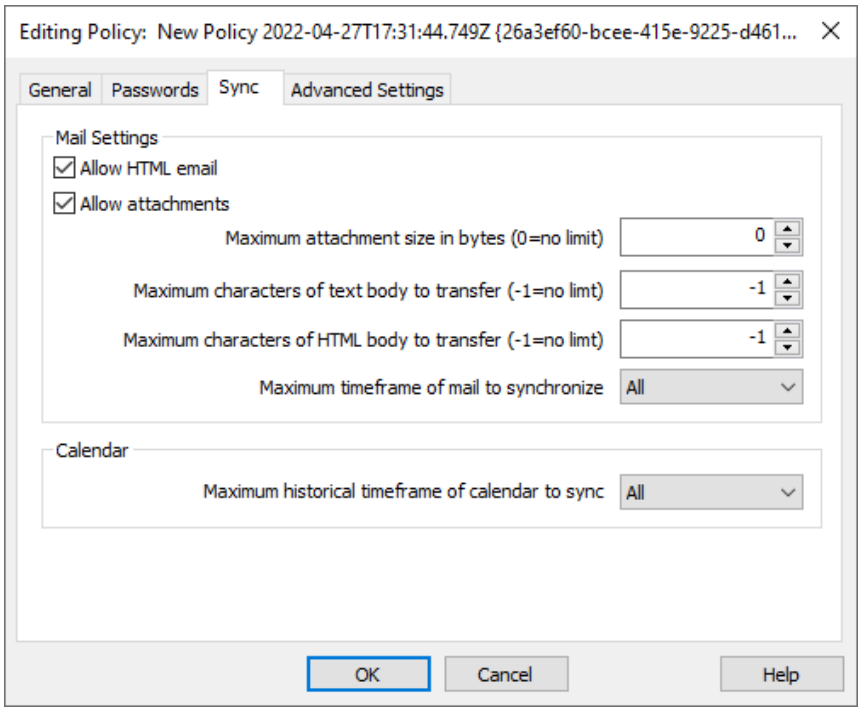
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

password attempts, the device will either lock itself for a certain amount of time or perform a wipe of all data, depending on the device. This option is disabled by default.

Failed password attempts before device wipes or enters 'Timed Lockout Mode'
When the "*Wipe device..*" option above is enabled and a user fails this many password attempts, the device will be wiped or the 'Timed Lockout Mode' will be triggered, depending on the device.

Sync

This screen contains various settings governing HTML email, allowing attachments, limiting the number of characters to transfer, and the maximum mail and calendar timeframes to sync.



Mail Settings

Allow HTML email
By default HTML-formatted email can be synced/sent to ActiveSync clients. Uncheck this box if you wish to send only plain text.

Allow attachments
Allows the device to download file attachments. This option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Max attachment size in bytes (0=no limit)
This is the maximum size of attachment that can be automatically downloaded to the device. There is no size limit set for this option by default (set to "0").

Maximum characters of text body to transfer (-1=no limit)
This is the maximum number of characters in the body of plain text-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum characters of HTML body to transfer (-1=no limit
This is the maximum number of characters in the body of HTML-formatted emails that will be sent to the client. If the message body contains more characters than are allowed, the body will be truncated to the specified limit. By default there is no limit set (option set to "-1"). If you set the option to "0" then only the message header is sent.

Maximum timeframe of mail to synchronize
This is the amount of past email, by date range from today, that can be synchronized by the device. By default this is set to "All," meaning that all email can be synchronized no matter how old it is.

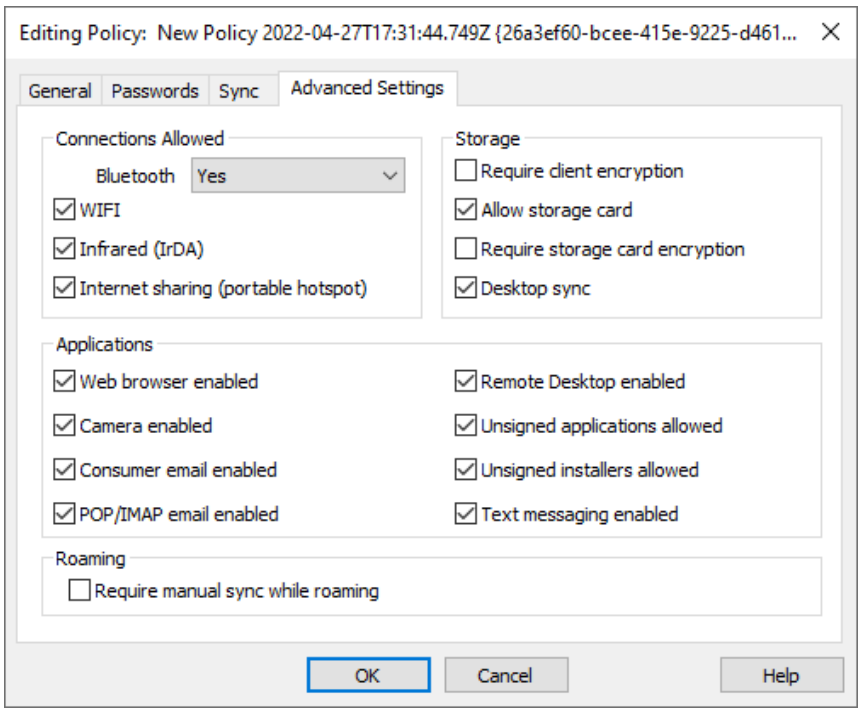
Calendar

Maximum historical timeframe of calendar to sync
This is how far back from today that past calendar entries can be synchronized by the device. By default this is set to "All," meaning that all past entries can be synchronized no matter how old they are.

Advanced Settings

The Advanced Settings tab contains options governing the types of connections allowed, whether certain applications can be enabled, storage and encryption, and roaming.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



This tab is hidden unless you activate *Enable editing of advanced policy options*[408], located on the ActiveSync for MDaemon screen.

Connections Allowed

Bluetooth
Use this option to designate whether or not Bluetooth connections are allowed on the device. You can choose **Yes** to allow Bluetooth connections, **No** to prevent them, or **Handsfree** to restrict Bluetooth to Handsfree only. This option is set to **Yes** by default.

WIFI
Allows WIFI connections. Enabled by default.

Infrared (IrDA)
Allows Infrared (IrDA) connections. Enabled by default.

Internet sharing (portable hotspot)
This option allows the device to use Internet sharing (portable hotspot). It is enabled by default.

Storage

Require device encryption
Click this option if you wish to require encryption on the device. Not all devices will enforce encryption. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow storage card
Allows a storage card to be used in the device. This is enabled by default.

Require storage card encryption
Use this option if you wish to require encryption on a storage card. This is disabled by default.

Desktop sync
Allows Desktop ActiveSync on the device. Enabled by default.

Applications

Web browser enabled
Allows the use of a browser on the device. This option is not supported on some devices, and it may not apply to 3rd party browsers. It is enabled by default.

Camera enabled
Allows the use of a camera on the device. This option is enabled by default.

Consumer email enabled
Device allows the user to configure a personal email account. When disabled, the types of email accounts or services that are prohibited is entirely dependent on the particular ActiveSync client. This option is enabled by default.

POP/IMAP email enabled
Allows access to POP or IMAP email. Enabled by default.

Remote Desktop enabled
Allows the client to use Remote Desktop. Enabled by default.

Unsigned applications allowed
This option allows unsigned applications to be used on the device. This is enabled by default.

Unsigned installers allowed
This option allows unsigned installers to be run on the device. This is enabled by default.

Text messaging enabled
This option allows text messaging on the device. Text messaging is enabled by default.

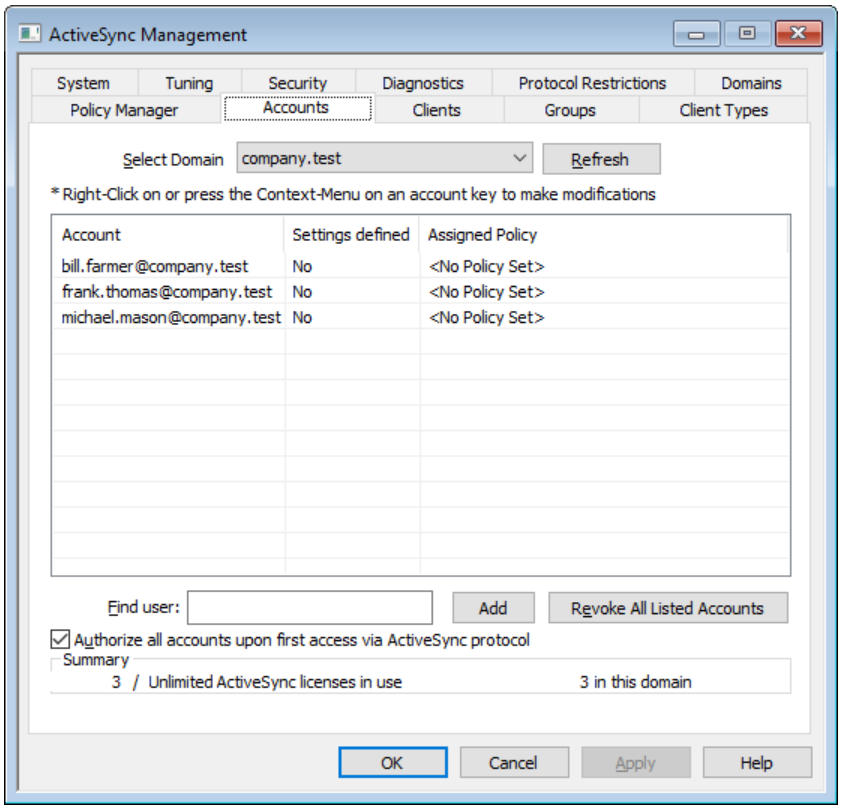
Roaming

Require manual sync while roaming
Use this policy option if you wish to require the device to synchronize manually while roaming. Allowing automatic synchronization while roaming

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

could increase data costs for the device, depending on its carrier and data plan. This option is disabled by default.

3.10.8 Accounts

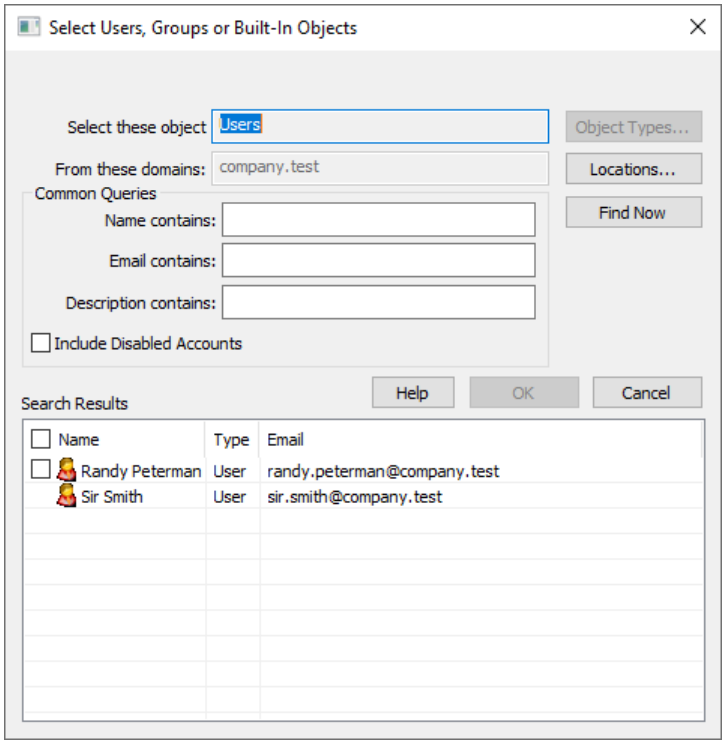


Use this screen to designate the accounts that are authorized to use ActiveSync. You can manually authorize or revoke accounts, or set MDaemon to authorize them automatically one at a time as each account connects using ActiveSync.

Manually Authorizing Accounts

On the Accounts screen, select a domain in the *Select Domain* drop-down list, and click **Add** to manually authorize one or more of its account to use ActiveSync. This opens the Select Users dialog for finding and selecting the accounts.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



From these domains
This lists the domain that you selected in the *Select Domain* option on the Accounts screen. You can search for users from this domain.

Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description[697]. Leave these fields blank if you want the search results to contain every one of the selected domain's users.

Include Disabled Accounts
Check this box if you wish to include disabled accounts[697] in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired users in the Search Results and click **OK** to add them to the list of authorized accounts.

Revoking Accounts

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

To revoke an account's authorization to use ActiveSync, right-click an account in the list and click **Revoke ActiveSync Permission**. If you wish to revoke all accounts, click the **Revoke All Listed Accounts** button.

If you have enabled the option to *Authorize all accounts upon first access via ActiveSync protocol*, revoking an account's access will remove it from the list, but the next time a device connects for the account it will be authorized again.

Authorize all accounts upon first access via ActiveSync protocol

Check this box if you wish to authorize accounts automatically, one at a time, whenever they connect to MDaemon using ActiveSync.

Assigning an ActiveSync Policy

To assign a Policy 434 to the account:

1. Right-click an account in the list.
2. Click **Apply Policy**.
3. Under "Policy to Assign" select the desired policy in the drop-down list (to manage your available policies, see the Policy Manager 434).
4. Click **OK**.

This policy will be assigned to any new device that connects for this account.

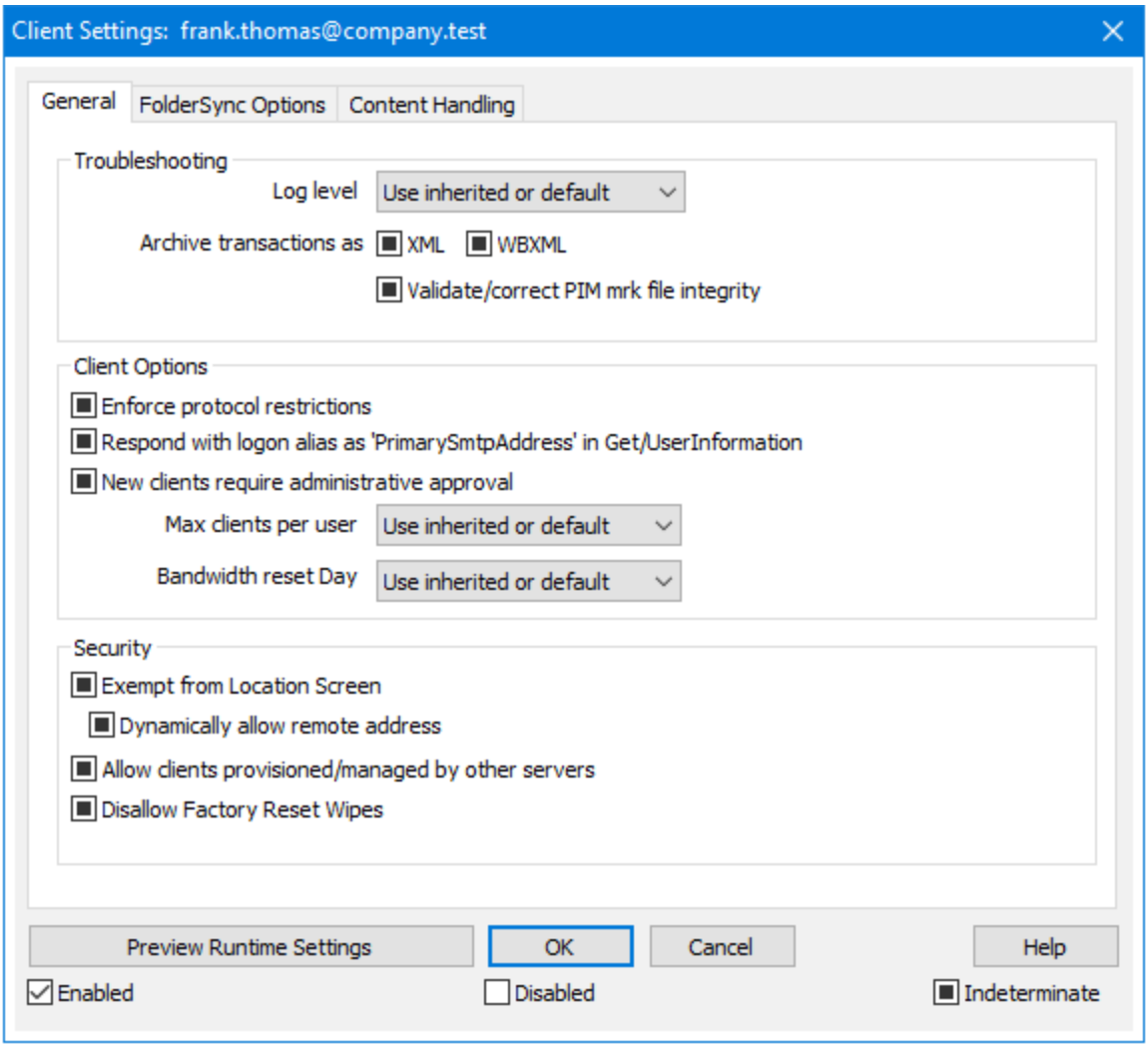
Searching the List of Authorized Accounts

If you have a large number of accounts authorized to use ActiveSync, you can use the **Find user** box to search the list for a specific account. Simply type the first few letters of the account's email address to select the user.

Account Client Settings

Right-click an account and click **Customize Client Settings** to manage the Client Settings for the account. These settings will be applied to any ActiveSync clients that connect for the account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



By default all of the options on this screen are set to "Use inherited or default," which means that if the account is a member of a Group 460, then each option's setting will be taken from that group's Client Settings. If the account is not in a group, or if no Client Settings are configured for that group, then each option will take its setting from the corresponding option on the domain's Client Settings 208 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the group or domain-level setting for this account.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Debug	This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.
Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.
Inherit	By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder

By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders

By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders

By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy

Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching

Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)

By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders

Use this option if you wish to limit the number of Public Folders allowed on the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

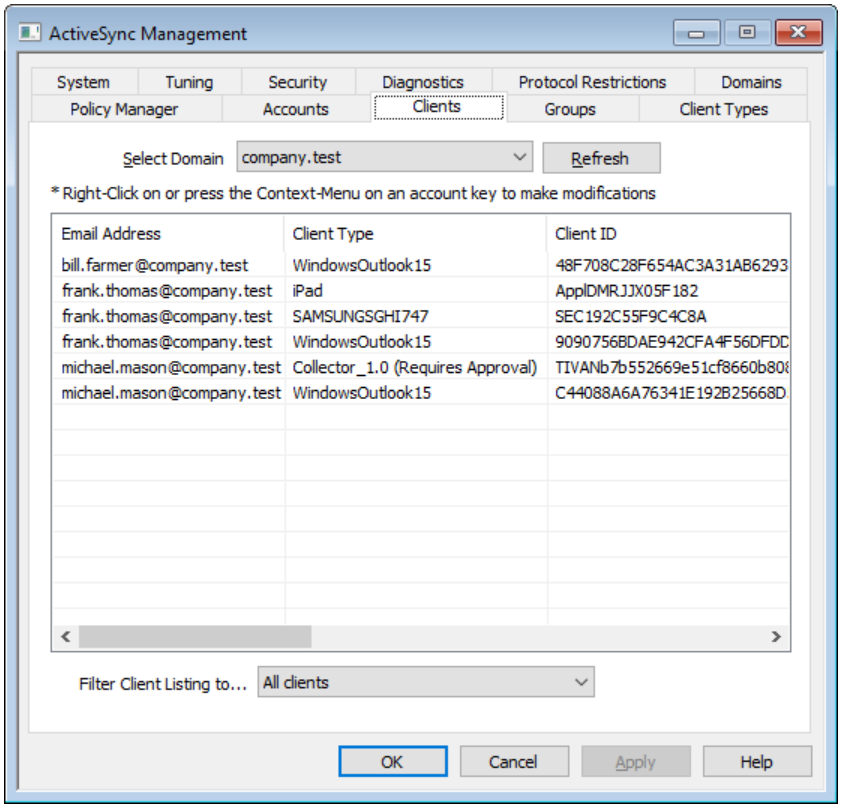
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 413
ActiveSync » Domains 426
ActiveSync » Clients 451
Accounts » ActiveSync Client Settings 748
Accounts » ActiveSync Clients 755

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

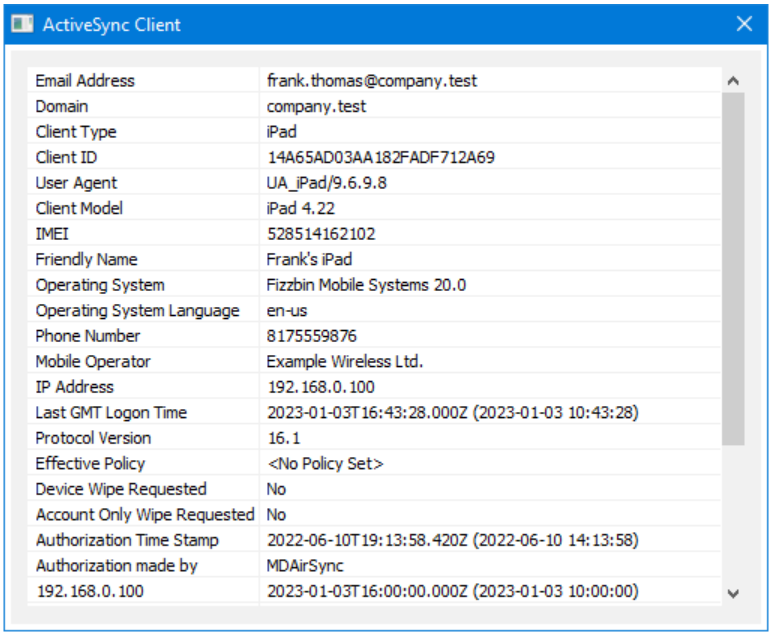
3.10.9 Clients



This screen contains an entry for each ActiveSync client associated with the selected domain. Double-click any entry to see more details about the client. Right-click an entry to open the shortcut menu, from which you can customize its client settings, view statistics, and perform various other functions.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ActiveSync Client Details



Double-click an entry, or right-click the entry and click **View Client Details**, to open the Client Details dialog. This screen contains information about the client, such as its Client Type, Client ID, last login time, and the like.

Client Settings

Right-click a client and click **Customize Client Settings** to manage its Client Settings. By default these settings are inherited from the Client Type settings, but they can be adjusted however you like. See Managing a Device's Client Settings 453 below.

Assigning an ActiveSync Policy

To assign a Policy 434 to the device:

1. Right-click a device in the list.
2. Click **Apply Policy**. This opens the Apply Policy dialog.
3. Click the **Policy to Assign** drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Right-click an entry and then click **View Statistics** to open the Client Statistics dialog, containing various usage stats for the client.

Reset Statistics

If you wish to reset a client's statistics, right-click the client, click **Reset Statistics**, and then **OK** to confirm the action.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Removing an ActiveSync Client

To remove an ActiveSync client, right-click the client and click **Delete**, and then **Yes**. This will remove the client from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same client, MDaemon will treat the client as if it had never before been used on the server; all client data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Client

When a policy 434 has been applied to a selected ActiveSync client, and the client has applied it and responded, then there will be a Full Wipe option available for that client. To do a Full Wipe, right-click the client (or select it if you are using MDRA) and click **Full Wipe**. The next time the client connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the client, this may remove everything on it, including downloaded apps. Further, as long as the client's ActiveSync entry exists, MDaemon will continue to send the wipe request any time that device connects in the future. If at some point you wish to delete the client, make sure you add it to the Block List 420 first, so that it cannot connect again in the future. Finally, if a wiped device is recovered and you wish to allow it to connect again, you should select the device and click **Cancel Wipe Actions**. You must also remove it from the Block List.

Account Wiping an ActiveSync Client

To wipe the account's mail and PIM data from the client or device, right-click and click **Account Wipe Account Mail and PIM from client**. The *Account Wipe* option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

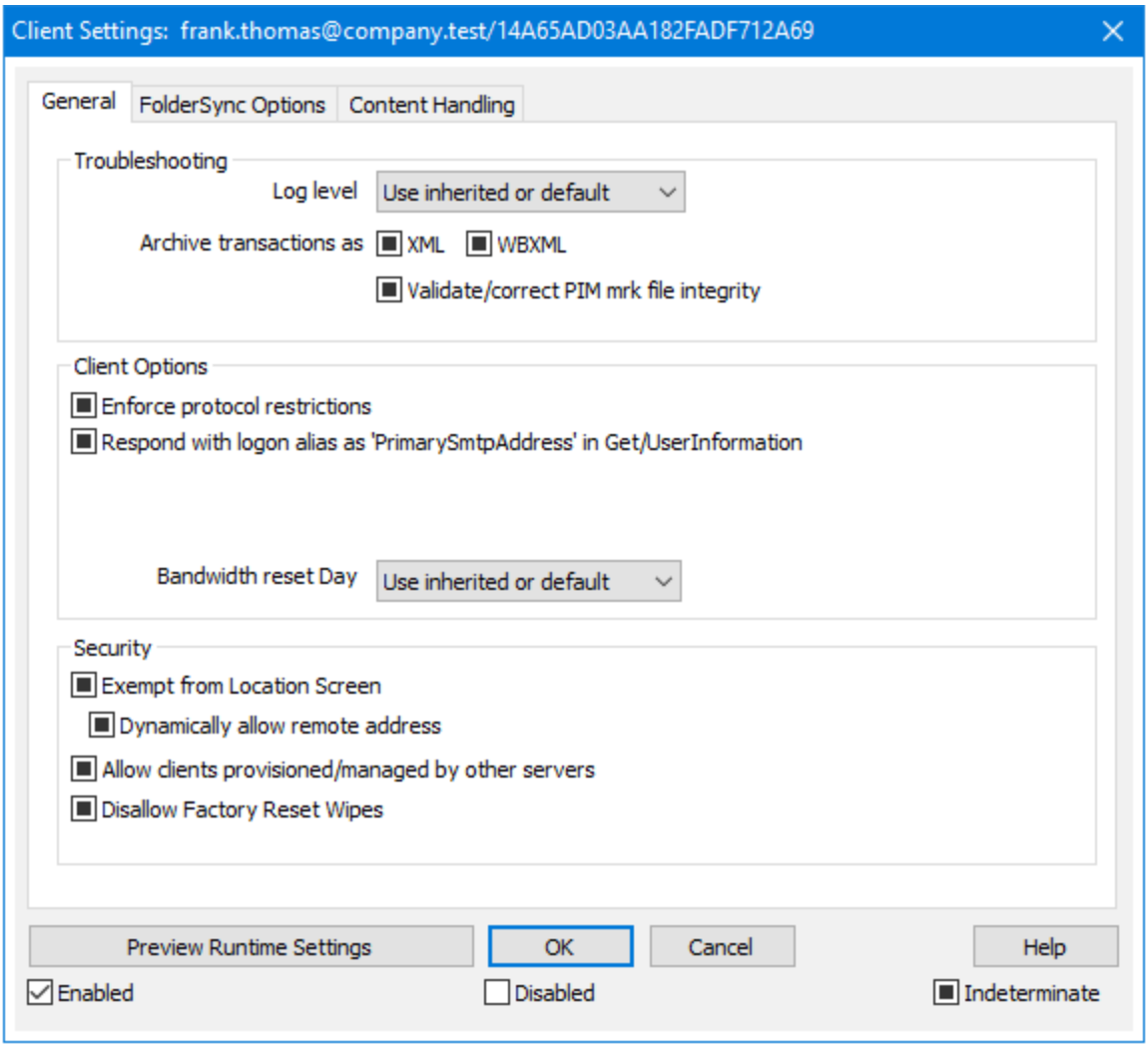
Authorizing Client

If the "*New clients require administrative approval*" option on the ActiveSync Client Settings 413 screen is set to require approval, select a client and click Approve client to sync, to authorize it for synchronization with the server.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the Client-Types Client Settings 466 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the client-type-level setting for this device.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.
Inherit	By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder

By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders

By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders

By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy

Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching

Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)

By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders

Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

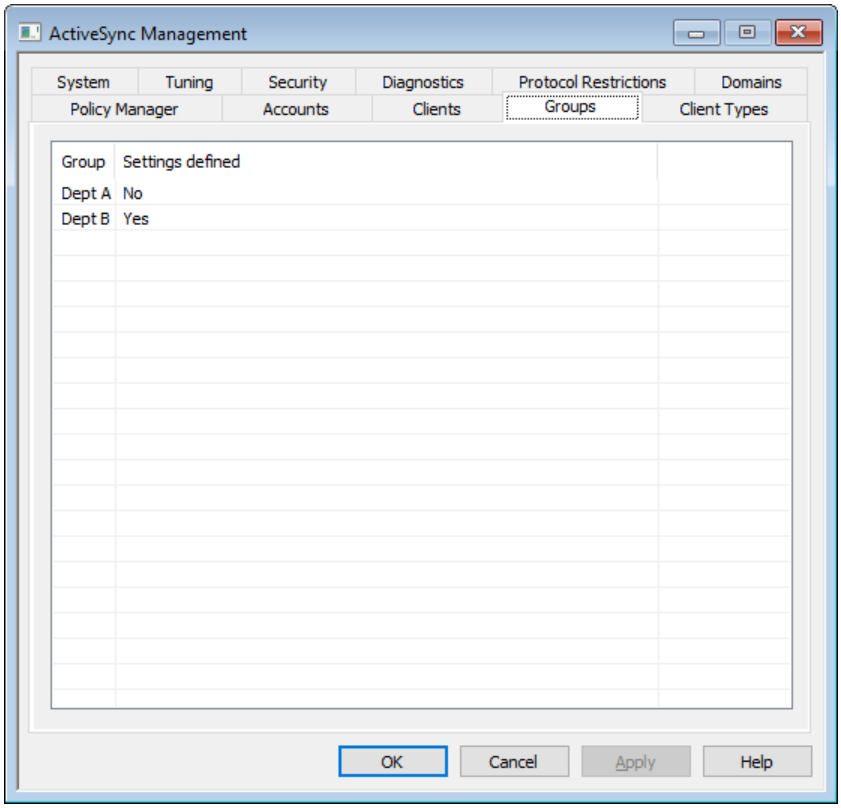
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Client Settings 413
ActiveSync » Domains 426
ActiveSync » Accounts 442

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

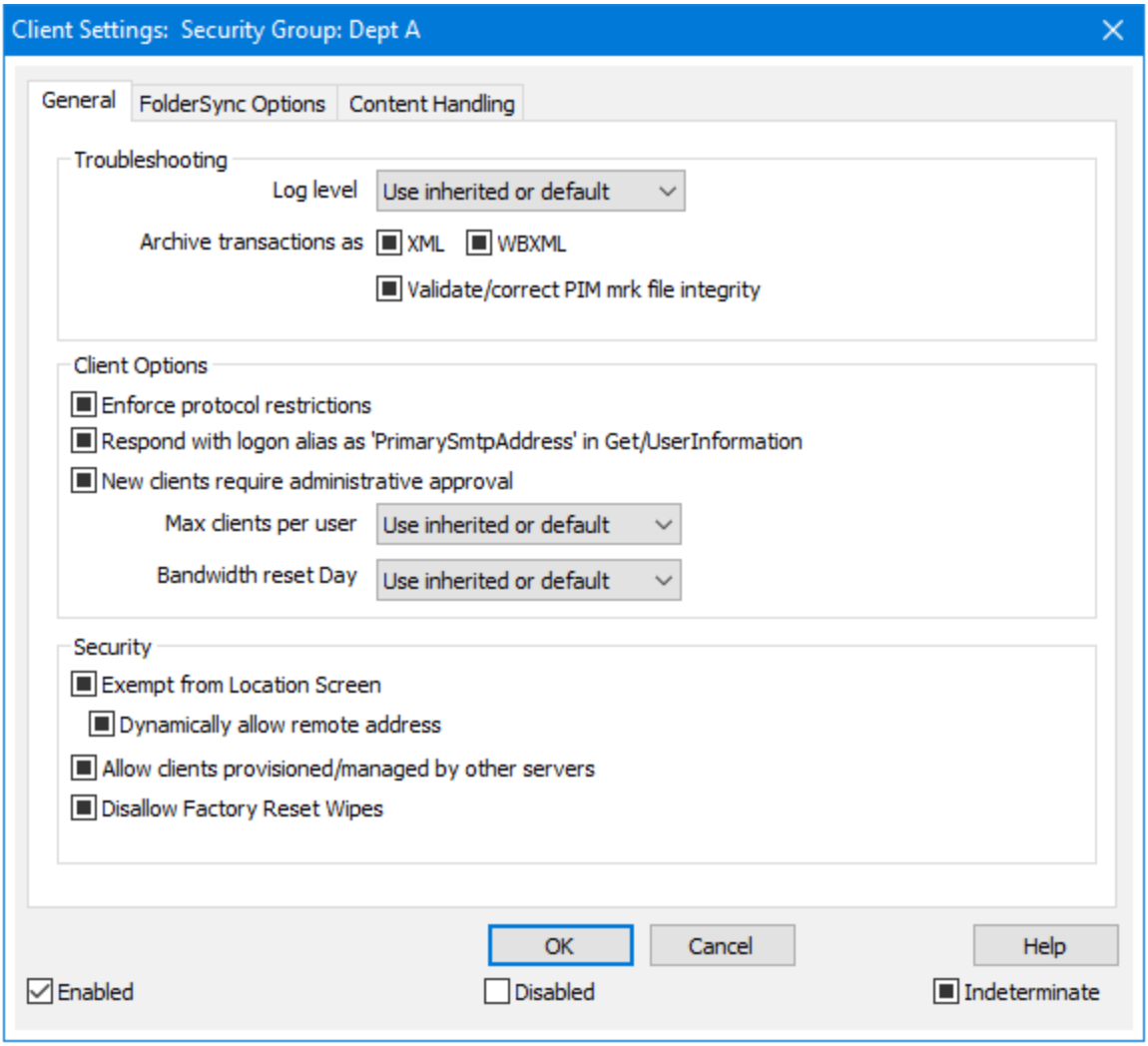
3.10.10 Groups



If you wish to define customized ActiveSync Client Settings for an account Group 764, use this screen to manage those settings. All groups are listed here, and each group's entry indicates whether or not customized settings have been defined for it. To edit a Group's Client Settings, double-click the Group, or right-click the Group and click **Customize Client Settings**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Group Client Settings



By default each Group client setting is set to inherit its state from the user's Domain Client Settings 208. Changing a group setting will override the domain setting for any account that is a member of the group. If you do not want the Group Client Settings to apply to a specific group member or device, then you can override the group settings by editing the Client Settings for the Account 442, Client Type 466, or Client 451.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder

By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders

By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders

By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy

Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching

Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)

By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders

Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

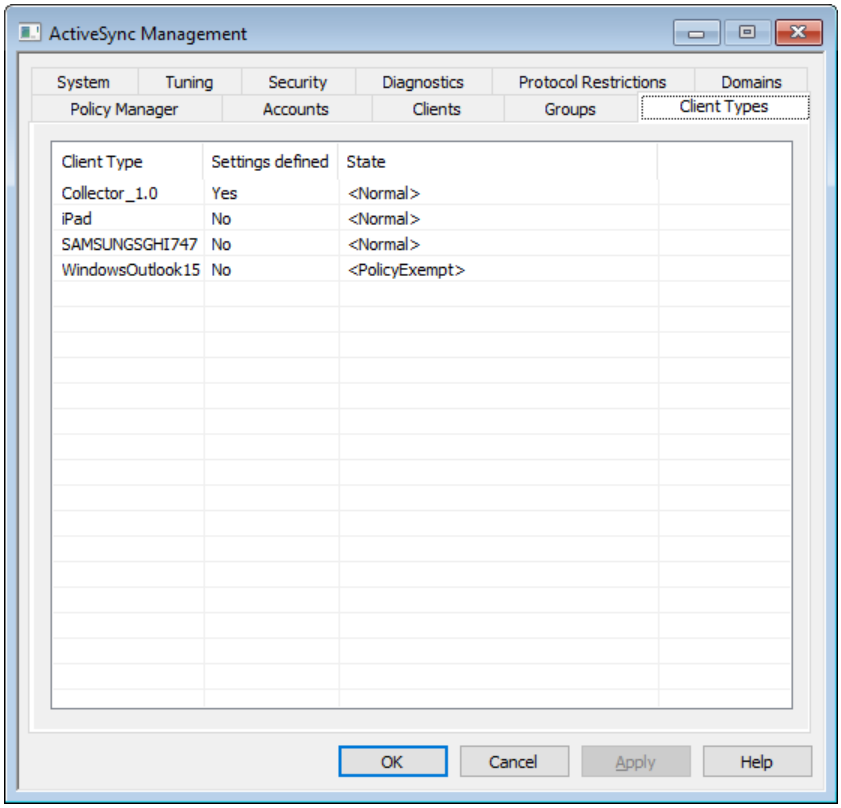
Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Domains 426
ActiveSync » Accounts 442
ActiveSync » Clients 451

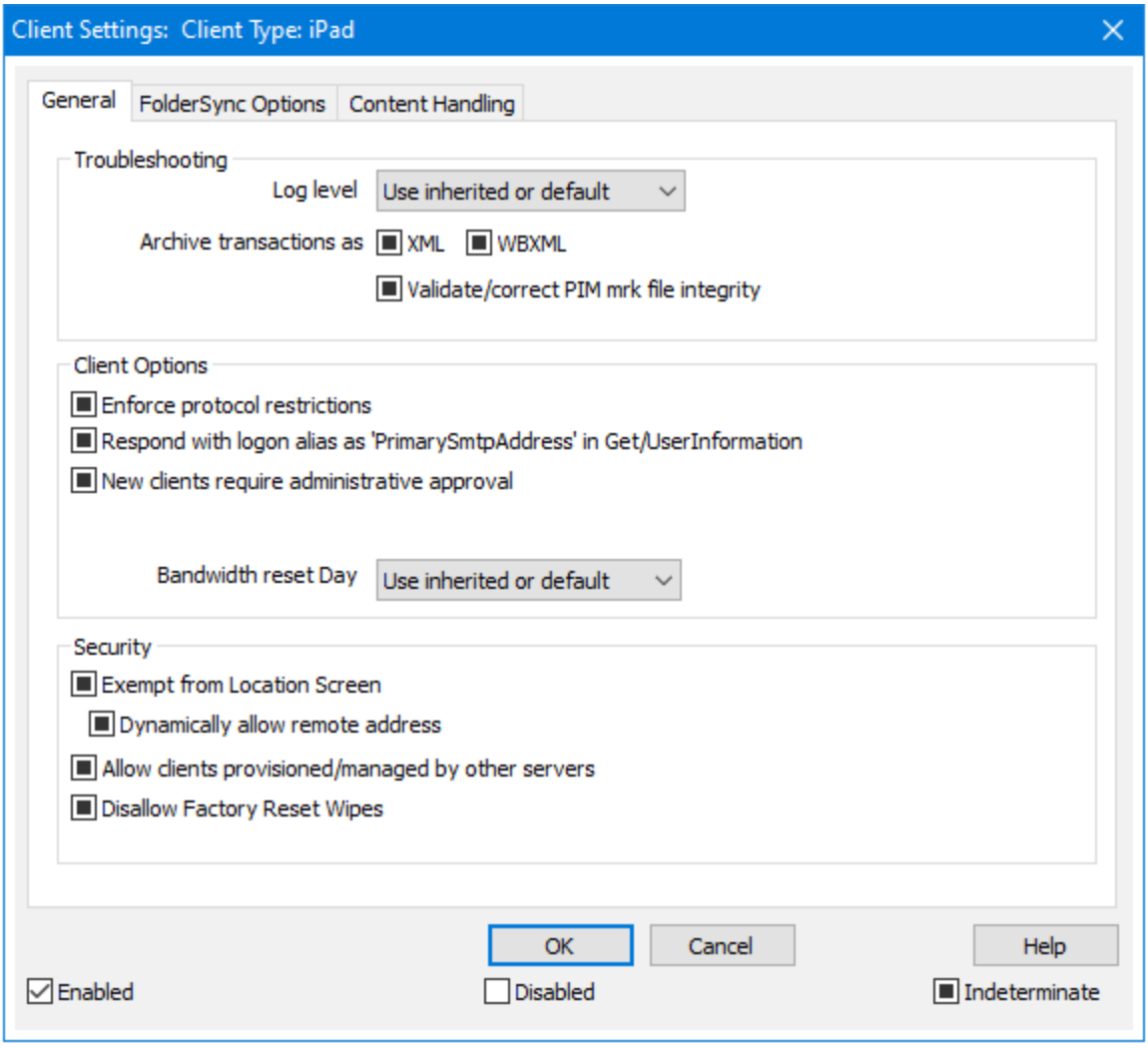
3.10.11 Client Types



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If you wish to define customized ActiveSync Client Settings for a specific type of ActiveSync client, use this screen to manage those settings. The Client-Type of all clients currently authorized 451 to use ActiveSync are listed here, and each Client-Type's entry indicates whether or not its settings have been defined. To edit a Client-Type's Client Settings, double-click the entry, or right-click it and click **Customize Client Settings**. You can also right-click an entry to remove the customized settings or add or remove the Client-Type from the ActiveSync Allow List or Exempt List 420.

Client-Type Client Settings



By default each Client-Type client setting is set to inherit its state from the Account Client Settings 748. Changing a Client-Type setting will override the account setting for any account using a client of that type. If you do not want the Client-Type Client Settings to apply to a specific client, then you can override Client-Type settings by editing that Client's Client Settings 451.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]

Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity

This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions

Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Shared folders
Check this box if you want the shared folders 113 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders 726 to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients 451 and client types 466 that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

added to the Exchange ActiveSync (EAS) protocol 424 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias 818 for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

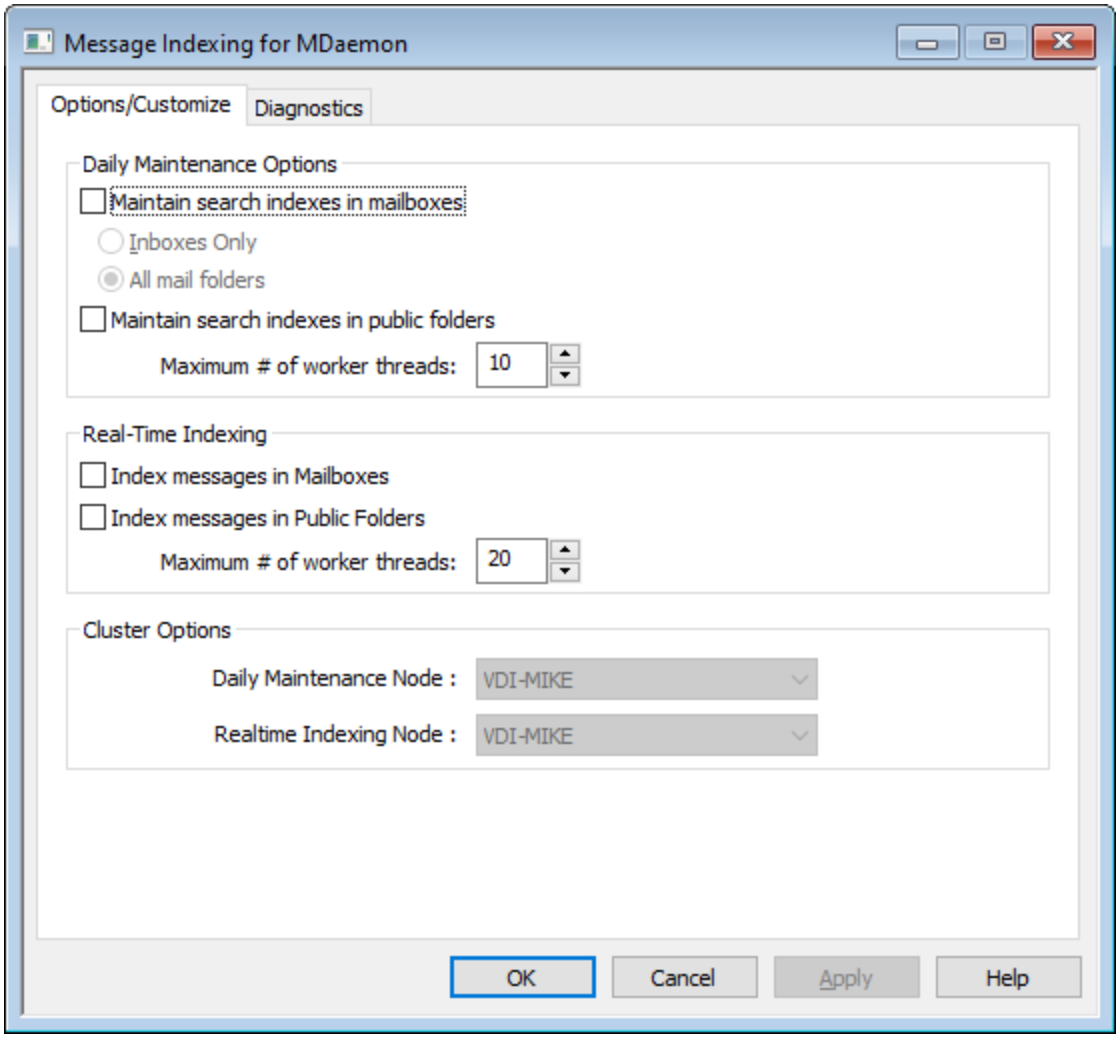
See:

ActiveSync » Accounts 442
ActiveSync » Clients 451
ActiveSync » Security 420

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.11 Message Indexing

3.11.1 Options/Customize



The Message Indexing dialog is used for the configuration of real-time and nightly maintenance of the search indexes used by Webmail, ActiveSync, and Remote Administration.

Daily Maintenance Options

The options in this section govern nightly search indexing.

Maintain search indexes in mailboxes
Check this box if you wish to maintain search indexes in your mailbox folders. You can choose to do this for either Inboxes only or for all mail folders.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Maintain search indexes in public folders
Enable this option if you wish to maintain search indexes in your public folders. You can also specify a maximum number of threads that will be allowed to work on this simultaneously.

Real-Time Indexing

Index messages in Mailboxes
Enable this option if you wish to perform real-time search indexing in Mailboxes, so that search indexes are always up to date.

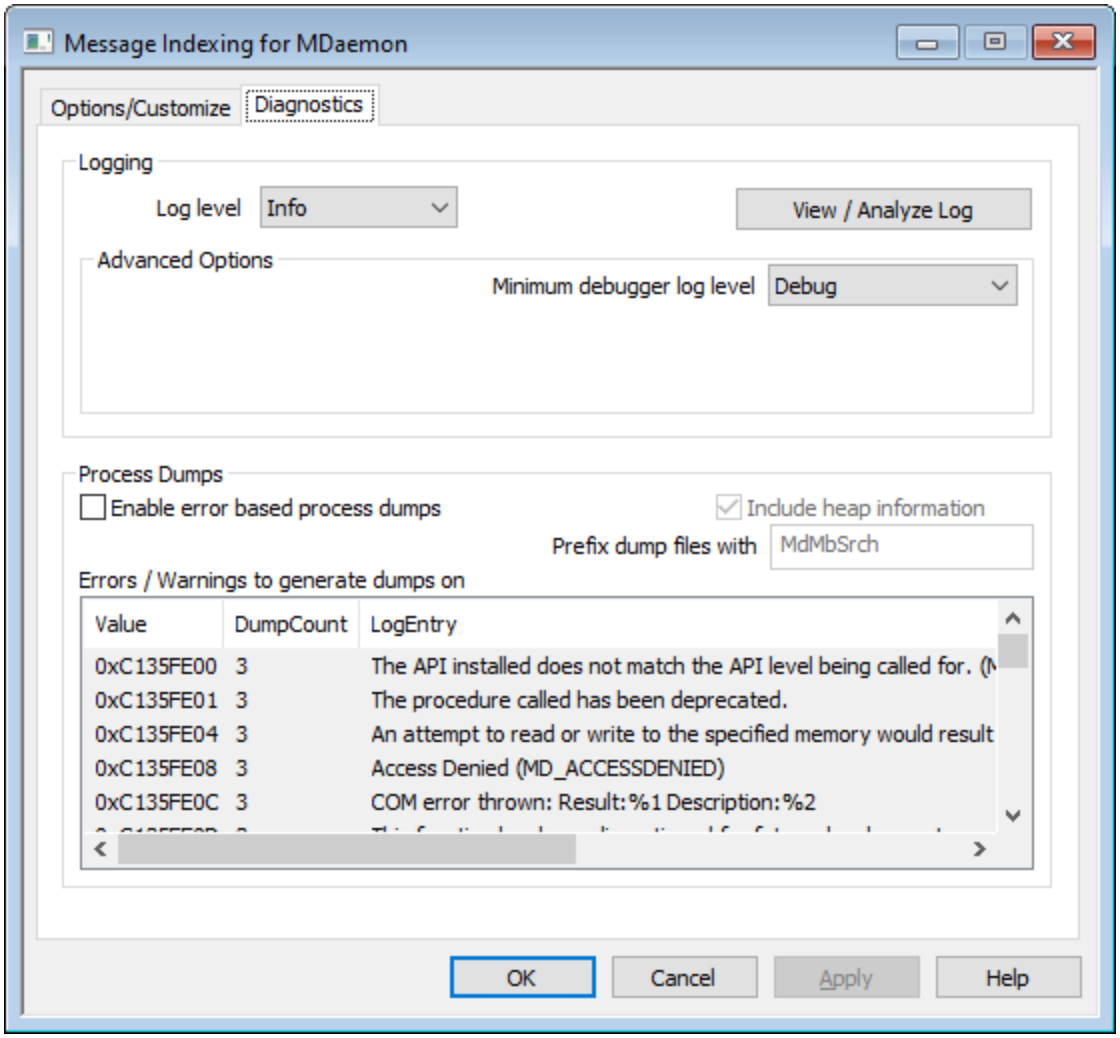
Index messages in Public Folders
Check this box if you wish to do real-time search indexing of Public Folders.

Cluster Options

If using Clustering, use the options is this section to designate the cluster nodes that will be dedicated to daily indexing maintenance and real-time indexing.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.11.2 Diagnostics



This screen contains advanced options that in most cases will not need to be used unless you are attempting to diagnose a problem with Message Indexing or are dealing with technical support.

Logging

Log level
Six levels of logging are supported, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem, or when the administrator wants detailed information.

Info Moderate logging. Logs general operations without details. This is the default log level.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.

View/Analyze Log
Click this button to open the MDaemon Advanced System Log Viewer. By default the logs are stored in: "..\MDaemon\Logs\"

Advanced Options

Minimum debugger log level
This is the minimum level of logging to emit to the debugger. The available log levels are the same as those outlined above.

Process Dumps

Enable error based process dumps
Enable this option if you want to generate process dumps whenever a specific warning or error occurs that you have designated below.

Include heap information in dumps
By default, heap information is included in the process dumps. Clear this checkbox if you do not wish to include it.

Prefix dump files with
Process dump filenames will begin with this text.

Errors/Warnings to generate dumps on
Right-click this area and use the *Add/Edit/Delete Entry...* options to manage the list of errors or warnings that will trigger process dumps. For each entry you can specify the number of process dumps allowed before it will be deactivated.

See:

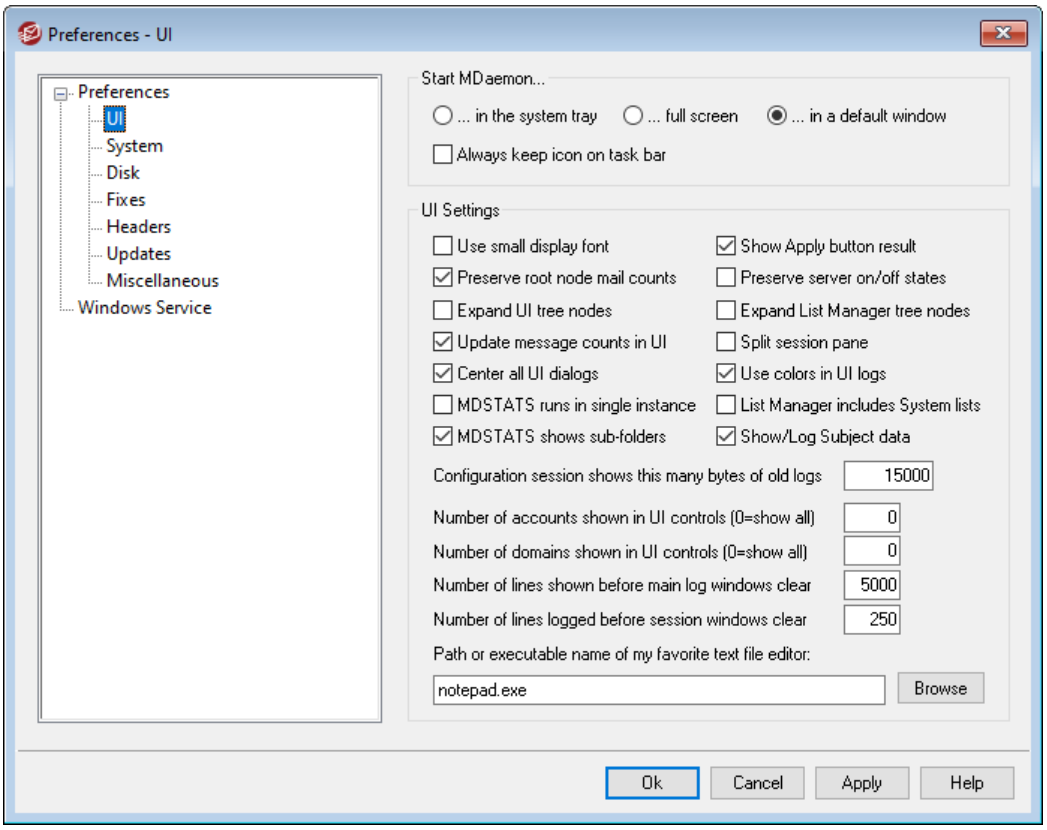
Dynamic Screening » Options/Customize 596

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.12 Preferences

3.12.1 Preferences

3.12.1.1 UI



Start MDaemon...

...in the system tray
Choose this option if you do not wish to display MDaemon's interface at startup. The MDaemon icon will still appear in the system tray.

...full screen
Choose this option if you want MDaemon's interface to be maximized at startup.

...in a default window
Choose this option if you want MDaemon's interface to appear in a default window at startup.

Always keep icon on task bar
When this option is enabled, MDaemon will start minimized to the taskbar, and it will appear on both the taskbar and in the system tray when minimized. Clear this checkbox if you do not want MDaemon to appear on the Windows taskbar when minimized; only the tray icon will be visible.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

UI Settings

Use small display font
Enables the small display font in the Event Tracking and Session windows.

Show Apply button result
By default, whenever you click the Apply button on a dialog a message box will open confirming that the changes you made to the dialog's settings have been saved. Uncheck this box if you wish to apply the changes without displaying the message.

Preserve root node mail counts
Enable this option if you wish to save the root node counters across server reboots. The root node counters are listed in the "Statistics" section of the Stats pane on MDaemon's main GUI.

Preserve server on/off states
If this control is enabled, MDaemon will ensure that the state of its servers (enabled or disabled) remains the same after a reboot.

Expand UI tree nodes
Click this box if you want the navigation tree nodes in the left-hand pane of various dialog to be expanded automatically. This does not apply to the Mailing List Manager 259. If you wish to automatically expand the mailing list tree nodes, use the *Expand List Manager tree nodes* option below.

Expand List Manager tree nodes
Click this checkbox if you want the Mailing List Manager's 259 navigation tree nodes in the left-hand pane to be expanded automatically.

Update message counts in UI
This option governs whether MDaemon will check the disk to count waiting messages in the mail queues.

Split session pane
Enable this option if you want the Sessions tab in the main MDaemon UI to be split from the other tabs into its own pane. Changing this setting requires a restart of the MDaemon UI, and the option on the Windows menu to switch panes will no longer be available.

Center all UI dialog
By default all dialogs are centered on the screen when they are opened, rather than overlap each other. Clear this checkbox if you wish dialogs to overlap, but this can occasionally cause them to be partially off the screen or out-of-frame.

Use colors in UI logs
This option will colorize the text displayed on several of the Event Tracking and Logging 69 tabs on MDaemon's user interface. It is enabled by default, and changing its setting will require an MDaemon interface restart before the change will take effect. See: Colorized Session Logs 172 for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

List Manager includes System lists
Enable this option if you wish to display MDaemon's system-generated mailing lists (e.g. Everyone@ and MasterEveryone@) in the Mailing List Manager 259. System generated lists have limited items available for user configuration. When this option is disabled, system lists will be hidden but still available for use. This option is disabled by default.

MDSTATS runs in single instance
Click this checkbox if you do not want more than one copy of MDaemon's Queue and Statistics manager 867 to be able to run at once. Attempting to launch the manager when it is already running will simply cause the currently running instance to become the active window.

MDSTATS shows subfolders
Click this checkbox if you want the Queue and Statistics manager 867 to display subfolders contained in the various queues and user mail folders.

Show/Log Subject data
By default the Subject: line data is shown in MDaemon UI tabs and written into log files. Note, however, that the Subject: line can contain information the sender of a message would not wish to display and wouldn't want tracked into log files, and mailing lists can have a password which users place in the Subject: line. Therefore disabling this option is recommended.

Configuration session shows this many bytes of old logs
When running a configuration session, this is the maximum amount of log data that will be displayed on an Event Tracking and Logging 69 tab. The default setting is 15000 bytes.

Number of accounts shown in UI controls (0=show all)
This is the maximum number of accounts that will be shown in the drop-down list boxes on various dialogs. Further, when the value in this option is set lower than the number of accounts that currently exist, the "Edit Account" and "Delete Account" options will no longer appear on the Accounts menu; you will only be able to edit and delete accounts by using the Account Manager 694. You must restart MDaemon before any changes to this option will take effect. The default setting is "0", which causes all accounts to be shown.

Number of domains shown in UI controls (0=show all)
This is the maximum number of domains that will be displayed on the main GUI, regardless of how many domains actually exist. After changing this value you must restart MDaemon before the changes will be visible. The default setting is "0", which causes all domains to be shown.

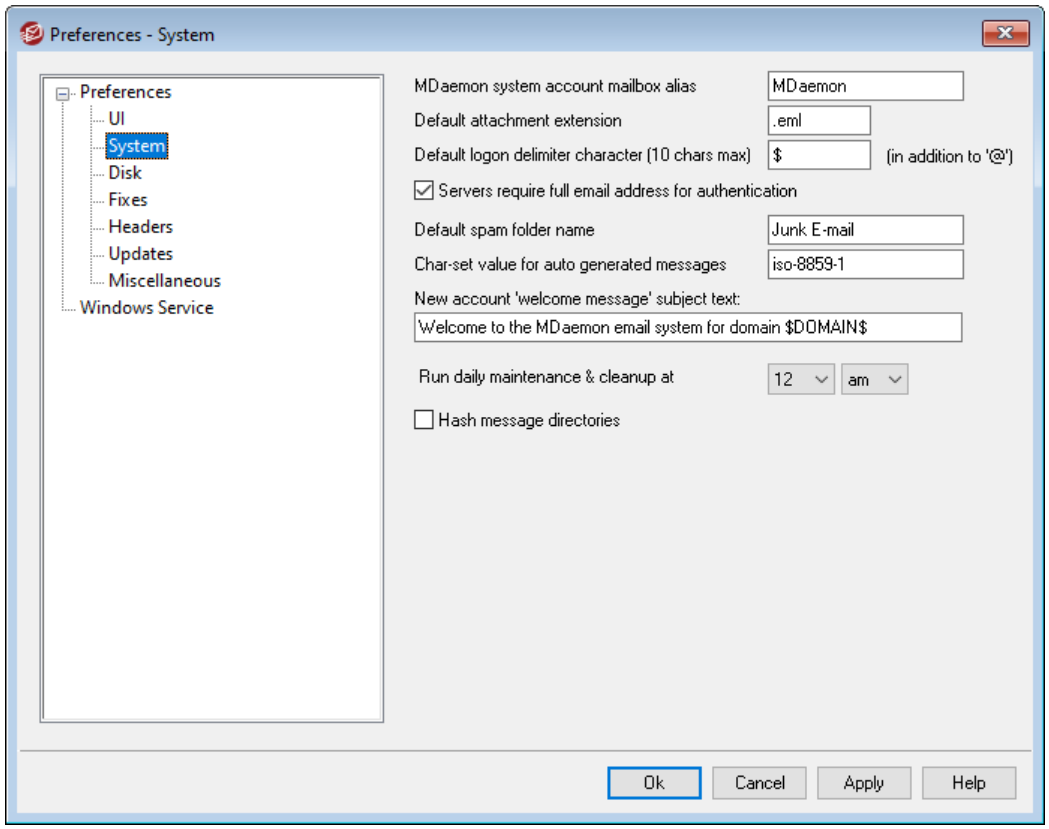
Number of lines shown before main log windows clear
This is the maximum number of lines that will be displayed in the logging windows of the main display. When this number of lines is reached the window will be cleared. This has no affect on the log file; only the display will be cleared.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Number of lines logged before session windows clear
This is the maximum number of lines that will appear in each Session Window 82 before it is cleared. This has no affect on the log file.

Path or executable name of my favorite text file editor
Notepad.exe is the general text editor that the MDaemon UI will launch by default when needed. If you prefer to use a different text editor, enter its file path or executable name here.

3.12.1.2 System



MDaemon system account mailbox alias [address]
This is the email address from which system generated messages will come. Subscription confirmations, delivery status notification (DSN) messages, various other notification messages, and the like are all system messages.

Default attachment extension
System generated messages will be created using this extension. This will also be the extension assigned to attachments included with system generated messages. For example, if MDaemon generates a warning message to the postmaster about a specific message it will attach that message with this value as the file extension.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Default logon delimiter character (10 characters max)
When using an email address as the account logon parameter, this character or string of characters can be used as an alternative to "@". This may be necessary for some users that have email clients which do not support "@" in the logon field. For example, if you used "$" in this field then users could login using "user1@example.com" or "user1$example.com".

Servers require full email address for authentication
MDaemon's POP and IMAP servers require you to use your full email address by default when logging in to MDaemon. If you wish to allow mailbox only logins (e.g. "user1" instead of "user1@example.com") then you can disable this option, but it is not recommended as mailbox only logins are ambiguous when MDaemon is serving multiple domains.

Default spam folder name
Use this text box to specify the default name for the Spam folder that MDaemon can create automatically for your users. The default name is "Junk E-mail" to match the default value of various other widely distributed products.

Char-set value for auto-generated messages
Specify the character set that you wish to be used for auto-generated messages. The default setting is iso-8859-1.

New account "welcome message" subject text:
MDaemon typically sends a "welcome message" to new accounts. The text specified here will appear as the message's "Subject" header. The welcome message is constructed from the `NEWUSERHELP.DAT` file contained in the `…\MDaemon\app\` folder, and this subject header may contain any macros permitted in auto response scripts 828.

Run daily maintenance and cleanup at [1-12] [am/pm]
Use this option to set the hour at which the daily maintenance and cleanup event takes place. The default and recommended setting is 12am.

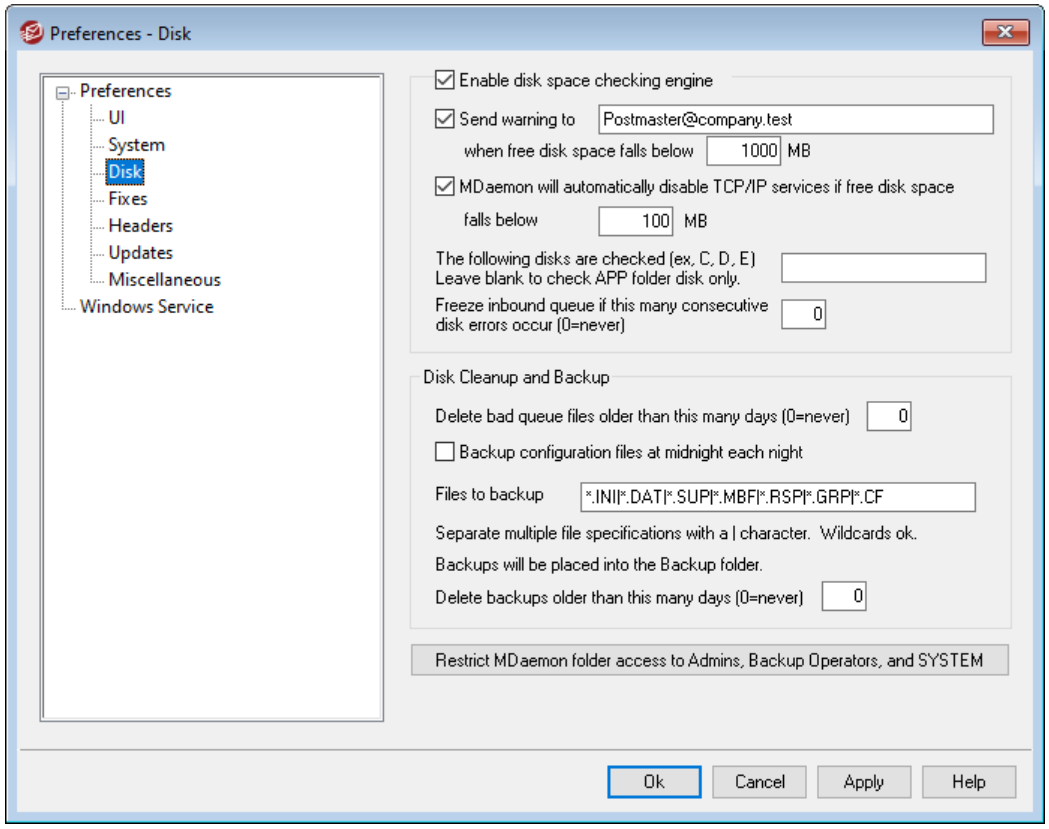
Regardless of the hour you set for this option, there are some daily events that will always happen at midnight, such as log file maintenance and running `midnight.bat`.

Move account mail folders when domain or mailbox values change
If this checkbox is enabled, when you change a domain name or mailbox the mail folders for the affected accounts will be moved to the new location. Otherwise, MDaemon will continue to use the old mail folder names.

Hash message directories
Click this check box if you wish to enable directory hashing — MDaemon will hash certain directories by making up to 65 sub-directories. Hashing can increase performance for certain hi-volume sites but may degrade performance slightly for typical MDaemon sites. This option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.12.1.3 Disk



Enable disk space checking engine
Activate this checkbox if you want MDaemon to monitor the amount of disk space that is available on the drive where the `MDaemon.exe` is located.

Send warning to [user or address] when free disk space falls below [xx] MB
By using this option you can configure MDaemon to send a notification message to the user or address of your choice when disk space drops below a certain level. The default value is 1000 MB.

MDaemon will automatically disable TCP/IP services if free disk space falls below [xx] MB
Enable this feature if you want MDaemon to disable TCP/IP Services if free disk space drops to a certain level. The default value is 100 MB.

The following disks are checked (ex: C, D, E)
Use this option if you wish to monitor the available disk space on multiple disks, specifying the drive letter for each one. If you leave it blank then only the disk that contains MDaemon's `\app\` folder will be checked.

Freeze inbound queue if this many consecutive disk errors occur (0=never)
If this number of disk errors occurs when processing the inbound queue, MDaemon will stop processing the queue until you resolve the situation. An email is placed in the postmaster's mailbox when this shut down occurs.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Disk cleanup and backup

Delete bad queue files older than this many days (0=never)
Use this option if you want MDaemon to delete old files from the bad message queue whenever they are older than the specified number of days. If you do not wish to delete messages automatically, use "0" in this option.

Backup configuration files at midnight each night
Click this checkbox if you want to archive all MDaemon configuration files at midnight each night to the Backups directory.

Files to backup
Use this text box to specify exactly which files and file extensions to back up. Wildcards are permitted and each filename or extension must be separated be the "|" character.

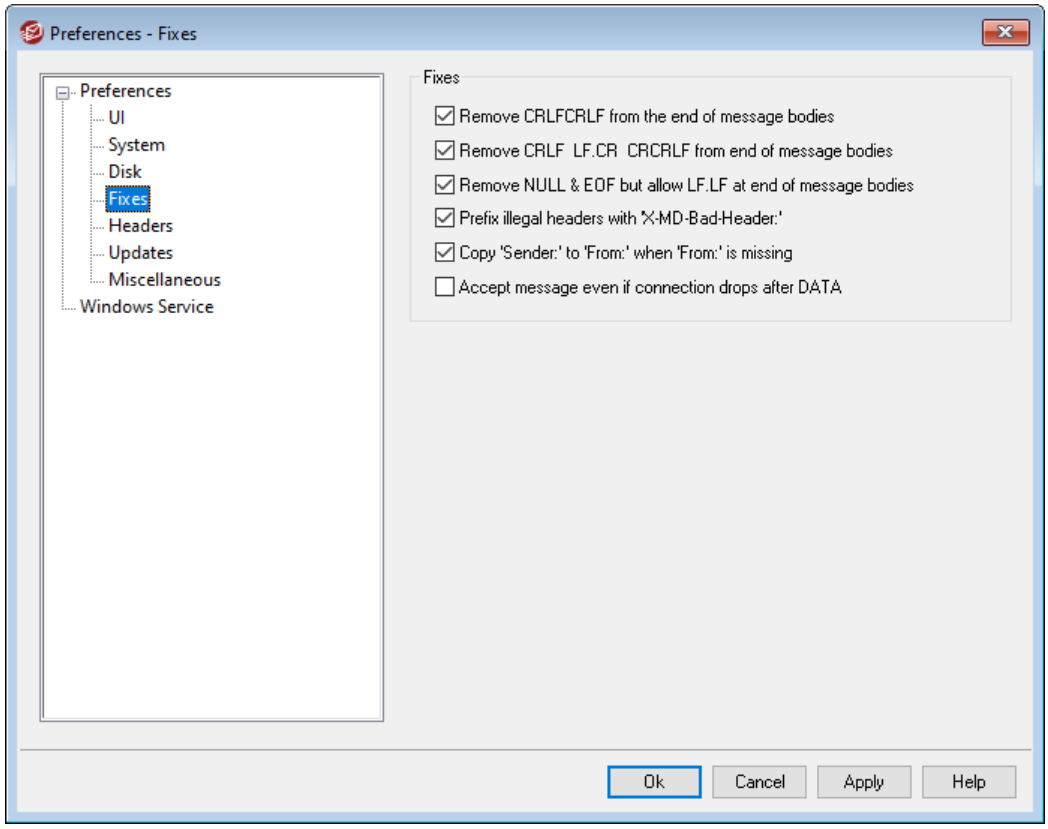
Delete backups older than this many days (0=never)
Use this option if you wish to delete old backup files automatically. Files older than the specified number of days will be deleted as part of the daily midnight cleanup event. The default setting is "0", which means that old backup files will not be deleted.

Restrict MDaemon folder access to Admins, Backup Operators, and SYSTEM

Click this button to restrict access to the `\MDaemon\` root folder and its subfolders to the following Windows accounts/groups: Administrators, Backup Operators, and SYSTEM.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.12.1.4 Fixes



Remove CRLFCRLF from the end of message bodies
Certain mail clients have problems displaying messages that end with consecutive Carriage Return Line Feeds (i.e. CRLFCRLF). When this box is checked, MDaemon will strip consecutive `CRLFCRLF` sequences from the end of the message body. This option is enabled by default.

Remove CRLF LF.CR CRCRLF from the end of message bodies
By default, MDaemon will remove this sequence from the end of messages, as it can cause problems for some mail clients. Uncheck this box if you do not wish to remove this sequence from messages.

Remove NULL & EOF but allow LF.LF at the end of message bodies
When this box is checked MDaemon will remove `Null` and EOF characters from the end of message bodies, but it will allow messages ending in `LF.LF`, as well as messages ending with the normal `CRLF.CRLF` sequence that signifies the end of a message. This option is enabled by default.

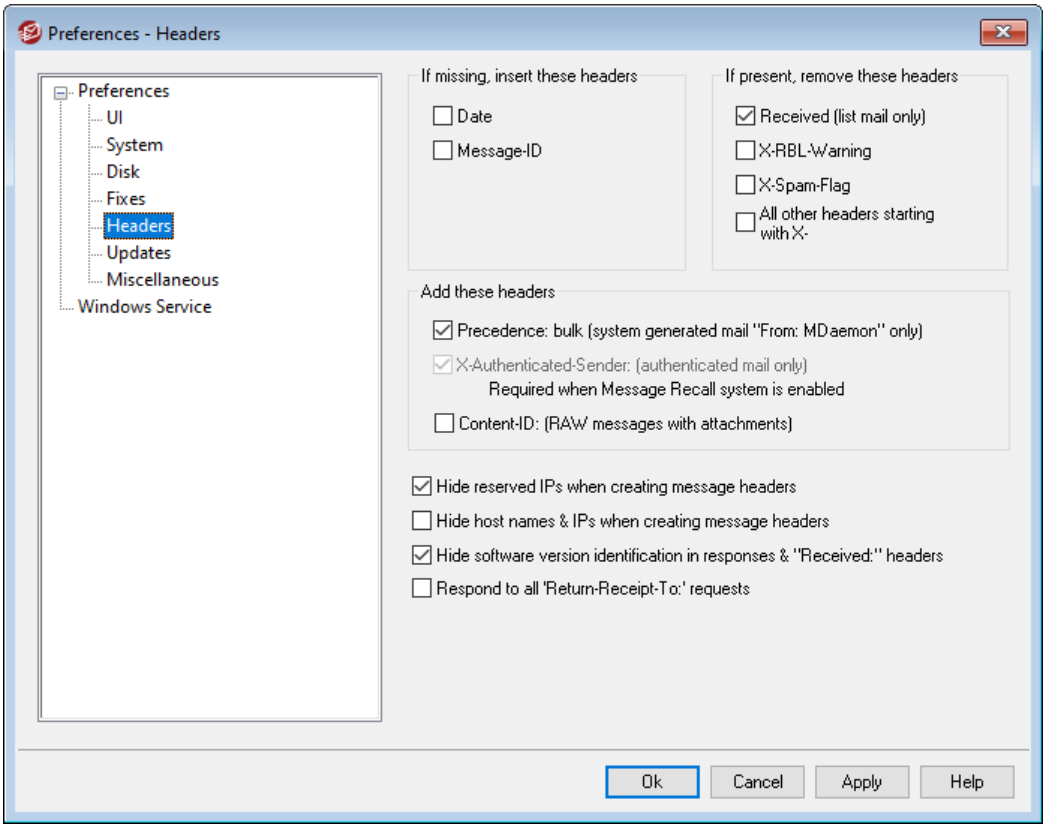
Prefix illegal headers with "X-MD-Bad-Header:"
When this option is enabled and MDaemon encounters a bad message header, it will prefix the bad header with "`X-MD-Bad-Header:`" This option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Copy 'Sender:' to 'From:' when 'From:' is missing
Some mail clients fail to create a `FROM:` header when you compose a message. Instead, the `FROM:` header's information is placed in the `Sender:` header. This can cause problems for some mail servers as well as the recipient of your message. To help prevent these problems, MDaemon will create the missing `FROM:` header by using the contents of the `Sender:` header when this box is checked. This option is enabled by default.

Accept message even if connection drops after DATA
When this option is enabled, MDaemon will accept and deliver a message even if there's a connection abort during or immediately after the `DATA` command during the SMTP process. This should not be used under normal circumstances as it can lead to duplicate messages.

3.12.1.5 Headers



If missing, insert these headers

Date
When a message is encountered that doesn't have a "`Date:`" header, MDaemon will create one and add it to the message file if this option is enabled. It will be the date on which MDaemon first receives the message, not when it was created by the sender. There are some mail clients that do not create this header, and since some

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

mail servers refuse to honor such messages, this feature will enable them to be delivered.

Message-ID
When a message is encountered that doesn't have a "Message-ID" header, MDaemon will create one and insert it into the message.

If present, remove these headers

Received (list mail only)
Check this box if you wish to strip all existing "Received:" headers from mailing list messages.

X-RBL-Warning
Click this checkbox if you wish to strip out all "X-RBL-Warning:" headers found in messages. This option is disabled by default.

X-Spam-Flag
Enable this option if you wish to strip old "X-Spam-Flag:" headers from messages.

All other headers starting with X-
MDaemon and other mail servers use many server specific headers called X-Type headers in order to route mail and perform various other functions. When this option is enabled, MDaemon will strip these headers from messages. **Note:** this option does not remove X-RBL-Warning headers. If you wish to remove those headers, use the "*X-RBL-Warning*" option above.

Add these headers

Precedence: bulk (system generated mail 'From: MDaemon' only)
When this box is checked all system generated messages from MDaemon (welcome messages, warnings, "could not deliver" messages, and so on) will have a "Precedence: bulk" header inserted.

X-Authenticated-Sender: (authenticated mail only)
By default MDaemon will add the "X-Authenticated-Sender:" header to messages that arrive on an authenticated session using the AUTH command. Uncheck this box if you do not wish to add this header.

Content-ID: (RAW messages with attachments)
Check this box if you wish to add unique MIME Content-ID headers to messages that MDaemon creates from a RAW file that contains attachments.

Hide reserved IPs when creating message headers
This option is enabled by default and prevents reserved IP addresses from appearing in certain MDaemon created message headers. Reserved IP addresses include: 127.0.0.*, 192.168.*.*, 10.*.*.*, and 172.16.0.0/12. If you also wish to hide your domain IPs (including LAN domains) from the headers then you can set the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

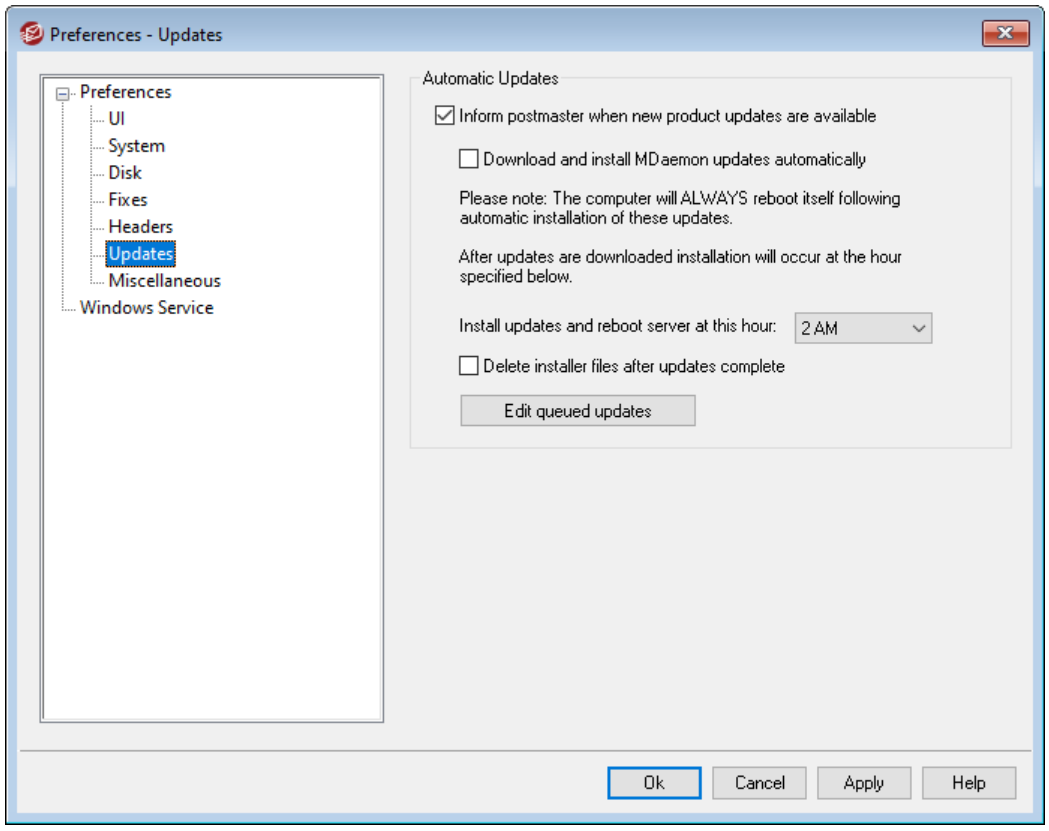
following switch in MDaemon's `app\MDaemon.ini` file manually: `[Special] HideMyIPs=Yes` (default is `No`).

Hide host names and IPs when creating message headers
Click this option if you wish to omit host names & IP addresses from "Received:" headers when they are constructed. This option is disabled by default.

Hide software version identification in responses and 'Received:' headers
Use this option if you wish to prevent MDaemon from stating its software version and other identifying information when creating `Received` headers or responding to various protocol requests. This option is disabled by default.

Respond to all 'Return-Receipt-To:' requests
Click this check box if you wish to honor requests for delivery confirmation from incoming messages and automatically send a confirmation message to the sender. This option is disabled by default.

3.12.1.6 Updates



Automatic Updates

Using the Automatic Updates features you can configure MDaemon to inform the postmaster whenever an update is available for MDaemon, and you can set it to download and install the updates automatically. The server will always be rebooted

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

whenever an update is installed automatically. Files are downloaded when the update is detected, but the installation and reboot occur later at whichever hour you have designated. All installation activity is logged in the MDaemon system log, and the postmaster is informed after an update has occurred.

Inform postmaster when new product updates are available
This option causes MDaemon to notify the postmaster whenever there is an MDaemon update available. This is enabled by default.

WhenMDaemon is set to update automatically, this message is not sent. Instead the postmaster is informed that an update was installed, and is informed of any Special Considerations regarding the update.

Download and install MDaemon updates automatically
Check this box if you want to download and install MDaemon updates automatically. Updates are downloaded when they are detected and then installed at the hour designated below. This option is disabled by default.

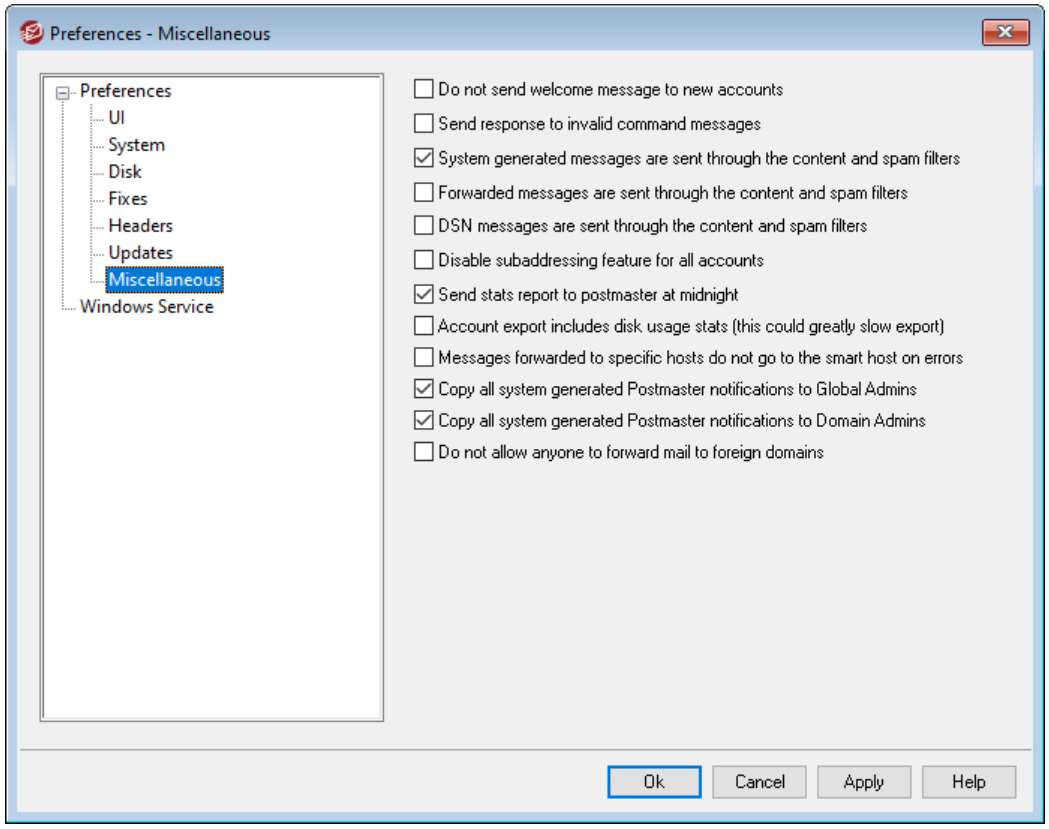
Install updates and reboot server at this hour:
Automatic updates are downloaded at the time they are detected and then stored in the `\MDaemon\Updates` folder, but they are not installed until the hour designated here. The server on which MDaemon is installed will be rebooted automatically after each update. This option is set to 2 AM by default.

Delete installer files after updates complete
Check this box if you wish to delete the stored installer files after an update is completed.

Edit queued updates
When an update is detected and downloaded, it is then queued for installation later. The list of pending updates is stored in the `QueuedUpdates.dat` file. Click this button to review that list or remove a pending update.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.12.1.7 Miscellaneous



Do not send welcome message to new accounts
By default, MDaemon will generate a Welcome message based upon the `NEWUSERHELP.DAT` file and distribute it to new users when their account is created. Enable this control if you want to prevent the message from being generated.

Send response to invalid command messages
By default when someone sends an email to the system account that does not contain a valid command, MDaemon does not respond with a "No valid command found" email. Enable this option if you wish to send a response to those emails.

System generated messages are sent through the content and spam filters
By default, system generated messages are processed through the Content Filter and Spam Filter. Clear this checkbox if you want them to be excluded from content and spam filtering.

Forwarded messages are sent through the content and spam filters
Check this box if you want forwarded messages to be processed through the Content Filter and Spam Filter. This is disabled by default.

DSN messages are sent through the content and spam filters
Enable this option if you wish to send DSN messages 864 through the content and spam filters. This option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Disable subaddressing feature for all accounts
Click this option if you wish to globally disable the Subaddressing feature. Subaddressing will not be permitted for any account, regardless of the individual account settings. For more on Subaddressing, see the IMAP Filters 720 screen of the Account Editor.

Send stats report to postmaster at midnight
By default a statistics report will be sent to the postmaster each night at midnight. Clear this checkbox if you do not want the report to be sent. This option corresponds to the Statistics 69 tab located on MDaemon's main display.

Account export includes disk usage stats (this could greatly slow export)
By default, account exports do not include disk file counts and space consumed. If you wish to include this information in exports, enable this checkbox. This may, however, significantly slow export speeds.

Messages forwarded to specific hosts do not go to the smart hosts on errors
Using the "Advanced Forwarding Settings" on the Account Editor's Forwarding 711 screen, accounts can be set to forward messages to a specific smart host rather than using MDaemon's standard delivery process. By default, when MDaemon encounters a delivery error when attempting to forward one of those messages, it will be placed in the bad message queue. Enable this option if you instead want MDaemon to place the message into the Retry Queue 856 for further delivery attempts using MDaemon's normal delivery process.

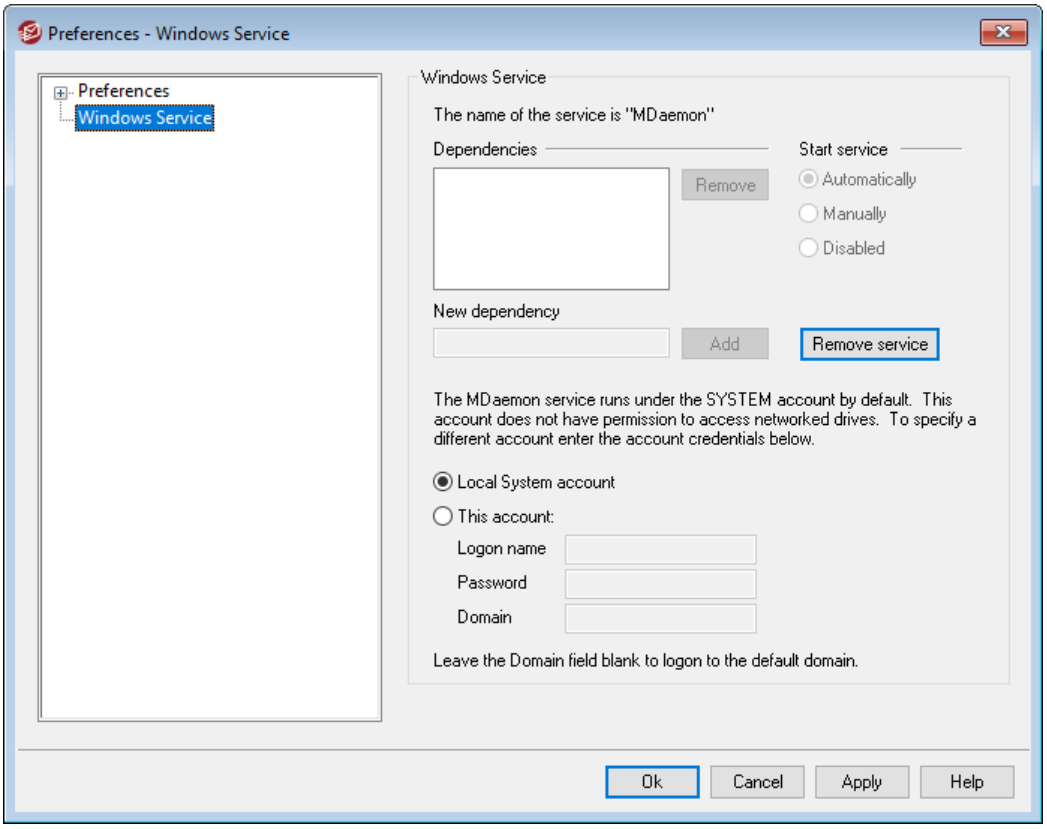
Copy all system generated Postmaster notifications to Global Admins
By default, system generated notifications sent to the Postmaster will also be sent to the Global Administrators 741. Global administrators receive everything including the Queue Summary report, Statistics report, Release Notes, 'No Such User' found (for all domains), Disk Error notifications, Account Freeze and Disable notifications for all domains (which, like Domain admins, they can unfreeze and re-enable), warnings about licenses and beta test versions about to expire, Spam Summary reports, and so on. If you do not want your global administrators to receive these notifications, disable this setting.

Copy all system generated Postmaster notifications to Domain Admins
By default, system generated notifications sent to the Postmaster will also be sent to the Domain Administrators 741. However, Domain Administrators are restricted to receiving only those emails that are for their domain. If you do not want your domain administrators to receive these notifications, disable this setting.

Do not allow anyone to forward mail to foreign domains
Check this box if you do not wish to allow account mail forwarding to send any emails outside the domain. If a user configures mail forwarding for their account to send to a foreign domain, the remote forwarding addresses are ignored. This setting only applies to messages that are forwarded using the mail forwarding options for the account. This setting only applies to messages that are forwarded using the mail forwarding options 711 for the account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3.12.2 Windows Service



Windows Service

When MDaemon is running as a service, the service's name is "MDaemon."

Dependencies

Use this option to designate any services what you wish to require to be running **before** the MDaemon service starts.

Start service

This is the initial state of the service: automatically starts, must be started manually, or disabled.

Install/Remove service

Click this button to install or remove the MDaemon service.

Network Resource Access

When running MDaemon as a Windows service, by default it runs under the SYSTEM account. Because this account does not have access to network devices, MDaemon will not be able to access mail if you wish to store it on other computers across your LAN. That is, not unless you provide logon credentials for an account that can be used to provide the MDaemon service access to network shares. If you need to do this then you can create a Windows user account specifically designed for running MDaemon with whatever restrictions that you desire, but which has access to those network

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

shares that you want MDaemon to be able to use. Further, all applications launched by MDaemon will use the same credentials.

Logon name
This is the logon name of the Windows account under which the MDaemon service should run.

Password
This is the Windows account's password.

Domain
This is the Windows Domain on which the account resides. Leave this field blank to login to the default domain.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section

4 Security Menu

MDaemon is equipped with an extensive suite of security features and controls. Click Security on MDaemon's menu bar to reach the following security features:

- **Health Check** 496 — This page provides a convenient list of important security settings consolidated onto a single page, and it displays each setting's current value and its default value. Where those values differ, the setting is highlighted so that the Global Administrators can quickly review those particular settings. If desired, admins can select any of those settings to change back to their default values, or they can click a link next to any setting to jump to the page where that setting is located. In addition, admins can easily undo the most recent change made on the Health Check page. They can also view previous changes made during the current browser session, and then undo specific changes. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.
- **AntiVirus** 630 — MDaemon AntiVirus can help you stop email-borne computer viruses by providing the highest level of integrated protection available for MDaemon customers. It will catch, quarantine, repair, and/or remove any email message found to contain any virus. AntiVirus also contains a feature called Outbreak Protection, which can be used to protect you from certain spam, phishing, and virus outbreaks that can sometimes be missed by the other traditional, content and signature-based security measures.
- **Content Filter** 631 — a highly versatile and fully multi-threaded Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and much more.
- **Spam Filter** 660 — uses spam filtering technology to heuristically examine email messages in order to compute a "score". This score is used to determine the likelihood of a message being spam. Based on that determination the server can then take certain actions such as refusing or flagging the message. See also: Spam Traps 690
- **DNS Block Lists** 683 —allows you to specify several DNS block listing services that will be checked each time someone tries to send a message to your server. If the connecting IP has been listed by any one of these hosts, the message will be refused.
- **Relay Control** 498 — used to control what MDaemon will do when a message arrives at your mail server that is neither from nor to a local address.
- **IP Shield** 507 — if a domain name specified in this list attempts to connect to your server, its IP address must match the one that you have assigned to it.
- **Reverse Lookup** 500 — MDaemon can query DNS servers to check the validity of the domain names and addresses reported during incoming messages. Controls on this screen can be used to cause suspicious messages to be refused or a special header inserted into them. Reverse Lookup data will also be reported in the MDaemon logs.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- **POP Before SMTP** 504 — the controls on this screen are used to require each user to first access his or her mailbox before being allowed to send a message through MDaemon, thus authenticating that the user is a valid account holder and allowed to use the mail system.
- **Trusted Hosts** 505 — domain names and IP addresses that will be considered as exceptions to the relay rules listed on the Relay Control screen.
- **SMTP Authentication** 509 — used for setting several options that denote how MDaemon will behave when a user sending a message to MDaemon has or has not been authenticated first.
- **SPF** 512 — Most domains publish MX records to identify the machines that may receive mail for them, but this doesn't identify the locations allowed to send mail for them. Sender Policy Framework (SPF) is a means by which domains can also publish "reverse MX" records to identify those locations authorized to send messages.
- **DomainKeys Identified Mail** 514 — DomainKeys Identified Mail (DKIM) is an email verification system that can be utilized to prevent spoofing. It can also be used to ensure the integrity of incoming messages, ensuring that the message hasn't been tampered with between the time it left the sender's mail server and arrived at yours. This is accomplished by using an encrypted public/private key pairs system. Outgoing messages are signed using a private key and incoming messages have their signatures verified by testing them with the public key published on the sender's DNS server.
- **Certification** 538 — Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. The Certification feature is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It can also help lower the resources required to process each message.
- **Sender Block List** 545 — lists addresses that are not allowed to send mail traffic through your server.
- **IP Screen** 548 — used to designate IP addresses from which you will allow or refuse connections to your server.
- **Host Screen** 550 — used to designate hosts (domain names) from which you will allow or refuse connections to your server.
- **Dynamic Screening** 596 — Using Dynamic Screening, MDaemon can track the behavior of incoming connections to identify suspicious activity and then respond accordingly. You can block an IP address 600 (or range of addresses) from connecting when it fails authentication a specified number times within a specified amount of time. You can also freeze the accounts 600 attempting to authenticate when they fail too many times too quickly.
- **SSL & TLS** 561 — MDaemon supports the Secure Sockets Layer (SSL) protocol for SMTP, POP, and IMAP, and for Webmail's web server. SSL is the standard method for securing server/client Internet communications.
- **Backscatter Protection** 582 — "Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a Return-Path address that is forged. Backscatter Protection helps prevent this by ensuring that only

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the Return-Path address of your users' outgoing messages.

- **Bandwidth Throttling** 585 — the Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress, setting different rates for each of MDaemon's major services on a per-domain basis, including Domains and Domain Gateways.
- **Tarpitting** 588 — makes it possible for you to deliberately slow down a connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to send unsolicited bulk email to you. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to do so again in the future.
- **Greylisting** 590 — Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a sender not on the allow list or otherwise previously unknown, its sender, recipient, and sending server's IP address will be logged and then the message will be refused by Greylisting with a temporary error code during the SMTP session. Then, when the legitimate servers attempt to deliver the messages again a few minutes later, they will be accepted. Because spammers do not typically make further delivery attempts, Greylisting can significantly help to reduce the amount of spam your users receive.
- **LAN IPs** 594 — use this screen to list IP addresses that reside on your LAN (local area network). These IP addresses are therefore treated as local traffic for the purposes of bandwidth throttling, and may be exempt from various other security and spam prevention restrictions.
- **Site Policy** 595 — used for creating a site policy to be transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "This server does not relay."

4.1 Health Check

This page provides a convenient list of important security settings consolidated onto a single page, and it displays each setting's current value and its default value. Where those values differ, the setting is highlighted so that Global Administrators can quickly review those particular settings and then restore any of them to their default values if desired. Each group of settings also has a shortcut icon next to it, so that you can jump to the page on which those settings are located. Further, you can also view a list of all Health Check changes made during the current browser session, and undo any of those listed changes if necessary. **Note:** This feature is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Restoring Settings to their Default Values
To restore one or more settings to their default values:

1. Click one or more desired settings.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

2. Click **Restore Default** on the toolbar.

Undoing the Last Change
Click **Undo Last** on the toolbar if you use Health Check to make a change and then immediately wish to undo it.

Reviewing/Undoing Session Changes
Click **Session Changes** to review a list of any Health Check changes you have made during the current browser session. If you wish to undo any of the listed changes, select the box next to any of those changes and click **Undo Selected**. Click **Clear** if you wish to erase the list of session changes; it will not change any settings and cannot be undone.

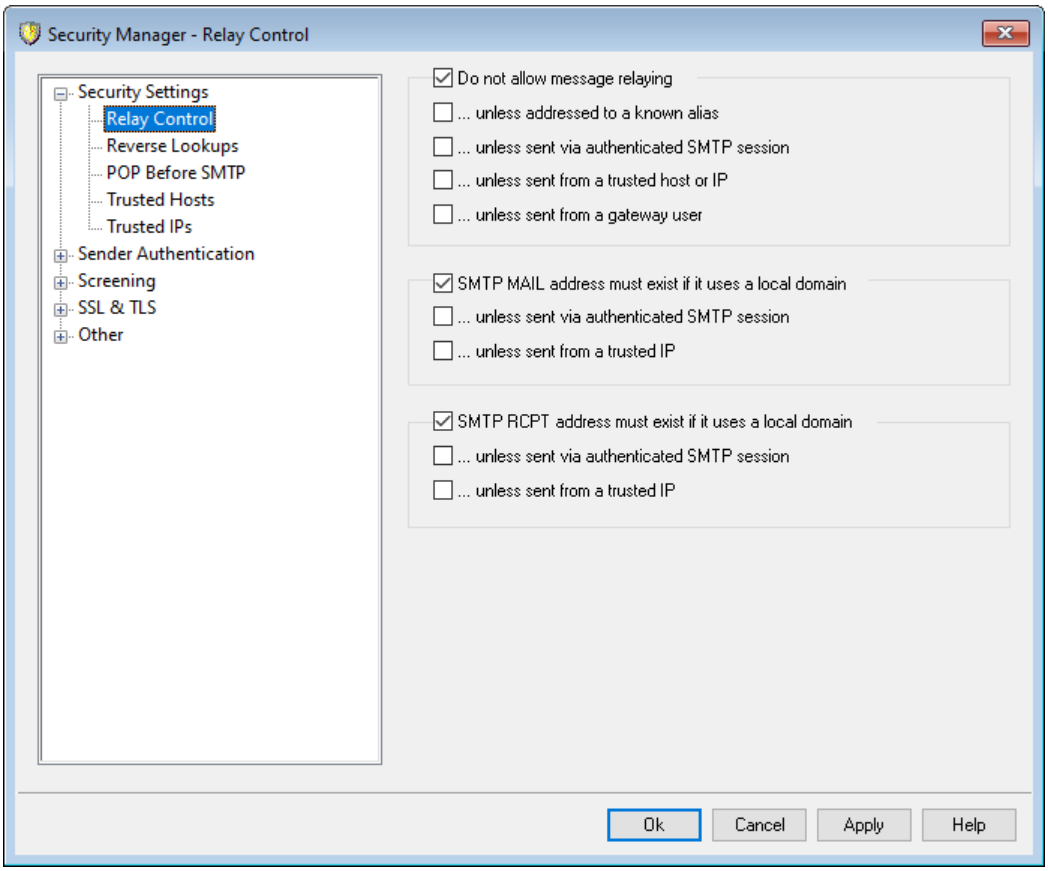
The default values of these security settings are not necessarily what is best for your particular setup. Please take care when using Health Check to make any changes.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2 Security Manager

4.2.1 Security Settings

4.2.1.1 Relay Control



Use Relay Control at Security » Security Settings » Relay Control to define how your server reacts to mail relaying. When a message arrives at your mail server that is neither from nor to a local address, your server is being asked to relay (i.e. deliver) the message on behalf of another server. If you do not want your server to relay mail for unknown users, you can use the settings provided here to control that.

Relaying email indiscriminately for other servers could result in your domain being block-listed by one or more DNS-BL services. Open relaying is greatly discouraged because spammers exploit open servers to hide their tracks.

Mail Relaying

Do not allow message relaying
When this option is enabled, MDaemon will refuse to accept messages for delivery that are both FROM and TO a non-local user.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...unless addressed to a known alias
Click this checkbox if you want MDaemon to relay mail for Aliases 818 regardless of your Relay settings.

...unless sent via authenticated SMTP session
When this checkbox is enabled, MDaemon will always relay mail when it is sent via an authenticated SMTP session.

...unless sent from a trusted host or IP
Enable this option is you wish to allow relaying when the mail is coming from a Trusted Host or Trusted IP address.

...unless sent from a gateway user
Enable this checkbox if you want MDaemon to permit mail relaying through domain gateways regardless of your Relay settings. This feature is disabled by default and isn't recommended.

Account Verification

SMTP MAIL address must exist if it uses a local domain
Click this option is you wish to verify that the MAIL value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain or gateway.

...unless sent via authenticated SMTP session
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent via an authenticated SMTP mail session.

...unless sent from a trusted host or IP
Click this option if you wish to exempt a message from the *SMTP MAIL address must exist...* option when it is being sent from a Trusted IP address.

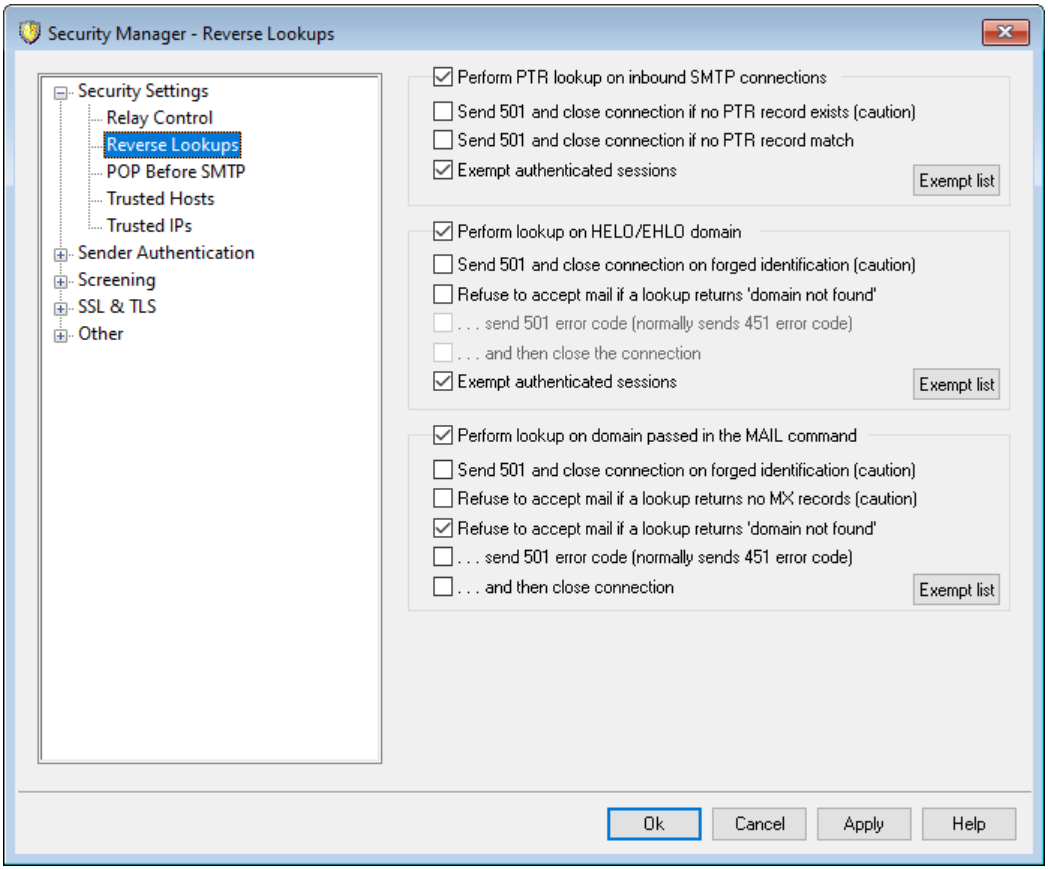
SMTP RCPT address must exist if it uses a local domain
Click this option is you wish to verify that the RCPT value passed during the SMTP process points to an actual valid account when it is purported to be from a local domain.

...unless sent via authenticated SMTP session
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent via an authenticated SMTP mail session.

...unless sent from a trusted host or IP
Click this option if you wish to exempt a message from the *SMTP RCPT address must exist...* option when it is being sent from a Trusted IP address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.1.2 Reverse Lookup



With the options on this screen, MDaemon can be configured to do a reverse lookup on the domain passed in the `HELO/EHLO` and `MAIL` commands. When performing the lookups MDaemon will attempt to acquire all of the MX and A record IP addresses for the given domain. Then the IP of the server making the connection is compared to this list in an attempt to determine whether the sender might be using a forged identity.

You can also perform reverse lookups on pointer records (PTR) of incoming IP addresses. When using this option the connection can be aborted or a warning header inserted into the message if the incoming IP address does not match any PTR record.

Finally, it is generally agreed that accepting mail from sources that identify themselves by using a domain that does not exist should be optional. Therefore, a switch exists that makes it possible for you to refuse messages for which the reverse lookup process returns a "domain not found" message from the DNS server. In such cases, MDaemon will return a `451` error code, refuse to accept the message, and then allow the SMTP session to progress. However, should you wish to return a `501` error code, close the socket connection, or do both, other switches are provided for those purposes.

Trusted IP addresses and localhost (127.0.0.1) are always exempt from reverse lookups.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Perform PTR lookup on inbound SMTP connections
Enable this option if you want MDaemon to perform pointer record lookups on all inbound SMTP connections.

...send 501 and close connection if no PTR record exists (caution)
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if no PTR record exists for the domain.

...send 501 and close connection if no PTR record match
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and close the connection if the result of a pointer record lookup fails to match.

Exempt authenticated sessions
Click this option if you wish to defer the PTR lookup on inbound SMTP connections until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

Exempt List
Click this button to open the PTR Lookup Exempt List, on which you can specify IP addresses that will be exempt from PTR reverse lookups.

Perform lookup on HELO/EHLO domain
Click this box if you want a lookup to be performed on the domain name that is reported during the `HELO/EHLO` portion of the session. The `HELO/EHLO` command is used by the client (sending machine) to identify itself to the server. The domain name passed by the client in this command is used by the server to populate the `from` portion of the `Received` header.

...send 501 and close connection on forged identification (caution)
Click this check box if you want a 501 error code to be sent and then the connection closed when the result of the lookup appears to be a forged identification.

When the result of a reverse lookup states that the server is using a forged identification, this result may frequently be incorrect. It is very common for mail servers to identify themselves with values that do not match their IP addresses. This can be due to ISP limitations and restrictions and other legitimate reasons. For this reason, you should exercise caution before enabling this option. It is likely that using this option could result in your server refusing some legitimate messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Refuse to accept mail if a lookup returns 'domain not found'
When a lookup results in "`domain not found`", enabling this option will cause the message to be refused with a `451` error code (Requested action aborted: local error in processing) and then the session will be allowed to progress normally to its conclusion.

...send 501 error code (normally sends 451 error code)
Enable this checkbox if you want the error code that is sent in response to a "domain not found" result to be `501` (syntax error in parameters or arguments) instead of `451`.

...and then close the connection
Click this checkbox if you want the connection to be closed immediately instead of allowed to progress when "`domain not found`" is the result of the reverse lookup.

Exempt authenticated sessions
Click this option if you wish to defer the lookup until after the SMTP MAIL command in order to see whether or not the connection will use authentication.

Exempt List
Click this button to open the HELO/EHLO Lookup Exempt List, for listing IP addresses and domain/host names of sites that you wish to exempt from HELO/EHLO reverse lookups.

Perform lookup on value passed in the MAIL command
Enabling this switch will cause a lookup to be performed on the domain name that is passed during the `MAIL` command portion of the mail transaction. The address passed in the `MAIL` command is supposed to be the reverse-path for the message, and is usually the mailbox from which the message is originating. Sometimes, however, it is the address to which error messages should be directed instead.

...send 501 and close connection on forged identification (caution)
Click this check box if you want a 501 error code to be sent and then the connection closed when the result of a lookup appears to be a forged identification.

When the result of a reverse lookup states that the server is using a forged identification, this result may frequently be incorrect. It is very common for mail servers to identify themselves with values that do not match their IP addresses. This can be due to ISP limitations and restrictions and other legitimate reasons. For this reason, you should exercise caution before enabling this option. It is likely that using this option could result in your server refusing some legitimate messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Refuse to accept mail if a lookup returns no MX records (caution)
Check this box if you wish to refuse MAIL from domains that do not have MX records. This option is disabled by default and should be used with caution, because domains do not need MX records in order to exist, be valid, or send/receive mail.

Refuse to accept mail if a lookup returns 'domain not found'
When a lookup results in "`domain not found`", enabling this option will cause the message to be refused with a `451` error code (Requested action aborted: local error in processing) and then the session will be allowed to progress normally to its conclusion.

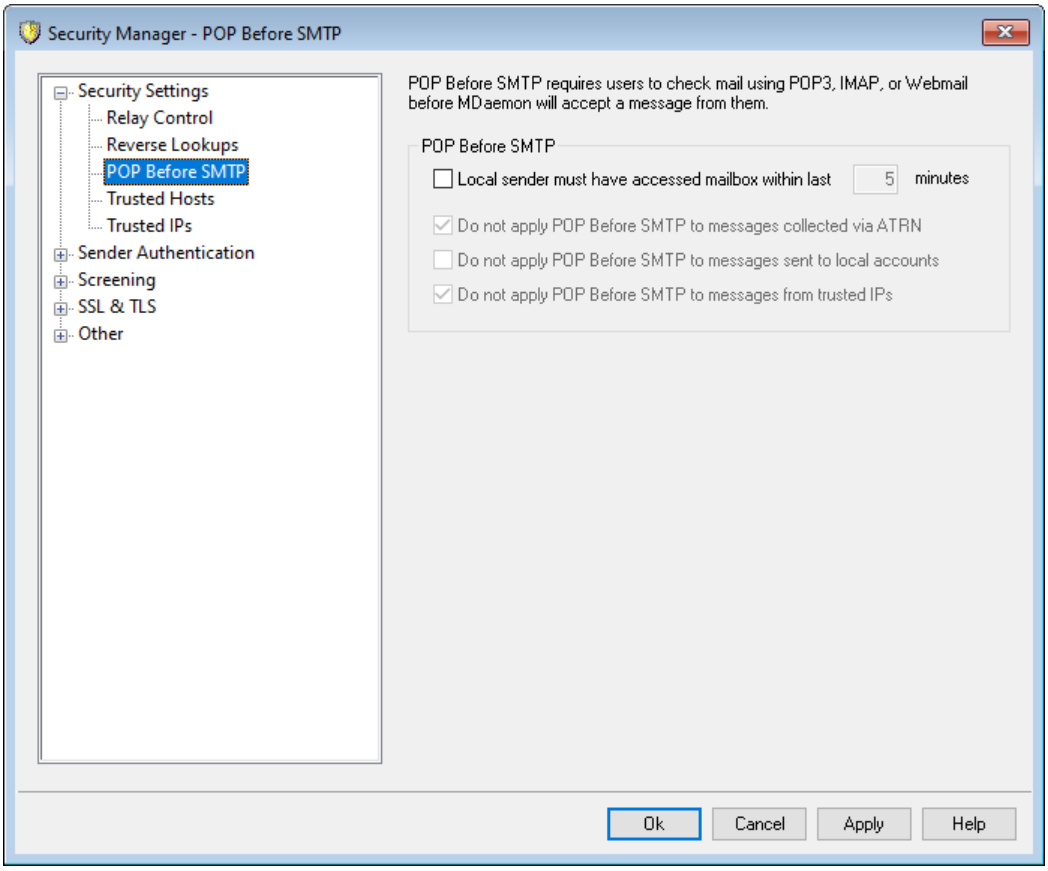
...send 501 error code (normally sends 451 error code)
Enable this checkbox if you want the error code that is sent in response to a "domain not found" result to be `501` (syntax error in parameters or arguments) instead of `451`.

...and then close the connection
Click this checkbox if you want the connection to be closed immediately instead of allowed to progress when "`domain not found`" is the result of the reverse lookup.

Exempt list
Click this button to open the MAIL Lookup Exempt List. On it you can designate the IP addresses and domain/host names of sites that you wish to exempt from MAIL reverse lookups.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.1.3 POP Before SMTP



POP Before SMTP

Local sender must have accessed mailbox within last [XX] minutes
With this feature enabled, whenever a message is purported to be from a local user, that user account must have logged in and checked its local mailbox within the specified number of minutes before it will be allowed to send mail.

Do not apply POP Before SMTP to messages collected via ATRN
Check this box if you want messages collected via ATRN 253 to be exempt from the POP Before SMTP restriction.

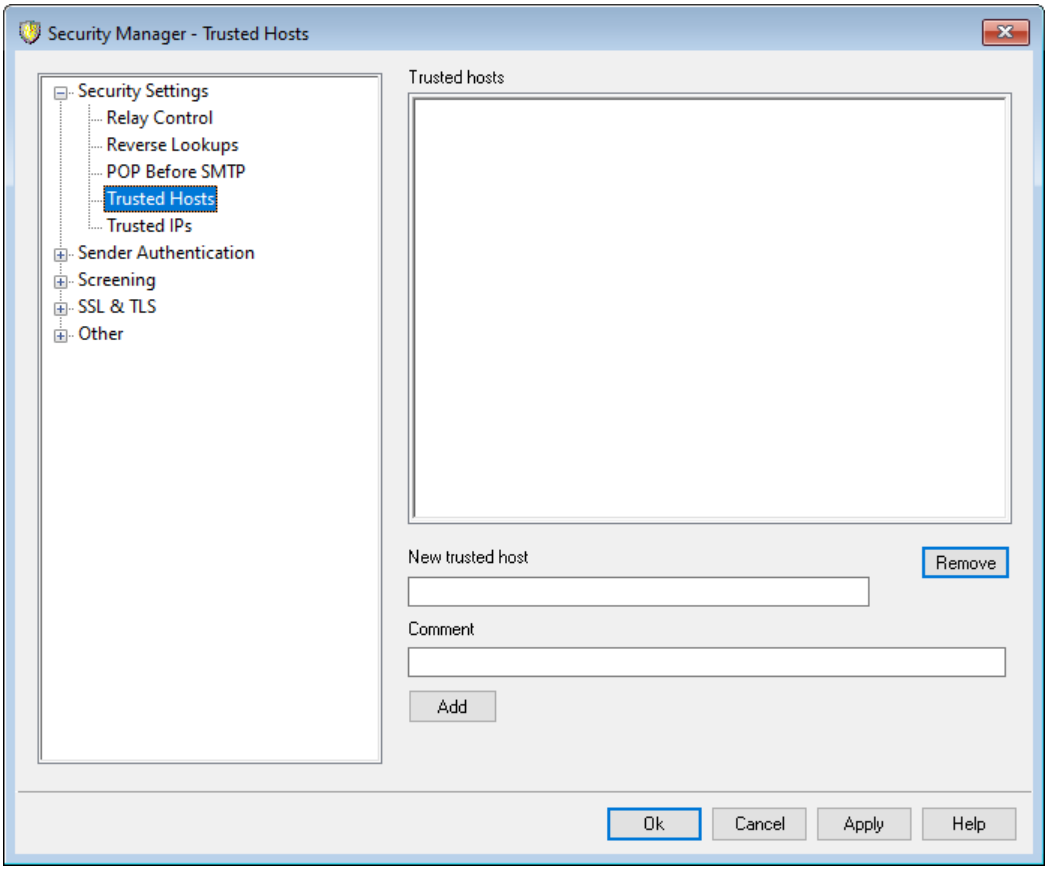
Do not apply POP Before SMTP to messages sent to local accounts
Click this checkbox if you want messages that are sent from one local user to another to be exempt from the POP Before SMTP requirement. Ordinarily, MDaemon will enforce the requirement as soon as the sender is known, but when this control is enabled MDaemon will wait until the recipient of the message is revealed before determining whether or not it is required.

Do not apply POP Before SMTP to messages from trusted IPs
If this checkbox is enabled, messages arriving from an IP address listed on the Trusted Hosts 505 screen will be exempt from POP Before SMTP.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

You can exempt authenticated sessions from the POP Before SMTP restriction via an option on the SMTP Authentication 509 screen.

4.2.1.4 Trusted Hosts



On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted Hosts" or "Trusted Domains" will be exceptions to or exempt from those options. The hosts you list on this screen are the ones to which those options refer.

Trusted hosts
This is the list of hosts that will be exempt from certain designated security options.

New trusted host
Enter a new host to be added to the *Trusted hosts* list.

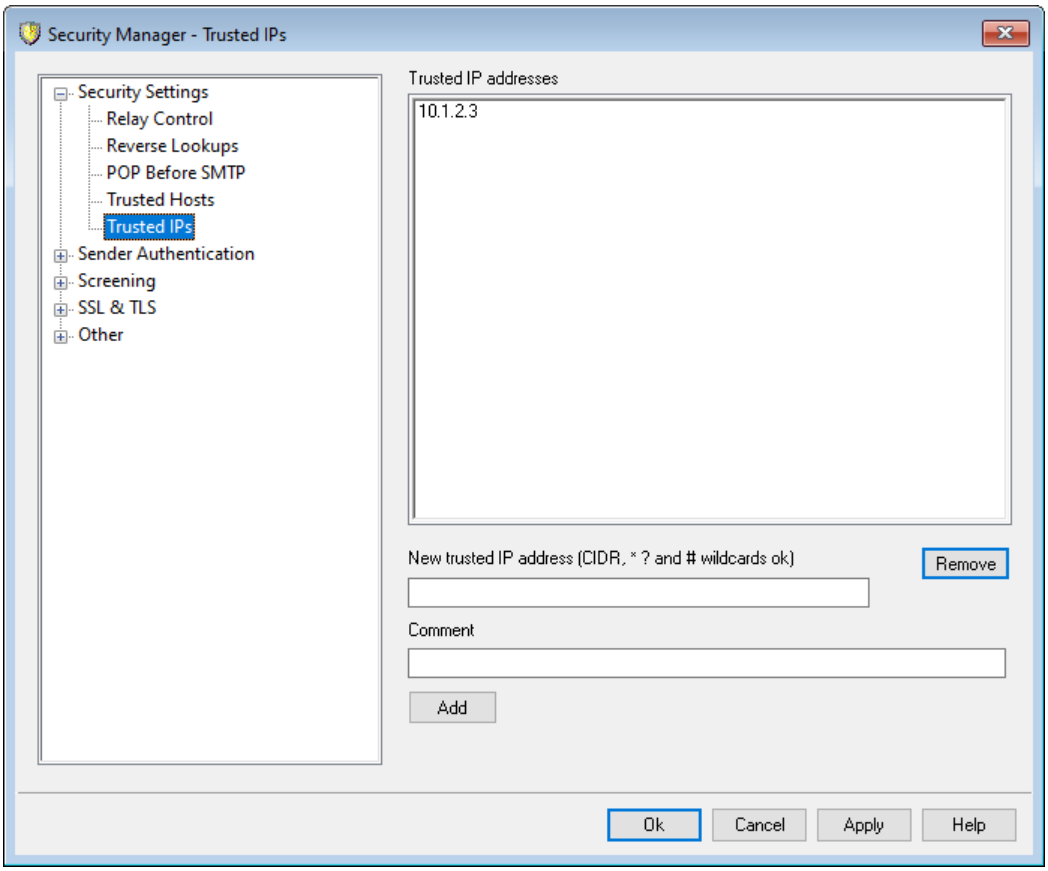
Comment
Use this for any comment text about an entry.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add
Click this button to add the new domain to the *Trusted hosts* list.

Remove
Click this button to remove the selected entries from the *Trusted hosts* list.

4.2.1.5 Trusted IPs



On various dialogs and security features throughout MDaemon you will see options that allow you to choose whether or not "Trusted IPs" will be exceptions to or exempt from those options. The IP addresses you list on this screen are the ones to which those options refer.

Trusted IP addresses
This is the list of IP addresses that will be exempt from certain designated security options.

New trusted IP address
Enter a new IP address to be added to the *Trusted IP Addresses* list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

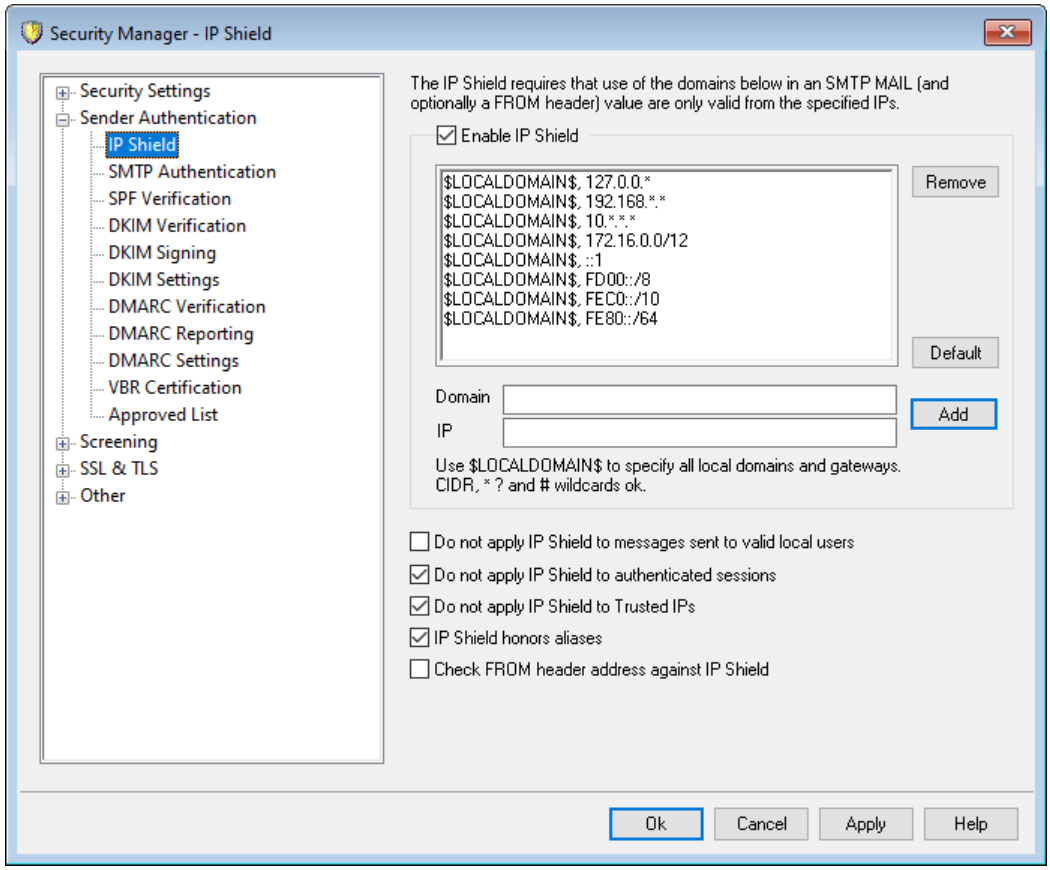
Comment
Use this for any comment text about an entry.

Add
Click this button to add the new IP address to the *Trusted IP Addresses* list.

Remove
Click this button to remove the selected entries from the *Trusted IP Addresses* list.

4.2.2 Sender Authentication

4.2.2.1 IP Shield



The IP Shield, located under the Security » Security Settings » Sender Authentication menu, is a list of domain names and matching IP addresses that will be checked during the `MAIL From` command during the SMTP session. An SMTP session claiming to be from someone at one of the listed domains will be honored only if it is coming from one of the associated IP addresses. For example, suppose your domain name is example.com and your local LAN computers use IP addresses in the range from 192.168.0.0 to 192.168.0.255. With this information you can setup the IP Shield to associate the domain name example.com with the IP address range 192.168.0.* (wildcards are allowed). Thus anytime a computer connects to your SMTP server and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

states, "MAIL FROM <someone@example.com>", the SMTP session will continue only if the connecting computer has an IP address within the required range from 192.168.0.0 to 192.168.0.255.

Enable IP Shield

Clear this checkbox if you wish to disable the IP Shield. The IP Shield is enabled by default.

Domain name

Enter the domain name that you wish to associate with a specific IP address range. You can also use the $LOCALDOMAIN$ macro to cover all local domains (including gateways). If you use this macro it will not be necessary to keep the IP Shield up to date when local domains or gateways change. By default, entries are added to the IP Shield associating all reserved IP address ranges with $LOCALDOMAIN$.

IP address

Enter the IP address that you wish to associate with a domain name. You must enter this address in dotted decimal form.

Add

Click the *Add* button to add the domain and IP address range to the listing.

Remove

Click this button to remove the selected entries from the listing.

Do not apply IP Shield to messages sent to valid local users

Click this option if you want only those messages that are destined for a non-local user or invalid local user to be checked for a domain/IP match. This will prevent others from posing as one of your local users in order to relay their mail through your server, but it will save resources by not checking messages that are addressed to your users. If you enable both this option and the *IP Shield honors aliases* option below, messages to valid aliases will be accepted as well.

Do not apply IP Shield to authenticated sessions

When this control is active, the IP Shield restrictions will not apply to authenticated users. Mail will be accepted from an authenticated user regardless of the IP address from which he or she connects. Further, when a user doesn't authenticate and access is refused, the message returned to the SMTP client will be "Authentication required" in order to give the user a clue that he can fix the problem by configuring the mail client to use authentication before sending a message. This option is enabled by default.

Do not apply IP Shield to Trusted IPs

When this control is active, the IP Shield will not be applied when the connection is from a Trusted IP address 505. This option is enabled by default.

IP Shield honors aliases

Enable this option if you want the IP Shield to honor address aliases when checking domain/IP address shields. The IP Shield will translate an alias to the true account to which it points and thus honor it if it passes the shield. Without this option

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

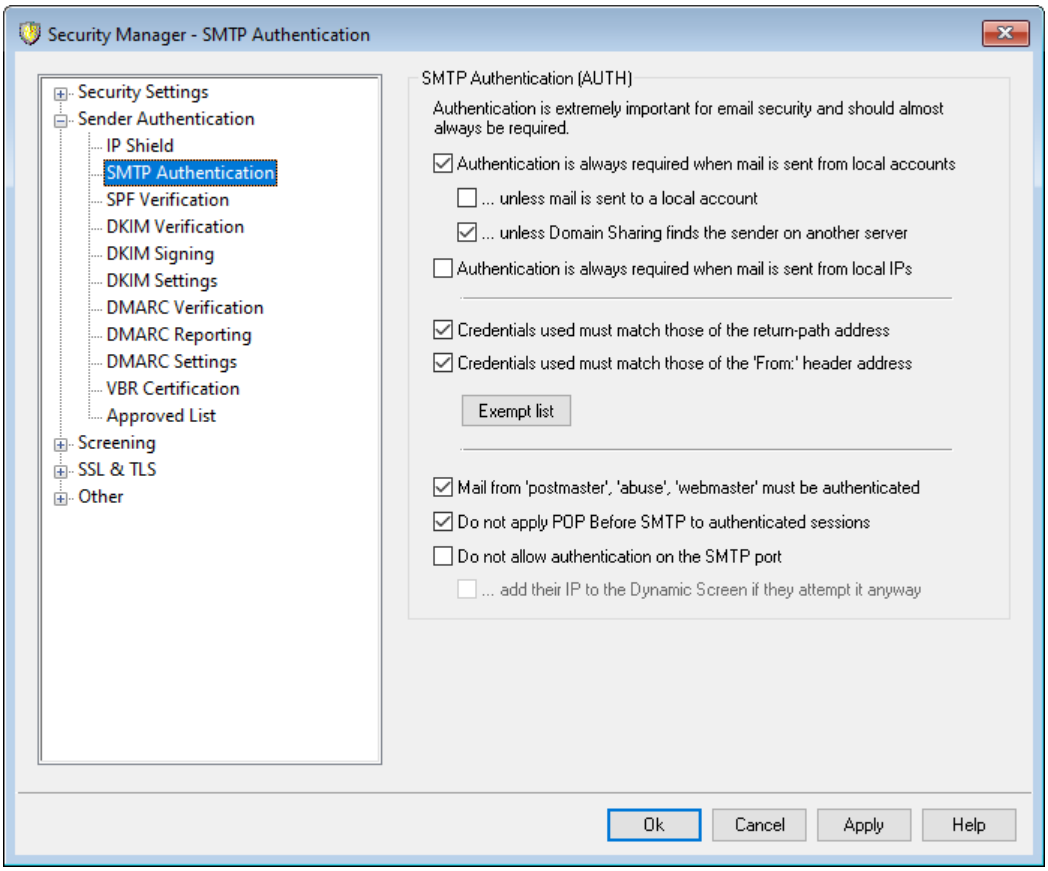
enabled, the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the Settings screen 820 of Aliases — changing the setting here will be reflected there.

If you want incoming messages that are addressed to valid aliases to be exempt from IP Shielding then click both this option and the *Do not apply IP Shield to messages sent to valid local users* option above.

Check FROM header address against IP Shield
Check this box if you want the IP Shield to compare the address taken from the message's FROM header in addition to that taken from the SMTP MAIL value. This option is disabled by default.

Using this option could cause problems with certain types of messages, such as those coming from mailing lists. It should therefore be enabled only if you are sure you need it.

4.2.2.2 SMTP Authentication



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SMTP Authentication (AUTH)

Authentication is always required when mail is from local accounts
When this option is enabled and an incoming message claims to be from one of MDaemon's domains, the account must first be authenticated or MDaemon will refuse to accept the message for delivery. This option is enabled by default.

...unless message is to a local account
If you are requiring authentication when a message is from a local sender, but wish to skip the authentication restriction when the recipient is local as well, then click this option. Note: this may be necessary in some situations where you require some of your users to use different mail servers for outgoing and incoming mail.

...unless Domain Sharing finds the sender on another server
By default, when Domain Sharing 108 finds the sender on another server, that sender will be exempt from the *Authentication is always required...* option above. Clear this checkbox if you wish to require authentication from those senders as well.

Authentication is always required when mail is sent from local IPs
Enable this option if you wish to require authentication when an incoming message is being sent from a local IP address. If unauthenticated the message will be rejected. Trusted IPs 506 are exempt, and this option is enabled by default for new installations.

Credentials used must match those of the return-path address
By default, the credentials used during SMTP authentication must match those of the address found in the message's return-path. Disable this option if you do not wish to require the return path to match. To support gateway mail storage and forwarding, there is a corresponding option located on the Global Gateway Settings 243 screen that will "*Exempt gateway mail from AUTH credential matching requirements*" by default.

Credentials used must match those of the 'From:' header address
By default, the credentials used during SMTP authentication must match those of the address found in the message's "From:" header. Disable this option if you do not wish to require the "From:" header to match. To support gateway mail storage and forwarding, there is a corresponding option located on the Global Gateway Settings 243 screen that will "*Exempt gateway mail from AUTH credential matching requirements*" by default.

Exempt list
Use the Credentials Matching Exempt List to exempt an address from the "*Credentials used must match...*" options above. To be exempt from the "*...must match those of the return-path address*" option, the exempt address must match the address in the message's **Return-Path**. To be exempt from the "*...must match those of the 'From:' header address*" option, the exempt address must match the address in the message's **From:** header.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mail from 'Postmaster', 'abuse', 'webmaster' must be authenticated
Click this checkbox to require messages claiming to be from one of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send mail through your system. This option will prevent them and other unauthorized users from being able to do so. This option is mirrored on the Settings screen 820 of Aliases. Changing the setting here will change it there as well.

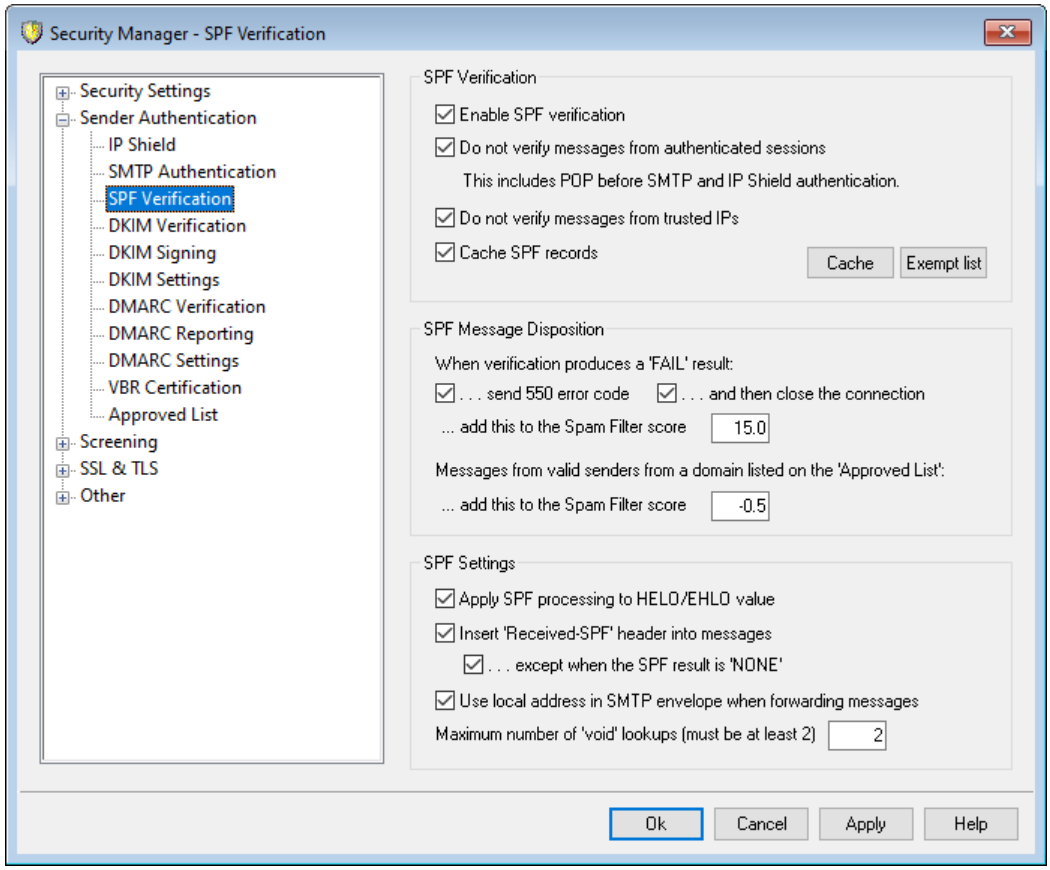
Do not apply POP Before SMTP to authenticated sessions
If you are utilizing the POP Before SMTP 504 security feature, you can click this option to make authenticated users exempt from this restriction. An authenticated user will not need to check his or her email before sending messages.

Do not allow authentication on the SMTP port
This option disables AUTH support over the SMTP port. AUTH will not be offered in the EHLO response, and will be treated as an unknown command if provided by the SMTP client. This setting and the "*...add their IP to the Dynamic Screen*" option below are useful in configurations where all legitimate accounts are using the MSA or other port to submit authenticated mail. In such configurations the assumption is that any attempt to authenticate on the SMTP port must be from an attacker.

> **...add their IP to the Dynamic Screen if they attempt it anyway**
> When using the *Do not allow authentication on the SMTP port* option above, this option will add to the Dynamic Screen any IP address of any client that attempts to authenticate on the SMTP port anyway. The connection will also be immediately terminated.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.3 SPF Verification



MDaemon supports Sender Policy Framework (SPF) to help verify sending servers and protect against spoofing and phishing, which are two common types of email forgery in which the sender of the message attempts to make the message appear to be coming from someone else.

Many domains publish MX records in the Domain Name System (DNS) to identify the locations permitted to receive mail for them, but this doesn't identify the locations allowed to *send* mail for them. SPF is a means whereby domains can also publish sender records to identify those locations authorized to send messages. By performing an SPF lookup on incoming messages, MDaemon can attempt to determine whether or not the sending server is permitted to deliver mail for the purported sending domain, and consequently determine whether or not the sender's address may have been forged or "spoofed".

Use the options on this screen to configure your server's SPF settings.

For more information on SPF, visit:

http://www.open-spf.org

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SPF Verification

Enable SPF verification
When this option is enabled, MDaemon will perform a DNS query for SPF record data on each incoming message's purported sender, to ensure that the sending server is permitted to send messages on its behalf. The host MDaemon will verify is taken from the `MAIL` value passed during SMTP processing. SPF verification is enabled by default.

Do not verify messages from authenticated sessions
By default authenticated connections are exempt from SPF queries. Authenticated sessions include those verified via SMTP Authentication 509, POP before SMTP 504, or the IP Shield 507. Disable this option if you do not wish to exempt authenticated sessions from SPF.

Do not verify messages from trusted IPs
By default any message from a trusted IP address 506 is exempt from SPF verification.

Cache verification results
By default MDaemon will temporarily cache each domain's SPF policy record obtained during the DNS query. Clear the checkbox if you do not wish to cache SPF policies.

Cache
This button opens the SPF cache, which lists all currently cached SPF records.

Exempt List
Click this button to open the SPF Exception List on which you can designate IP addresses, email addresses, and domains that you wish to exempt from SPF lookups. Email addresses are compared against the SMTP envelope not the message From header. Domains are exempted by placing the word "spf" in front of the domain name. MDaemon will include that domain's SPF record in every SPF evaluation using an MDaemon specific "wlinclude:<domain>" tag. In this way you can have your backup MX provider treated as a valid SPF source for all senders.

SPF Message Disposition

When verification produces a FAIL result:

...send 550 error code
Click this check box if you want a 550 error code to be sent when the result of the SPF query is "Fail".

...and then close the connection
Enable this option if you want the connection to be closed immediately after sending the 550 error code.

...add this to the Spam Filter score
Specify the amount that you wish to add to the message's Spam Score when it fails to pass SPF verification.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Messages from valid sender from a domain listed on the 'Approved List'

...add this to the Spam Filter score
Specify the amount that you wish to add to a message's Spam Score when SPF confirms that it originated from a domain found on the Approved List 544.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for the approved messages.

SPF Settings

Apply SPF processing to HELO/EHLO value
The option applies SPF verification to the value passed in the HELO or EHLO command at the beginning of the SMTP process. It is enabled by default.

Insert 'Received-SPF' header into messages
Click this option if you want a "Received-SPF" header to be inserted into each message.

...except when the SPF result is 'NONE'
Enable this option if you do not wish the "Received-SPF" header to be inserted into a message when the result of the SPF query is "none".

Use local address in SMTP envelope when forwarding messages
Enable this option if you want all mail forwarded by MDaemon to use a local address in the SMTP envelope. This helps reduce problems associated with forwarding. Normally, forwarded messages are sent using the email address of the original sender and not the email address that is actually doing the forwarding. In some situations, using a local address may be necessary in order to prevent the receiving server from falsely identifying the forwarded message as having a "spoofed" address. This option is enabled by default.

Maximum number of 'Void' lookups (must be at least 2)
This is the maximum number of void lookup results permitted in an SPF query before MDaemon generates a permanent error. A Void lookup is one that results in "domain does not exist" or "no answers exist." This value must be a least "2".

4.2.2.4 DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) is a cryptographic email verification system that can be utilized to prevent spoofing (forging another person's email address in order to pose as a different message sender). Additionally, because most junk email (spam) messages contain spoofed addresses, DKIM can help greatly in the reduction of spam even though the specifications weren't specifically designed to be an anti-spam tool. DKIM can also be used to ensure the integrity of incoming messages, or ensure that the message hasn't been tampered with between the time it left the signing mail server and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

arrived at yours. In other words, with DKIM cryptographic verification the receiving server can be certain that the arriving message is from the server that signed it, and that no one changed that message in any way.

In order to ensure the validity and integrity of messages, DKIM uses a public and private key-pairs system. An encrypted public key is published to the sending server's DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the receiving server sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's cryptographic signature to determine its validity. If the incoming message cannot be verified then the receiving server knows it contains a spoofed address or has been tampered with or changed. A failed message can then be rejected, or it can be accepted but have its spam score adjusted.

To configure MDaemon to verify incoming cryptographically signed messages, use the options provided on the DKIM Verification 516 screen. To configure MDaemon to sign outgoing messages, use the options provided on the DKIM Signing 518 screen. Both are located under the Sender Authentication section of the Security Settings dialog, at: Security » Security Settings » Sender Authentication. MDaemon's main interface 68 includes a "DKIM" tab (located under the Security tab) that can be used for monitoring DKIM activity in real time, and you can log DKIM activity using the option at: Setup » Server Settings » Logging » Settings.

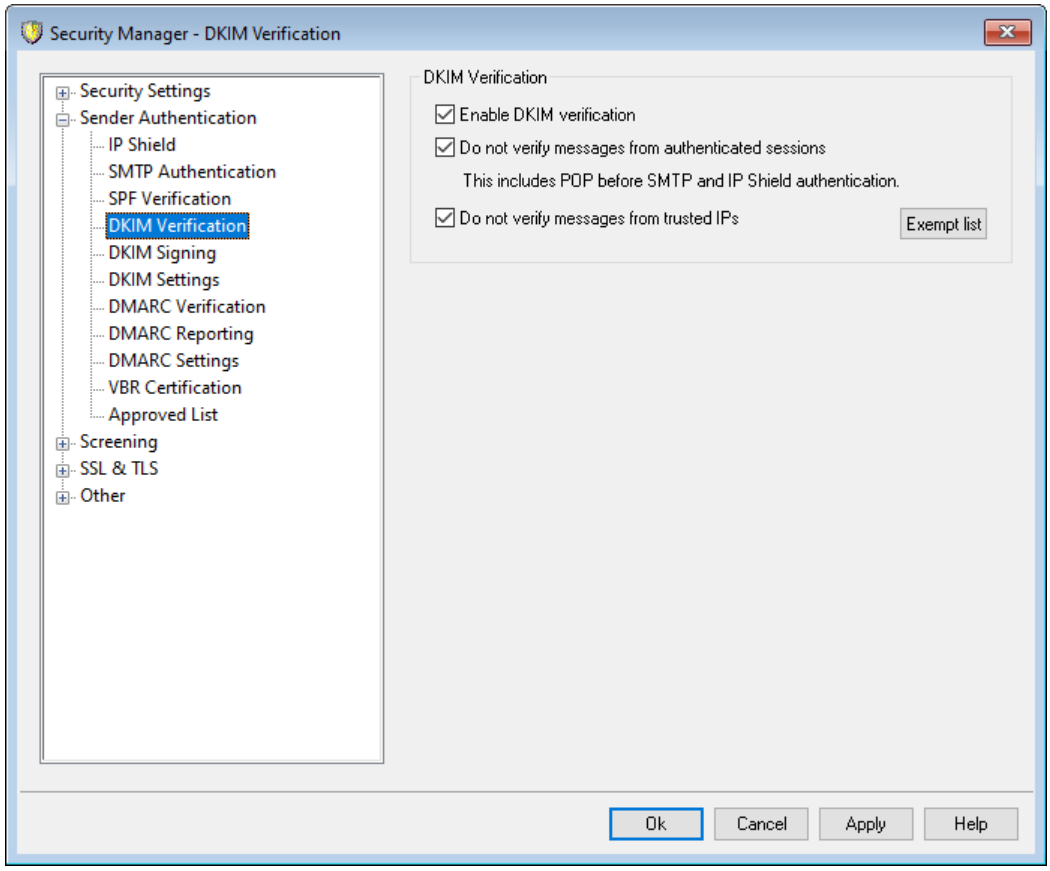
See:

DKIM Verification 516
DKIM Signing 518
DKIM Settings 521

For more on DomainKeys Identified Mail, visit: http://www.dkim.org/.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.4.1 DKIM Verification



Use this screen to configure MDaemon to verify DomainKeys Identified Mail (DKIM) signatures in incoming remote messages. When this feature is enabled and an incoming message has been cryptographically signed, MDaemon will retrieve the public key from the DNS record of the domain taken from the signature and then use that key to test the message's DKIM signature to determine its validity.

If the signature passes the verification test, the message will continue on to the next step in the regular delivery process. Additionally, if the domain taken from the signature also appears on the Approved List 544, the message's Spam Filter score will receive a beneficial adjustment.

For more on DKIM see: http://www.dkim.org/

DKIM Verification

Enable DKIM verification
Click this option to enable DomainKeys Identified Mail verification of incoming remote messages.

Do not verify messages from authenticated sessions
Click this option if you want to exempt messages from cryptographic verification when the message session is authenticated. Authenticated sessions include those verified via SMTP Authentication 509, POP before SMTP 504, or the IP Shield 507.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not verify messages from trusted IPs
Use this option if you want connections from trusted IP addresses[505] to be exempt from DKIM verification.

Exempt list
Click this button to open the exception list. Messages originating from any IP addresses specified on the list will not be subject to cryptographic verification.

Authentication-Results header

Whenever a message is authenticated using SMTP AUTH, SPF, DomainKeys Identified Mail, or DMARC, MDaemon will insert the Authentication-Results header into the message, listing the results of the authentication process. If MDaemon is configured to accept messages even when they fail authentication, then the Authentication-Results header will contain a code to identify the reason for the failure.

There is ongoing work via the Internet Engineering Task Force (IETF) on this header and the authentication protocols mentioned in this section. You can find more information on this at the IETF web site, located at: http://www.ietf.org/.

DKIM Headers in Mailing List Messages

By default, MDaemon strips DKIM signatures from incoming list messages because those signatures can be broken by changes made to the message headers or content during list processing. If you would like MDaemon to leave signatures in list messages, you can configure it to do so by manually setting the following option in the `MDaemon.ini` file:

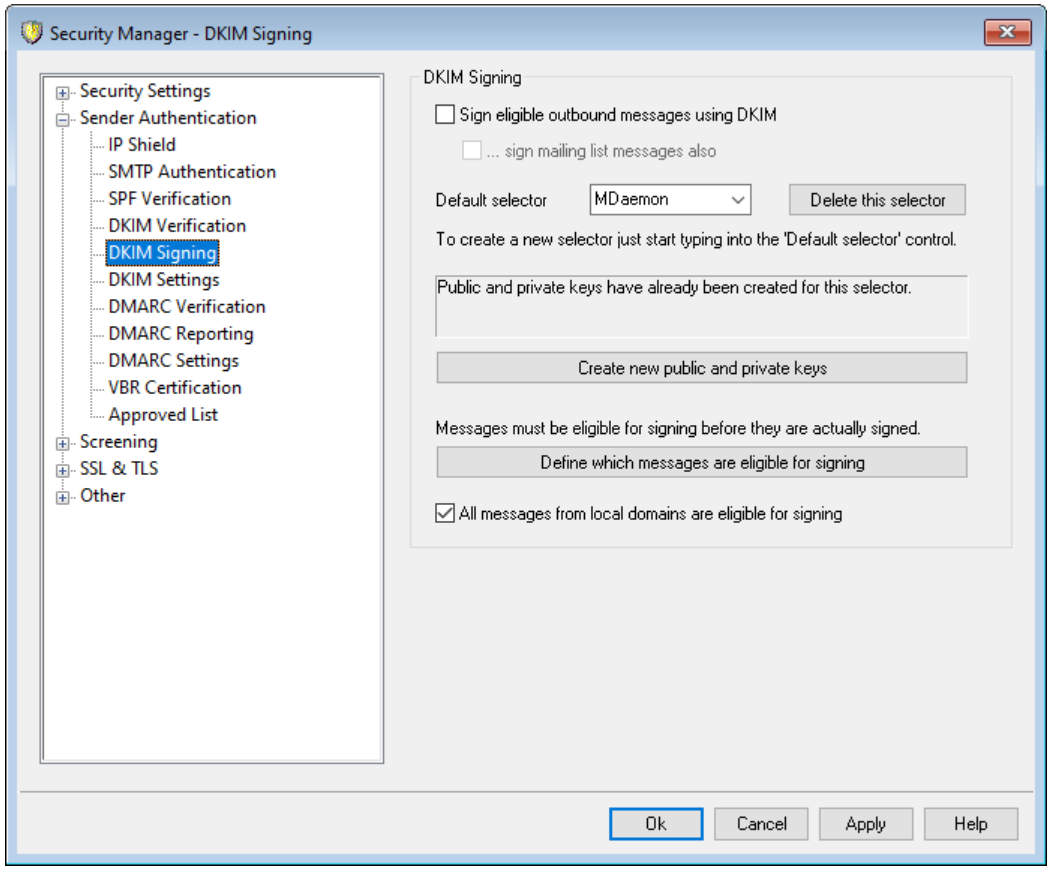
```
[DomainKeys]
StripSigsFromListMail=No (default is "Yes")
```

See:

DomainKeys Identified Mail[514]
DKIM Signing[518]
DKIM Settings[521]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.4.2 DKIM Signing



Use the options contained on the DKIM Signing screen to configure MDaemon to sign eligible outbound messages using DKIM, and to define the criteria that will make a message eligible. You can also use this screen to designate selectors and generate corresponding public and private keys suitable for use with the DKIM specification. A default selector ("MDaemon") and a default public and private key are created for you automatically on startup. All keys are unique—they are never the same from one site to another, regardless of the selector specified. By default, keys are generated with a secure bit depth of 2048 bits.

DKIM Signing

Sign eligible outbound messages using DKIM
Click this option if you wish to use DomainKeys Identified Mail to cryptographically sign some outgoing messages. In order for a message to be signed, it must meet the criteria designated under the *Define which messages are eligible for signing* button and be received by MDaemon for delivery on an authenticated session. There is also a Content Filter action, "*Sign with DKIM selector...*" that you can use to cause messages to be signed.

...sign mailing list messages
Click this check box if you wish to cryptographically sign all outgoing Mailing List messages. Because MDaemon will sign all mail to all of your lists, you do not need

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

to use the "*Define which messages are eligible for signing*" option to authorize them for cryptographic signing.

Signing list mail requires content filter processing for each list message after "cracking" the list. This could affect server performance when dealing with large and highly active mailing lists.

Default selector
From the drop-down list, choose the selector whose corresponding public/private key pair you wish to use when signing messages. If you wish to create a new key pair with a different selector, type the desired selector name here and click "*Create new public and private keys*" below. If you wish to sign some messages using an alternate selector, designate a specific selector under the "*Define which messages are eligible for signing*" option, or create a Content Filter rule using the "*Sign with DKIM selector...*" action.

Delete this selector
Click this button if you wish to delete a selector. Follow the on-screen instructions that appear.

Create new public and private keys
Click this button to generate a public/private key pair for the selector specified above. A public/private key pair will be generated for the selector, and the file `dns_readme.txt` will be generated and automatically opened. This file contains example DKIM data that you will need to publish to your domain's DNS records listing your DKIM Policy and the public key for the designated selector. The file lists samples for both testing and not testing status, and for whether you are signing all messages or just some messages originating from your domain. If you are currently testing DKIM or this selector, then you will need to use the information contained in the Testing entries for either the Policy or the selector, depending on what you are testing. Otherwise you will need to use the Not Testing entries.

All keys are stored in `PEM` format, and all selectors and keys are stored under the `\MDaemon\Pem` folder in the following way:

```
\MDaemon\Pem\<Selector>\rsa.public - public key for this selector
\MDaemon\Pem\<Selector>\rsa.private - private key for this selector
```

The files contained in these folders are not encrypted or hidden, but they contain RSA private encryption keys that should never be accessed by anyone without permission. You should therefore take steps to secure these folders and subfolders using your OS tools.

Define which messages are eligible for signing
If you have elected to sign eligible outbound messages, click this button to edit the `DKSign.dat` file, which contains the list of domains and addresses that MDaemon will use to determine whether or not a message should be signed. For each address

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

listed you must designate whether or not the message should be `To` or `From` that address in order for it to qualify to be signed, or you can designate some other header such as "`Reply-To`" or "`Sender`". Optionally, you can designate a selector for each entry, which will be used when signing a message that matches that entry. Finally, you can specify an optional signing domain to be used in the "d=" tag within the signature header. This can be useful, for example, when you have multiple sub-domains signing messages. In such cases you could use the "d=" tag to tell the receiving servers to look for the DKIM keys in a single domain's DNS record, thus making it possible for you to manage all of the keys in one record rather than having to manage separate records for each sub-domain. Wildcards are permitted in domains and addresses.

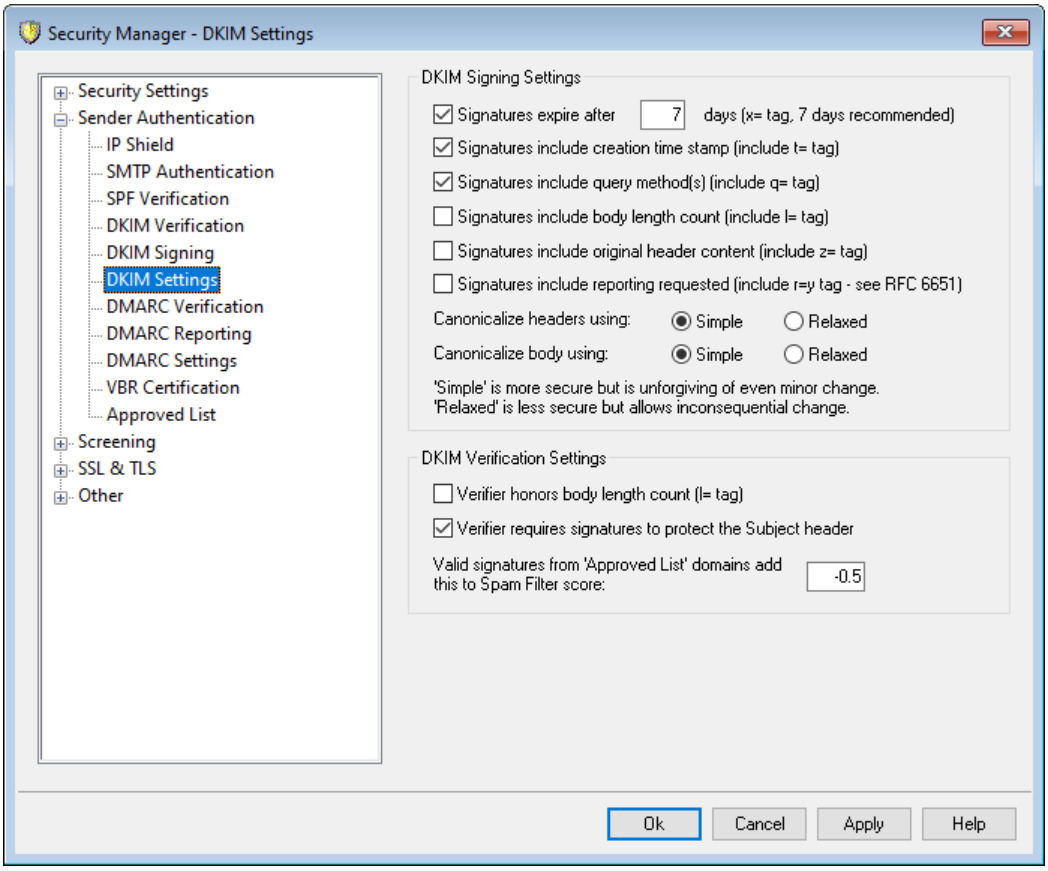
All messages from local domains are eligible for signing
Use this option if you wish to make all messages from your local domains eligible for signing. If you use this option then you do not need to add any of your local domains to the eligibility list (i.e. the `DKSign.dat` file) unless you wish to designate a specific selector or "`d=`" tag to be used when signing a specific domain's messages. This option is enabled by default.

See:

DomainKeys Identified Mail 514
DKIM Settings 521
DKIM Verification 516

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.4.3 DKIM Settings



DKIM Signing Settings

Signatures expire after [XX] days ("x=" tag, 7 days recommended)
If you wish to limit the number of days that a DKIM signature can be considered valid, activate this option and specify the desired number of days. Messages with expired signatures will always fail verification. This option corresponds to the signature's "x=" tag. This option is enabled by default, with the value set to 7 days.

Signatures include creation time stamp (include t= tag)
When this option is enabled, the signature creation time stamp ("t=" tag) will be included in the signature. This is enabled by default.

Signatures include query method(s) (include q= tag)
By default this option is enabled. It causes the signature to include the query method tag (e.g. "q=dns").

Signatures include body length count (include l= tag)
Enable this option if you wish to include the body length count tag in DKIM signatures.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Signatures include original header content (include z= tag)
Click this option if you wish to include the "z=" tag in the DKIM signature. This tag will contain a copy of the message's original headers. This can potentially make signatures quite large.

Signatures include reporting requested (include r=y tag)
Enable this option if you wish include the r=y tag in your signed messages. The presence of this tag indicates to receiving servers who honor the tag that you wish to receive AFRF failure reports from them when they encounter messages purporting to be from your domain but fail DKIM verification. To receive these reports, however, you must also configure a DKIM reporting TXT record in your domain's DNS. See RFC-6651: *Extensions to DomainKeys Identified Mail (DKIM) for Failure Reporting*, for syntax and instructions on how to do that. Since this option requires DNS changes, it is disabled by default.

Canonicalization

Canonicalization is a process whereby the message's headers and body are converted into a canonical standard and "normalized" before the DKIM signature is created. This is necessary because some email servers and relay systems will make various inconsequential changes to the message during normal processing, which could otherwise break the signature if a canonical standard was not used to prepare each message for signing. Currently there are two canonicalization methods used for DKIM signing and verification: Simple and Relaxed. Simple is the strictest method, allowing little to no changes to the message. Relaxed is more forgiving than Simple, allowing several inconsequential changes.

Canonicalize headers using: Simple, Relaxed
This is the canonicalization method used for the message headers when signing the message. Simple allows no changes to the header fields in any way. Relaxed allows for converting header names (not header values) to lower case, converting one or more sequential spaces to a single space, and other innocuous changes. The default setting is "Simple."

Canonicalize body using: Simple, Relaxed
This is the canonicalization method used for the message body when signing the message. Simple ignores empty lines at the end of the message body—no other changes to the body are allowed. Relaxed allows for blank lines at the end of the message, ignores spaces at the end of lines, reduces all sequences of spaces in a single line to a single space character, and other minor changes. The default setting is "Simple."

DKIM Verification Settings

Verifier honors body length count (l= tag)
When this option is enabled, MDaemon will honor the body length count tag when it is found in an incoming message's DKIM signature. When the actual body length count is greater than the value contained in this tag, MDaemon will only verify the amount specified in the tag — the remainder of the message will remain unverified. This indicates that something was appended to the message, and consequently that unverified portion could be considered suspect. When the actual body length count is less than the value contained in this tag, the signature will not pass verification

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

(i.e. it will receive a "FAIL" result). This indicates that some portion of the message was deleted, causing the body length count to be less than the amount specified in the tag.

Verifier requires signatures to protect the Subject header
Enable this option if you wish to require the DKIM signature of incoming messages to protect the Subject header.

Valid signatures from 'Approved List' domains add this to Spam Filter score:
The value specified here will be added to the Spam Filter score of any DKIM signed messages that receive a "Pass" result when the domain taken from the signature appears on the Approved List 544. When a message's signature is verified but the domain is not on the Approved List, the Spam Filter score will not be adjusted—the verified signature will have no effect on the score. However, normal Spam Filter processing and scoring will still be applied to that message.

Ordinarily the value specified here should be a negative number so that the spam score will be reduced for messages containing a valid cryptographic signature when the domain taken from the signature is on the Approved List 544. MDaemon's default value for this option is -0.5.

See:

DomainKeys Identified Mail 514
DKIM Verification 516
DKIM Signing 518

4.2.2.5 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a specification designed to help reduce email message abuse, such as incoming spam and phishing messages that misrepresent their origins by forging the message's From: header. DMARC makes it possible for domain owners to use the Domain Name System (DNS) to inform receiving servers of their DMARC policy, which is how they want those servers to handle messages that purport to be sent from their domain but cannot be authenticated as having actually come from it. This policy, which is retrieved by the receiving server via a DNS query while processing the incoming message, can state that the server should quarantine or reject messages that do not align with the policy, or take no action at all (i.e. let the message proceed normally). In addition to the policy, the domain's DMARC DNS record can also contain requests for the server to send DMARC reports to some, outlining the number of incoming messages purporting to be from that domain and whether or not they passed or failed authentication, and with details about any failures. DMARC's reporting features can be useful for determining the effectiveness of your email authentication procedures and how frequently your domain name is being used in forged messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Under the Sender Authentication section of the Security Settings dialog, there are three screens for configuring MDaemon's DMARC verification and reporting features: DMARC Verification, DMARC Reporting, and DMARC Settings.

DMARC Verification 530

As part of the DMARC verification process, MDaemon performs a DMARC DNS query on the domain found in the `From:` header of each incoming message. This is done to determine whether or not the domain uses DMARC, and if so, to retrieve its DMARC DNS record 525, which contains its policy and other DMARC related information. Additionally, DMARC utilizes SPF 512 and DKIM 516 to validate each message and requires it to pass at least one of those tests in order to pass DMARC verification. If the message passes then it will proceed normally through the rest of MDaemon's delivery and filtering processes. If it fails, however, then the fate of the message is determined by a combination of the domain's DMARC policy and how you have configured MDaemon to deal with those messages.

If a message fails DMARC verification and the DMARC domain has a policy of "`p=none`" then no punitive action will be taken and normal message processing will continue. Conversely, when the DMARC domain has a restrictive policy of "`p=quarantine`" or "`p=reject`," MDaemon can optionally filter the message automatically to the receiving user's spam (i.e. junk e-mail) folder. You can also choose to have MDaemon reject the failed message completely when the domain is using the "`p=reject`" policy. Additionally for failed messages with restrictive policies, MDaemon will insert the "`X-MDDMARC-Fail-policy: quarantine`" or "`X-MDDMARC-Fail-policy: reject`" header, depending on the policy. This makes it possible for you to use the Content Filter to perform some action based on the presence of those headers, such as sending the message to a specific folder for further scrutiny.

DMARC Verification is enabled by default and recommended for most MDaemon configurations.

DMARC Reporting 533

When MDaemon queries DNS for a DMARC record, the record may contain tags indicating that the domain owner wishes to receive DMARC aggregate or failure reports regarding messages claiming to be from that domain. The options on the DMARC Reporting screen are for designating whether or not you are willing to send the requested types of reports, and for specifying the meta-data those reports should contain. Aggregate reports are sent daily at Midnight UTC and failure reports are sent per message, as each incident occurs that triggers the report. Reports are always sent as zipped XML file attachments, and there are various parsing tools available online that can make them easy for the recipients to view.

By default MDaemon does not send aggregate or failure reports. If you are willing to send either type of report, enable its corresponding options on the DMARC Reporting screen.

DMARC Settings 537

The DMARC Settings screen contains various options for including certain info in DKIM reports, logging DMARC DNS records, and updating the Public Suffix file used by MDaemon for DMARC.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

DMARC Verification and Mailing Lists

Because the purpose of DMARC is to ensure that the domain found in a message's `From:` header hasn't been forged, the sending server must be permitted to send messages on behalf of that domain. This can pose a unique problem for mailing lists, because it is common for lists to distribute messages on behalf of list members from outside domains, and yet leave the `From:` header unchanged. This means that when a receiving server attempts to use DMARC verification on one of these messages, the message will have been sent by a server that is not officially affiliated with the `From:` header domain. If the DMARC domain happens to be using a restrictive DMARC policy, this could cause the message to be quarantined or even rejected by the receiving server. In some cases this could also cause the recipient to be removed from the list's membership. To circumvent this problem, when MDaemon finds that a messages for a list is coming from a domain with a restrictive DMARC policy, MDaemon will replace the message's `From:` header with the mailing list's address. Alternatively, you can configure MDaemon to refuse to accept any message for a list when it is from a domain with a restrictive policy. This latter option would effectively make it impossible for a user from a domain with a restrictive policy to post a message to the list. The option to replace the `From:` header is located on the mailing list editor's Headers 271 screen. The option to reject messages is located on the Settings 268 screen.

Using DMARC for Your MDaemon Domains

If you would like to use DMARC for one of your own domains, meaning that you want receiving mail servers that support DMARC to use DMARC to verify messages claiming to be from you, then you must first ensure that you have created properly formatted SPF and DKIM DNS records for the domain; you must have at least one of those options working correctly to use DMARC. If you are using DKIM then you must also configure MDaemon's DKIM Signing 518 options to sign the domain's messages. Additionally, you must create a DMARC DNS record for the domain. By querying DNS for this specially formatted `TXT` record, the receiving server can determine your DMARC policy and various optional parameters such as: the mode of authentication you use, whether or not you wish to receive aggregate reports, the email address to which reports should be sent, and others.

Once you have properly configured DMARC and have begun to receive DMARC XML reports, there are a variety of online tools you can use to read those reports and diagnose any potential problems. For your convenience there is also a DMARC Reporter tool provided for you in the \MDaemon\App\ folder. See DMARCReporterReadMe.txt for instructions on how to use it.

Defining a DMARC TXT Resource Record

The following is an overview of the most basic, commonly used components of a DMARC record. For more detailed information, or for information on more advanced configurations, see: www.dmarc.org.

Owner Field

The Owner (also called "Name" or "left-hand") field of the DMARC resource record must always be **`_dmarc`**, or it can take the form **`_dmarc.domain.name`** if you wish to specify the domain or subdomain to which the record applies.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Example:

DMARC record for the domain **example.com**

```
_dmarc IN TXT "v=DMARC1;p=none"
```
This record would apply to emails from user@example.com or any subdomains of example.com, such as user@support.example.com, user@mail.support.example.com, and so on.

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```
This record would only apply to emails from user@support.example.com, not to emails from, for example, user@example.com.

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```
This record would apply to emails from: user@support.example.com, user@a.support.example.com, user@a.b.support.example.com, and so on.

DMARC Record Tags and Values

Required Tags

Tag	Value	Notes
v=	**DMARC1**	The is the Version tag, which must be the first tag in the DMARC specific text portion of the record. Although other DMARC tag values are not case sensitive, the value of the **v=** tag must have the uppercase value: **DMARC1**. Example: `_dmarc IN TXT "v=DMARC1;p=none"`
p=	**none** **quarantine** **reject**	This is the Policy tag, which must be the second tag in the DMARC record, following the **v=** tag. **p=none** means that the receiving server should take no action based on results of the DMARC query. Messages that fail the DMARC check should not be quarantined or rejected based on that failure. They could still be quarantined or rejected for other reasons, such as for failing spam filter tests or other security checks unrelated to DMARC. Using **p=none** is sometimes called "monitoring" or "monitor mode" because you can use it with the **rua=** tag to receive aggregate reports from recipient domains about your messages, but those messages will not be penalized by the domains for failing to pass the DMARC check. This is the policy to use until you have thoroughly tested your DMARC implementation and are sure you are ready to move on to the more restrictive **p=quarantine** policy.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

		p=quarantine is the policy to use when you want other mail servers to treat a message as suspicious when its **From:** header says that it is coming from you but the message fails the DMARC check. Depending upon the server's local policy, this could mean subjecting the message to additional scrutiny, placing it into the recipient's spam folder, routing it to a different server, or taking some other action. **p=reject** indicates that you want the receiving server to reject any message that fails DMARC verification. Some servers, however, may still accept these message but quarantine them or subject them to additional scrutiny. This is the most restrictive policy and should generally not be used unless you have total confidence about your email policies and the types of messages or services you wish to allow your accounts to use. For example, if you wish to allow your users to join 3rd party mailing lists, use mail forwarding services, utilize "share this" features on websites, or the like, then using **p=reject** would almost certainly cause some legitimate messages to be rejected. It could also cause some users to be automatically dropped or banned from certain mailing lists. Example: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-report@example.net"`

Optional Tags
All of the tags listed below are optional. When any of these tags are not used in a record then their default values are assumed.

Tag	Value	Notes
sp=	**none** **quarantine** **reject** — **Default:** If **sp=** is not used, the **p=** tag applies to the	This tag is for specifying a policy to be used for subdomains of the domain to which the DMARC record applies. For example, if this tag is used in a record that has scope over example.com, then the policy designated in the **p=** tag will apply to messages from example.com and the policy designated in the **sp=** tag will apply to messages from subdomains of example.com, such as mail.example.com. If this tag is omitted from the record, the **p=** tag will apply to the domain and its subdomains. Example: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

	domain and subdomains.	

rua=	Comma-separated list of email addresses to which DMARC aggregate reports should be sent. The addresses must entered as URIs in the form: **mailto:user@example.com** — **Default: none** If this tag is not used then no aggregate reports will be sent.	This tag indicates that you wish to receive DMARC aggregate reports from servers who receive messages claiming to be **From:** a sender at your domain. Specify one or more email addresses as URIs in the form: **mailto:user@example.com**, separating multiple URIs with commas.
		Example:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:user01@example.com,mailto:user02@example.com"`
		Ordinarily these addresses will be at the domain covered by this record. If you wish to send reports to an address at some other domain, then that domain's DNS zone file must also contain a special DMARC record indicating that it will accept DMARC reports for the domain.
		Example record at example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:non-local-user@example.net"`
		Required record at example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ruf=	Comma-separated list of email addresses to which DMARC failure reports should be sent. The addresses must entered as URIs in the form: **mailto:user@example.com**
	—
	Default: none
	If this tag is not used then no failure reports will be sent.
		This tag indicates that you wish to receive DMARC failure reports from servers who receive messages claiming to be **From:** a sender at your domain, when the conditions specified in the **fo=** tag have been met. By default, when there is no **fo=** tag specified, failure reports are sent when the message fails all DMARC verification checks (i.e. fails both SPF and DKIM). Specify one or more email addresses as URIs in the form: **mailto:user@example.com**, separating multiple URIs with commas.
		Example:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		Ordinarily these addresses will be at the domain covered by this record. If you wish to send reports to an address at some other domain, then that domain's DNS zone file must also contain a special DMARC record indicating that it will accept DMARC reports for the domain.
		Example record at example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		Required record at example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

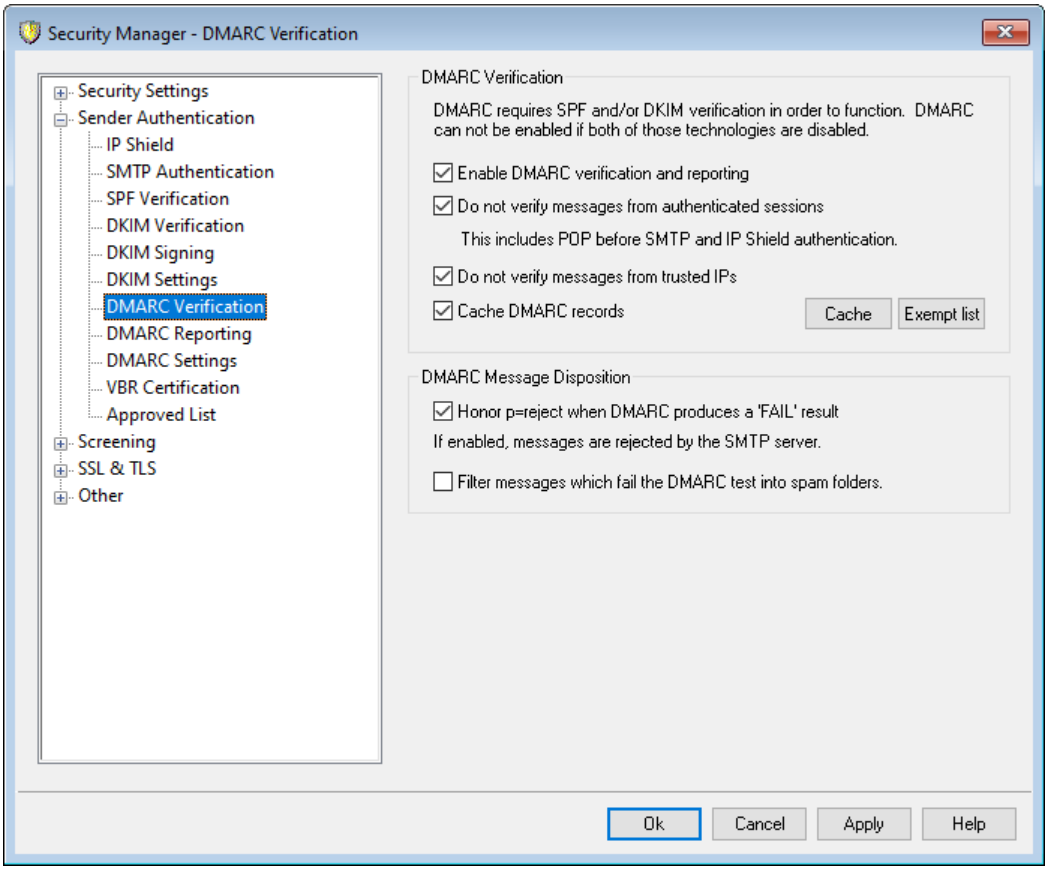
For more extensive information on the DMARC specification, see: www.dmarc.org.

See:

DMARC Verification 530
DMARC Reporting 533
DMARC Settings 537
Mailing List » Settings 268
Mailing List » Headers 271

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.5.1 DMARC Verification



DMARC Verification

Enable DMARC verification and reporting
When this option is enabled, MDaemon will perform DMARC DNS queries on the domain found in the `From:` header of incoming messages, and it will send aggregate and failure reports if you have set it to do so on the DMARC Reporting 533 screen. DMARC uses SPF 512 and DKIM 516 to validate messages, therefore at least one of those features must be enabled before DMARC can be used. DMARC verification and reporting is enabled by default and should be used in most MDaemon configurations.

Disabling support for DMARC could allow an increase in spam, phishing, or otherwise forged messages getting to your users. It could also cause some of your mailing list messages to be rejected by other servers and even cause some list members to be dropped from your lists. You should not disable DMARC unless you are absolutely sure that you have no need of it.

Do not verify messages from authenticated sessions
By default MDaemon will not perform DMARC queries on messages that are received over an authenticated session. Authenticated sessions include those verified by SMTP Authentication 509, POP before SMTP 504, or the IP Shield 507.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not verify messages from trusted IPs
By default MDaemon will not perform DMARC queries on messages that are coming from a trusted IP address 506.

Cache DMARC records
By default MDaemon will cache the DMARC record data found during the DNS lookup. By temporarily caching this information, you can increase efficiency when processing similar messages that arrive in the near future from the same domain.

Cache
This button opens the DMARC cache, which lists all currently cached DMARC records.

Exempt list
Click this button to open the DMARC exempt list. Messages originating from any IP addresses specified on the list will not be subject to DMARC verification.

DMARC Verification also honors VBR certification 541, and the Approved List 544, which can exempt based on verified DKIM identifiers and SPF paths from sources you trust. So, for example, if a message arrives that fails the DMARC check but has a valid DKIM signature from a domain on the Approved List, the message is not subject to punitive DMARC policy (i.e..the message is treated as if the policy were "p=none"). The same happens if SPF path verification matches a domain on the Approved List.

DMARC Message Disposition

Honor p=reject when DMARC produces a 'FAIL' result
By default this option is enabled, meaning that MDaemon will honor the `p=reject` DMARC policy when a message's `From:` domain has published that policy in its DMARC record and the message fails DMARC verification. Messages failing DMARC verification will be refused during the SMTP session.

When this option is disabled and a message fails DMARC verification, MDaemon will insert the "`X-MDDMARC-Fail-policy: reject`" header into the message instead of refusing to accept it. In that case you could use the Content Filter to perform some action based on the presence of that header, such as sending the message to a specific folder for further scrutiny. Further, you could use the "*Filter messages which fail the DMARC test into spam folders*" option below to cause the message to be placed into the recipient's spam folder.

Even if you leave this option disabled, the message could still be rejected for some other reason unrelated to DMARC, such as having a Spam Filter score 661 above the permitted threshold.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Filter messages which fail the DMARC test into spam folders
Enable this option if you wish to filter messages automatically into the recipient account's spam (i.e. junk e-mail) folder whenever a message fails DMARC verification. If this folder doesn't yet exist for the user, MDaemon will create one when needed.

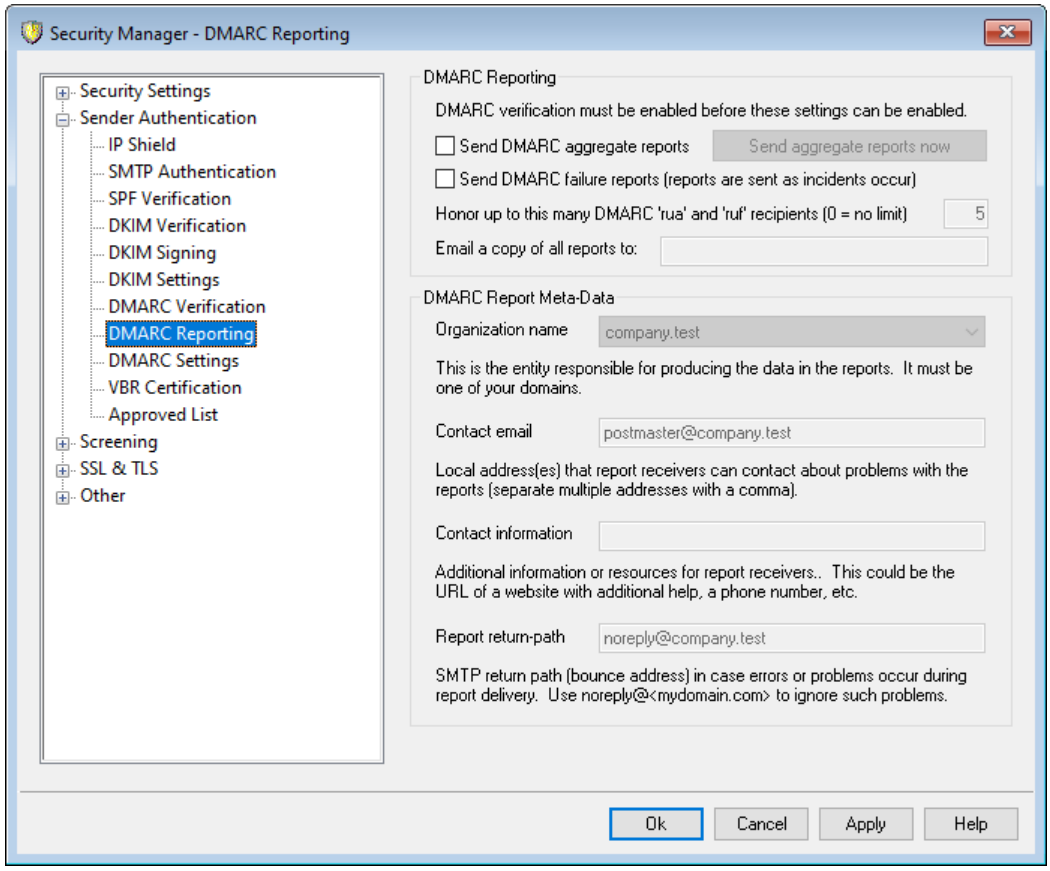
When enabled, this option is only applied when the From: domain has published a restrictive DMARC policy (i.e. p=quarantine or p=reject). When the domain publishes a p=none policy then that indicates that the domain is only monitoring DMARC and no punitive measure should be taken.

See:

DMARC 523
DMARC Reporting 533
DMARC Settings 537
Mailing List » Settings 268
Mailing List » Headers 271
Approved List 544

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.5.2 DMARC Reporting



When MDaemon queries DNS for a DMARC record, the record may contain various tags indicating that the domain owner wishes to receive DMARC reports regarding messages claiming to be from that domain. The options on the DMARC Reporting screen are for designating whether or not you wish to send DMARC aggregate or failure reports to the domains whose DMARC records request them, and for specifying the meta-data those reports will contain. The options on this screen are only available when the "*Enable DMARC verification and reporting*" option is enabled on the DMARC Verification 530 screen. Further, the DMARC specification requires the use of STARTTLS 563 whenever it is offered by report receivers. You should therefore enable STARTTLS if possible.

DMARC Reporting

Send DMARC aggregate reports
Enable this option if you are willing to send DMARC aggregate reports to domains who request them. When a DMARC DNS query on an incoming message's `From:` domain indicates that its DMARC record contains the "`rua=`" tag (e.g. `rua=mailto:dmarc-reports@example.com`), then that means the domain owner wishes to receive DMARC aggregate reports. MDaemon will therefore store DMARC related information about the domain and about the incoming messages claiming to be from that domain. It will log the email addresses to which the aggregate report should be sent, the verification methods used for each message (SPF, DKIM, or both), whether or not the message passed or failed, the sending server, its IP address, the DMARC policy applied, and so on. Then, each day at Midnight UTC

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon will use the stored data to generate each domain's report and send it to the designated addresses. Once the reports are sent, the stored DMARC data is cleared and MDaemon will start the whole process again.

MDaemon does not support the DMARC report interval tag (i.e. "ri=") for aggregate reporting. MDaemon will send aggregate reports each day at Midnight UTC, to any domain for which it has compiled DMARC data since the last time the DMARC reports were generated and sent.

Send aggregate reports now
Click this button if you wish to generate and send a batch of aggregate reports from the currently stored DMARC data, instead of waiting until MDaemon does so automatically at the next Midnight UTC batch event. This sends the reports immediately and clears the stored DMARC data, exactly like what happens each day at Midnight UTC. MDaemon will then begin storing DMARC data again until the next Midnight UTC event, or until you click the button again, whichever come first.

Because MDaemon must be running at Midnight UTC to send aggregate reports and clear stored DMARC data automatically, if you have MDaemon shut down at that time then no reports will be generated and the DMARC data will not be cleared. DMARC data collection will continue whenever MDaemon is running again, but reports will not be generated and data will not be cleared until the next Midnight UTC event, or until you click the "*Send aggregate reports now*" button.

Send DMARC failure reports (reports are sent as incidents occur)
Enable this option if you are willing to send DMARC failure reports to domains who request them. When a DMARC DNS query on an incoming message's `From:` domain indicates that its DMARC record contains the "ruf=" tag (e.g. `ruf=mailto:dmarc-failure@example.com`), then that means the domain wishes to receive DMARC failure reports. Unlike aggregate reports, these reports are created in real-time as the incidents which trigger them occur, and they contain extensive detail regarding each incident and the errors that caused the failure. These reports can be used for forensic analysis by the domain's administrators to correct problems with their email system configuration or identify other problems, such as ongoing phishing attacks.

The type of failure that will trigger a failure report is dependent upon the value of the "fo=" tag in the domain's DMARC record. By default a failure report will only be generated if all of the underlying DMARC checks fail (i.e. both SPF and DKIM fail), but domains can use various "fo=" tag values to indicate that they wish to receive the reports only if SPF fails, only if DKIM fails, if either fail, or some other combination. Consequently, multiple failure reports can be generated from a single message depending upon the number of recipients in the DMARC record's "ruf=" tag, the value of the "fo=" tag, and number of independent authentication failures that are encountered for the message during processing. If you wish to limit the number

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

of recipients to which MDaemon will send any given report, use the "*Honor up to this many DMARC 'rua' and 'ruf' recipients*" option below.

For the report format, MDaemon will only honor the `rf=afrf` tag (Authentication Failure Reporting Using the Abuse Reporting Format), which is the DMARC default. All reports are sent in this format, even if a domain's DMARC record contains the `rf=iodef` tag.

In order to support DMARC failure reporting, MDaemon fully supports: 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, and RFC 6692: Source Ports in Abuse Reporting Format (ARF) Reports.

When the DMARC "`fo=`" tag requests reporting of SPF related failures, MDaemon sends SPF failure reports according to RFC 6522. Therefore, that specification's extensions must be present in the domain's SPF record. SPF failure reports are not sent independent of DMARC processing or in the absence of RFC 6522 extensions.

When the DMARC "`fo=`" tag requests reporting of DKIM related failures, MDaemon sends DKIM failure reports according to RFC 6651. Therefore, that specification's extensions must be present in the DKIM-Signature header field, and the domain must publish a valid DKIM reporting TXT record in DNS. DKIM failure reports are not sent independent of DMARC processing or in the absence of RFC 6651 extensions.

Honor up to this many DMARC 'rua' and 'ruf' recipients (0 = no limit)
If you wish to limit the number of recipients to which MDaemon will send any given DMARC aggregate report or DMARC failure report, specify the maximum number here. If a DMARC record's "`rua=`" or "`ruf=`" tag contains more addresses than your designated limit, then MDaemon will send a given report to the listed addresses, in order, until the maximum number of addresses is reached. By default there is no limit set.

Email a copy of all reports to:
Enter one or more comma-separated email addresses here to send them a copy of all DMARC aggregate and DMARC failure reports (fo=0 or fo=1 only).

DMARC Report Meta-Data

Use these options to specify your company or organization's meta-data, which will be included with the DMARC reports you send.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Organization name
This is the entity responsible for producing the DMARC reports. It must be one of your MDaemon domains. Choose the domain from the drop-down list.

Contact email
Use this option to specify local email addresses that report receivers can contact about problems with the report. Separate multiple addresses with a comma.

Contact information
Use this option to include any additional contact information for report receivers, such as a website, a phone number, or the like.

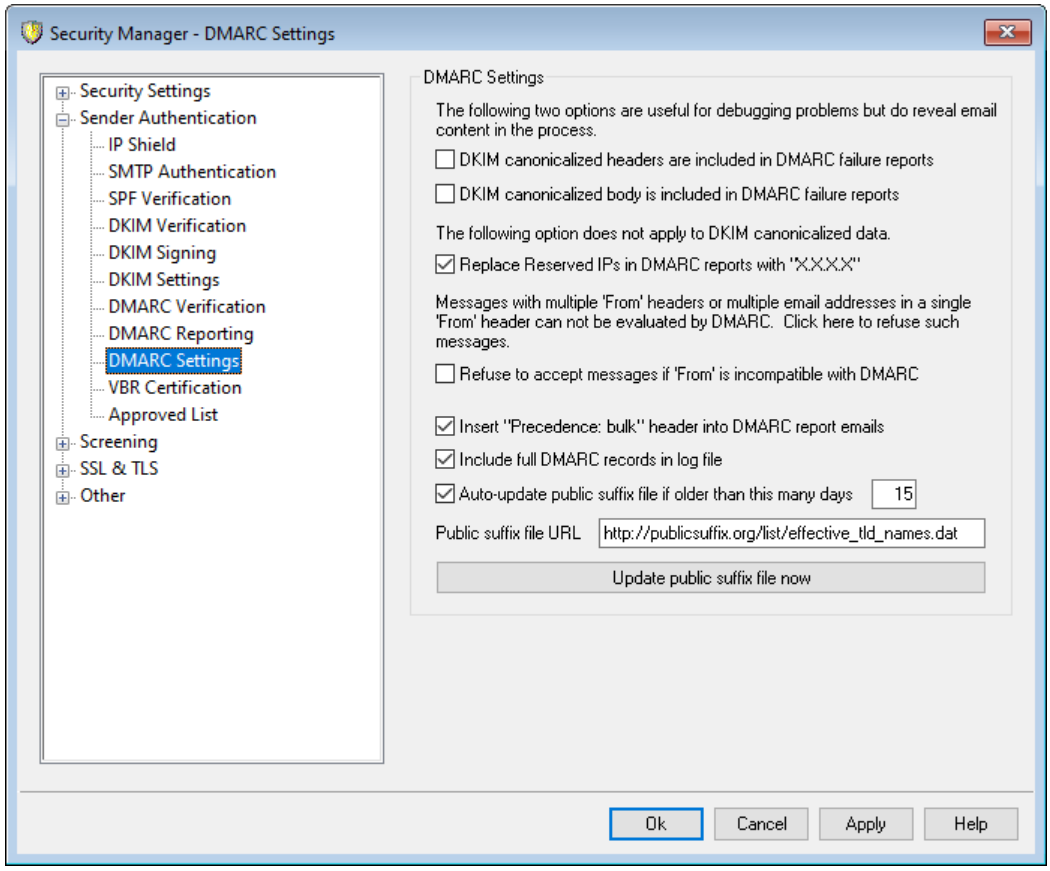
Report return-path
This is the SMTP return path (bounce address) used for report messages that MDaemon sends, in case there are delivery problems. Use `noreply@<mydomain.com>` to ignore such problems.

See:

DMARC 523
DMARC Verification 530
DMARC Settings 537

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.5.3 DMARC Settings



DMARC Settings

DKIM canonicalized headers are included in DMARC failure reports
Enable this option if you wish to include DKIM canonicalized headers[521] in DMARC failure reports[533]. This is disabled by default.

DKIM canonicalized body is included in DMARC failure reports
Enable this option if you wish to include the DKIM canonicalized body[521] in DMARC failure reports[533]. This is disabled by default.

Replace Reserved IPs in DMARC reports with "X.X.X.X"
By default MDaemon replaces your reserved IP addresses in DMARC reports with "X.X.X.X". Disable this option if you wish to make your reserved IPs visible in DMARC reports. This option does not apply to DKIM canonicalized data.

Refuse to accept messages if 'From' is incompatible with DMARC
Enable this option if you wish to refuse messages that are incompatible with DMARC requirements regarding 'From' header construction. These are messages with multiple 'From' headers or multiple email addresses in a single 'From' header. Such messages are currently exempt from DMARC processing. This setting is disabled by default because having multiple addresses in a single 'From' header is not technically a

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

protocol violation, but enabling the setting would help maximize DMARC protection. This setting is only applied when DMARC verification 530 is enabled.

Insert "Precedence: bulk" header into DMARC report emails
By default MDaemon will insert a bulk mail header into DMARC report emails. Clear this checkbox if you do not wish to insert this header.

Include full DMARC records in log file
By default MDaemon logs the full DMARC DNS record it obtains during DMARC DNS queries. Disable this option if you do not with to include the full DMARC record in the log file.

Auto-update public suffix file if older than this many days
DMARC requires a public suffix file to reliably determine the proper domains to query for DMARC DNS records. By default MDaemon will automatically update its stored public suffix file whenever it exceeds 15 days old. Change the value of this option if you wish to update the public suffix file more or less often. Disable the option if you do not wish to update it automatically.

Public suffix file URL
This is the URL of the public suffix file that MDaemon will download to use for DMARC. By default MDaemon uses the file located at: http://publicsuffix.org/list/effective_tld_names.dat.

Update public suffix file now
Click this button to manually update the public suffix file, from the *Publix suffix file URL* specified above.

See:

DMARC 523
DMARC Verification 530
DMARC Reporting 533
DKIM Settings 521

4.2.2.6 Message Certification

Message Certification is a process by which one entity vouches for or "certifies" the good email conduct of another entity. Consequently, when this certifying entity is one whom a receiving email server trusts, messages sent from a domain who is vouched for by that entity can be viewed with less suspicion. Thus the receiving server can be reasonably assured that the sending domain adheres to a set of good email practices and doesn't send spam or other problematic messages. Certification is beneficial because it can help ensure that messages will not be erroneously or needlessly subjected to unwarranted spam filter analysis. It also helps lower the resources required to process each message.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon supports Message Certification by including the world's first commercial implementation of a new Internet mail protocol called "Vouch-By-Reference" (VBR), which MDaemon Technologies is working to help create and expand through its participation in the Domain Assurance Council (DAC). VBR provides the mechanism through which Certification Service Providers (CSP) or "certifiers" vouch for the good email practices of specific domains.

Certifying Incoming Messages

It is easy to configure MDaemon's Message Certification feature to check incoming messages. All you have to do is click the *Enable certification of inbound messages* option on the VBR Certification dialog (Security » Security Settings » Sender Authentication » VBR Certification) and include one or more certification providers whom you trust to vouch for incoming email (e.g. `vbr.emailcertification.org`). You can also choose either to exempt certified messages from spam filtering or give their Spam Filter scores a beneficial adjustment.

Certifying Outgoing Messages

Before you can configure MDaemon to insert certification data into your outgoing messages, you will first need to arrange to have one or more CSPs certify your email. MDaemon Technologies provides a certification service for MDaemon customers. For details, visit: www.mdaemon.com.

To configure your MDaemon server to use Message Certification with your outgoing mail, after you have registered with a CSP:

1. Open the VBR Certification dialog: click Security » Security Settings » Sender Authentication » VBR Certification.
2. Click "*Insert certification data into outgoing messages*."
3. Click "*Configure a domain for message certification*." This opens the Certification Setup dialog.
4. Type the *Domain name* whose outgoing messages will contain the certification data.
5. Use the *Mail type* drop-down list to choose the type of email that your CSP agrees to certify for this domain, or enter a new type if the desired type isn't listed.
6. Enter one or more CSPs who will certify the domain's outbound email. If you have more than one CSP then use a space to separate each one.
7. Click "*OK*."
8. Configure your server to sign the domain's outgoing messages with DKIM 514, or ensure that they are being sent from an SPF 512 approved server. This is necessary in order to guarantee that the message originated from you. A message cannot be certified unless the receiving server can first determine that the message is authentic.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

VBR does not require the certified messages to be signed by or transmitted to your CSP. The CSP is not signing or validating specific messages—it is vouching for the domain's good email practices.

For information on the certification services provided by MDaemon Technologies, visit:

http://www.mdaemon.com/email-certification/

VBR Specification - RFC 5518:

http://tools.ietf.org/html/rfc5518

For more information on DKIM visit:

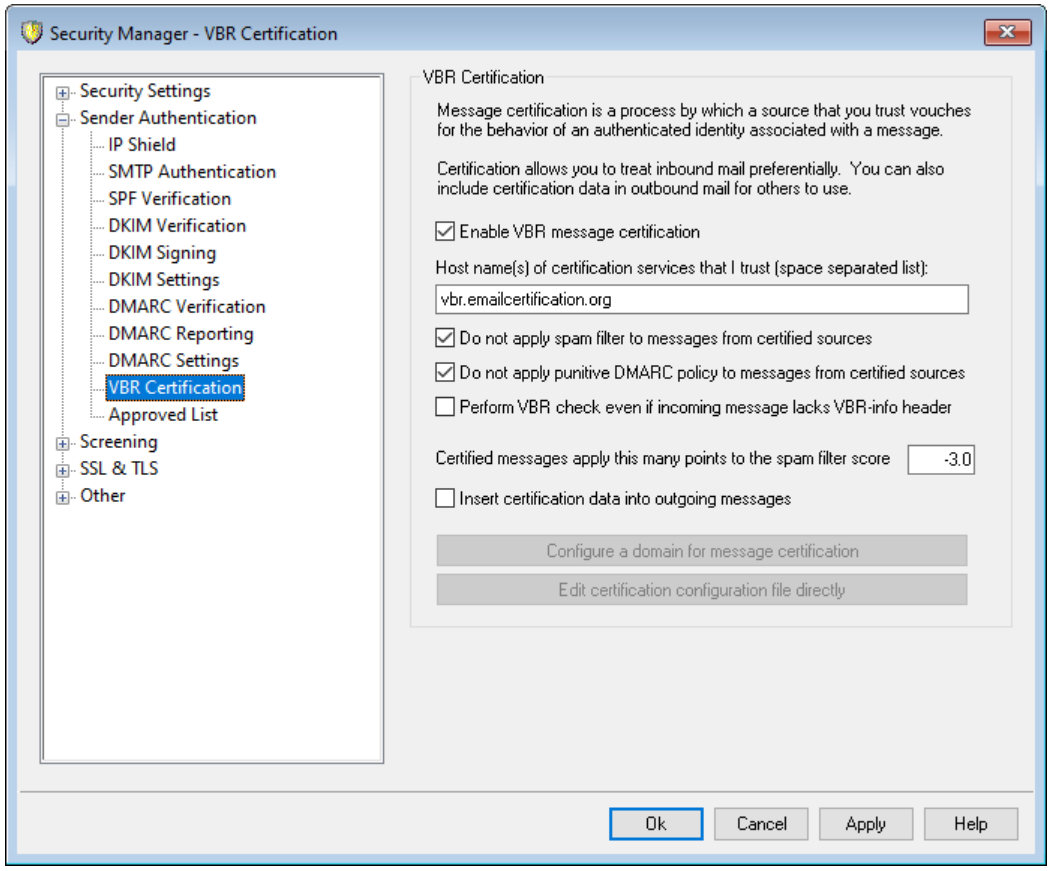
http://www.dkim.org/

See:

VBR Certification 541

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.2.6.1 VBR Certification



The VBR Certification dialog is located at: Security » Security Settings » Sender Authentication » VBR Certification.

VBR Certification

Enable VBR message certification
Click this checkbox to enable certification of inbound messages. When MDaemon receives an inbound message needing certification, it will query the trusted certification service providers (CSP) to confirm whether or not the message should actually be considered "certified." If so then the message will either be exempt from spam filtering or have its Spam Filter 660 score adjusted, depending up which option you have selected below.

Host name(s) of certification services that I trust (space separated list):
Use this box to enter the host names of the certification services that you trust. If you trust multiple services then separate each one with a space.

Do not apply spam filter to messages from certified sources
Choose this option if you want messages from certified sources to be exempt from the Spam Filter.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not apply punitive DMARC policy to messages from certified sources
This option ensures that verified messages from certified sources will not be penalized if the sending domain publishes a restrictive DMARC policy 530 (i.e. p=quarantine or p=reject) and the message fails the DMARC check. This option is enabled by default.

Perform VBR check even if incoming message lacks VBR-info header
Enable this option if you wish to perform VBR checks even on incoming messages that lack the VBR-Info header. Normally this header is necessary but VBR can still work without it. When the header is missing MDaemon will query your trusted CSPs using the "all" mail type. This option is disabled by default.

Certified messages apply this many points to the spam filter score
If you do not wish to exempt certified messages from spam filtering, use this option to designate the amount by which you wish to adjust the message's Spam Filter score. Ordinarily this should be a negative number so that certified messages will receive a beneficial adjustment. The default setting is "-3.0".

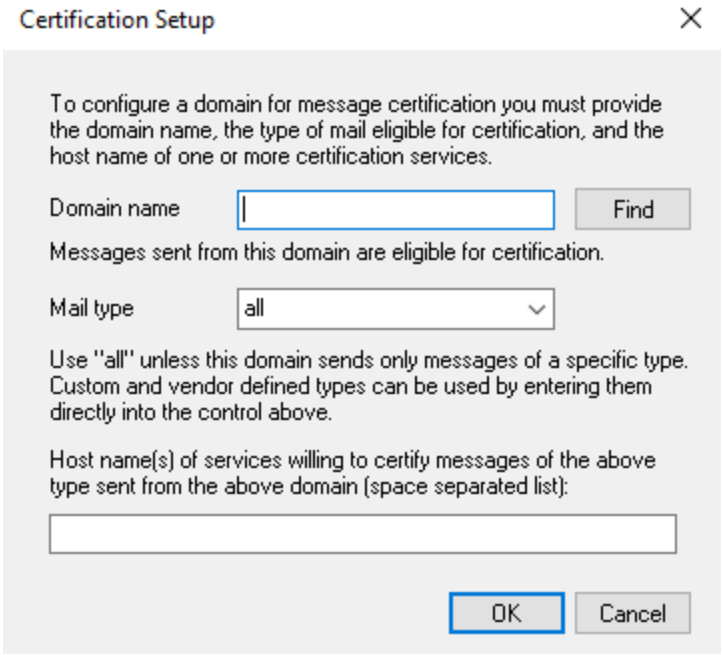
Insert certification data into outgoing messages
Click this checkbox to insert the certification data into outgoing messages. Then, click the *Configure a domain for message certification* button to open the Certification Setup dialog to designate the specific domains to be certified and CSPs associated with them.

Configure a domain for message certification
After enabling the *Insert certification data into outgoing messages* option above, click this button to open the Certification Setup dialog. On this dialog you will designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

Edit certification configuration file directly
After enabling the *Insert certification data into outgoing messages* option above, click this button to open the Vouch-by-Reference (VBR) Configuration File. Any domains that you have configured via the Certification Setup dialog to use VBR will be listed in this file, along with the associated VBR data. You can use this file to edit those entries or manually create new entries.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Certification Setup



After enabling the *Insert certification data into outgoing messages* option on the Certification dialog, click the *Configure a domain for message certification* button to open the Certification Setup dialog. This dialog is used to designate the domain whose outbound messages will be certified, the types of mail that will be certified, and the CSPs associated with the domain.

Certification Setup

Domain name
Use this option to enter the domain whose outbound messages will be certified.

Find
If you have previously configured the Message Certification settings for a particular domain, type the *Domain name* and then click this button and that domain's settings will be listed in the Certification Setup dialog's options.

Mail type
Use this drop-down list to choose the type of mail that the associated CSP has agreed to certify for this domain. If the type is not listed then you can type it in manually.

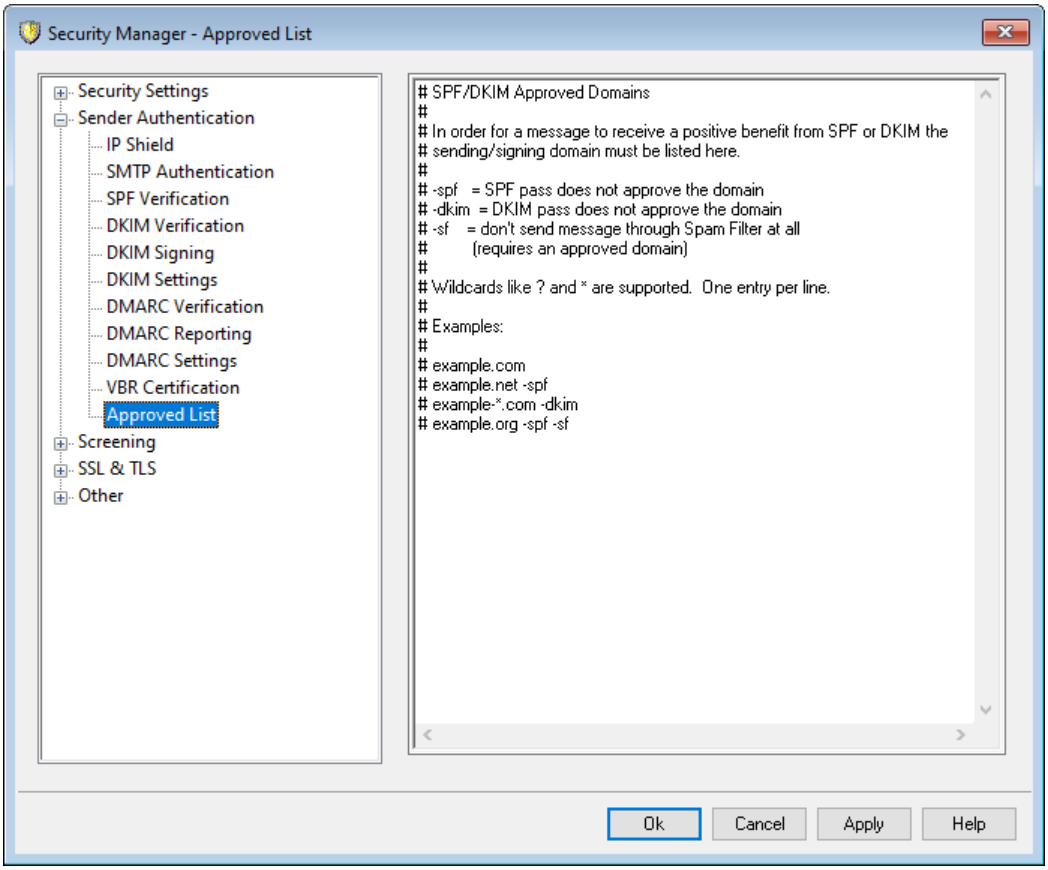
Host names(s) of services...
Enter the host names of the CSPs who have agreed to certify the domain's outbound messages (for example, `vbr.emailcertification.org`). If you enter more than one CSP then separate each one with a space.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Message Certification 538

4.2.2.7 Approved List



Because some spammers and senders of bulk email have begun using SPF or signing messages with a valid DKIM signature, the fact that a message is signed and verified is no guarantee that you won't consider it to be spam, even though it does ensure that the message originated from a valid source. For this reason, a message's spam score will not be lowered as a result of SPF or DKIM verification unless the domain taken from the signature is on the Approved List. This is essentially an allow list that you can use to designate domains permitted to have their messages' spam scores reduced when those incoming messages are verified.

When a message signed by one of these domains is verified by SPF or DKIM, its spam score will be reduced according to the settings found on the SPF 512 and DKIM Verification 516 screens. You can, however, append any of the flags listed below if you wish to prevent either of those verification methods from reducing the score. There is also a flag that you can use to prevent verified messages from being passed through the Spam Filter.

-spf Don't lower the spam score for SPF verified messages sent by this domain.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

-dkim Don't lower the spam score for DKIM verified messages from this domain.

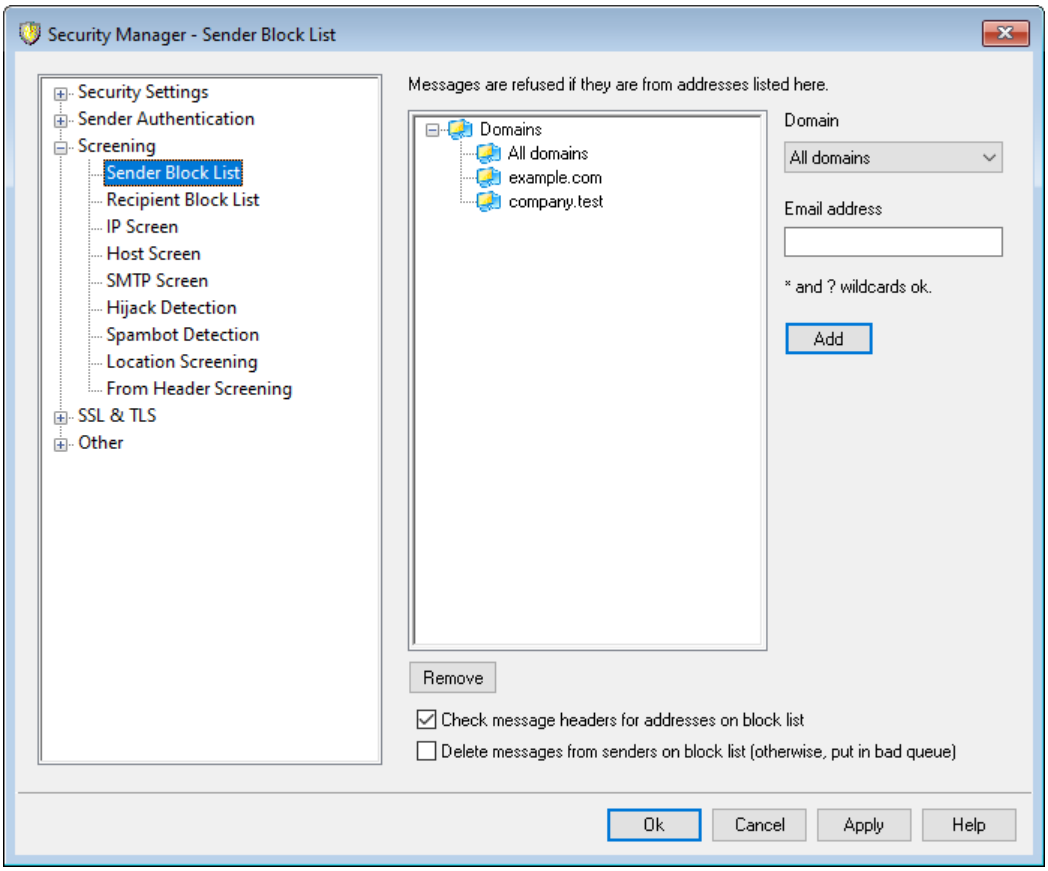
-sf Don't process verified messages from this domain through the Spam Filter.

DMARC and the Approved List

DMARC Verification 530 also utilizes the Approved List, which can exempt based on verified DKIM identifiers and SPF paths from sources you trust. So, for example, if a message arrives that fails the DMARC check but has a valid DKIM signature from a domain on the Approved List, the message is not subject to punitive DMARC policy (i.e..the message is treated as if the policy were "`p=none`"). The same happens if SPF path verification matches a domain on the Approved List.

4.2.3 Screening

4.2.3.1 Sender Block List



The Sender Block List is located at: Security » Security Settings » Screening. This list contains addresses that are not allowed to send mail traffic through your server. If a message arrives from an address on this list, it will be refused during the SMTP session. This is useful for controlling problem users. Addresses may be blocked on a per domain basis or globally (applied to all MDaemon domains).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Messages are refused if they are from addresses listed here
This window displays all currently blocked addresses, listed by the domain that is blocking them.

Domain
Choose the domain with which this blocked address will be associated. In other words, what domain do you wish to prevent from receiving mail from the specified address? Choose "All Domains" from this list to block the address globally.

Email address
Enter the address that you wish to block. Wildcards are accepted, therefore "*@example.net" will suppress any message from any user at "example.net", and "user1@*" will suppress any message from any address beginning with "user1@", regardless of the domain the message is from.

Add
Click this button to add the designated address to the block list.

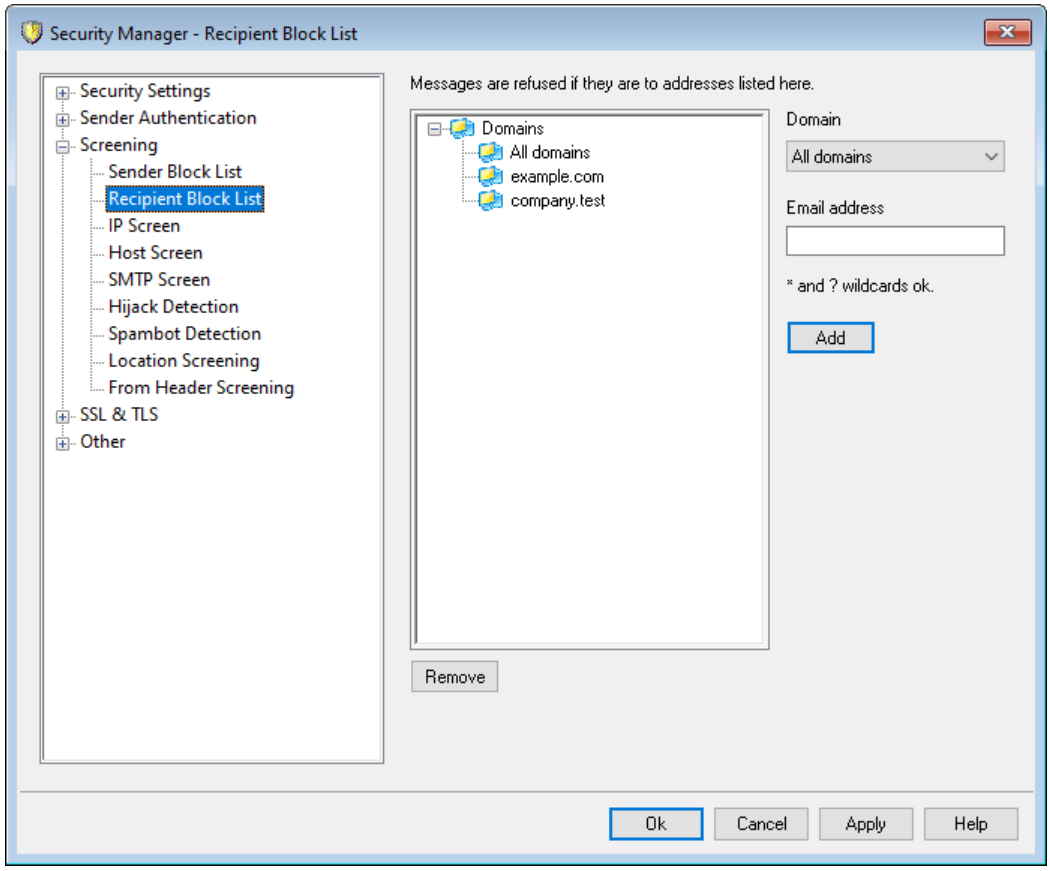
Remove
Click this button to remove an entry that you have selected in the list.

Check message headers for addresses on block list
By default, MDaemon applies the block list to values taken from the message's From/Sender header(s) during the SMTP session. This prevents the message from getting caught later and moved into the bad queue by the MTA thread.

Delete messages sent from senders on block list (otherwise put in bad queue)
Enable this option if you want MDaemon to delete incoming messages from senders who are on the block list. In addition to regular mail, this option also applies to messages arriving via MultiPOP and DomainPOP. When this option is disabled, the message will be placed into the Bad Message Queue instead of being deleted. This option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.3.2 Recipient Block List



The Recipient Block List is located at: Security » Security Settings » Screening. This list contains email addresses that are not allowed to receive mail through your server. If a message arrives for an address on this list, it will be refused. Addresses may be blocked on a per domain basis or globally (applied to all MDaemon domains). The Recipient Block List operates on SMTP envelope RCPT data only (not message headers).

Messages are refused if they are to addresses listed here
This window displays all currently blocked addresses, listed by the domain that is blocking them.

Domain
Choose the domain with which this blocked address will be associated. In other words, what domain do you wish to prevent from receiving mail for the specified address? Choose "All Domains" from this list to block the address globally.

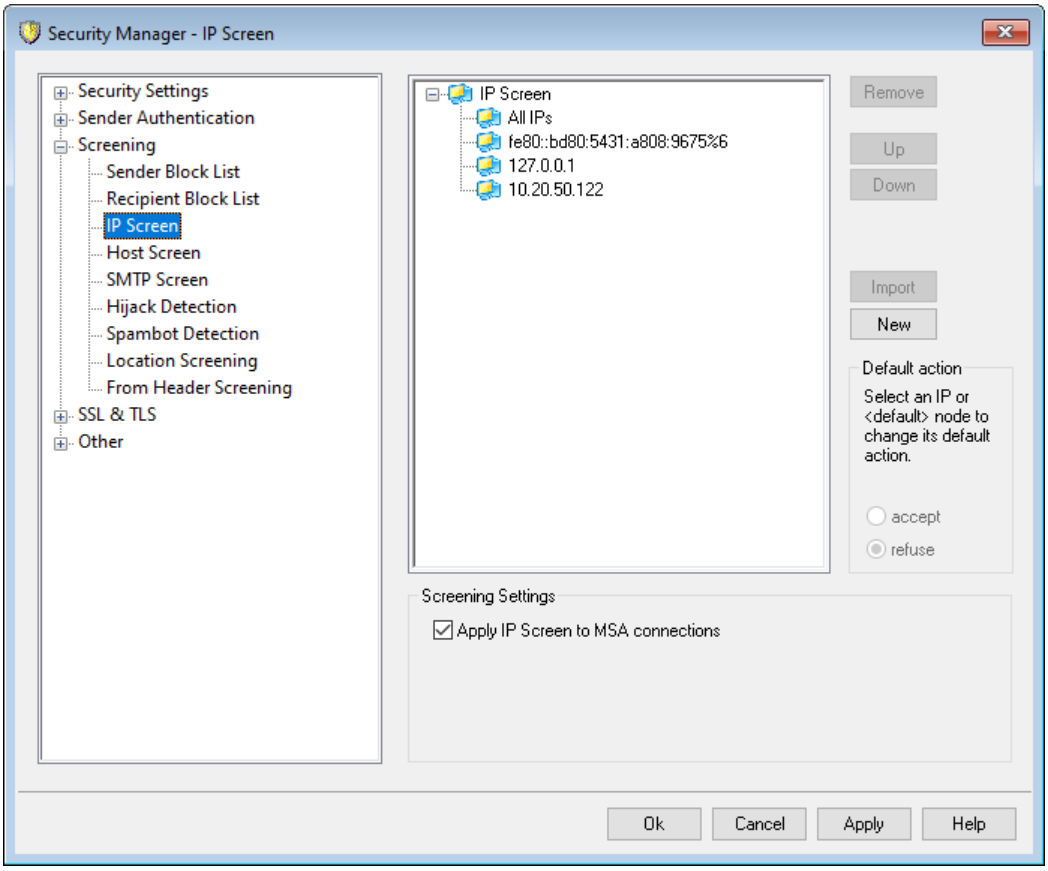
Email address
Enter the address that you wish to block. Wildcards are accepted, therefore "*@example.net" will suppress any message for any user at "example.net", and "user1@*" will suppress any message for any address beginning with "user1@", regardless of the domain to which the message is addressed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add
Click this button to add the designated address to the block list.

Remove
Click this button to remove an entry that you have selected in the list.

4.2.3.3 IP Screen



The IP Screen is located under: Security » Security Settings » Screening. It is used to define specific remote IP addresses that will be allowed to connect, or not allowed to connect, to your local IP addresses. The remote IP addresses you place on the IP Screen can be associated with either all of you local IP addresses or with individual IPs. CIDR notation and the wildcards *, #, and ? are allowed.

For example:

..*.*	Matches to any IP address
#.#.#.#	Matches to any IP address
192.*.*.*	Matches to any IP that begins with 192
192.168.*.239	Matches to IP addresses from 192.168.0.239 to 192.168.255.239
192.168.0.1??	Matches to IP addresses from 192.168.0.100 to 192.168.0.199

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New IP Screen Item

To create a new IP Screen entry, click **New**. This will open the New IP Screen Item dialog for creating the entry.

Local IP
In the drop-down list choose either "All IP's" or the specific IP to which this item will apply.

Remote IP (CIDR, * ? and # wildcards are ok)
Enter the remote IP address that you wish to add to the list, associated with the Local IP designated above.

Accept connections
Selecting this option means that the specified remote IP addresses will be allowed to connect to the associated local IP address.

Refuse connections
Selecting this option means that the specified remote IP addresses will NOT be allowed to connect to the associated local IP address. The connection will be refused or dropped.

Add
When you have finished entering the information in the options above, click this button to add the entry to the list.

Import

Select an IP address and click this button if you wish to import IP address data from an APF or .htaccess file. MDaemon's support for these files is currently limited to the following:

- "deny from" and "allow from" are supported
- only IP values are imported (not domain names)
- CIDR notation is allowed but partial IP addresses are not.
- Each line can contain any number of space-separated or comma-separated IP addresses. For example, "deny from 1.1.1.1 2.2.2.2/16", ""3.3.3.3, 4.4.4.4, 5.5.5.5", and the like.
- Lines starting with # are ignored.

Remove

To remove an entry, select the entry in the list and click **Remove**.

Default Action

To specify the default action for connections from remote IP addresses that have not been defined, select an IP address from the list and click **accept** or **refuse**. Once a default action has been specified, you can change it by selecting the "<default>" node beneath the IP address and then selecting the new default setting.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

accept
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be accepted.

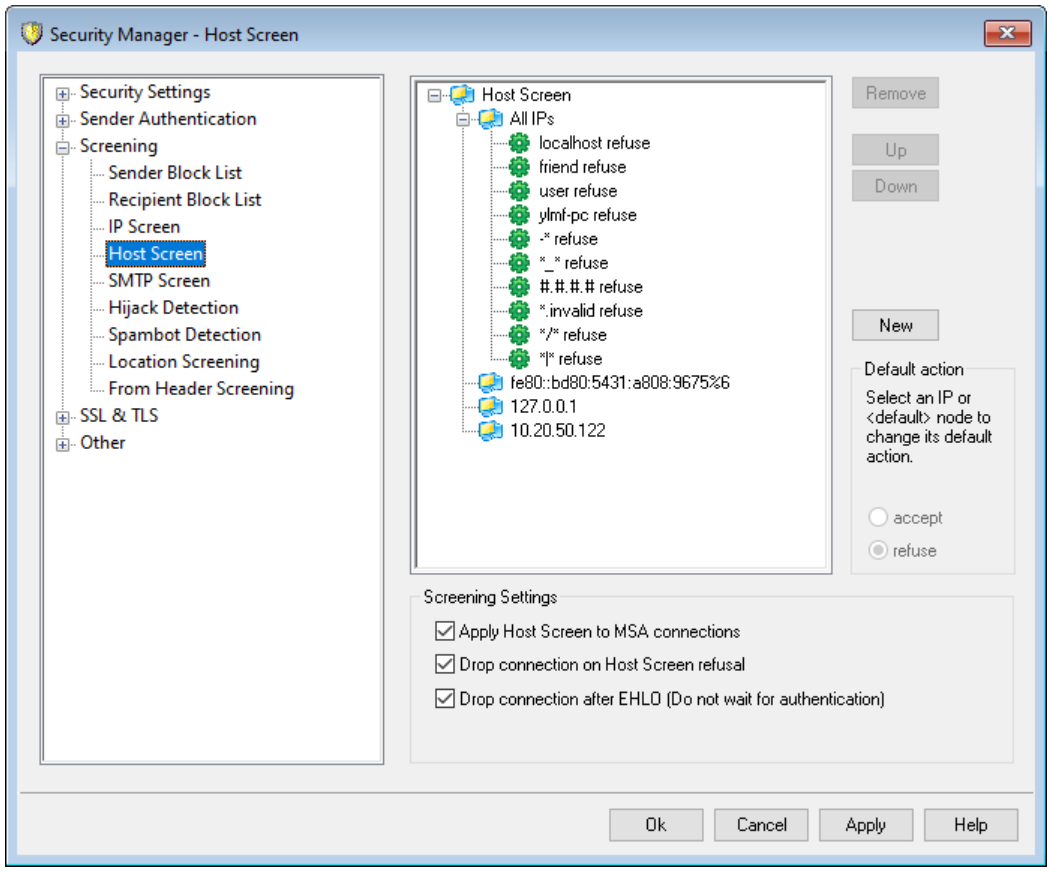
refuse
When this option is chosen, connections from any IP addresses not specifically defined on the IP Screen will be dropped, or refused.

The IP Screen will never block trusted IPs[505] or local IPs.

Screening Settings

Apply IP Screen to MSA connections
Use this option to apply IP Screening to connections made to the server's MSA port[101]. Normally this is not necessary. This setting is enabled by default.

4.2.3.4 Host Screen



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The Host Screen is located at: Security » Security Settings » Screening. It is used to define which remote hosts will be allowed to connect to your local IP addresses. You may specify a list of hosts and configure the server to allow only connections from those hosts, or you can configure it to refuse connections from the listed hosts. Host screening compares the EHLO and PTR values determined during the SMTP session with the values specified here.

New Host Screen Item

To create a new Host Screen entry, click **New**. This will open the New Host Screen Item dialog for creating the entry.

Local IP
Use this drop-down list to choose the local IP address to which this Host Screen entry will apply. Choose "All IPs" if you wish it to apply to all of your local IP addresses.

Remote host (* and # wildcards ok)
Enter the remote host that you wish to add to the list, associated with the Local IP designated above.

Accept connections
Selecting this option means that the specified remote host will be allowed to connect to the associated local IP address.

Refuse connections
Selecting this option means that the specified remote host will NOT be allowed to connect to the associated local IP address. The connection will be refused or dropped.

Remove

To remove an entry, select the entry in the list and click **Remove**.

Default Action

To specify the default action for connections from remote hosts that have not been defined, select an IP address from the list and click **accept** or **refuse**. Once a default action has been specified, you can change it by selecting the "<default>" node beneath the IP address and then selecting the new default setting.

accept
When this option is chosen, connections from any host not specifically defined on the Host Screen will be accepted.

refuse
When this option is chosen, connections from any host not specifically defined on the Host Screen will be refused.

The Host Screen will never block trusted 505 or local hosts.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

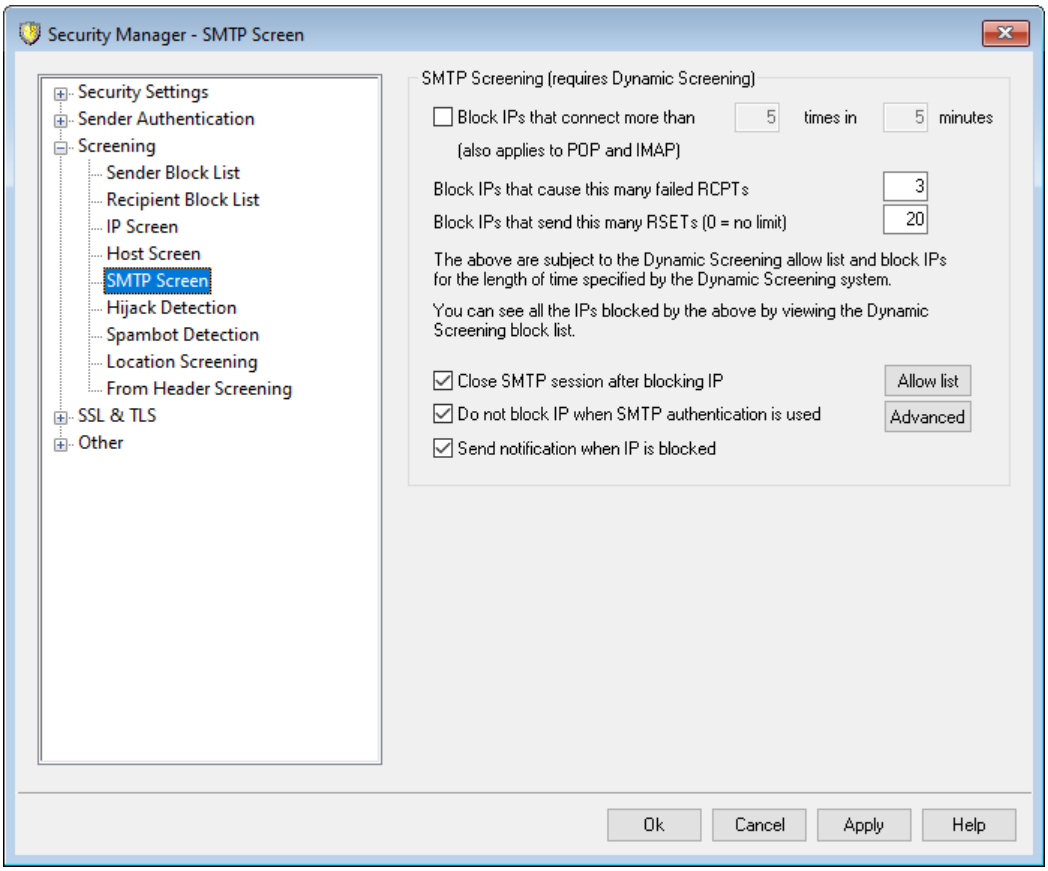
Screening Settings

Apply Host Screen to MSA connections
Use this option to apply Host Screening to connections made to the server's MSA port 101. This setting is enabled by default.

Drop connection on Host Screen refusal
When this option is enabled, the connection will be dropped immediately upon a Host Screen refusal.

Drop connection after EHLO (Do not wait for authentication)
Enable this option if you wish to drop banned connections immediately following EHLO/HELO. Normally you would wait for authentication. This setting is enabled by default.

4.2.3.5 SMTP Screen



Using the SMTP Screen you can block IP addresses that connect to MDaemon too many times within a specified number of minutes. You can also block those the cause too many failed RCPTs, and those that send too many RSET commands. The SMTP Screen requires Dynamic Screening and uses the Dynamic Block List 611 and Dynamic Allow List 609.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Block IPs that connect more than [X] times in [X] minutes
Click this check box if you wish to temporarily block IP addresses that connect to your server an excessive number of times in a limited time period. Specify the number of minutes and the number of connections allowed in that period. The addresses are blocked for the amount of time specified on the Auth Failure Tracking 600 screen. This option also applies to POP and IMAP connections.

Block IPs that cause this many failed RCPTs
When an IP address causes this number of "Recipient unknown" errors during a mail session it will be automatically blocked for the amount of time specified on the Auth Failure Tracking 600 screen. Frequent "Recipient unknown" errors are often a clue that the sender is a spammer, since spammers commonly attempt to send messages to outdated or incorrect addresses.

Block IPs that send this many RSETs (0 = no limit)
Use this option if you wish to block any IP address that issues the designated number of RSET commands during a single mail session. Use "0" if you do not wish to set a limit. There is a similar option on the Servers 86 screen under Server Settings that can be used to set a hard limit on the allowed number of RSET commands. A blocked IP address will be blocked for the amount of time specified on the Auth Failure Tracking 600 screen.

Close SMTP session after blocking IP
Enabling this option causes MDaemon to close the SMTP session after the IP address is blocked. This is enabled by default.

Do not block IP when when SMTP authentication is used
Click this checkbox if you want senders who authenticate their mail sessions before sending to be exempt from Dynamic Screening. This is enabled by default.

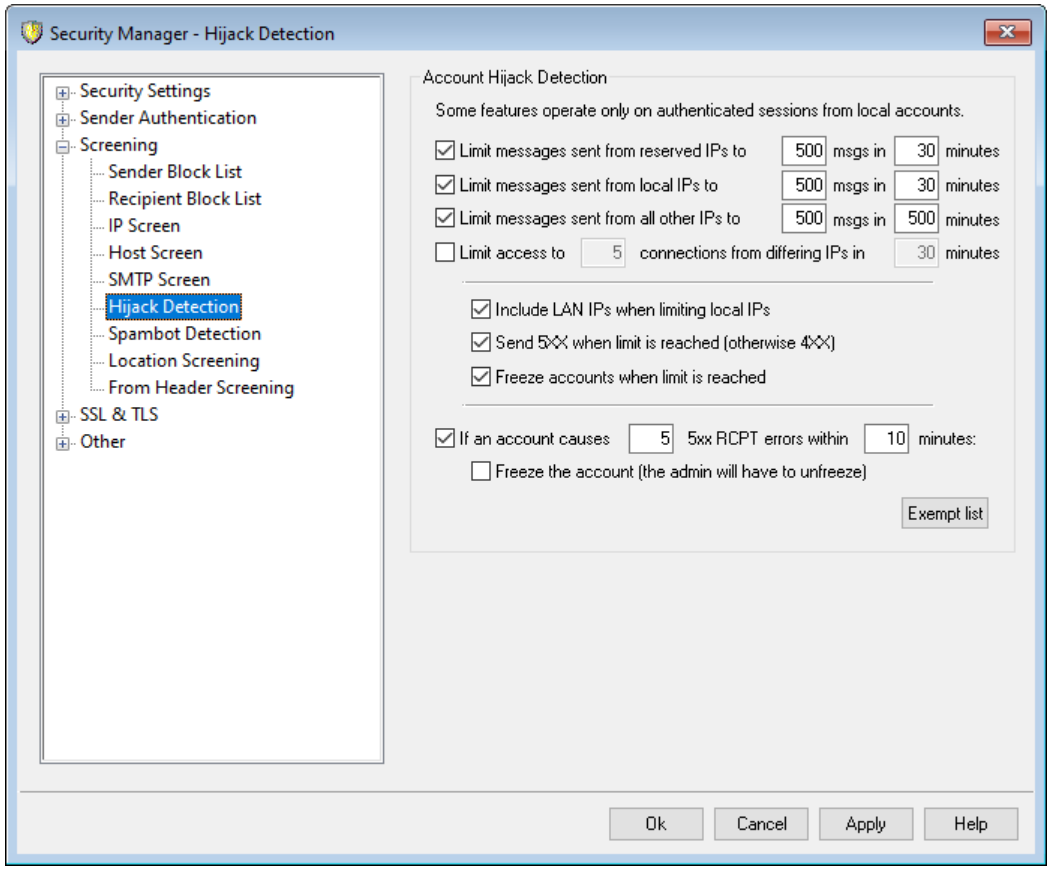
Send notification when IP is blocked
By default, when an IP addresses is automatically blocked by the Dynamic Screening system, the Dynamic Screening *IP Address Blocking Reports* 604 options will be used to notify you of that action. Clear this checkbox if you do not wish to be notified when an IP address is blocked due to SMTP Screening feature.

Allow list
Click this button to open the Dynamic Allow List 609. IP addresses listed there are exempt from SMTP Screening.

Advanced
This button opens the Dynamic Screening 596 dialog.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.3.6 Hijack Detection



Account Hijack Detection

The options on this screen can be used to detect a possibly hijacked MDaemon account and automatically prevent it from sending messages through your server. For example, if a spammer somehow obtained an account's email address and password then this feature could prevent the spammer from using the account to send bulk junk e-mail through your system. You can designate a maximum number of messages that may be sent by an account in a given number of minutes, based on the IP address from which it is connecting. You can also choose to disable accounts that reach the limit. There is also an *Exempt List* that can be used to exempt certain addresses from this restriction. Account Hijack Detection is enabled by default.

Account Hijack Detection only applies to local accounts over authenticated sessions, and the Postmaster account is automatically exempt.

Limit messages sent from reserved IPs to [xx] msgs in [xx] minutes

Use this option to prevent MDaemon accounts connecting from reserved IPs from sending more than the specified number of messages in the designated number of minutes. Reserved IP addresses are mostly as defined by RFCs (for example,

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

127.0.0.*, 192.168.*.*, 10.*.*.*, 172.16.0.0/12, ::1, FD00::/8, FEC0::/10, and FE80::/64).

Limit messages sent from local IPs to [xx] msgs in [xx] minutes
Use this option to prevent MDaemon accounts connecting from any local IPs from sending more than the specified number of messages in the designated number of minutes. Local IPs are all IP addresses configured for any of your MDaemon domain.

Limit messages sent from all other IPs to [xx] msgs in [xx] minutes
Use this option to prevent MDaemon accounts connecting from any other IPs from sending more than the specified number of messages in the designated number of minutes.

Limit access to [xx] connections from differing IPs in [xx] minutes
Use this option to limit the number of connections from different IP addresses allowed within the specified number of minutes. For example, in normal circumstances if your account is accessed from ten different IP addresses within just a few minutes, it is likely the account has been hijacked. This option is disabled by default.

Include LAN IPs when limiting local IPs
By default LAN IPs 594 are included when using the "*Limit messages sent from local IPs...*" option above. Uncheck this box if you do not wish to include LAN IPs when limiting local IPs.

Send 5XX when limit is reached (otherwise 4XX)
By default when one of the limits is reached, MDaemon will send a 5XX reply code to the hijacked account. Disable this option if you wish to send a 4XX code instead.

Freeze accounts when limit is reached
Check this box if you wish to freeze accounts that attempt to send more than the allowable number of messages. When this happens, the server sends a 552 error, the connection is dropped, and the account is immediately frozen. The frozen account will no longer be able send mail or check its mail, but MDaemon will still accept incoming mail for the account. Finally, when the account is frozen an email is then sent to the postmaster about the account. If the postmaster wishes to re-enable the account, he can simply reply to the message.

If an account causes [xx] 5xx RCPT errors within [xx] minutes
This option monitors how many times an account attempts to send messages to an invalid recipient within a fixed amount of time. One common characteristic of spam email is that the messages are often sent to a large number of invalid recipients, due to the spammer attempting to send them to old email addresses or otherwise guess new ones. Therefore if an MDaemon account begins sending messages to a notable number of invalid recipients in a short amount of time, that is a good indication that the account has been hijacked and is being used to send spam. Using this option with the "*Freeze the account...*" option below can help stop a hijacked account

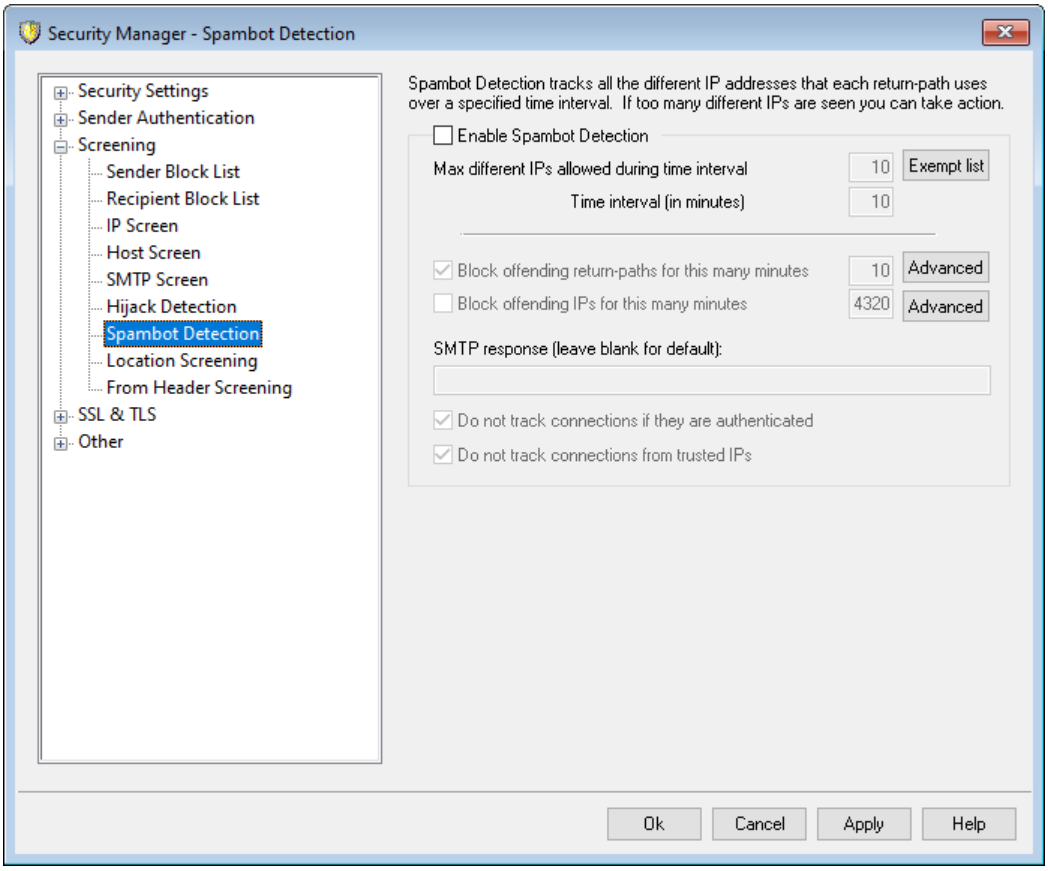
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

before too much damage is done. Note: For this option, an invalid recipient is defined as a 5xx error code in response to a RCPT command when trying to send the account's mail.

Freeze the account (the admin will have to unfreeze)
Use this option if you wish to freeze an account when the "*If an account causes [xx] 5xx RCPT errors...*" threshold above is reached. When this happens the administrator will be notified via email, so that he can investigate the problem and unfreeze the account.

Exempt List
Use the *Exempt List* to designate any addresses that you wish to exempt from Account Hijack Detection. Wildcards are permitted. For example, "`newsletters@example.com`" would exempt example.com's "newsletters" MDaemon account, while "`*@newsletters.example.com`" would exempt all MDaemon accounts belonging to the newsletters.example.com domain. The Postmaster account is automatically exempt from Account Hijack Detection.

4.2.3.7 Spambot Detection



Spambot Detection tracks the IP addresses that every `SMTP MAIL` (return-path) value uses over a given period of time. If the same return-path is used by an inordinate number of different IP addresses in a short time, this could indicate a spambot network.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

When a spambot is detected, the current connection is immediately dropped and the return-path value is optionally blocked for a length of time you specify You can also optionally block all the known spambot IP addresses for a designated period.

Enable Spambot Detection
Click this box to enabled Spambot detection. It is disabled by default.

Max different IPs allowed during time interval
This is the number of different IP addresses from which a given return-path can connect during the specified time interval.

Time interval (in minutes)
Specify the time interval (in minutes) to use when attempting to detect spambot networks.

Exempt List
Click this button to open the Spambot Detection exempt list. There you can specify IP addresses, senders, and recipients that are exempt from spambot detection.

Block offending return-paths for this many minutes
Use this option if you wish to block detected spambot return-paths. MDaemon will not accept messages with a blocked return-path for the designated number of minutes. This option is enabled by default.

Advanced
Click this button to open the Spambot Senders File. It displays the return-paths currently blocked and the number of minutes remaining before they will be removed from the block list.

Block offending IPs for this many minutes
Use this option if you wish to block detected spambot IP addresses. MDaemon will not accept messages from a blocked IP address for the designated number of minutes. This option is disabled by default.

Advanced
Click this button to open the Spambot IP File. It displays the IP addresses currently blocked and the number of minutes remaining before they will be removed from the block list.

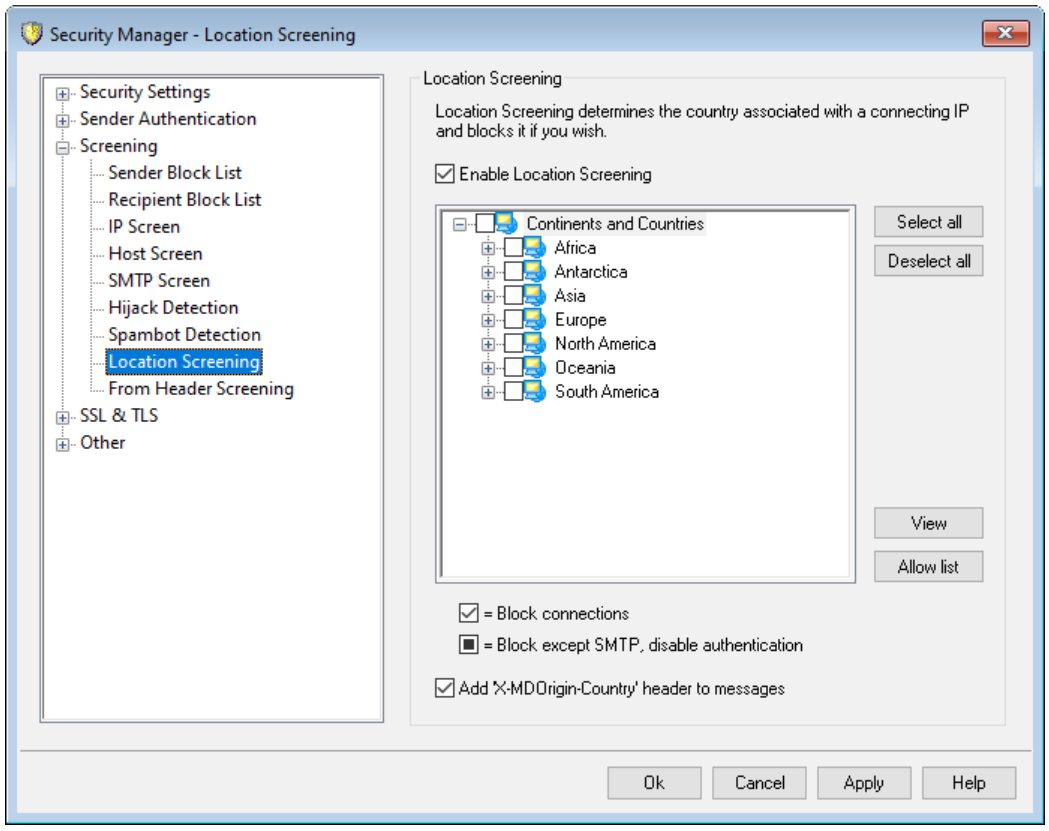
SMTP response (leave blank for default)
Use this option if you wish to customize the SMTP response to spambots attempting to send messages from a blocked return-path or IP address. MDaemon will return the SMTP response, "`551 5.5.1 <your custom text>`", rather than the default response. Leave it blank to use MDaemon's default response.

Do not track connections if they are authenticated
By default MDaemon will not track authenticated[509] sessions for Spambot Detection. Clear this checkbox if you do not wish to exempt authenticated connections.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not track connections from trusted IPs
By default Spambot Detection will not tack connections from Trusted IP 506 addresses. Clear this checkbox if you do not wish to exempt Trusted IPs.

4.2.3.8 Location Screening



Location Screening

Location Screening is a geographically based blocking system that you can use to block incoming SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 73, XML API, Remote Administration, CalDAV/CardDAV, XMPP, and Minger connections from unauthorized regions of the world. MDaemon determines the country associated with the connecting IP address and then blocks that connection if it is from a restricted location, and adds a line to the Screening log. For SMTP, Location Screening can optionally block only connections using AUTH. This is useful, for example, if you have no users in a specific country but still wish to be able to receive mail from there. That way you would only block those attempting to log in to your server.

The `\MDaemon\Geo\` folder contains database files that serve as the master country IP database. The files were provided by MaxMind (www.maxmind.com), and updates can be downloaded from their site if desired.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable Location Screening
Location Screening is on by default, but no regions or countries are blocked; MDaemon just logs the connecting country or region. To block a location, click the box until a check mark appears next to the region or country that you wish to block. If you wish to block only AUTH connections, which means SMTP connections will still be allowed, then click the box again so that it is completely filled. When Location Screening is on, regardless of whether or not any locations are being blocked, MDaemon will insert the "`X-MDOrigin-Country`" header into messages, for content filtering or other purposes. This header contains two-letter ISO 3166 country and continent codes.

Select/Deselect all
Use these button to select or deselect all locations in the list.

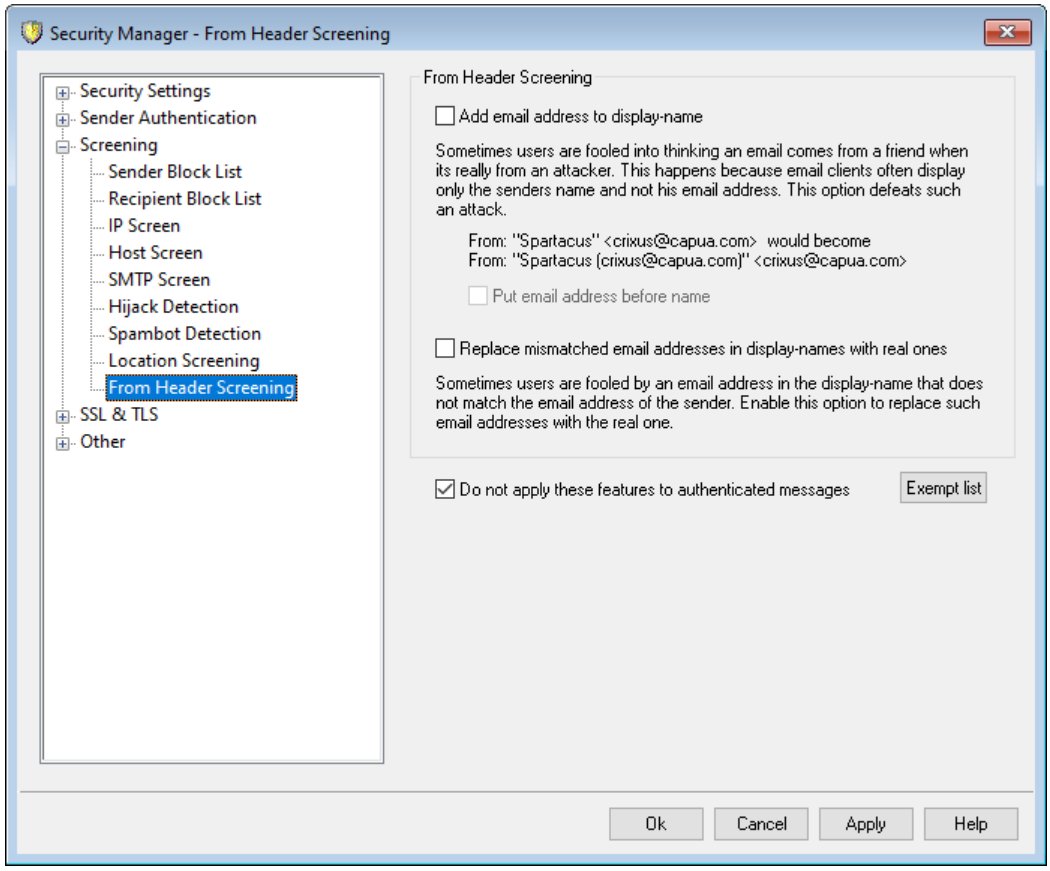
View
Click this button to view a text file list of all the locations that are currently blocked by Location Screening. If you check/uncheck any box in the list of locations then the *View* button will not be available until after you click **Apply**.

Allow list
This button opens the Dynamic Screening Allow List 609, which is also used for Location Screening. If you wish to exempt an IP address from Location Screening, click this button and specify the IP address and when you wish the entry to expire.

Add 'X-MDOrigin-Country' header to messages
By default, when Location Screening is on, MDaemon will insert the "`X-MDOrigin-Country`" header into messages, for content filtering or other purposes. This header contains two-letter ISO 3166 country and continent codes instead of full names. Clear this checkbox if you do not wish to insert the header into messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.3.9 From Header Screening



From Header Screening

This security feature modifies the "From:" header of incoming messages to cause the name-only portion of the header to contain both the name and email address. This is done to combat a common tactic used in spam and attacks where the message is made to appear to be coming from someone else. When displaying a list of messages, email clients commonly display only the sender's name rather than the name and email address. To see the email address, the recipient must first open the message or take some other action, such as right-click the entry, hover over the name, or the like. For this reason attackers commonly construct an email so that a legitimate person or company name appears in the visible portion of the "From:" header while an illegitimate email address is hidden. For example, a message's actual "From:" header might be, `"Honest Bank and Trust" <lightfingers.klepto@example.com>`, but your client might display only `"Honest Bank and Trust"` as the sender. This feature changes the visible portion of the header to display both parts. In the above example the sender would now appear as `"Honest Bank and Trust (lightfingers.klepto@example.com)" <lightfingers.klepto@example.com>`, giving you a clear indication that the message is fraudulent.

Add email address to display-name
Enable this option if you wish to modify the client-visible portion of the "From:" header of incoming messages to include both the name and email address of the sender. The construction of the new header will change from `"Sender's Name"`

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

<mailbox@example.com> to "Sender's Name (mailbox@example.com)" <mailbox@example.com>. This only applies to messages to local users, and this option is disabled by default. Consider carefully before enabling this option as some users may neither expect nor want the From: header to be modified, even if it might help them identify fraudulent emails.

Put email address before name
When using the *Add email address to display-name* option above, enable this option if you wish to swap the name and email address in the modified "From:" header, putting the email address first. Using the example above, "Sender's Name" <mailbox@example.com> would now be modified to: "mailbox@example.com (Sender's Name)" <mailbox@example.com>.

Replace mismatched email addresses in display-names with real ones
Another tactic used in spam is to put a seemingly legitimate name and email address in the display-name portion of the "From:" header, even though it is not the actual sending email address. Use this option if you wish to replace the visible email address in messages like this with the actual sender's address.

Do not apply these features to authenticated messages
Check this box if you do not wish to apply the From Header Screening options to incoming messages that have been authenticated by MDaemon.

Exempt List
Use this option to add addresses to the From Header Screening Exempt List. Messages sent to the listed addresses will not have their "From:" headers modified.

4.2.4 SSL & TLS

MDaemon supports the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol for SMTP, POP, and IMAP 563, and for MDaemon Remote Administration 570 and Webmail's 566 web server. The SSL protocol, developed by Netscape Communications Corporation, is the standard method for securing server/client Internet communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connection. Further, because SSL is built into all current major browsers, simply installing a valid digital certificate on your server will activate the connecting browser's SSL capabilities when connecting to MDRA or Webmail.

If you are connecting to the standard mail ports via a mail client instead of using Webmail, MDaemon supports the STARTTLS extension over TLS for SMTP and IMAP, and the STLS extension for POP3. However, you must first have your client configured to use SSL, and it must support those extensions—not all mail clients support them. Use the No STARTTLS List 574 and STARTTLS List 575 pages to designate specific hosts and addresses that must not or must, respectively, use STARTTLS.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The SSL & TLS dialog also contains a page for enabling DNSSEC 579 (DNS Security Extensions), the SMTP Extensions 576 page for enabling RequireTLS, MTA-STA, and TLS Reporting, and the Let's Encrypt 580 page for when using the Let's Encrypt Certificate Authority (CA).

The options for enabling and configuring SSL are located under the SSL & TLS section of the Security Settings dialog at: Security » Security Manager » SSL & TLS. The SSL port settings for SMTP, POP3, and IMAP are located on the Ports 101 screen at: Setup » Server Settings » DNS & IPs. The HTTPS ports for Webmail 566 and Remote Administration 570 are located on there respective screens.

For information on creating and using SSL Certificates, see:

Creating & Using SSL Certificates 896

—

The TLS/SSL protocol is addressed in RFC-4346: The Transport Layer Security (TLS) Protocol Version 1.1

The STARTTLS extension for SMTP is addressed in RFC-3207: SMTP Service Extension for Secure SMTP over Transport Layer Security

Using TLS with the IMAP and POP3 protocols is addressed in RFC-2595: Using TLS with IMAP, POP3 and ACAP

DNSSEC (DNS Security Extensions) is defined in: RFC-4033: DNS Security Introduction and Requirements and RFC-4035: Protocol Modifications for the DNS Security Extensions as

For a complete description of RequireTLS, see: RFC 8689: SMTP Require TLS Option.

MTA-STS support is described in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

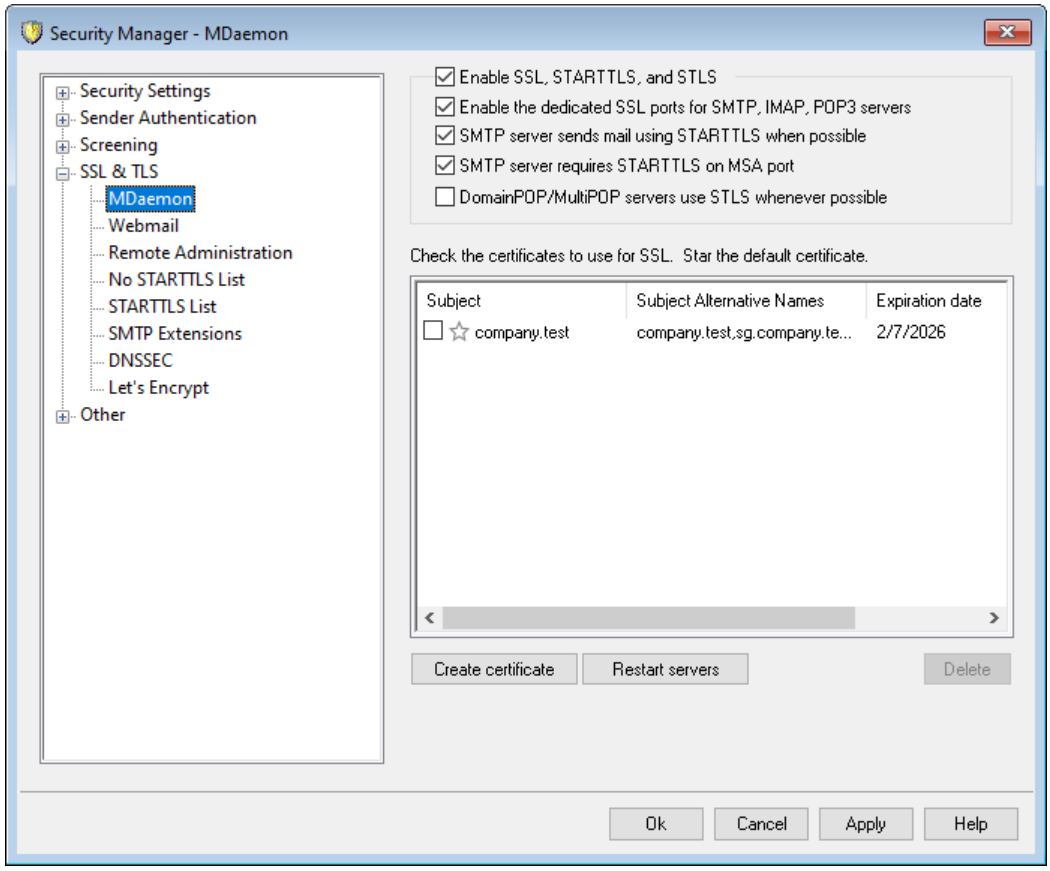
TLS Reporting is discussed in RFC 8460: SMTP TLS Reporting.

See:

SSL & TLS » MDaemon 563
SSL & TLS » Webmail 566
SSL & TLS » Remote Administration 570

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.4.1 MDaemon



Enable SSL, STARTTLS, and STLS
Click this check box to activate support for the SSL/TLS protocol and the STARTTLS and STLS extensions. Then, choose the certificate that you want to use from the list below.

Enable the dedicated SSL ports for SMTP, IMAP, POP3 servers
Enable this option if you want to make available the dedicated SSL ports specified on Ports 101 under Default Domains & Servers. This will not affect clients using STARTTLS and STLS on the default mail ports — it merely provides an additional level of support for SSL.

SMTP server sends mail using STARTTLS when possible
Click this option if you want MDaemon to attempt to use the STARTTLS extension for every SMTP message it sends. If a server to which MDaemon is connecting doesn't support STARTTLS then the message will be delivered normally without using SSL. Use the No STARTTLS List 574 if you wish to prevent the use of STARTTLS for certain domains.

SMTP server requires STARTTLS on MSA port
Enable this option if you wish to require STARTTLS for connections to the server made on the MSA port 101.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

DomainPOP/MultiPOP servers use STLS whenever possible
Check this box if you want the DomainPOP and MultiPOP servers to use the STLS extension whenever possible.

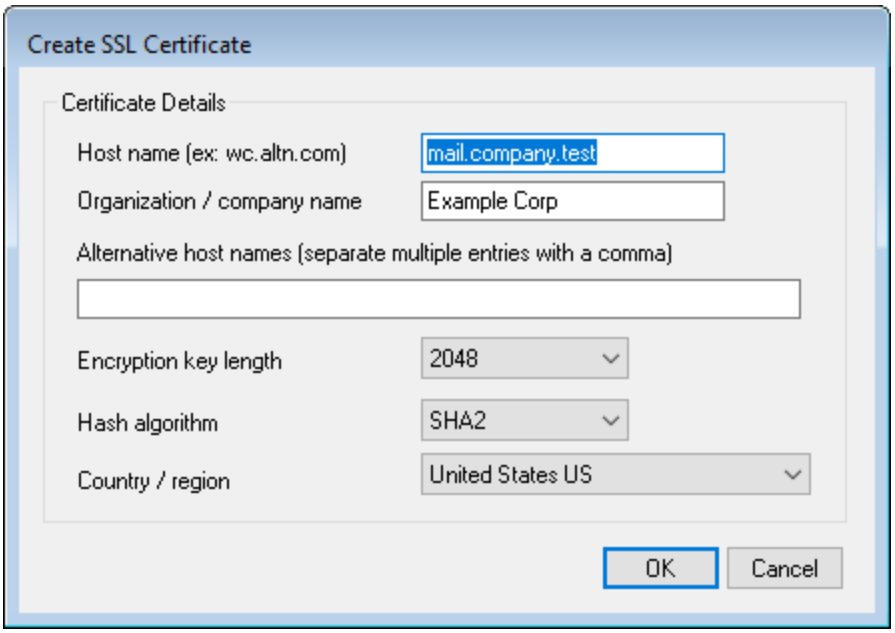
Select certificate to use for SSL

This box displays your SSL certificates. Check the box next to any certificates you wish to be active. Click the star next to the one that you wish to set as the default certificate. MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used. Double-click a certificate to open it in Windows' Certificate dialog for review (only available in the application interface, not in the browser-based remote administration).

Delete
Select a certificate in the list and then click this button to delete it. A confirmation box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Certificate Details

Host name
When creating a certificate, enter the host name to which your users will connect (for example, "mail.example.com").

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field. If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Country/region
Choose the country or region in which your server resides.

Restart servers

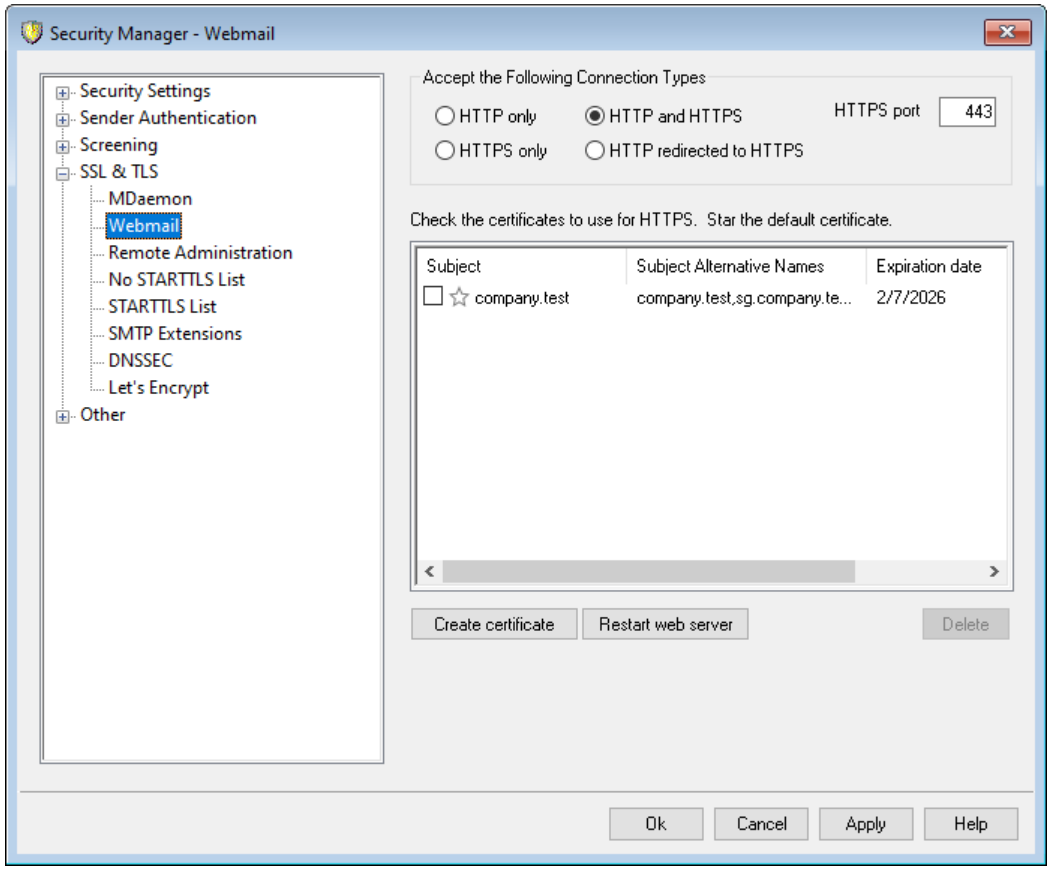
Click to restart the SMTP/IMAP/POP servers. The servers must be restarted when a certificate changes.

See:

SSL & TLS 561
Creating and Using SSL Certificates 896

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.4.2 Webmail



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Webmail to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Webmail". For your convenience, however, these options are also mirrored under "Security » Security Manager » SSL & TLS » Webmail".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 561

This screen only applies to Webmail when using MDaemon's built-in web server. If you configure Webmail to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Accept the Following Connection Types

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Webmail. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Webmail, but do not wish to force your Webmail users to use HTTPS. Webmail will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Webmail TCP port designated on the Web Server 313 screen of Webmail.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Webmail. Webmail will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Webmail will listen to for SSL connections. The default SSL port is 443. If the default SSL port is used, you will not have to include the port number in Webmail's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:443").

This is not the same as the Webmail port that is designated on the Web Server 313 screen of Webmail. If you are still allowing HTTP connections to Webmail then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Check the box next to any certificates you wish to be active. Click the star next to the one that you wish to set as the default certificate. MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used. Double-click a certificate to open it in Windows' Certificate dialog for review (only available in the application interface, not in the browser-based remote administration).

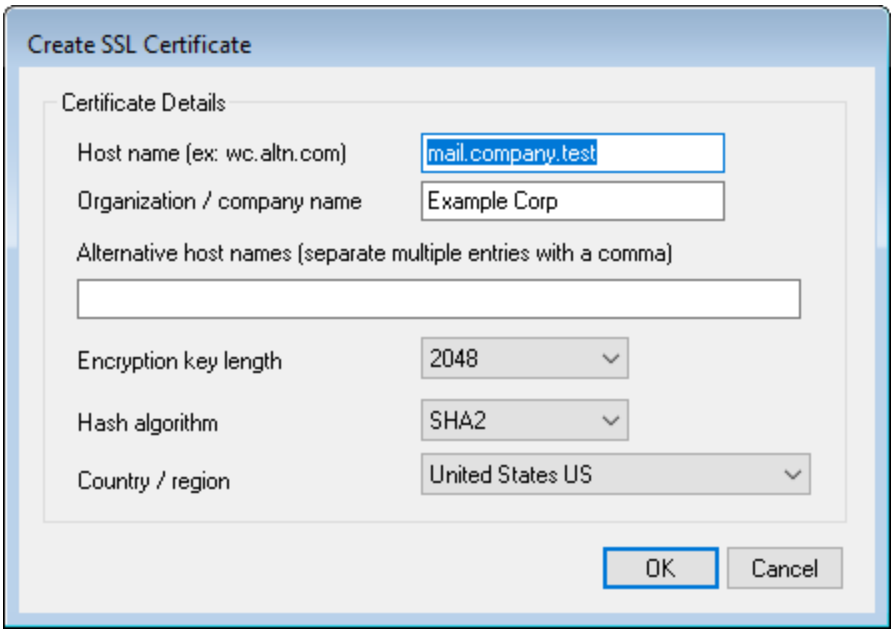
Delete
Select a certificate in the list and then click this button to delete it. A confirmation

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Certificate Details

Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field. If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

Using Let's Encrypt to Manage Your Certificate

Let's Encrypt is a Certificate Authority (CA) that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

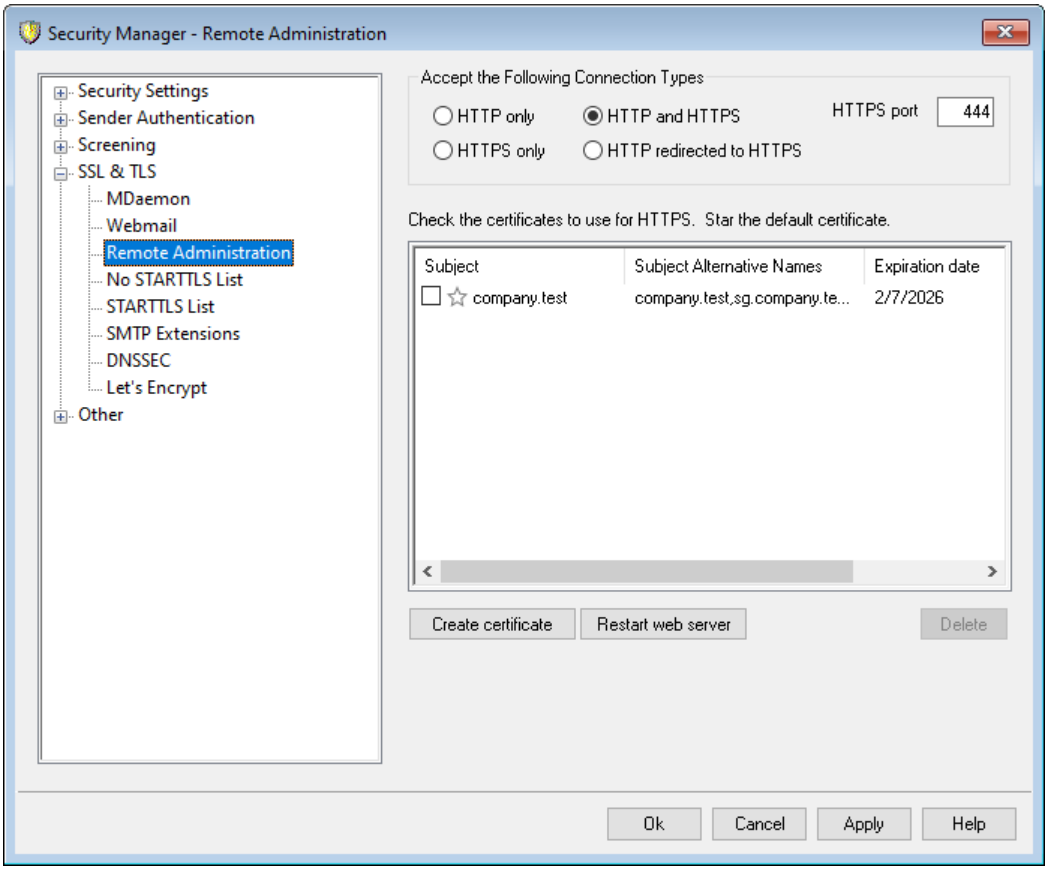
To support using Let's Encrypt's automated process to manage a certificate, the Let's Encrypt 580 screen is provided to help you easily configure and run the PowerShell script included in the "`MDaemon\LetsEncrypt`" folder. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*. See the Let's Encrypt 580 topic for more information.

See:

SSL & Certificates 561
Creating and Using SSL Certificates 896

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.4.3 Remote Administration



MDaemon's built-in web server supports the Secure Sockets Layer (SSL) protocol. SSL is the standard method for securing server/client web communications. It provides server authentication, data encryption, and optional client authentication for TCP/IP connections. Further, because HTTPS support (i.e. HTTP over SSL) is built into all major browsers, simply installing a valid digital certificate on your server will activate the connecting client's SSL capabilities.

The options for enabling and configuring Remote Administration to use HTTPS are located on the SSL & HTTPS screen under Setup » Web & IM Services » Remote Administration". For your convenience, however, these options are also mirrored under "Security » Security Settings » SSL & TLS » Remote Administration".

For more information on the SSL protocol and Certificates, see: **SSL & Certificates** 561

This screen only applies to Remote Administration when using MDaemon's built-in web server. If you configure Remote Administration to use some other web server such as IIS, these options will not be used — SSL/HTTPS support will have to be configured using your the other web server's tools.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Accept the Following Connection Types

HTTP only
Choose this option if you do not wish to allow any HTTPS connections to Remote Administration. Only HTTP connections will be accepted.

HTTP and HTTPS
Choose this option if you want to enable SSL support within Remote Administration, but do not wish to force your Remote Administration users to use HTTPS. Remote Administration will listen for connections on the HTTPS port designated below, but it will still respond to normal http connections on the Remote Administration TCP port designated on the Web Server 343 screen.

HTTPS only
Choose this option if you wish to require HTTPS when connecting to Remote Administration. Remote Administration will respond only to HTTPS connections when this option is enabled — it will not respond to HTTP requests.

HTTP redirected to HTTPS
Choose this option if you wish to redirect all HTTP connections to HTTPS on the HTTPS port.

HTTPS port
This is the TCP port that Remote Administration will listen to for SSL connections. The default SSL port is 444. If the default SSL port is used, you will not have to include the port number in Remote Administration's URL when connecting via HTTPS (i.e. "https://example.com" is equivalent to "https://example.com:444").

This is not the same as the Remote Administration port that is designated on the Web Server 343 screen. If you are still allowing HTTP connections to Remote Administration then those connections must use that other port to connect successfully. HTTPS connections must use the HTTPS port.

Select certificate to use for HTTPS/SSL

This box displays your SSL certificates. Check the box next to any certificates you wish to be active. Click the star next to the one that you wish to set as the default certificate. MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field (you can specify the alternate names when creating the certificate). If the client does not request a host name, or if no matching certificate is found, then the default certificate is used. Double-click a certificate to open it in Windows' Certificate dialog for review (only available in the application interface, not in the browser-based remote administration).

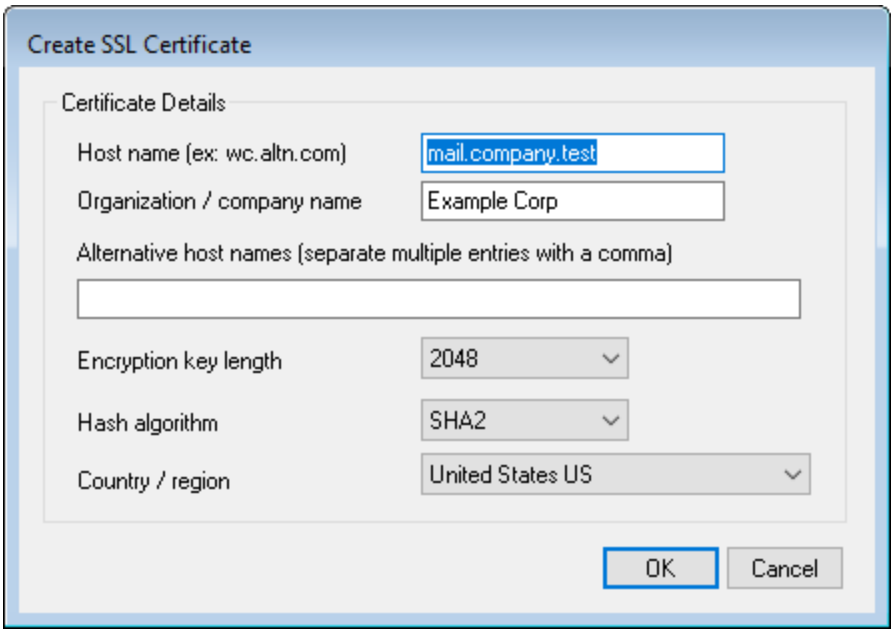
Delete
Select a certificate in the list and then click this button to delete it. A confirmation

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

box will open and ask you if you are sure that you want to delete the certificate.

Create Certificate

Click this button to open the Create SSL Certificate dialog.



Certificate Details

Host name
When creating a certificate, enter the host name to which your users will connect (for example, "wc.example.com").

Organization/company name
Enter the organization or company that "owns" the certificate here.

Alternative host names (separate multiple entries with a comma)
If there are alternative host names to which users may be connecting and you want this certificate to apply to those names as well, then enter those domain names here separated by commas. Wildcards are permitted, so "`*.example.com`" would apply to all sub domains of `example.com` (for example, "`wc.example.com`", "`mail.example.com`", and so on).

MDaemon supports the Server Name Indication (SNI) extension to the TLS protocol, which allows a different certificate to be used for each of your server's host names. MDaemon will look at the active certificates and choose the one that has the requested host name in its Subject Alternative Names field. If the client does not request a host name, or if no matching certificate is found, then the default certificate is used.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Encryption key length
Choose the desired bit-length of the encryption key for this certificate. The longer the encryption key the more secure the transferred data will be. Note, however, that not all applications support key lengths longer than 512.

Country/region
Choose the country or region in which your server resides.

Hash algorithm
Choose the hash algorithm that you wish to use: SHA1 or SHA2. The default setting is SHA2.

Restart web server

Click this button to restart the web server. The web server must be restarted before a new certificate will be used.

Using Let's Encrypt to Manage Your Certificate

Let's Encrypt is a Certificate Authority (CA) that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

To support using Let's Encrypt's automated process to manage a certificate, the Let's Encrypt 580 screen is provided to help you easily configure and run the PowerShell script included in the "`MDaemon\LetsEncrypt`" folder. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*. See the Let's Encrypt 580 topic for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

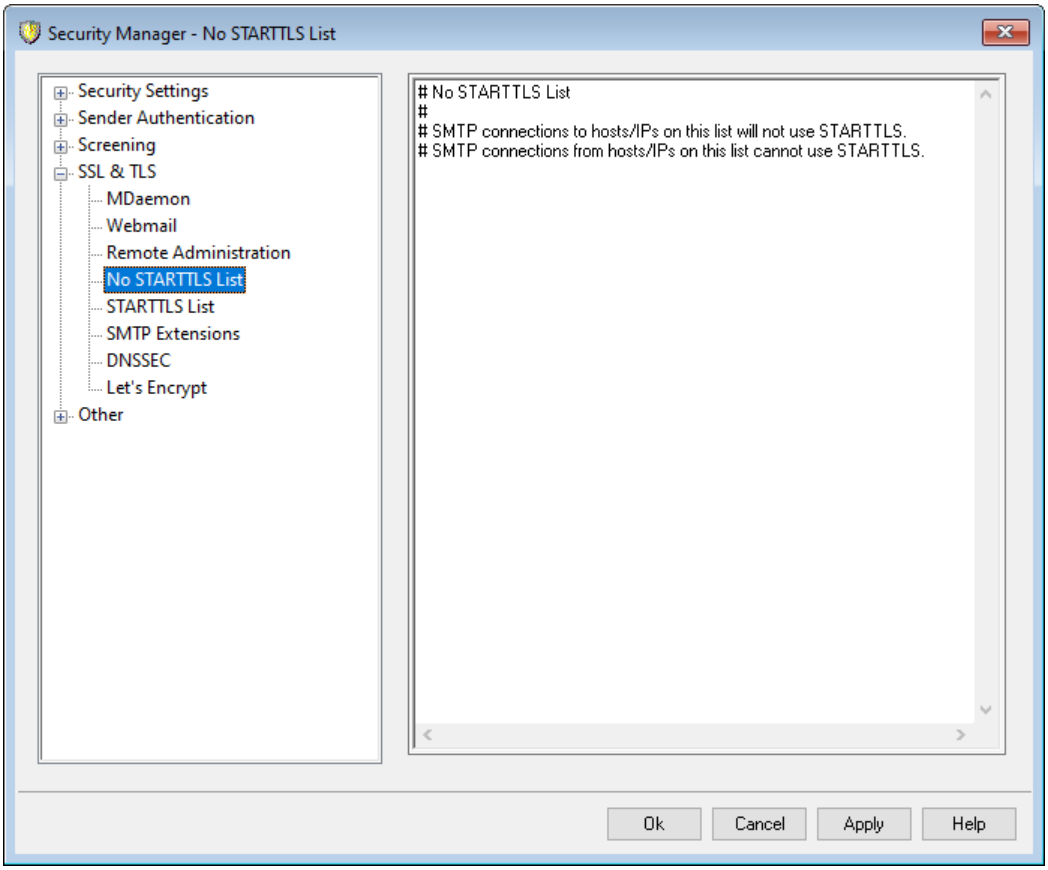
For more information on SSL and Certificates, see:

Running Remote Administration under IIS 352
SSL and Certificates 561
Creating and Using SSL Certificates 896

For more information on Remote Administration, see:

Remote Configuration 341
Remote Administration » Web Server 343
Web Access Defaults 782
Account Editor » Web 703

4.2.4.4 No STARTTLS List



Use this list to prevent the use of STARTTLS when sending or receiving mail to or from certain hosts or IP addresses.

The No STARTTLS List takes precedence over the STARTTLS Required List 575 and the *SMTP server requires STARTTLS on*

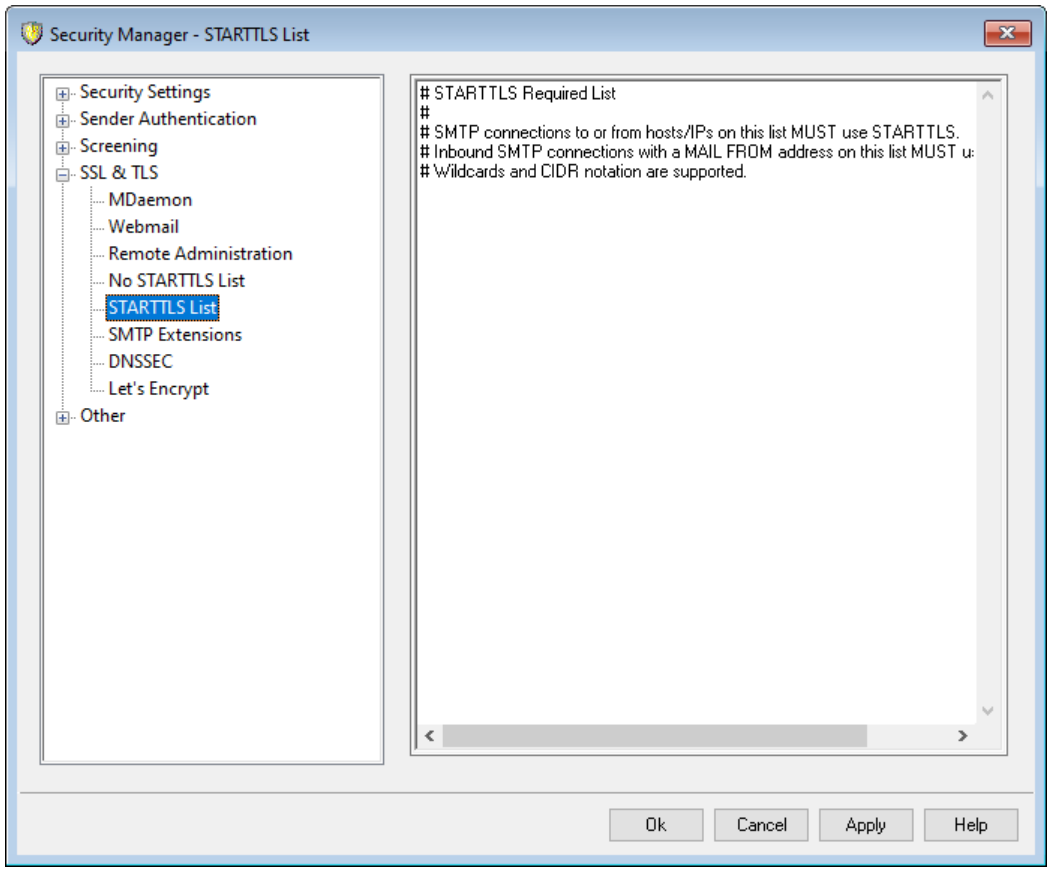
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MSA port 563 option.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

4.2.4.5 STARTTLS List



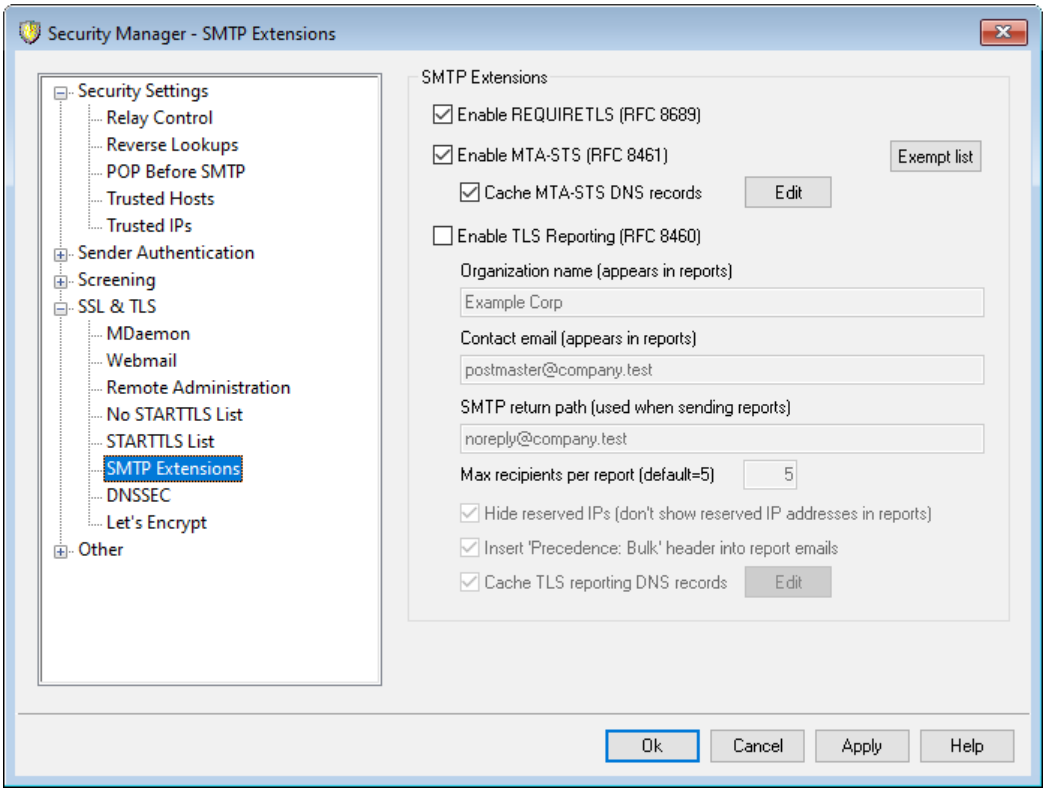
Use this screen to specify hosts, IP addresses, and MAIL FROM addresses that require the use of the STARTTLS extension in order to send or receive mail to or from your server.

The STARTTLS extension for SMTP is addressed in RFC-3207, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc3207.txt

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.4.6 SMTP Extensions



SMTP Extensions

Enable REQUIRETLS (RFC 8689)
RequireTLS allows you to flag messages that **must** be sent using TLS. If TLS is not possible (or if the parameters of the TLS certificate exchange are unacceptable) messages will be bounced rather than delivered insecurely. For a complete description of RequireTLS, see: RFC 8689: SMTP Require TLS Option.

RequireTLS is enabled by default, but the only messages that will be subject to the RequireTLS process are messages specifically flagged by a Content Filter rule using the new Content Filter action 633, "*Flag message for REQUIRETLS...*", or messages sent to `<local-part>+requiretls@domain.tld` (for example, `arvel+requiretls@mdaemon.com`). All other messages are treated as if the service is disabled. Several requirements must be met in order for a message to be sent using RequireTLS. If any of them fail, the message will bounce back rather than be sent in the clear. The requirements are:

- RequireTLS must be enabled.
- The message must be flagged as needing the RequireTLS treatment, via the Content Filter action or the "`<localpart>+requiretls@...`" address.
- DNS lookups for recipient MX hosts must use DNSSEC 579 (see below), or the MX must be validated by MTA-STS.
- The connection to the receiving host must use SSL (STARTTLS).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- The SSL certificate of the receiving host must match the MX host name and chain to a trusted CA.
- The receiving mail server must support REQUIRETLS and say so in the EHLO response.

RequireTLS requires DNSSEC lookups of MX record hosts, or the MX must be validated by MTA-STS. You can configure DNSSEC[579] by specifying criteria whereby lookups will request DNSSEC service. MDaemon's IP Cache[106] has an option for accepting DNSSEC assertions, and there are DNSSEC related instructions at the top of the MX Hosts file[99]. Finally, DNSSEC requires appropriately configured DNS servers, which is beyond the scope of this help file.

Enable MTA-STS (RFC 8461)
MTA-STS support is enabled by default and is described in RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate. To set up MTA-STS for your own domain, you will need an MTA-STS policy file that can be downloaded via HTTPS from the URL https://mta-sts.domain.tld/.well-known/mta-sts.txt, where "domain.tld" is your domain name. The policy text file should contain lines in the following format:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

Mode can be "none", "testing", or "enforce". There should be an "mx" line for each of your MX hostnames. A wildcard can be used for subdomains, such as "*.domain.tld". Max age is in seconds. Common values are 86400 (1 day) and 604800 (1 week).

Also needed is a DNS TXT record at _mta-sts.domain.tld, where "domain.tld" is your domain name. It must have a value in the format:

```
v=STSv1; id=20200206T010101;
```

The value for "id" must be changed every time the policy file is changed. It is common to use a timestamp for the id.

Exempt List
Use this list to make specific domains exempt from MTA-STS.

Cache MTA-STS DNS records
By default MDaemon caches MTA-STS DNS records. Click **Edit** to view or edit the current cache file.

Enable TLS Reporting (RFC 8460)
TLS Reporting is disabled by default and discussed in RFC 8460: SMTP TLS Reporting.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

TLS Reporting allows domains using MTA-STS to be notified about any failures to retrieve the MTA-STS policy or negotiate a secure channel using STARTTLS. When enabled, MDaemon will send a report daily to each STS-enabled domain that it has sent (or attempted to send) mail to that day. There are several options provided for configuring the information that your reports will contain.

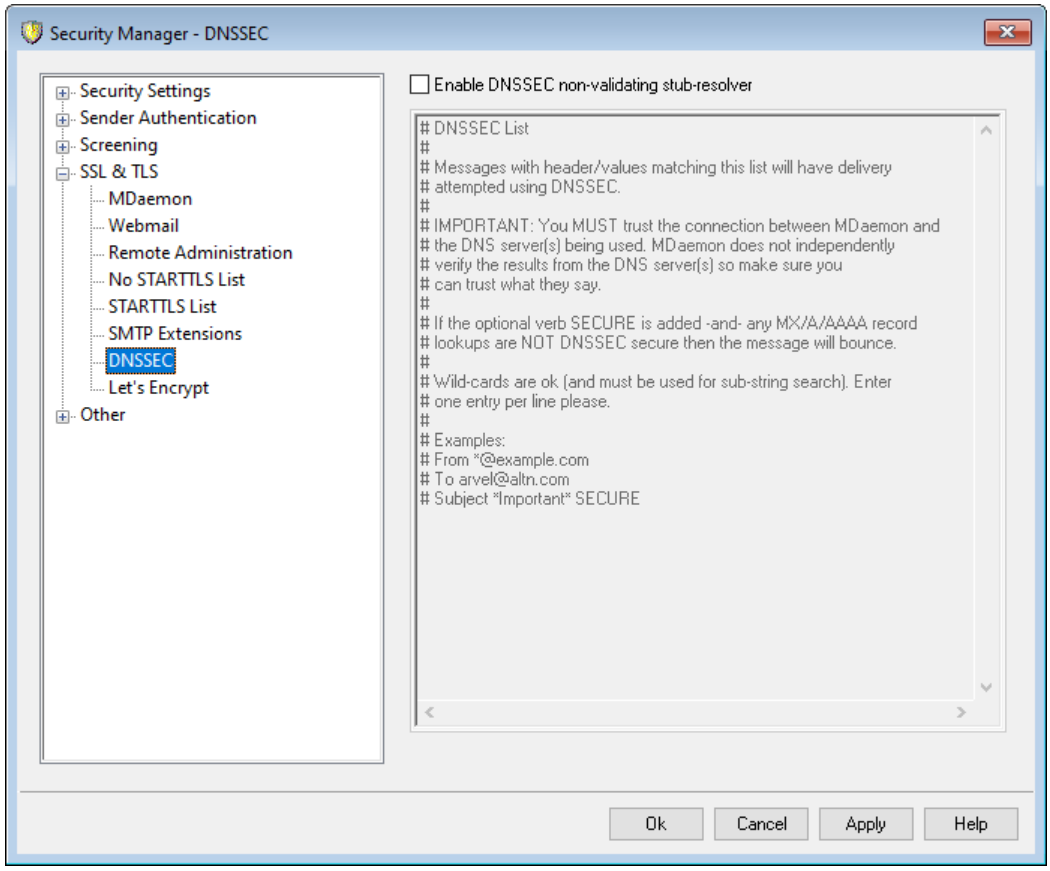
To set up TLS Reporting for your domain, enable DKIM signing 518, and create a DNS TXT record at `_smtp._tls.domain.tld`, where "domain.tld" is your domain name, with a value in the format:

```
v=TLSRPTv1; rua=mailto:mailbox@domain.tld
```

Where mailbox@domain.tld is the email address where you want reports for your domain to be sent.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.4.7 DNSSEC



The DNSSEC (DNS Security Extensions) option allows MDaemon to act as a Non-Validating Security-Aware Stub Resolver, which is defined in RFCs 4033 and 4035 as "an entity that sends DNS queries, receives DNS responses, and is capable of establishing an appropriately secured channel to a security-aware recursive name server that will provide these services on behalf of the security-aware stub resolver." What this means is that during MDaemon's DNS queries it can request DNSSEC service from your DNS servers, setting the AD (Authentic Data) bit in the queries and checking for it in the answers. This can provide an additional level of security during the DNS process for some messages, although not all, because DNSSEC is not yet supported by all DNS servers or for all top-level domains.

When enabled, DNSSEC service is only applied to messages that meet your selection criteria; it can be requested or required as broadly or narrowly as you choose. Simply designate any "`Header Value`" combinations you choose on this screen and MDaemon will request DNSSEC service for any messages matching that criteria whenever performing a DNS query. When the DNS results fail to include authenticated data then no negative consequences result; MDaemon simply falls back to normal DNS behavior. If, however, you wish to *require* DNSSEC for certain messages, add "SECURE" to the header/value combination (e.g. `To *@example.net SECURE`). For those messages, when the DNS results fail to include authenticated data, the message will be bounced back to the sender. **Note:** Because DNSSEC lookups take more time and resources, and because DNSSEC is not yet supported by all servers, MDaemon is not configured to

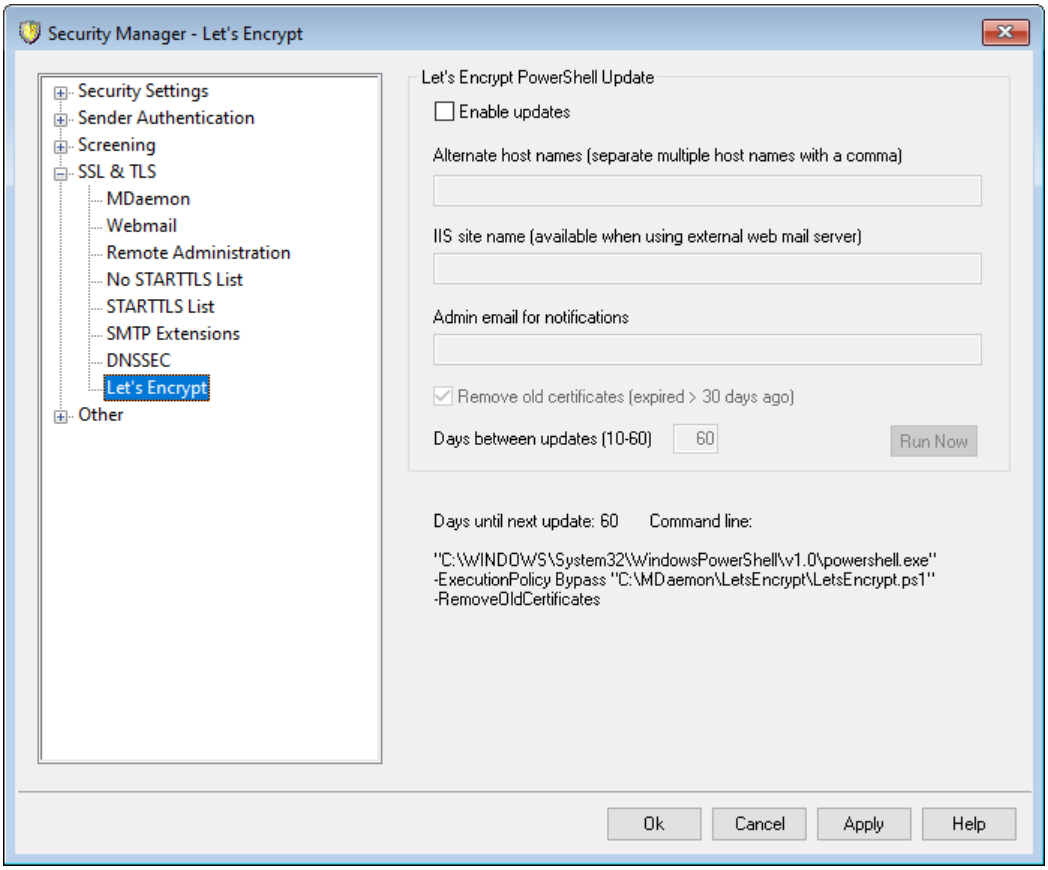
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

apply DNSSEC to every message delivery by default. However, if you wish to request DNSSEC for every message you can do so by included "`To *`" in your criteria.

Mail session logs will include a line at the top if DNSSEC service was used and "DNSSEC" will appear next to secure data in the logs.

Because MDaemon is a non-validating stub-resolver, it will request authenticated data from your DNS server but it has no way to independently verify that the data it gets from the server is secure. For this reason, to successfully use the DNSSEC option you must ensure that you trust your connection to your DNS server. For example, it runs on localhost or within a secure LAN or workplace.

4.2.4.8 Let's Encrypt



Using Let's Encrypt to Manage Your Certificate

To support SSL/TLS and HTTPS 561 for MDaemon 563, Webmail 566, and Remote Administration 570, you need an SSL/TLS Certificate. Certificates are small files issued

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

by a Certificate Authority (CA) that are used to verify to a client or browser that it is connected to its intended server, and that enable SSL/TLS/HTTPS to secure the connection to that server. Let's Encrypt is a CA that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

To support using Let's Encrypt's automated process to manage a certificate, this screen is provided to help you easily configure and run the PowerShell script included in the "MDaemon\LetsEncrypt" folder. Running the script will set up everything for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name 177 of the default domain 174 as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "MDaemon\Logs\" folder, called LetsEncrypt.log. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*.

Let's Encrypt requires PowerShell 5.1 and .Net Framework 4.7.2, which means that it will not work on Windows 2003. Also, Webmail 313 must be listening on port 80, and the script will not work if you have an SMTP host name 177 (i.e. FQDN) setup for your default domain that does not point to the MDaemon server.

Let's Encrypt PowerShell Updates

Enable updates
Click this checkbox if you wish to automatically create and update an SSL/TLS certification via the Let's Encrypt script. The certificate will be updated every 10-60 days according to your *Days between updates* setting below.

Alternate host names (separate multiple host names with a comma)
If you wish to setup alternate host names in the certificate, specify those host names here, separated by commas. You do not need to include the SMTP host name for the default domain in this list. For example, if your default domain were "example.com," configured with an SMTP host name of "mail.example.com," and you wanted to use an alternate host name of "imap.example.com," then you would only include "imap.example.com" as an alternate host name. If you do not wish to use any alternate host names then leave this option blank. **Note:** if you include alternate host names, an HTTP challenge from Let's Encrypt must be completed for each one to validate your server's control of that host name. If the challenges are not all completed then the process will fail.

IIS site name (available when using external web mail server)
If you are running Webmail via IIS, enter the IIS site name here. You must have Microsoft's Web Scripting tools installed in order for the certificate to be automatically set up in IIS.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Admin email for notifications
Specify an administrator email address here if you wish to be notified when an error occurs during a Let's Encrypt update.

Remove old certificates (expired > 30 days ago)
By default MDaemon will remove any old certificates that have been expired longer than 30 days. Uncheck this box if you do not wish to remove them automatically.

Days between updates (10-60)
Use this option to specify how often your certificate should be updated, from 10-60 days. The default setting is 60 days.

Run Now
Click this button to immediately run the script.

4.2.5 Other

4.2.5.1 Backscatter Protection - Overview

Backscatter

"Backscatter" refers to response messages that your users receive to emails that they never sent. This occurs when spam messages or messages sent by viruses contain a "Return-Path" address that is forged. Consequently, when one of these messages is rejected by the recipient's server, or if the recipient has an Autoresponder or "out of office"/vacation message associated with his account, the response message will then be directed to the forged address. This can lead to huge numbers of bogus Delivery Status Notifications (DSNs) or auto response messages ending up in your users' mailboxes. Further, spammers and virus authors frequently take advantage of this phenomenon and will sometimes use it to launch Denial of Service (DoS) attacks against email servers, causing a flood of invalid emails to arrive from servers located all over the world.

MDaemon's Solution

To combat backscatter, MDaemon contains a feature called Backscatter Protection (BP). BP can help to ensure that only legitimate Delivery Status Notifications and Autoresponders get delivered to your accounts, by using a private key hashing method to generate and insert a special time-sensitive code into the "Return-Path" address of your users' outgoing messages. Then, when one of these messages encounters a delivery problem and is bounced back, or when an auto-reply is received with a "`mailer-daemon@...`" or `NULL` reverse path, MDaemon will see the special code and know that it is a genuine automated reply to a message that was sent by one of your accounts. If the address doesn't contain the special code, or if the code is more than seven days old, it will be logged by MDaemon and can be rejected.

Backscatter Protection 583 is located under MDaemon's Security menu at: Security » Security Settings » Other » Backscatter Protection.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

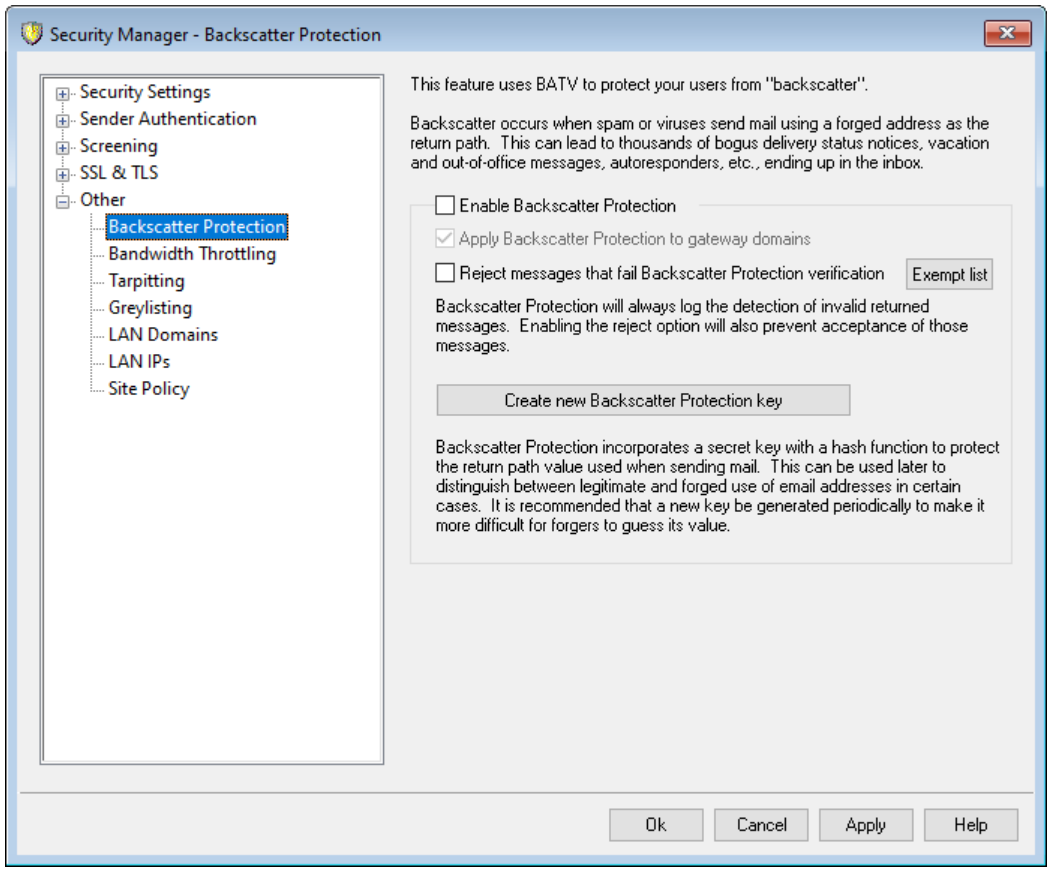
Backscatter Protection is an implementation of Bounce Address Tag Validation (BATV). For more on BATV, visit:

http://www.mipassoc.org/batv/

See:

Backscatter Protection 583

4.2.5.1.1 Backscatter Protection



Backscatter Protection

Enable Backscatter Protection
Click this checkbox if you wish to insert a special Backscatter Protection code into each outgoing message's "Return-Path" address. MDaemon will generate this special code by using the private key found in the `rsa.private` file located in MDaemon's `PEM\_batv\` folder, and the code will be valid for seven days. Any incoming DSNs or other auto-response messages (with a "`mailer-daemon@...`" or `NULL` reverse path) must have a valid, non-expired BP code or they will fail BP verification.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If you disable this option, MDaemon will not insert the special Backscatter Protection code into outgoing messages. It will, however, continue to check incoming DSNs and auto-response messages to ensure that any incoming message with a valid code is not rejected by mistake.

Apply Backscatter Protection to gateway domains
When Backscatter Protection is enabled, click this option if you also wish to apply it to domains for which MDaemon is acting as a gateway or backup server (see Gateway Manager 239).

Reject messages that fail Backscatter Protection verification
Click this checkbox if you wish to reject DSNs or other auto-response messages that fail BP verification. Messages with a "mailer-daemon@..." or NULL reverse path will fail if they do not contain the special code or if the code's seven day life-cycle has expired. Because of Backscatter Protection's solid reliability, there are no false positives or "gray areas" — a message is valid or it isn't. For this reason it is safe to configure MDaemon to reject invalid messages, as long as you ensure that all of your accounts' outgoing messages contain the special BP code. In all cases, however, the result of BP verification will be logged into the SMTP-in log file, even when you choose not to reject messages that fail verification. Incoming messages for gateways will not be rejected unless you have checked the *...apply Backscatter Protection to gateway domains* option above.

When you enable Backscatter Protection, you should wait about a week before setting it to reject invalid auto-response messages. This is because during that time you might still receive DSNs or auto-responses to messages that were sent out before BP was activated. If BP were configured to reject invalid message during that time then those legitimate response messages would be rejected by mistake. After a week it should be safe to start rejecting invalid messages. This same warning applies when you create a new BP key and choose to delete the old key immediately instead of allowing it to continue working for another seven days. (see the *Create new Backscatter Protection key* option below).

Exempt List
Click this button to open the Backscatter Protection exempt list. Use this list to designate any IP addresses or domains that you wish to exempt from Backscatter Protection.

Create new Backscatter Protection key
Click this button to generate a new Backscatter Protection key. This key is used by MDaemon to create and then verify the special BP codes that are inserted into messages. The key is located in a file called rsa.private in MDaemon's PEM_batv\ folder. When the new key is generated, a box will open to inform you that the old key will continue to work for seven more days unless you wish to delete it

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

immediately. In most cases you should click "**No**", electing to allow the key to work for seven more days. If you choose to delete the key immediately then that could cause some incoming messages to fail BP verification, since they would be responses to messages containing the special code generated by the old key.

If you have your email traffic split across multiple servers, you may need to share the key file with all of your other servers or Mail Transfer Agents (MTAs).

See:

Backscatter Protection - Overview 582

4.2.5.2 Bandwidth Throttling - Overview

The Bandwidth Throttling feature makes it possible for you to police the consumption of bandwidth used by MDaemon. You can control the rate at which sessions or services progress — you can set different rates for each of MDaemon's major services on a per-domain basis, including the Domains and Domain Gateways. You can also set limits on local connections by selecting "Local traffic" from a drop down box. This will allow you to create special bandwidth settings that will take effect if the connection is either from or to a local IP address or domain name.

Bandwidth Throttling can be applied on either a per-session or per-service basis. When using the per-session mode, each session will be independently throttled to the associated rate. Thus multiple sessions of the same service type occurring simultaneously could exceed a service's configured value. When configured to throttle bandwidth on a per-service basis, MDaemon will monitor the combined use of all sessions of the same service type and allocate equal fractions of the total bandwidth to each. Multiple sessions will then share the configured maximum bandwidth equally. This will allow you to set a limit on an entire service.

When extending Bandwidth Throttling to a Domain Gateway, it must be handled a bit differently than a normal domain since a Domain Gateway doesn't have a specific IP address associated with it. MDaemon must use the value passed in the RCPT command to determine whether or not an inbound SMTP session is bound for the gateway. If it is, then inbound SMTP bandwidth throttling will be applied. Due to the limitations of SMTP, if even one recipient of a multiple recipient message is destined for a Domain Gateway then the entire session will be throttled.

The Bandwidth Throttling system is calibrated in kilobytes per second (KB/s). A value of "0" means that no limit will be applied to the speed at which a session (or service) progresses, thus it will use the maximum amount of available bandwidth. A value of "10", for example, will force MDaemon to deliberately throttle back on the speed of transmission so as to remain at or slightly above 10 KB/s.

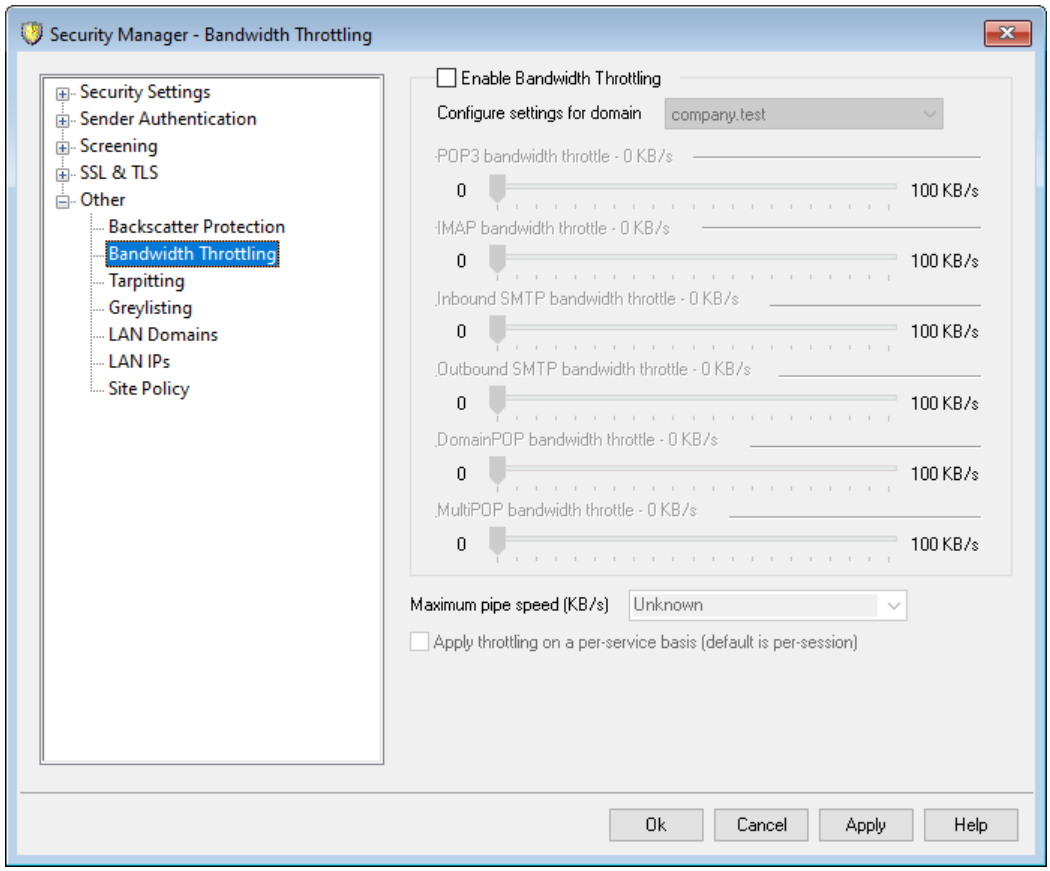
Bursts of activity at the beginning of a session can and will exceed the fixed limits. Throttling takes place and becomes more defined as the session progresses.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Bandwidth Throttling 586
LAN IPs 594

4.2.5.2.1 Bandwidth Throttling



Enable Bandwidth Throttling
Check this box if you wish to activate the Bandwidth Throttling feature.

Configure settings for domain
Choose a domain from the drop-down list box and then adjust the options corresponding to the various services to configure bandwidth throttling for the selected domain. A setting of "0" in any particular control means no bandwidth limit is set for that service type. In the drop-down list box, the bottom entry listed is *Local traffic*. Setting bandwidth throttling for this option will determine the limits placed on local traffic (i.e. sessions and services occurring on your local LAN rather than externally). The LAN IPs 594 screen can be used for listing IP addresses that should be treated as local.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Services

[Service type] bandwidth throttle – XX KB/s
After selecting a domain from the drop-down list box, adjust these controls to set bandwidth limitations for the selected domain. A setting of "0" means no bandwidth limit is applied to that particular service type. Setting a slider to any number other than "0" will limit the maximum bandwidth to that number of Kilobytes per second for the designated service.

Maximum pipe speed (KB/s)
From the drop-down list box, choose the maximum speed of your connection in Kilobytes per second.

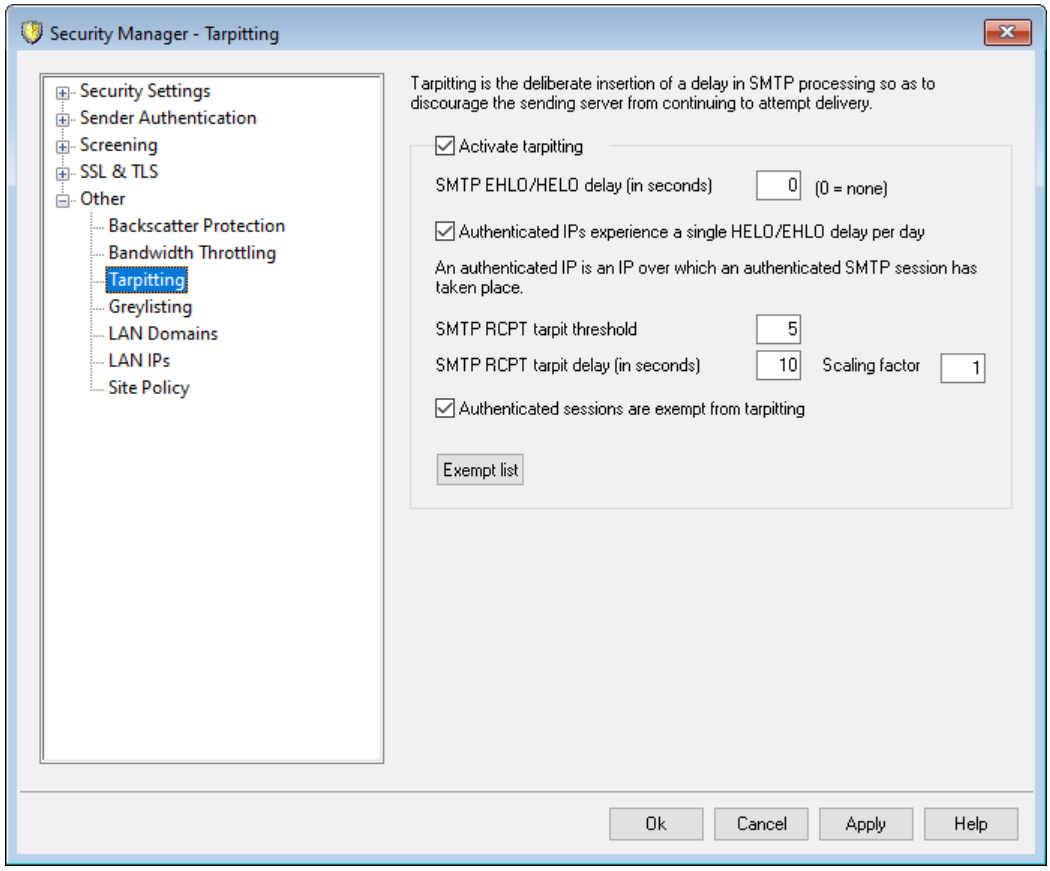
Apply throttling on a per-service basis (default is per-session)
Click this checkbox if you want to throttle bandwidth on a per-service basis rather than the default per-session basis. When throttling on a per-service basis, the service's designated amount of bandwidth will be divided equally among all active sessions of the given service type. Thus, the total amount of bandwidth used, for example, by multiple IMAP clients connecting at the same time could never exceed the designated amount regardless of how many clients were connected. If throttling on a per-*session* basis, then no single IMAP session could exceed the designated limit but the total of multiple simultaneous sessions could.

See:

Bandwidth Throttling - Overview 585

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.5.3 Tarpitting



Tarpitting is located under the Security menu at: Security » Security Settings » Other » Tarpitting.

Tarpitting makes it possible for you to deliberately slow down a connection once a specified number of RCPT commands have been received from a message's sender. This is to discourage spammers from trying to use your server to send unsolicited bulk email ("spam"). You can specify the number of RCPT commands allowed before tarpitting begins and the number of seconds to delay the connection each time a subsequent command is received from that host during the connection. The assumption behind this technique is that if takes spammers an inordinately long period of time to send each message then that will discourage them from trying to use your server to do so again in the future.

Activate tarpitting
Click this check box to activate MDaemon's tarpitting features.

SMTP EHLO/HELO delay (in seconds)
Use this option to delay the server response to EHLO/HELO SMTP commands. Delaying the responses by even as little as ten seconds can potentially save a significant amount of processing time by reducing the amount of spam received. Frequently spammers depend on rapid delivery of their messages and therefore do not wait long for a response to EHLO/HELO commands. With even a small delay,

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

spam tools will sometimes give up and move on rather than wait for a response. Connections on the MSA port (designated on the Ports 101 screen under Server Settings) are always exempt from this delay. The default setting for this option is "0", meaning EHLO/HELO will not be delayed.

Authenticated IPs experience a single EHLO/HELO delay per day
Click this check box if you wish to limit the EHLO/HELO delay to once per day for authenticated connections from a given IP address. The first message from that IP address will be delayed, but any subsequent messages sent from the same IP address will not.

SMTP RCPT tarpit threshold
Specify the number of SMTP RCPT commands that you wish to allow for a given host during a mail session before MDaemon will begin tarpitting that host. For example, if this number was set to 10 and a sending host attempted to send a message to 20 addresses (i.e. 20 RCPT commands), then MDaemon would allow the first 10 normally and then pause after each subsequent command for the number of seconds specified in the *SMTP RCPT tarpit delay* control below.

SMTP RCPT tarpit delay (in seconds)
Once the *SMTP RCPT tarpit threshold* is reached for a host, this is the number of seconds that MDaemon will pause after each subsequent RCPT command is received from that host during the mail session.

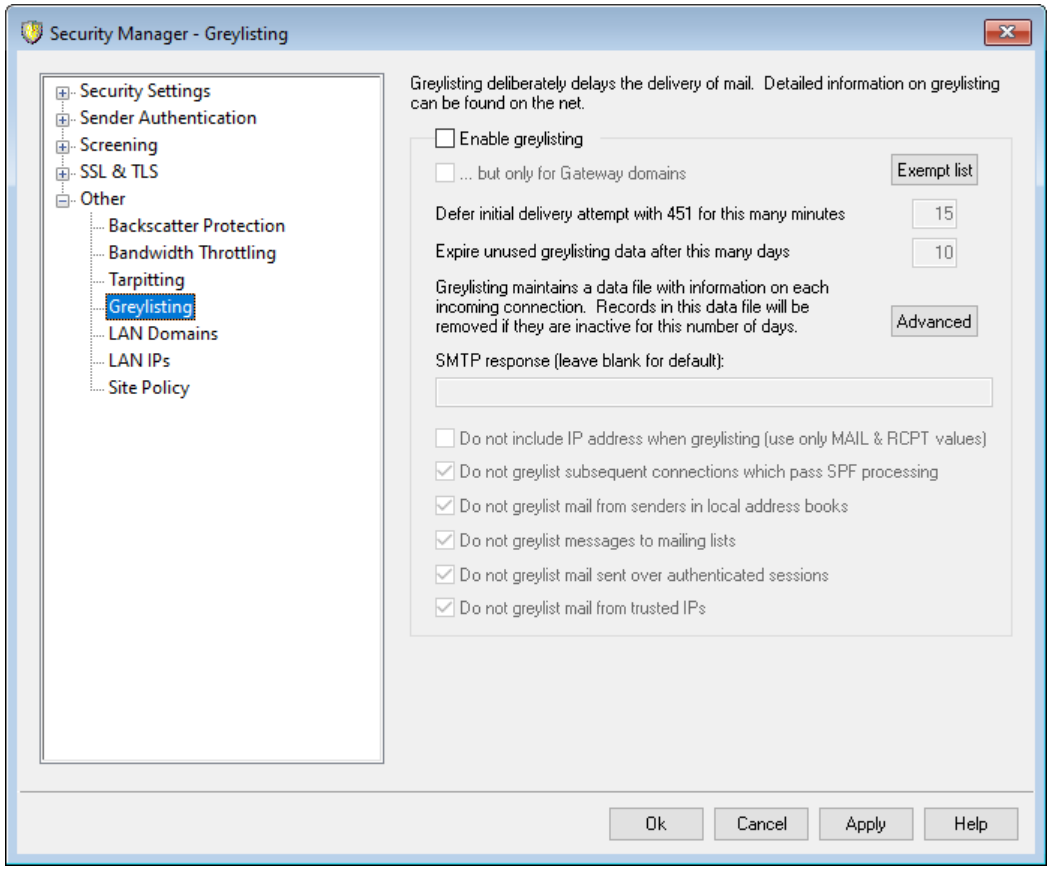
Scaling factor
This value is a multiplier by which the base tarpit delay will be increased over time. When the tarpit threshold is reached and the tarpit delay is applied to a session, each delay will be multiplied by this value to determine to length of the next delay in the session. For example, if the tarpit delay is set to 10 and the scaling factor is set to 1.5 then the first delay will be 10 seconds, the second will be 15 seconds, the third 22.5, then 33.75, and so on (i.e. 10 x 1.5 = 15, 15 x 1.5 = 22.5, etc.). The default Scaling factor is 1, meaning that the delay will not be increased.

Authenticated sessions are exempt from tarpitting
Click this checkbox if you want senders who authenticate their mail session to be exempt from Tarpitting.

Exempt list
Click this button to open the Dynamic Allow List 609, which is also used for Tarpitting. On it you can designate IP addresses that you wish to be exempt from tarpitting.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.5.4 Greylisting



Greylisting is located under the Security dialog at: Security » Security Settings » Other » Greylisting. Greylisting is a spam-fighting technique that exploits the fact that SMTP servers retry delivery of any message that receives a temporary (i.e. "try again later") error code. Using this technique, when a message arrives from a sender not on the allow list or otherwise previously unknown, its sender, recipient, and sending server's IP address will be logged and then the message will be refused by Greylisting during the SMTP session with a temporary error code. Furthermore, for a designated period of time (say, 15 minutes) any future delivery attempts will also be temporarily refused. Because "spammers" do not typically make further delivery attempts when a message is refused, greylisting can significantly help to reduce the amount of spam your users receive. But, even if the spammers should attempt to retry delivery at a later time, it is possible that by that time the spammers will have been identified and other spam-fighting options (such as DNS Block Lists 683) will successfully block them. It's important to note, however, that this technique can deliberately delay "good" email along with the "bad". But, the legitimate messages should still be delivered sometime later after the greylisting period has expired. It is also important to note that you have no way of knowing how long the sending servers will wait before making further delivery attempts. It is possible that purposely refusing a message with a temporary error code could cause it to be delayed by as little as just a few minutes or by as much as an entire day.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

There are several traditional problems and negative side-effects associated with greylisting, and the Greylisting screen contains a number of options designed to deal with them.

First, some sending domains use a pool of mail servers to send outbound mail. Since a different mail server could be used for each delivery attempt, each attempt would be treated as a new connection to the greylisting engine. This could multiply the length of time it would take to get past Greylisting because each of those attempts would be greylisted as if they were separate messages instead of retries of a previous message. By utilizing an SPF lookup option, this problem can be solved for sending domains who publish their SPF data. Furthermore, there is an option to ignore the IP of the sending mail server completely. Using this option lowers the efficiency of greylisting, but it does completely solve the server pool problem.

Second, greylisting traditionally entails a large database since each incoming connection must be tracked. MDaemon minimizes the need to track connections by placing the Greylisting feature nearly last in the SMTP processing sequence. This allows all of MDaemon's other options to refuse a message prior to reaching the greylisting stage. As a result, the size of the greylisting data file is greatly reduced, and since it is memory resident there is little practical performance impact.

Finally, several options are available to minimize the impact of greylisting on "good" messages. First, messages sent to mailing lists can be excluded. Next, Greylisting has its own exempt list on which you can designate IP addresses, senders, and recipients that you wish to be exempt from greylisting. Finally, Greylisting contains an option for using each account's address book as an exempt list. So, mail to a user from someone in that user's address book can be excluded from greylisting.

For more information about greylisting in general, visit Even Harris' site at:

http://projects.puremagic.com/greylisting/

Greylisting

Enable greylisting
Click this option to enable the Greylisting feature within MDaemon.

...but only for Gateway domains
Click this check box if you only wish to greylist messages destined for gateway domains.

Exempt list
This button opens the Greylisting exempt list on which you can designate senders, recipients, and IP addresses that will be exempt from greylisting.

Defer initial delivery attempt with 451 for this many minutes
Designate the number of minutes for which a delivery attempt will be greylisted after the initial attempt. During that period of time, any subsequent delivery attempts by the same server/sender/recipient combination (i.e. "greylisting triplet") will be refused with another temporary error code. After the greylist period has elapsed, no further greylisting delays will be implemented on that triplet unless its Greylisting database record expires.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Expire unused greylisting database records after this many days
After the initial greylisting period has elapsed for a given greylisting triplet, no further messages matching that triplet will be delayed by Greylisting. However, if no message matching that triplet is received for the number of days designated in this option, its Greylisting database record will expire. A subsequent attempt by that triplet will cause a new Greylisting record to be created it will have to go through the initial greylisting period again.

Advanced
Click this button to open the Greylisting database, which you can use to review or edit your greylisting triplets.

SMTP response (leave blank for default)
If you provide a custom string of text in this space then MDaemon will return the SMTP response, "`451 <your custom text>`" rather than the default "`451 Greylisting enabled, try again in X minutes.`" This is useful, for example, if you wish to provide a string that contains a URL to a description of greylisting.

Don't include IP address when greylisting (use only MAIL & RCPT values)
Click this check box if do not wish to use the sending server's IP address as one of the greylisting parameters. This will solve the potential problem that can be caused by server pools, but it will reduce Greylisting's efficiency.

Don't greylist subsequent connections which pass SPF processing
When using this option, if an incoming message matches a triplet's sender and recipient but not the sending server, but SPF processing determines that the sending server is a valid alternate to the one listed in the triplet, then the message will be treated as a subsequent delivery matching that triplet rather than a new connection requiring a new Greylisting record.

Don't greylist mail from senders in local address books
Click this option if you wish to exempt a message from greylisting when its sender is listed in the recipient's address book.

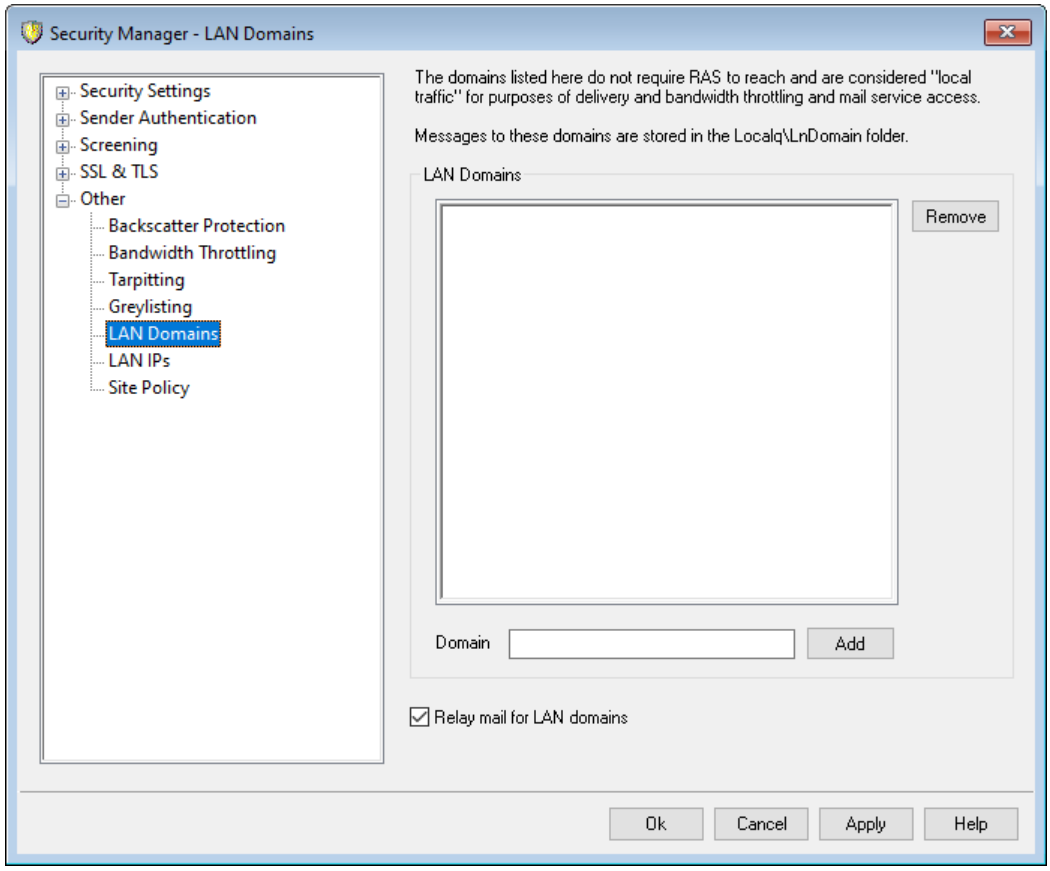
Don't greylist messages to mailing lists
Click this check box if you wish to exempt mailing list messages from greylisting.

Don't greylist mail sent over authenticated sessions
Use this option if you wish all messages coming in over an authenticated session to be exempt from greylisting.

Don't greylist mail from trusted IPs
Use this option if you wish all messages coming from trusted IP addresses to be exempt from greylisting.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.2.5.5 LAN Domains



LAN Domains

The domains listed here are considered by MDaemon to be part of your local LAN (local area network). Therefore, no dialup or Internet connection is required in order to deliver a message to one of them.

Domain
Enter a domain name and then click *Add* to add it to the list.

Add
After specifying a domain in the *Domain* option above, click this button to add it to the list.

Remove
Select a domain in the list and then click this button to remove it.

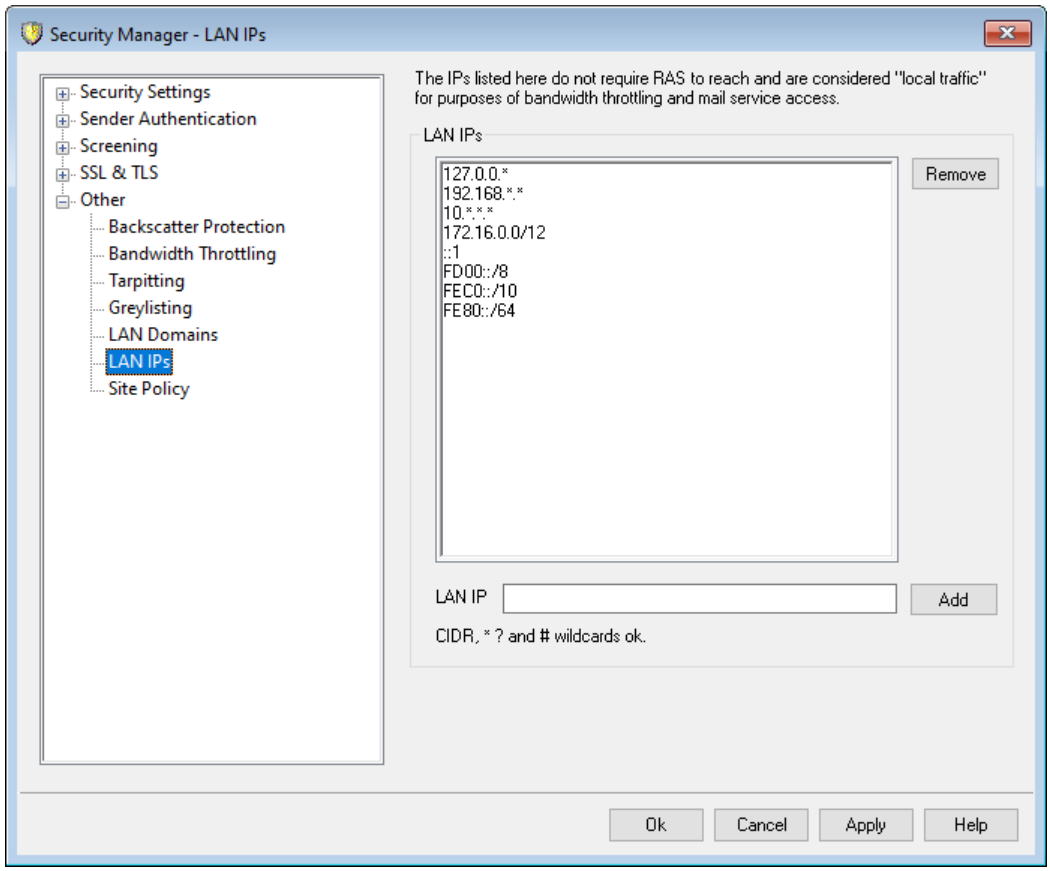
Relay mail for LAN domains
If this box is checked MDaemon will relay mail for these domains. This provides some measure of control over the traffic sent to and from these domains.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

LAN IPs 594

4.2.5.6 LAN IPs



LAN IPs

Similar to LAN Domains 593, this screen is used to list IP addresses that reside on your LAN (local area network). These IP addresses therefore do not require RAS or an Internet connection to reach them, and they are treated as local traffic for the purposes of bandwidth throttling. Further, there are various other security and spam prevention restrictions that they may be exempt from since they are local addresses.

Remove
Select an IP address from the list and then click this button to remove it.

LAN IP
Enter an IP address to add to the LAN IPs list and click *Add*. Wildcards like 127.0.*.* are permitted.

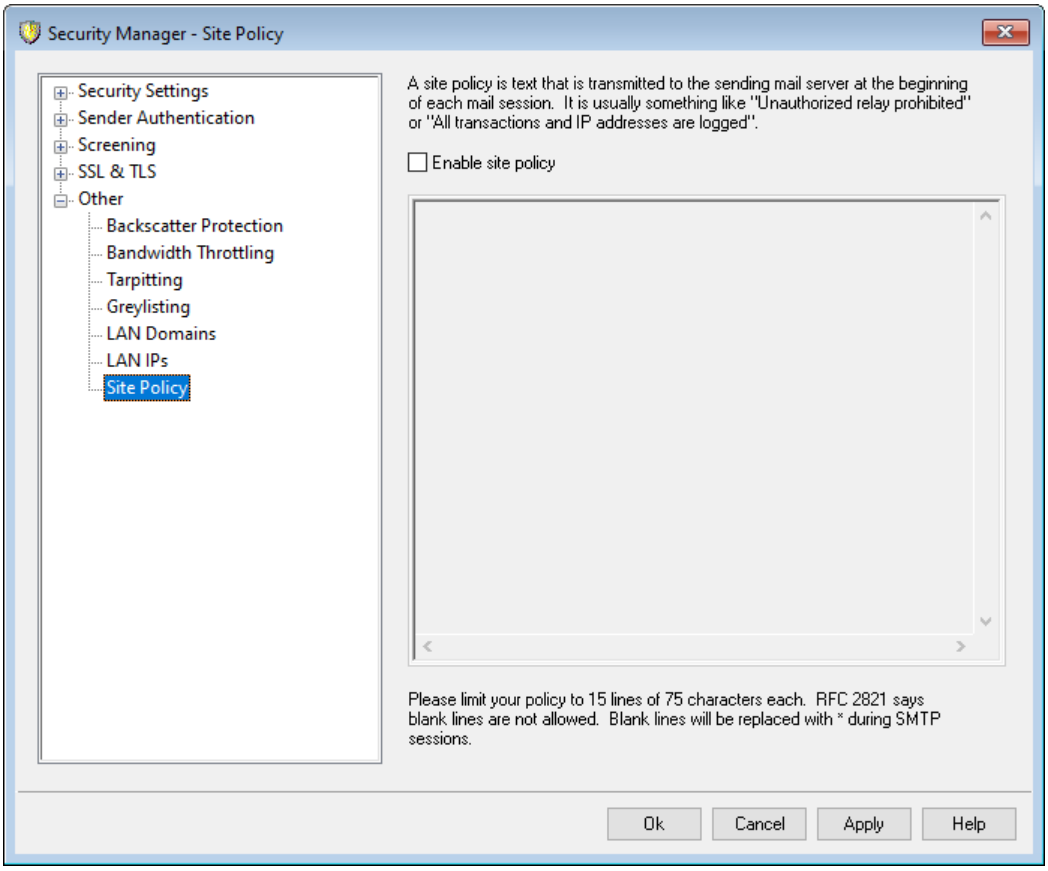
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add
After entering an IP Address into the *LAN IP* control, click this button to add it to the list.

See:

LAN Domains 593

4.2.5.7 Site Policy



Creating an SMTP Site Policy Statement
Use this dialog to specify a Site Policy statement for your server. The text is stored in the `policy.dat` file located in MDaemon's `\app\` subfolder and is transmitted to sending servers at the beginning of every SMTP mail session. An example of a common site policy is, "`This server does not relay`" or "`Unauthorized use prohibited.`" You do not need to prepend each line with "`220`" or "`220-`". MDaemon handles each line accordingly, either with or without these prepended codes.

A site usage policy with a statement regarding relaying of mail would look like this during the SMTP transaction:

```
220-MDaemon Technologies ESMTP MDaemon
```

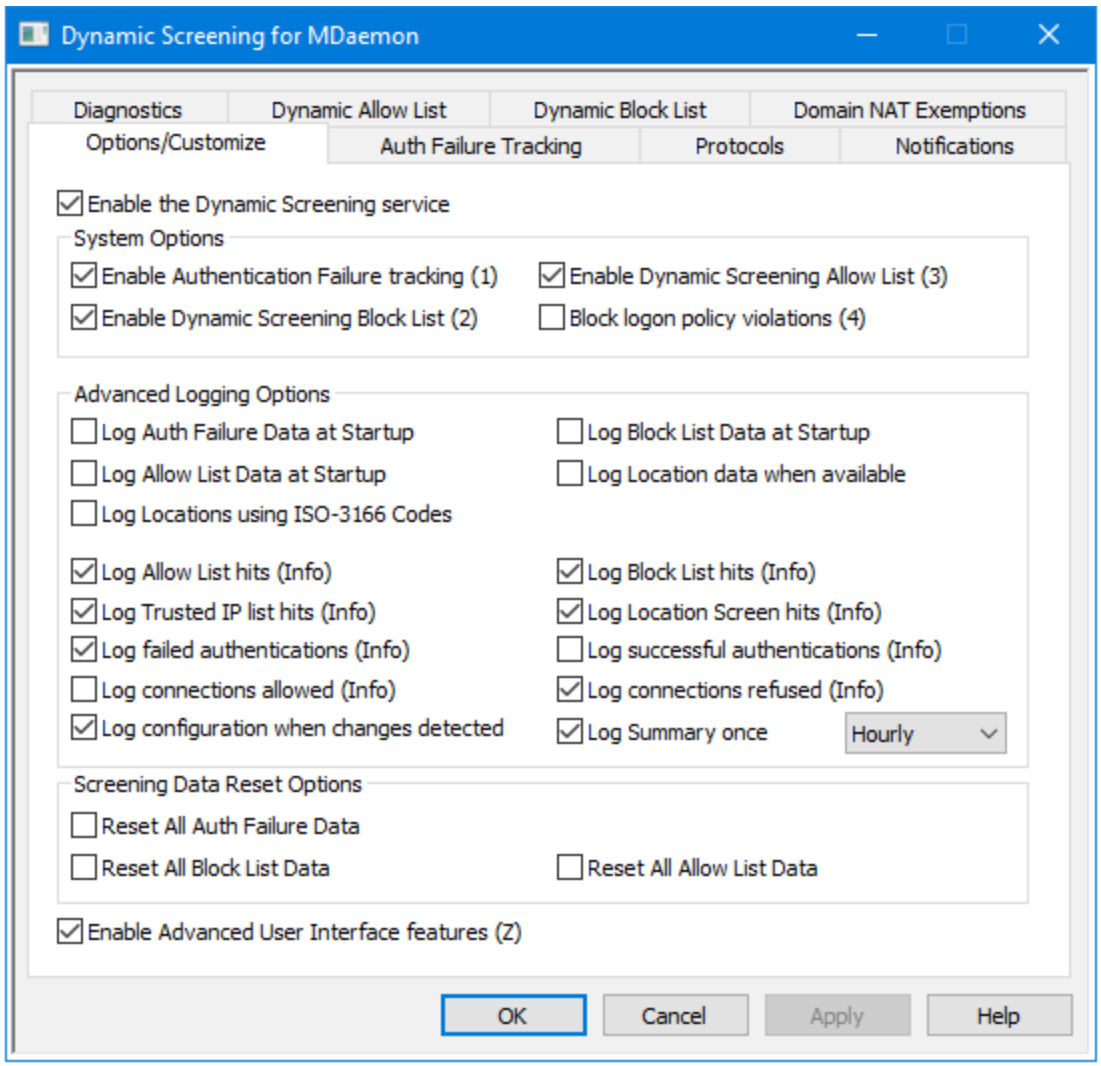
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
220-This site does relay unauthorized email.
220-If you are not an authorized user of our server
220-then you must not relay mail through this site.
220
HELO example.com...
```

The `POLICY.DAT` file must be comprised of printable ASCII text only and have no more than 512 characters per line; however it is highly recommended that you use no more than 75 characters per line. The maximum size of this file is 5000 bytes. MDaemon will not display files larger than 5000 bytes.

4.3 Dynamic Screening

4.3.1 Options/Customize



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Using Dynamic Screening, MDaemon can track the behavior of incoming connections to identify suspicious activity and then respond accordingly. You can block an IP address 600 (or range of addresses) from connecting when it fails authentication a specified number times within a specified amount of time. You can also freeze the accounts 600 attempting to authenticate when they fail too many times too quickly. Also, when an IP address is blocked or an account is frozen, it is not permanent. The connecting IP address will be blocked for the number of minutes, hours, or days that you specify, and frozen accounts can be "thawed" automatically after a specified amount of time, or manually by the admin.

Enable the Dynamic Screening service
Check this box to enable the Dynamic Screening service. You can also enable/disable the service under the Servers section in the navigation pane of MDaemon's main user interface.

System Options

Enable Authentication Failure Tracking
When this option is enabled, the Dynamic Screening service will track authentication failures for the protocols designated on the Protocols 603 tab and perform actions determined by the options on the Auth Failure Tracking 600 tab. This option is enabled by default.

Enable Dynamic Screening Block List
This option turns on the Dynamic Screening service's ability to block IP addresses and ranges. You can manage the block list from the Dynamic Block List 611 tab. The block list option is on by default.

Enable Dynamic Screening Allow List
This option turns on the Dynamic Screening service's Dynamic Allow List 609 feature, which you can use to exempt IP addresses and ranges, to exclude them from Dynamic Screening. The allow list is on by default.

Block Logon Policy Violations
By default MDaemon requires accounts to use their full email address when logging in instead of just the mailbox portion of their address (e.g. they must use "`user1@example.com`" instead of just "`user1`"). This is controlled by the "*Servers require full email address for authentication*" option on the Systems 480 page. When that option is on, you can also turn on this *Block Logon Policy Violations* option if you wish to block any IP address that attempts to logon without using the full email address. This option is off by default.

Advanced Logging Options

Log Auth Failure data at startup
This option enables the writing of all authentication failure data 600 that is currently stored by Dynamic Screening to the log file at startup. This is disabled by default.

Log Block List data at startup
Enables the writing of all Dynamic Block List 611 data that is currently stored to the log file at startup. This is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Log Allow List data at startup
Enables the writing of all Dynamic Allow List[609] data that is currently stored to the log file at startup. This is disabled by default.

Log Location data when available
Check this box if you wish to log each connection's location data, if it's available.

Log Locations using ISO-3166 Codes
Check this box if you wish to use ISO-3166 two-letter country codes when logging locations, instead using names.

Log all Allow List hits
This option adds an entry to the Dynamic Screening log each time an inbound connection is from an address that is on the Dynamic Allow List[609].

Log all Block List hits
This option adds an entry to the Dynamic Screening log each time an inbound connection is from an address that is on the Dynamic Block List[611].

Log all trusted IP list hits
This option adds an entry to the Dynamic Screening log each time an inbound connection is from a Trusted IP[506] address.

Log all Location Screen hits
This option adds an entry to the Dynamic Screening log each time an inbound connection is refused due to Location Screening[558].

Log all failed authentications
This option adds an entry to the Dynamic Screening log each time an inbound connection fails authentication.

Log all successful authentications
Enable this option if you wish to log every incoming authentication attempt that succeeds. This is disabled by default.

Log all connections allowed
Enable this option if you wish to create a log entry for every connection that passes Dynamic Screening and is allowed to proceed. This is disabled by default.

Log all connections refused
This option adds an entry to the log every time an incoming connection is refused by Dynamic Screening.

Log configuration when changes detected
This option adds entries to the log for all Dynamic Screening configurations when changes are detected from external sources (such as manually editing the INI file). Normal changes are logged at the Info level.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Log summary once [Daily | Hourly | Per minute]
Adds to the Dynamic Screening log a summary of Dynamic Screening stats once every day, hour, or minute. By default the summary is logged hourly.

Screening Data Reset Options

Reset all Auth Failure data
Click this checkbox if you wish to clear all Dynamic Screening authentication data. You must then click **Apply** or **OK** for the reset to occur.

Reset all Block List data
Click this checkbox if you wish to clear all Dynamic Screening Block List data. You must then click **Apply** or **OK** for the reset to occur.

Reset all Allow List data
Click this checkbox if you wish to clear all Dynamic Screening Allow List data. You must then click **Apply** or **OK** for the reset to occur.

Enable Advanced User Interface features

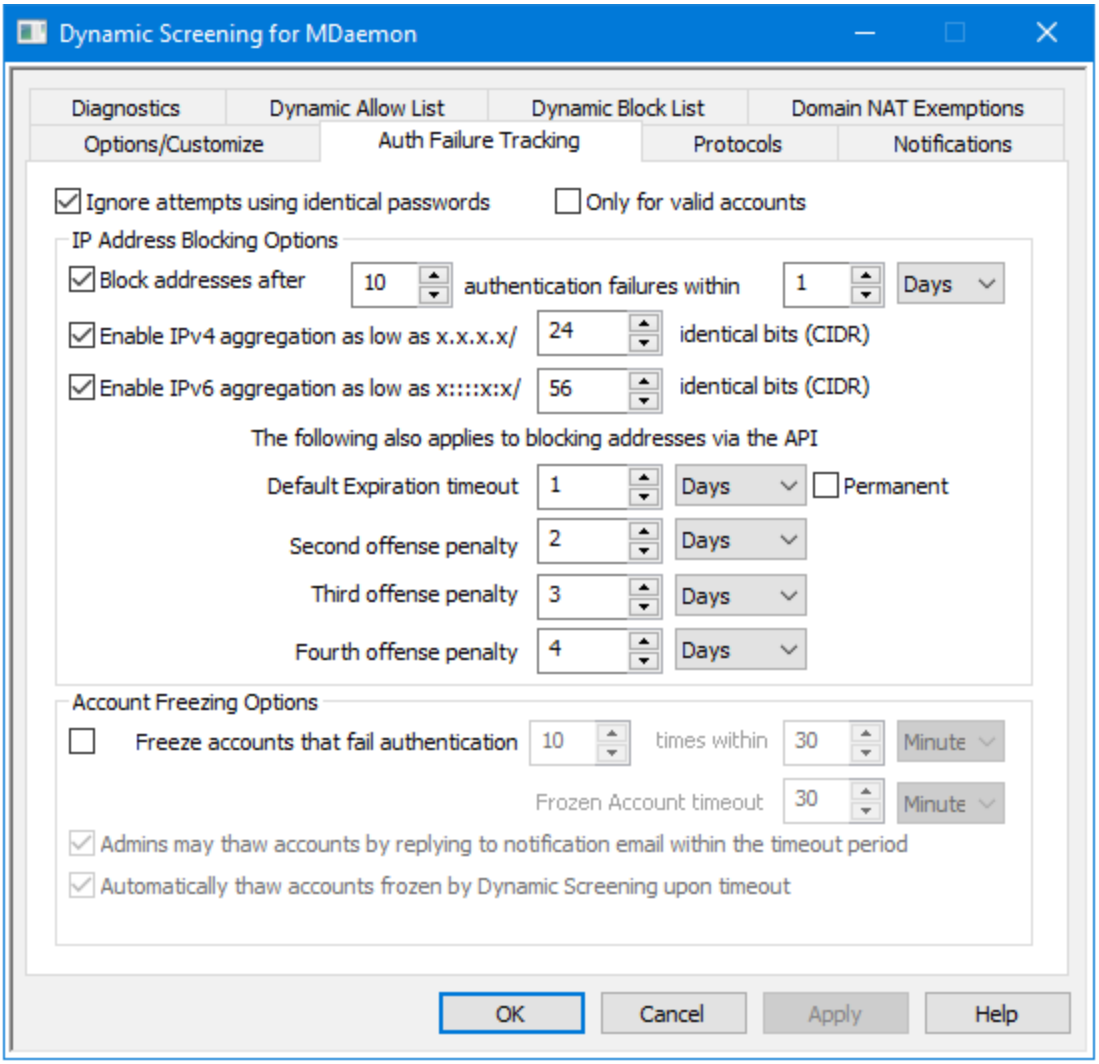
Check this box and then close/reopen the MDaemon configuration interface to add several advanced Dynamic Screening features. A Domain NAT Exemptions 613 screen is added to the Dynamic Screening dialog, from which you can designate specific IP address/domain combinations to exempt from Dynamic Screening blocking when valid users at that IP address fail password authentication. There are also several Dynamic Screening shortcuts added to the toolbar's Dynamic Screening section, and an option is added to the Dynamic Screening shortcut menu under the Servers section of the main interface that allows you to pause rather than disable the Dynamic Screening service, preventing clients from accessing the service while you manage its settings.

See:

Auth Failure Tracking 600
Dynamic Allow List 609
Dynamic Block List 611
Domain NAT Exemptions 613
Protocols 603
Location Screening 558
SMTP Screen 552

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.3.2 Auth Failure Tracking



Ignore authentication attempts using identical passwords

This option applies to the IP Address Blocking Options and to the Account Freezing Options below. By default, when an authentication attempt fails, subsequent authentication attempts will be ignored when using the same password. They will not count against the number of failures allowed before blocking the IP address or freezing the account. Multiple attempts using the same, incorrect password typically occur when, for example, the user's email password has changed or expired and their client is automatically attempting to log in using the old one.

Only for valid accounts

Activate this option if you only wish to ignore the duplicate password authentication attempts when they are attempting to sign in to a valid account. This means that if, for example, a user updates his password in one client but another client is still running with the old password, that old client's sign-in attempts will still be ignored, since it will have the correct sign-in name. A bot trying random sign-in names with a

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

similar password will not have that same benefit, and will be blocked as soon as it surpasses the auth failure threshold.

IP Address Blocking Options

Block addresses after [xx] authentication failures within [xx] [Minutes | Hours | Days]
Click this check box if you wish to block an IP address temporarily when it fails to authenticate to your server an excessive number of times in a limited time period. Specify the number of minutes, hours, or days and the number of failures allowed in that period.

Enable IPv4 aggregation as low as x.x.x.x/ [xx] identical bits (CIDR)
This option will block a range of IPv4 addresses when the authentication failures are coming from IP addresses near each other instead of from a single address.

Enable IPv6 aggregation as low as x::::x:x/ [xx] identical bits (CIDR)
This option will block a range of IPv6 addresses when the authentication failures are coming from IP addresses near each other instead of from a single address.

Multiple Offense Penalties

This is the amount of time that an IP address or IP address range will be blocked by the Dynamic Screening system when it fails the specified number of authentication attempts. By default the amount of time that the IP address is blocked increases with each subsequent offense. That is, by default if an IP address violates the authentication failure limit, it will be blocked for one day. Then if that same IP address subsequently violates the limit again, the *Second offense penalty* will be added to the *Default expiration timeout*, then the *Third offense penalty* will be added to the default timeout, and so on. The length of penalty maxes out with adding the *Fourth offense penalty*.

Default expiration timeout
This is the amount of time an IP address or IP address range will be blocked from connecting to MDaemon if it violates the authentication failure limit specified above. The default is 1 day.

Second offense penalty
This is the amount of time that will be added to the *Default expiration timeout* when an IP address or IP range is blocked by Dynamic Screening a second time.

Third offense penalty
This is the amount of time that will be added to the *Default expiration timeout* when an IP address or IP range is blocked by Dynamic Screening a third time.

Fourth offense penalty
This is the amount of time that will be added to the *Default expiration timeout* when an IP address or IP range is blocked by Dynamic Screening for the fourth time or any subsequent times.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Permanent
Click this box if you wish to permanently block the IP addresses that violate the authentication failure limit, rather than temporarily block them using the offense penalties specified above.

Account Freezing Options

Freeze accounts that fail authentication [xx] times within [xx] [Minutes | Hours | Days]
Check this box if you wish to switch an Account's Status 697 to FROZEN when it fails the specified number of authentication attempts in the designated amount of time. MDaemon will still accept incoming messages for a frozen account, but no one can sign in to the account to send or collect messages until it is "thawed" (i.e. the Account Status is switched back to ENABLED). This option is enabled by default.

Frozen account timeout
This is the amount of time that the account will remain frozen, if you have enabled the option below to *Automatically thaw accounts frozen by Dynamic Screening upon timeout*.

Admins may thaw accounts by replying to notification email within the timeout period
When an account is frozen by Dynamic Screening, by default an administrator will receive a notification email about it. The administrator can then "thaw" the account (i.e. switch its status back to "Enabled") by simply replying to the email, if this option is enabled. The option is enabled by default, and it requires the Frozen Account Reports options on the Notifications 604 tab to be enabled.

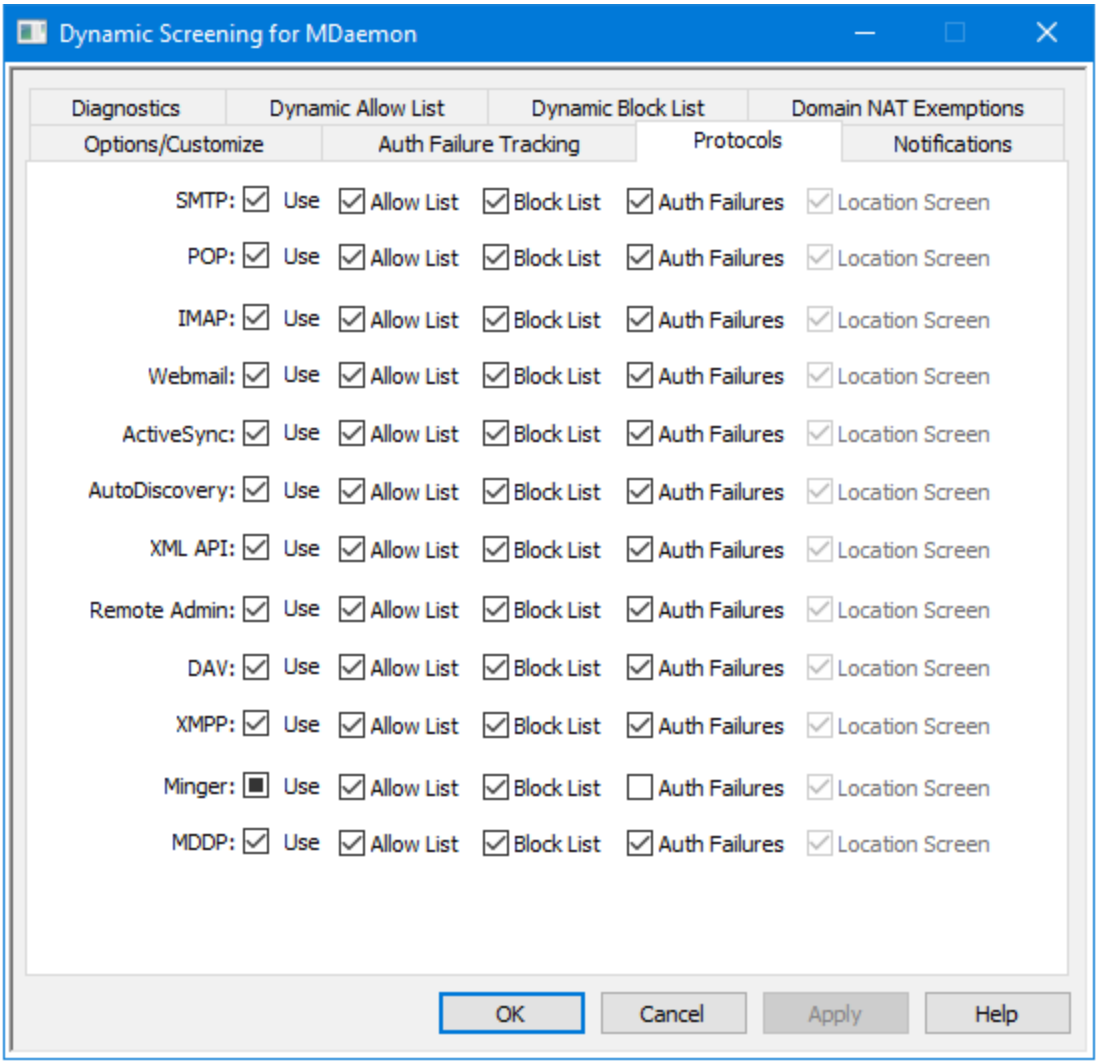
Automatically thaw accounts frozen by Dynamic Screening upon timeout
Check this box if you wish to automatically thaw frozen accounts when the *Frozen account timeout* period has elapsed. This option is disabled by default.

See:

Options/Customize 596
Dynamic Allow List 609
Dynamic Block List 611
Notifications 604

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.3.3 Protocols



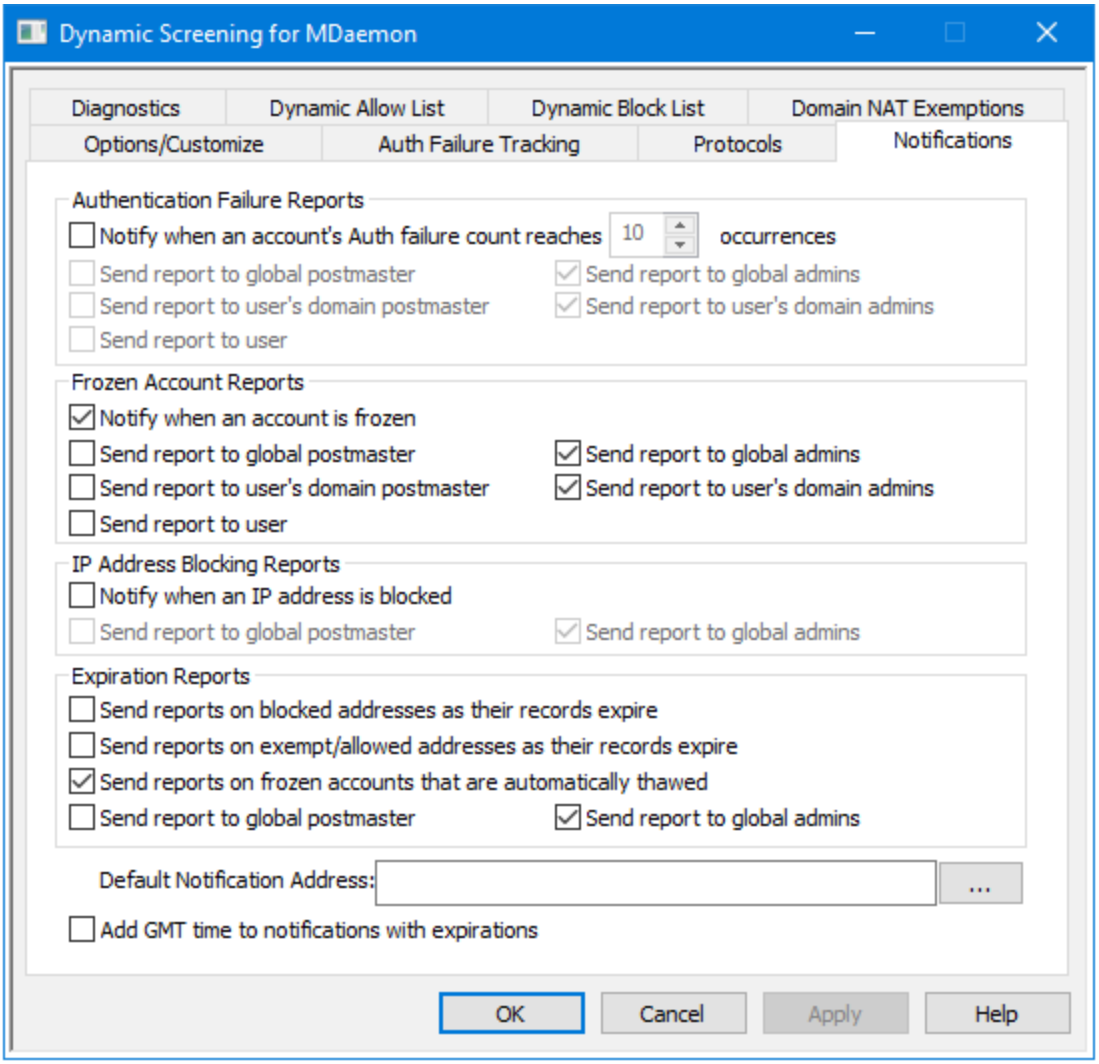
By default the Dynamic Screening service is applied to the following protocols: SMTP, POP, IMAP, Webmail, ActiveSync, AutoDiscovery 73, the Management API, MDaemon Remote Administration. WebDAV and CalDAV, XMPP, and Minger. Use the options on the Protocols tab to determine which protocols will have their inbound sessions checked against the Dynamic Allow List 609 and Dynamic Block List 611, which will have their authentication failures tracked 600, and to which Location Screening 558 will apply. By default all options on this dialog are enabled except for Minger Auth Failures.

See:

Auth Failure Tracking 600
Dynamic Allow List 609
Dynamic Block List 611

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.3.4 Notifications



Authentication Failure Reports

Notify when an account's Auth failure count reaches [xx] occurrences
This option causes MDaemon to send a notification message to a postmaster or other selected recipient when an account fails to authenticate a specified number of times in a row. If none of the selected addresses can be resolved, MDaemon will send the message to the *Default Notification Address* designated below. If no address has been specified, the message will not be sent. The option is enabled by default and set to 10 occurrences.

Send report to global postmaster
Check this box if you wish to send the reports to the global postmaster 818. This is enabled by default.

Send report to global admins
Check this box if you wish to send the reports to global administrators 741.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send report to user's domain postmaster
Check this box if you wish to send the reports to the domain postmaster[818] for the account that failed the authentication attempts.

Send report to user's domain admins
Check this box if you wish to send the reports to the domain administrators[741] for the account that failed the authentication attempts.

Send report to user
Check this box if you wish to send a failure report to the user whose account failed to authenticate.

Frozen Accounts Report

Notify when an account is frozen
This option causes MDaemon to send a notification message to a postmaster or other selected recipient when an account is frozen for too many authentication failures[600]. If none of the selected addresses can be resolved, MDaemon will send the message to the Default Notification Address designated below. If no address has been specified, the message will not be sent. The option is enabled by default.

Send report to global postmaster
Check this box if you wish to send the reports to the global postmaster[818]. This is enabled by default.

Send report to global admins
Check this box if you wish to send the reports to the global administrators[741].

Send report to user's domain postmaster
Check this box if you wish to send the reports to the domain postmaster[818] for the account that is frozen.

Send report to user's domain admins
Check this box if you wish to send the reports to the domain administrators[741] for the account that is frozen.

Send report to user
Check this box if you wish to send a report to the account that was frozen.

IP Address Blocking Reports

Notify when an IP address is blocked
This option causes MDaemon to send a notification message to a postmaster or other selected recipient any time an account is blocked by the Dynamic Screening system. If none of the selected addresses can be resolved, MDaemon will send the message to the Default Notification Address designated below. If no address has been specified, the message will not be sent. The option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send report to global postmaster
Check this box if you wish to send the reports to the global postmaster[818]. This is enabled by default.

Send report to global admins
Check this box if you wish to send the reports to the global administrators[741].

Expiration Reports

Send reports on blocked addresses as their records expire
This options sends a report to the designated addresses whenever a blocked IP address expires from the Dynamic Block List[611]. It is enabled by default.

Send reports on exempt/allowed addresses as their records expire
This options sends a report to the designated addresses whenever an allowed address expires from the Dynamic Allow List[609]. It is enabled by default.

Send reports on frozen accounts that are automatically thawed
This options sends a report to the designated addresses whenever a frozen account is automatically thawed[600] after the *Frozen account timeout* period has elapsed. It is enabled by default.

Send report to global postmaster
Check this box if you wish to send the reports to the global postmaster[818]. This is enabled by default.

Send report to global admins
Check this box if you wish to send the reports to the global administrators[741].

Default Notification Address
This is the address to which notification reports will be sent when no other addresses are specified or when none of the specified addresses can be resolved. If no address can be resolved and no *Default Notification Address* is designated, then no report will be sent.

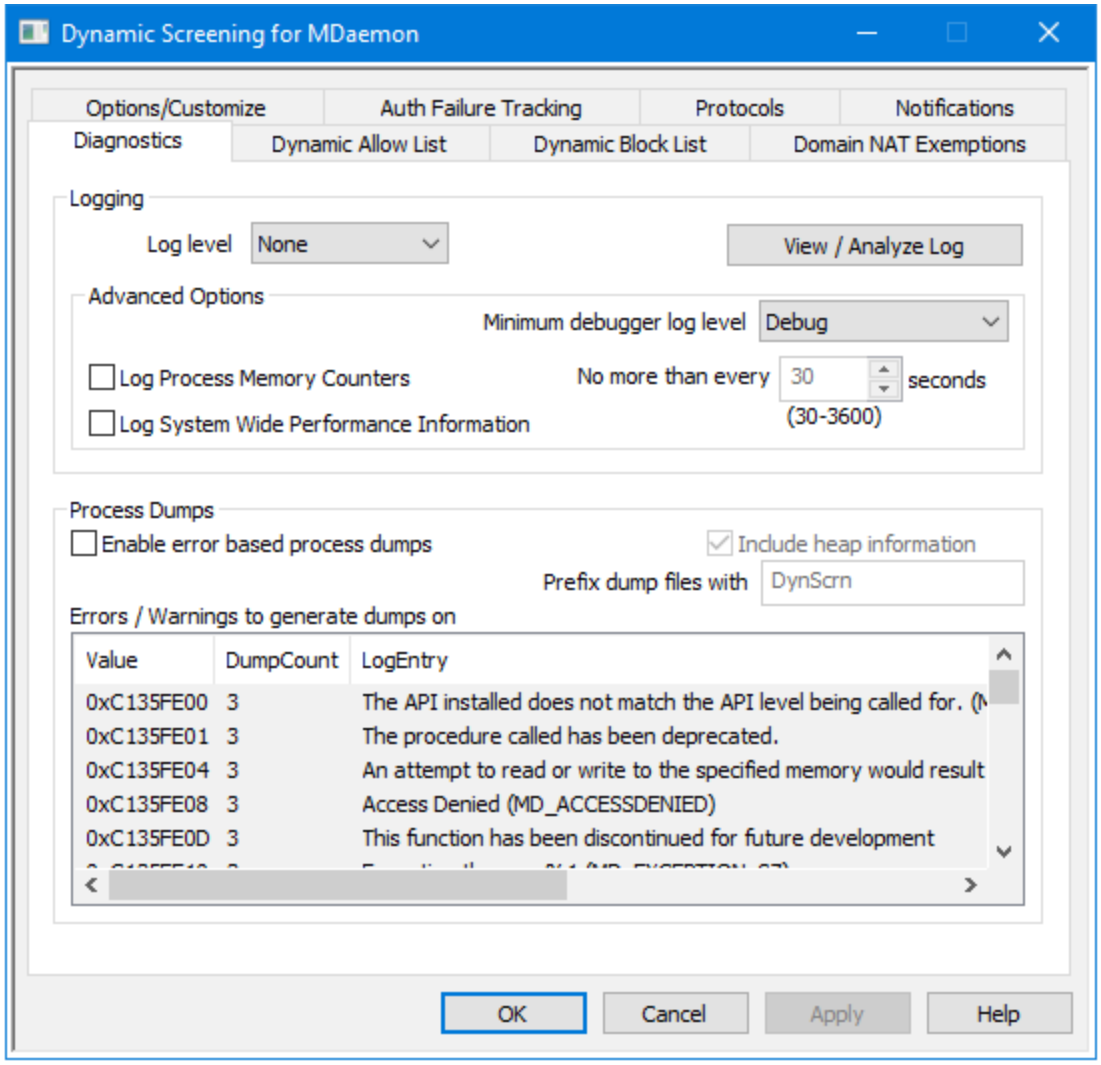
Add GMT time to notifications with expirations
By default when notification reports are sent that include an expiration time, the time listed is local server time. Enable this option if you also wish to include GMT time. This is useful when your email administrators are located in other timezones.

See:

Options/Customize[596]
Auth Failure Trackin[600]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.3.5 Diagnostics



This screen contains advanced options that in most cases will not need to be used unless you are attempting to diagnose a problem with Dynamic Screening or are dealing with technical support.

Logging

Log level
Six levels of logging are supported, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem, or when the administrator wants detailed information.

Info Moderate logging. Logs general operations without details. This is

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

View/Analyze Log
Click this button to open the MDaemon Advanced System Log Viewer. By default the logs are stored in: "..\MDaemon\Logs\"

Advanced Options

Minimum debugger log level
This is the minimum level of logging to emit to the debugger. The available log levels are the same as those outlined above.

Log process memory counters
Check this box to log process-specific Memory, Handle, and Thread information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

Log system wide performance information
Check this box if you with to log system-wide performance information to the log file. This is useful for finding potential leads and resource allocation issues. Log entries will only be emitted if the data has changed since the last time it was logged.

No more than every [xx] seconds
Use this option to set the limit on how often the process and performance information will be logged.

Process Dumps

Enable error based process dumps
Enable this option if you want to generate process dumps whenever a specific warning or error occurs that you have designated below.

Include heap information in dumps
By default, heap information is included in the process dumps. Clear this checkbox if you do not wish to include it.

Prefix dump files with
Process dump filenames will begin with this text.

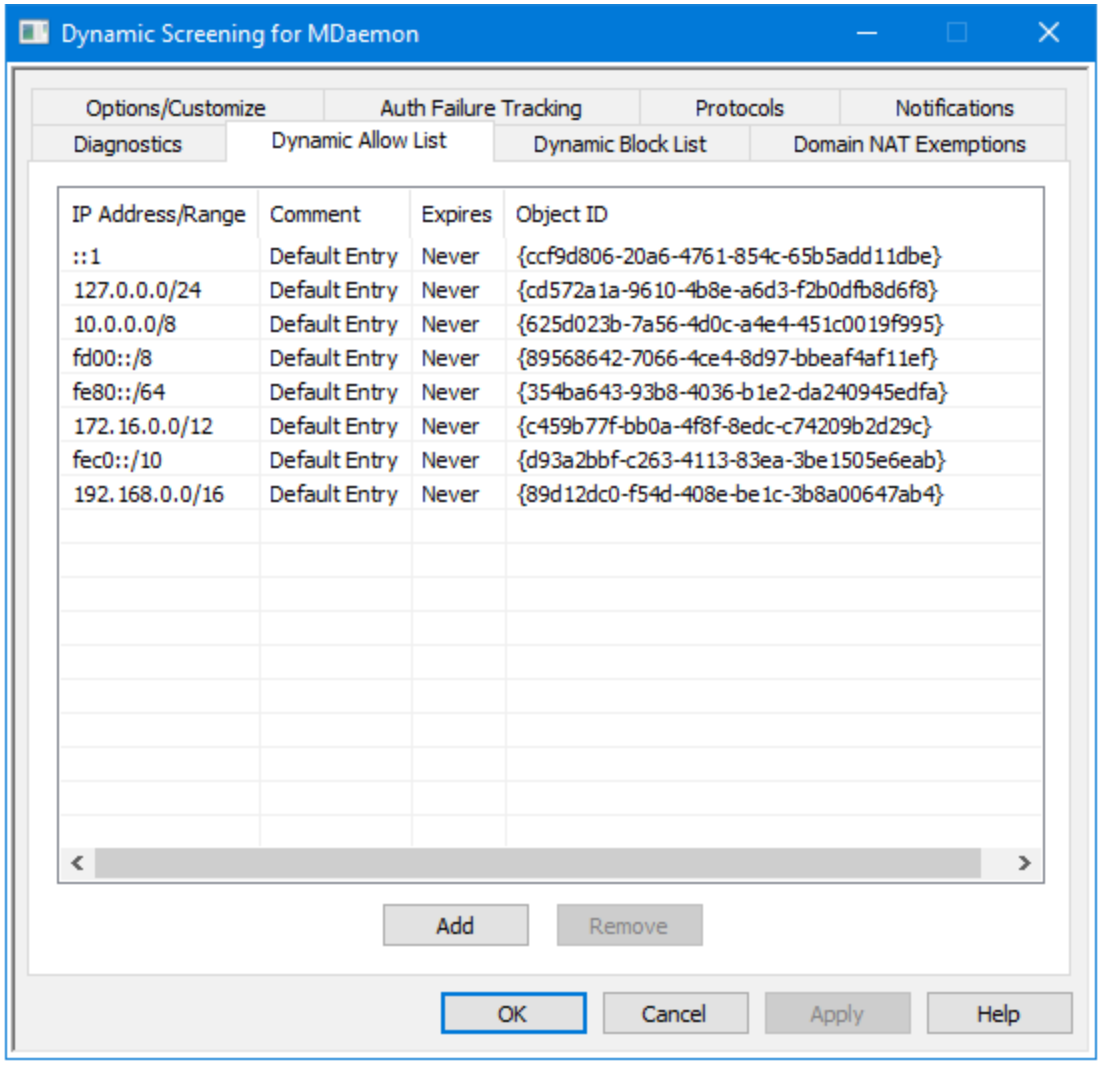
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Errors/Warnings to generate dumps on
Right-click this area and use the *Add/Edit/Delete Entry...* options to manage the list of errors or warnings that will trigger process dumps. For each entry you can specify the number of process dumps allowed before it will be deactivated.

See:

Dynamic Screening » Options/Customize 596

4.3.6 Dynamic Allow List



The Dynamic Allow List contains the list of IP addresses or address ranges that will be exempt from blocking by the Dynamic Screening service when they attempt to connect to MDaemon. Addresses can be added to the Dynamic Allow List by clicking the **Add** button. Each entry contains the IP address or range, the date and time that the entry will expire (or "Never," if it won't expire), any comment that you wish to make about

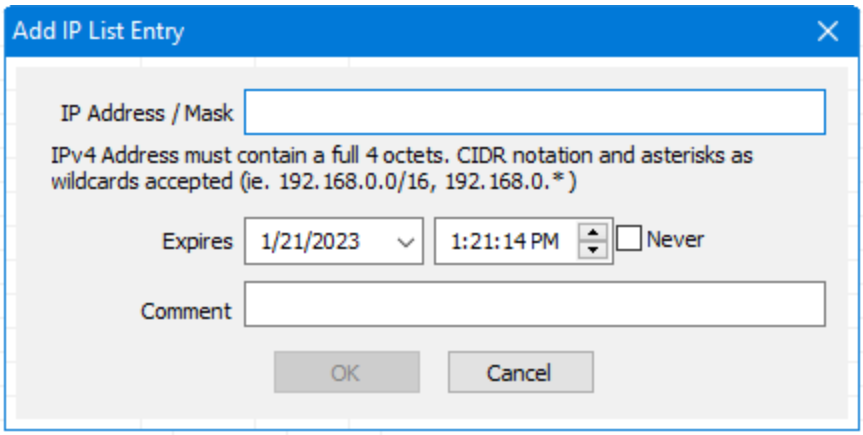
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the entry, and an Object ID. The Dynamic Allow List is also used by the SMTP Screen 552, Location Screening 558, and Tarpitting 588.

Adding an IP Address or Range to the Dynamic Allow List

To add an entry to the list:

1. Click **Add**. This opens the Add IP List Entry dialog.



2. Enter the IP address or IP address range.
3. Choose the date and time when you want the entry to expire, or click **Never**.
4. Enter a comment for the entry (optional).
5. Click **OK**.

Removing an Entry from the List

To remove one or more entries from the list:

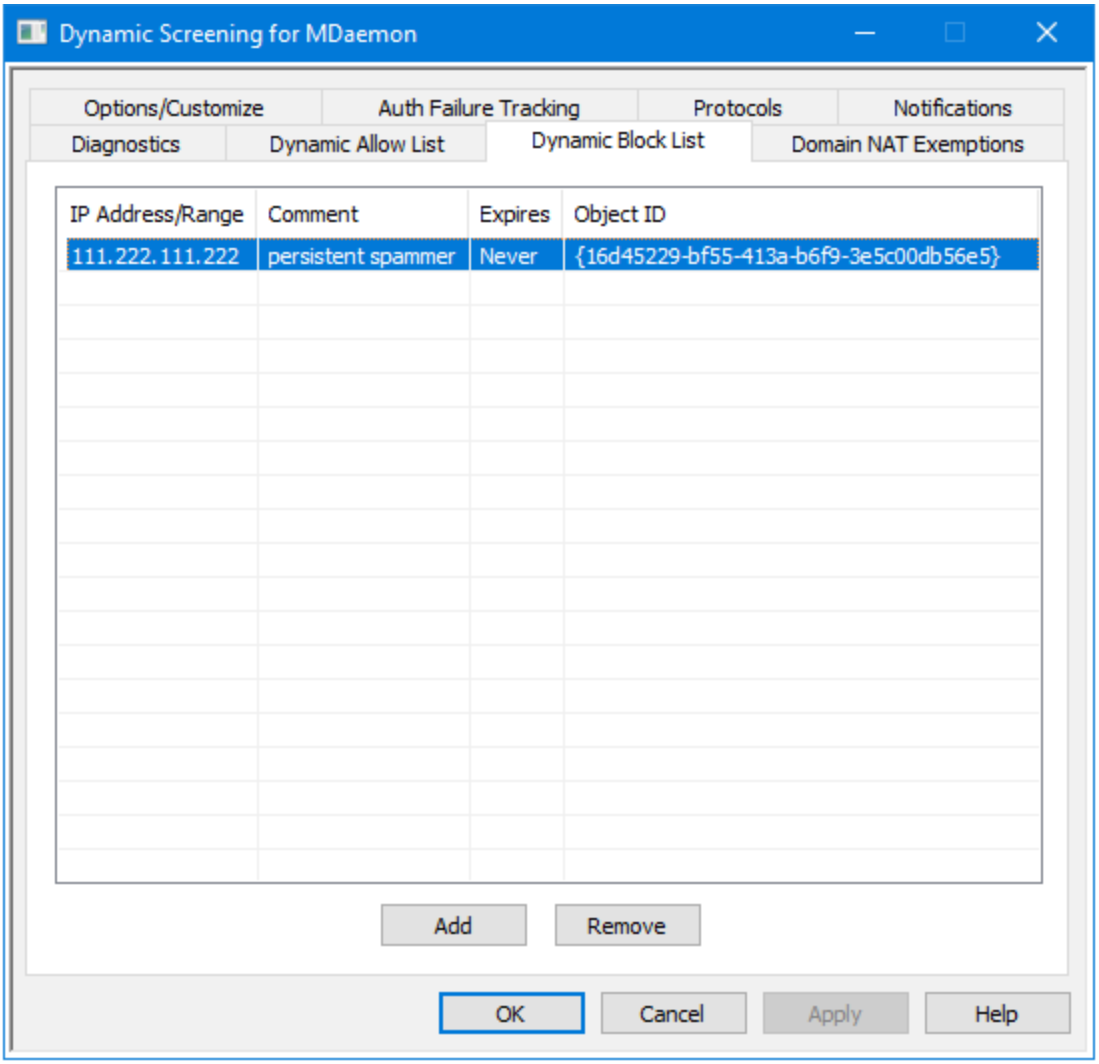
1. Select the entry or entries that you wish to remove from the list (Ctrl+click to select multiple entries).
2. Click **Remove**.

See:

Options/Customize 596
Auth Failure Tracking 600
Dynamic Block List 611
Protocols 603

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

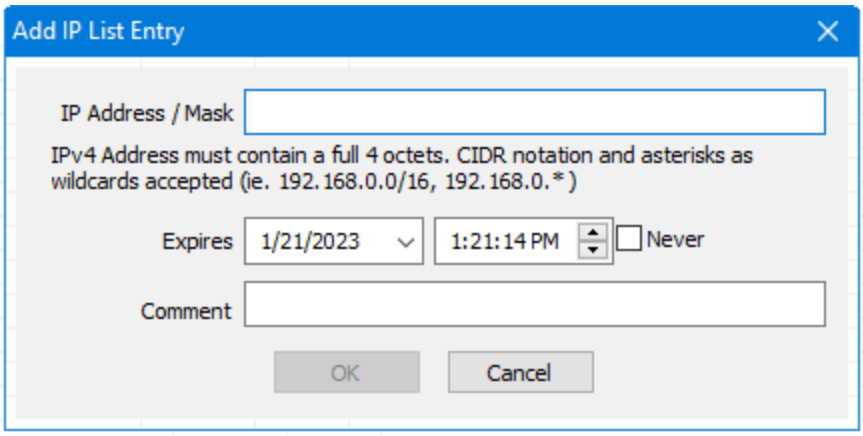
4.3.7 Dynamic Block List



The Dynamic Block List contains the list of IP addresses or address ranges that will be blocked by the Dynamic Screening service when they attempt to connect to MDaemon. Addresses can be added automatically by the Auth Failure Tracking 600 and SMTP Screen 552 options, and added manually by clicking the **Add** button. Each entry contains the IP address or range, the date and time that the entry will expire (or "Never," if it won't expire), any comment that you wish to make about the entry, and an Object ID.

1. Click **Add**. This opens the Add IP List Entry dialog.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



2. Enter the IP address or IP address range.
3. Choose the date and time when you want the entry to expire, or click **Never**.
4. Enter a comment for the entry (optional).
5. Click **OK**.

Removing an Entry from the List

To remove one or more entries from the list:

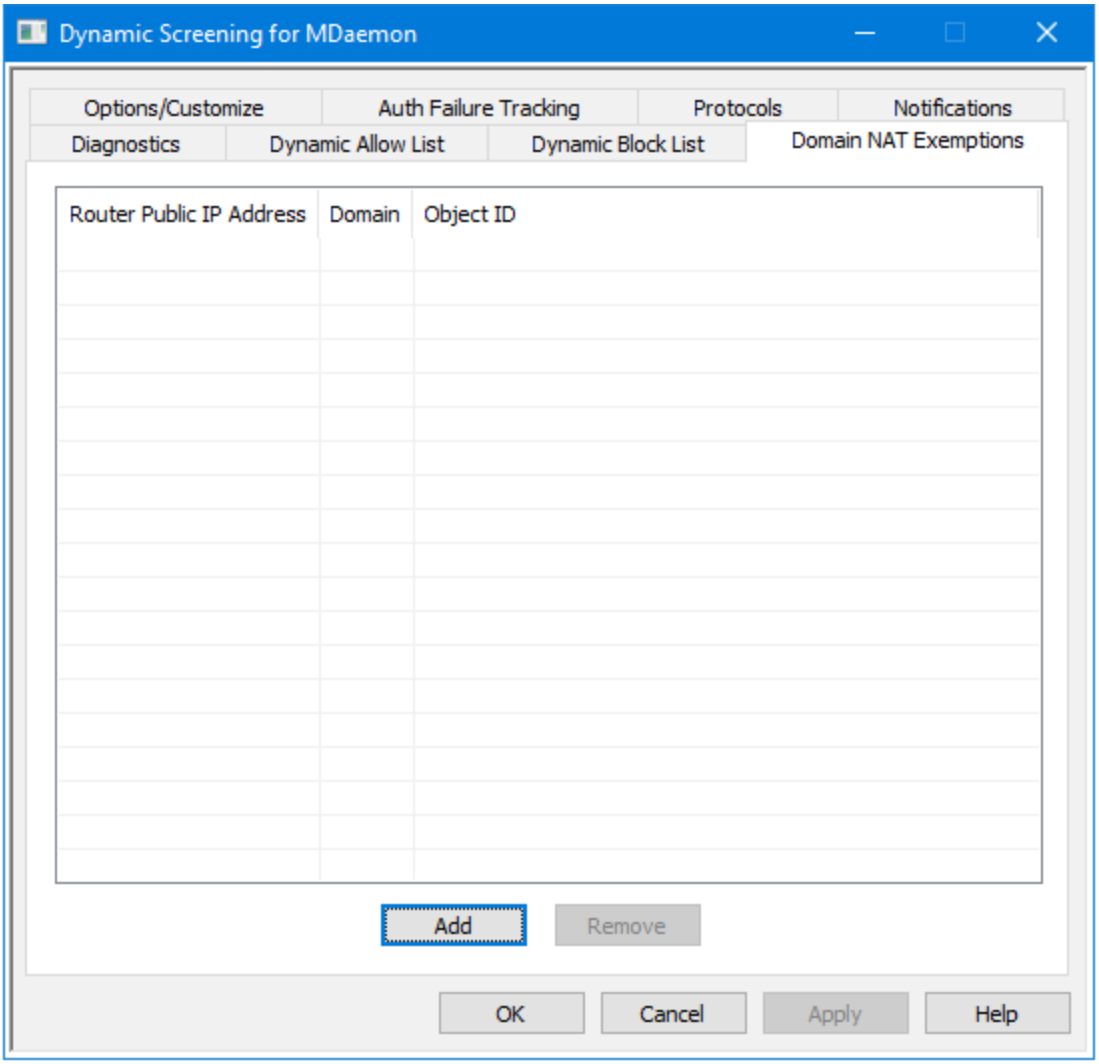
1. Select the entry or entries that you wish to remove from the list (Ctrl+click to select multiple entries).
2. Click **Remove**.

See:

Options/Customize 596
Auth Failure Tracking 600
Dynamic Allow List 609
Protocols 603

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.3.8 Domain NAT Exemptions



This screen is available when you have activated the *Enabled Advanced User Interface features* option on Dynamic Screening's Options/Customize 596 screen.

Use this feature to accommodate a group of MDaemon users who reside on the same external local area network (LAN), which uses network address translation (NAT) to provide a single shared public IP address for all of them. By adding their LAN's public IP address and the MDaemon domain to which the accounts belong, you can prevent the IP address from being blocked by Dynamic Screening when one or more of the users fail authentication due to an incorrect password. Without this feature, a valid user with a misconfigured mail client could cause the LAN's IP address to be blocked and thus prevent all of the users from being able to access their mail. This could happen, for example, when a user's password changes but the user forgets to update a mail client with the new password.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

IP addresses listed here could still be blocked for other reasons, such as bots attempting to log in to non-valid accounts, misconfigured clients attempting to log in to a different MDaemon domain than the one associated with the IP address, and so on. If you wish to completely exclude an IP address from Dynamic Screening then use the Dynamic Allow List 609.

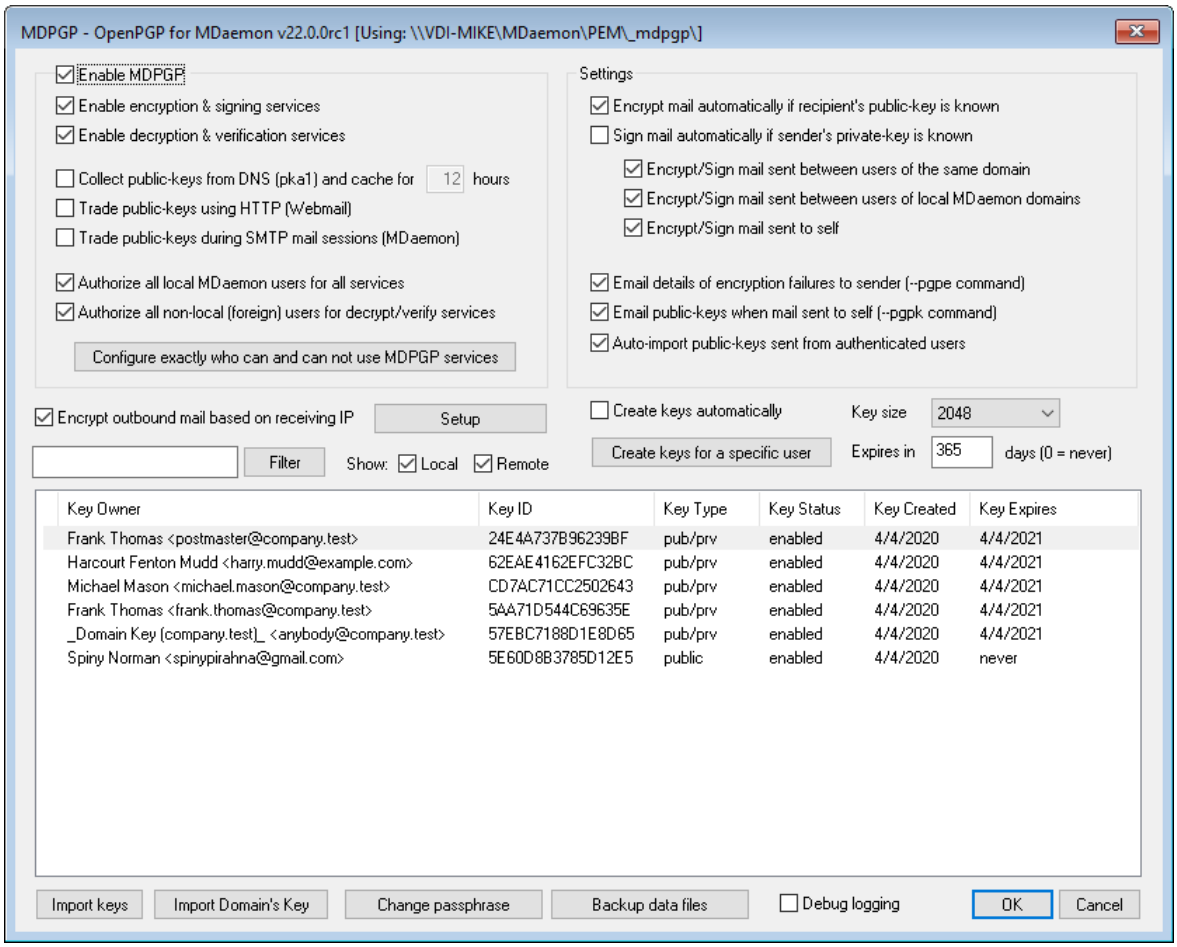
Adding a Domain NAT Exemption

Click **Add**, enter the *Router Public IP Address* of the external LAN, and select the MDaemon *Domain* whose users will be logging in from that IP address. Then, click **OK**.

See:

Options/Customize 596

4.4 MDPGP



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

OpenPGP is an industry standard protocol for exchanging encrypted data, and there are a variety of OpenPGP plugins for email clients that make it possible for users to send and receive encrypted messages. MDPGP is MDaemon's integrated OpenPGP component that can provide encryption, decryption, and basic key management services for your users without requiring them to use an email client plugin.

MDPGP encrypts and decrypts emails using a public-key/private-key system. To do this, when you wish to use MDPGP to send a private and secure message to someone, MDPGP will encrypt that message using a "key" that you previously obtained from that person (i.e. his "public key") and imported into MDPGP. Conversely, if he wishes to send a private message to you, then he must encrypt the message using your public key, which he obtained from you. Giving the sender your public key is absolutely necessary, because without it he can't send you an OpenPGP encrypted message. Your unique public key must be used to encrypt the message because your unique private key is what MDPGP will use to decrypt the message when it arrives.

In order for MDPGP to manage signing, encrypting, and decrypting messages, it maintains two stores of keys (i.e. keyrings)—one for public keys and one for private keys. MDPGP can generate your users' keys automatically as needed, or you can create them manually for specific users. You can also import keys that were created elsewhere. Further, MDaemon can look for public keys attached to authenticated messages from local users, and then import those keys automatically. That way a user can request a public key from someone and then email that key to himself so that MDPGP will detect it and then import it into the public keyring. MDPGP will never store multiple copies of the same key, but there can be multiple different keys for a single address. Finally, whenever a message arrives for an address that has a key in a keyring, MDPGP will sign, encrypt, or decrypt the message as needed, according to your settings. If an address has multiple keys, MDPGP will use the one you have designated as the preferred key to encrypt the message. If no preferred key has been designated then MDPGP will use the first one. When decrypting a message MDaemon will try each one.

You can configure MDPGP's signing and encryption services to operate either automatically or manually. When set to operate automatically, MDPGP will automatically sign and encrypt messages whenever possible. When set to operate manually, MDPGP will only sign or encrypt a message when the sending user inserts a special command into the message's Subject. In any case messages will only be signed or encrypted (or decrypted) when the account has been given permission to use those services.

The OpenPGP specification is outlined in RFCs 4880 and 3156.

Enabling MDPGP

Enable MDPGP
MDPGP is enabled by default, but it will still not sign, encrypt, or decrypt any messages until you create or import keys into its keyrings, or until you use the option below to set MDPGP to *Create keys automatically*.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable encryption & signing services
By default messages can be signed and encrypted when the required keys are in the keyring. Disable this option if you do not wish to allow MDPGP to sign or encrypt messages.

Messages can be signed without being encrypted, but any message that is encrypted by MDPGP will always be signed as well.

Enable decryption & verification services
By default incoming encrypted messages will be decrypted if the recipient's private key is known. Further, MDPGP will also verify embedded signatures in unencrypted messages. Note, however, that both the recipient and sender must be authorized to use the decryption and verification services, either through the "*Authorize all...*" options or "*Configure exactly who...*" option below (everyone is authorized by default). Disable this option if you do not wish to verify embedded signatures or allow MDPGP to decrypt any messages, for example if you want all of your users to handle their own decryption via an email client plugin. When disabled, any incoming encrypted message will be handled like a normal message and placed in the recipient's mailbox.

Collect public-keys from DNS (pka1) and cache for [xx] hours
Enable this option if you want MDPGP to query for message recipient public-keys over DNS using PKA1. This is useful because it automates the process of obtaining some recipients' public keys, preventing you or your users from having to obtain and import them manually in order to send encrypted messages. When PKA1 queries are made, any key URI found is immediately collected, validated, and added to the key-ring. Keys successfully collected and imported to the key-ring using this method are tracked in a file called `fetchedkeys.txt`, and these keys will automatically expire after the number of hours specified in this option or according to the TTL value of the PKA1 record that referred them, whichever value is greater. Therefore the value specified here is the minimum length of time that a key will be cached. The default value is 12 hours and the lowest value allowed is 1 hour.

If you wish to publish your own public-keys to DNS then you must create special TXT records. For example, for the user `frank@example.com` with the key-id: `0A2B3C4D5E6F7G8H`, in the DNS for domain "`example.com`" you would create a `TXT` record at "`frank._pka.example.com`" (replacing the `@` in the email address with the string "`._pka.`"). The data for the `TXT` record would look something like this: "`v=pka1; fpr=<key's full fingerprint>; uri=<Webmail-URL>/WorldClient.dll?view=mdpgp&k=0A2B3C4D5E6F7G8H`" where `<key's full fingerprint>` is the full fingerprint of the key (40 characters long representing the full 20 byte fingerprint value). You can see a key's full fingerprint value by double clicking on the key in the MDPGP GUI.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Trade public-keys using HTTP (Webmail)
Enable this option if you wish to use Webmail as a basic public-key server; Webmail will honor requests for your users' public-keys. The format of the URL to make the request looks like this: "`http://<Webmail-URL>/WorldClient.dll?View=MDPGP&k=<Key-ID>`". Where `<Webmail-URL>` is the path to your Webmail server (for example, "`http://wc.example.com`") and `<Key-ID>` is the sixteen character key-id of the key you want (for example, "`0A1B3C4D5E6F7G8H`"). The key-id is constructed from the last 8 bytes of the key fingerprint - 16 characters in total.

Trade public-keys during SMTP mail sessions (MDaemon)
Check this box if you wish to enable the automatic transmission of public keys as part of the SMTP message delivery process. To do so, MDaemon's SMTP server will honor an SMTP command called RKEY. When sending an email to a server that supports RKEY, MDaemon will offer to transmit the sender's current, Preferred public-key to the other host. That host will respond indicating that it either already has that key ("250 2.7.0 Key already known") or that it needs that key, in which case the key is immediately transferred in ASCII armored form ("354 Enter key, end with CRLF.CRLF") just like an email message. Keys that are expired or revoked are never transmitted. If MDaemon has multiple keys for the sender it will always send the key that is currently marked as preferred. If no key is preferred then the first one found is sent. If no valid keys are available then nothing is done. Only public-keys that belong to local users are offered.

Public-key transfers happen as part of the SMTP mail session that delivers the message from the user. In order for the public-keys transmitted in this way to be accepted, the public-key must be sent along with a message that has been DKIM signed 518 by the domain of the key owner with the i= set to the address of the key owner, which also must exactly match the From: header address of which there can be only one. The "key owner" is taken from within the key itself. Also, the message must arrive from a host in the sender's SPF path 512. Finally, the key owner (or his entire domain via use of wildcards) must be authorized for RKEY by adding an appropriate entry to the MDPGP rules file (instructions are in the rules file for this) indicating that the domain can be trusted for key exchange. All this checking is done automatically for you but you must have DKIM 514 and SPF verification 512 enabled or no work can be done.

The MDPGP log shows the results and details of all keys imported or deleted, and the SMTP session log also tracks this activity. This process tracks the deletion of existing keys and the selection of new preferred keys and updates all participating servers it sends mail to when these things change.

Authorize all local MDaemon users for all services
By default all local MDaemon user accounts are authorized to use any of the MDPGP services that you have enabled: signing, encryption, decryption, and verification. If there are specific users whom you do not wish to allow to use one or more of those services, you can use the "*Configure exactly who can and can not use MDPGP services*" option below to exclude them. Disable this option if you only wish to authorize specific local users. In that case use the "*Configure exactly who can and can not use MDPGP services*" option below to grant access to whomever you choose.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Authorize all non-local (foreign) users for decrypt/verify services
By default any incoming encrypted message for a local recipient from a non-local sender can be decrypted if MDPGP knows the local recipient's private key. Similarly, MDPGP will verify embedded signatures in incoming messages from non-local users. If there are certain non-local senders whose messages you do not wish to decrypt or verify, then you can use the "*Configure exactly who can and can not use MDPGP services*" option below to restrict those senders from those services. Disable this option if you do not wish to decrypt messages or verify embedded signatures when the sender is a non-local address. In that case you can still use the "*Configure exactly who can and can not use MDPGP services*" option below to specify exceptions to that restriction.

Configure exactly who can and can not use MDPGP services
Click this button to open the `rules.txt` file for configuring user permissions for MDPGP. Using this file you can specify who is allowed to sign messages, encrypt messages, and have messages decrypted. You can also specifically restrict users from these options. For example, you could use the rule "`+*@example.com`" to allow all `example.com` users to encrypt messages, but then add "`-frank@example.com`" to specifically prevent `frank@example.com` from being able to do so. See the text at the top of the `rules.txt` file for examples and instructions.

Rules.txt Notes and Syntax

- Only SMTP authenticated email from users of this MDaemon server are eligible for encryption service. You can, however, specify non-local addresses that you wish restrict from the encryption service, meaning that MDPGP will **not** encrypt messages to them, even if the public key is known.
- If there is a conflict between the settings in `rules.txt` and the global "*Authorize all local MDaemon users for all services*" option, the `rules.txt` setting is used.
- If there is a conflict between the settings in `rules.txt` and the global "*Authorize all non-local (foreign) users for decrypt/verify services*" option, the `rules.txt` setting is used.
- Text after # on a line is ignored.
- Separate multiple email addresses on the same line with a space.
- Wildcards (* and ?) in email addresses are permitted.
- Even though MDPGP encrypted messages are **always** signed, granting encryption permission to a user doesn't also grant that user permission to sign unencrypted messages. In order to sign an unencrypted message the account must be given signing permission.
- Each email address must be prefixed with one of the following tags:

+ (plus) - address can use MDPGP encryption service.

- (minus) - address **cannot** use MDPGP encryption service.

! (exclamation) - address can use MDPGP decryption service.

~ (tilde) - address **cannot** use MDPGP decryption service.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

^ (caret) - address can use MDPGP signing service.

= (equal) - address **cannot** use MDPGP signing service.

$ (dollar) - address can use MDPGP verification service.

& (ampersand) - address **cannot** use MDPGP verification service.

Examples:

`+*@*` — all users of all domains can encrypt.

`!*@*` — all users of all domains can decrypt.

`^*@*` — all users of all domains can sign.

`^*@example.com` — all users of example.com can sign.

`+frank@example.com ~frank@example.com` — the user can encrypt but not decrypt.

`+GROUP:EncryptingUsers` — members of MDaemon's `EncryptingUsers` group can encrypt

`^GROUP:Signers` — members of MDaemon's `Signers` group can sign

Encryption/Signing Modes

Automatic Mode

Use the Settings options to configure MDPGP to sign and encrypt messages automatically for accounts permitted to do so. When an account sends an authenticated message and MDPGP knows the required key, the message will be signed or encrypted according to the settings below.

The special Subject codes outlined in the Manual Mode section below always take precedence over the Automatic Mode options. Therefore if one of these options is disabled, an account that is permitted to sign or encrypt messages can still manually cause a message to be signed or encrypted by using one of the codes.

Settings

Encrypt mail automatically if recipient's public key is known
By default, if an account is allowed to encrypt messages, MDPGP will encrypt them automatically if the recipient's public key is known. Disable this option if you do not wish to encrypt them automatically; messages can still be encrypted manually by using the special codes outlined in the Manual Mode section below.

Sign mail automatically if sender's private key is known
Click this option if you want MDPGP to sign messages automatically when the sending account's private key is known, if the account is allowed to sign messages.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Even when this option is disabled, messages can still be signed manually by using the special codes outlined in the Manual Mode section below.

Encrypt/Sign mail between users of the same domain
When MDPGP is set to encrypt or sign messages automatically, this option causes MDPGP to do this even when messages are sent between users of the same domain, provided the required keys are known. This option is enabled by default.

Encrypt/Sign mail between users of local MDaemon domains
When MDPGP is set to encrypt or sign messages automatically, this option causes MDPGP to do this even when messages are being sent between users of local MDaemon domains, provided the required keys are known. For example, if your MDaemon domains include "example.com" and "example.net," then messages sent between those domains' users will be automatically encrypted or signed. This option is enabled by default.

Encrypt/Sign mail sent to self
When MDPGP is set to encrypt or sign messages automatically, this will be done even when the MDaemon user is sending a message to himself (e.g. frank@example.com sending to frank@example.com). Therefore if the account has permission to use both encryption and decryption (the default settings) then MDPGP will accept the user's message, encrypt it, and then immediately decrypt it and place it in the same user's mailbox. If, however, the account isn't configured for decryption, this will cause the message to be encrypted and then placed in the same user's mailbox still encrypted. This option is enabled by default.

Manual Mode

When you have disabled the *Sign mail automatically...* and *Encrypt mail automatically...* options outlined above, you are using MDPGP in Manual Mode. MDPGP will not sign or encrypt any messages except those that are authenticated and have one of the following codes in the message's Subject header:

--pgps Sign this message if possible. Code can be placed at the beginning or end of the Subject.

--pgpe Encrypt this message if possible. Code can be placed at the beginning or end of the Subject.

--pgpx The message **MUST** be encrypted. If it cannot be encrypted (e.g. because the recipient's key isn't known) then do not deliver it; the message will be bounced/returned to the sender. Code can be placed at the beginning or end of the Subject.

--pgpk Send me my public key. The user places this code at the beginning of the Subject and sends the message to himself. MDPGP will then email the user his public key.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

--pgpk<Email> Send me this address' public key. The user places this code at the beginning of the Subject and sends the message to himself. MDPGP will then email the user the address' public key.

Example:

```
Subject: --pgpk<frank@example.com>
```

Key Management

Public and private keys are managed using the options on the bottom half of the MDPGP dialog. There is an entry for each key, and you can right-click any entry to export the key, delete it, enable/disable it, set it as a Preferred Key (see "*Trade public-keys during SMTP mail sessions*" above), or set it as a Domain's Key (see below). When you click **Export Key** it will be saved to the `\MDaemon\Pem\_mdpgp\exports\` folder and you can optionally email the public key to an email address. "Show Local/Remote" and "Filter" options are provided to help you locate certain addresses or groups.

Using a Domain Key

Optionally you can use a single key to encrypt all messages going to a specific domain, regardless of the sender. This is useful if, for example, one of your domains and a domain hosted elsewhere wish to encrypt all emails sent between them, but they do not wish to setup and manage individual encryption keys for every user account within the domain. There are multiple ways to accomplish this:

- If you already have a public key for another domain and you wish to use that key for encrypting all outbound messages going to it, right-click the key and click **Set as Domain's Key**. Then enter the domain name and click **OK**. This will create a Content Filter rule to cause all messages "To:" that domain to be encrypted using the designated key.
- If the domain's public key has been provided to you but isn't yet in the list, click **Import Domain's Key**, enter the domain name and click OK, then navigate to the domain's `public.asc` file and click **Open**. This also will create the Content Filter rule for encrypting messages to the domain.
- Customize your Content Filter rules as needed to modify exactly which messages get encrypted before sending to the domains.
- To create a new key for one of your domains, to give to another domain for encrypting messages being sent to you, follow the instructions under the "*Create keys for a specific user*" option below, selecting "`_Domain Key (domain.tld)_ <anybody@domain.tld>`" from the list.

Do not use a key to encrypt outbound messages for which you also have the corresponding private key. If you do, MDPGP will encrypt a message and then immediately see that the decryption key is known and promptly decrypt that very same message.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Email details of encryption failures to sender (--pgpe command)
When someone uses the --pgpe command to send encrypted mail and that encryption fails (for example, because no encryption key is found), then this option will cause a notification email to be sent back to the sender informing him or her of the failure. This option is disabled by default, meaning no failure notification message will be sent.

Email public-keys when mail sent to self (--pgpk command)
When a user sends an email to himself with "--pgpk<email address>" as the subject (e.g. --pgpk<frank@example.com>). If a public-key for <email address> exists it will be emailed back to the requester.

Auto-import public-keys sent from authenticated users
By default, when an authenticated user sends an email message with a public key in ASCII armored format attached, MDPGP will import that public key into the keyring. This is a simple way for a user to get a contact's public key into MDPGP, by emailing the public key to himself as an attachment. Disable this option if you do not wish to auto-import public keys.

Create keys automatically
Enable this option if you want MDPGP to create a public/private key pair automatically for each MDaemon user. Rather than generate them all at once, however, MDPGP will create them over time, creating each user's key pair the next time a message is processed for that user. This option is disabled by default to conserve resources and avoid needlessly generating keys for accounts that may never use MDPGP.

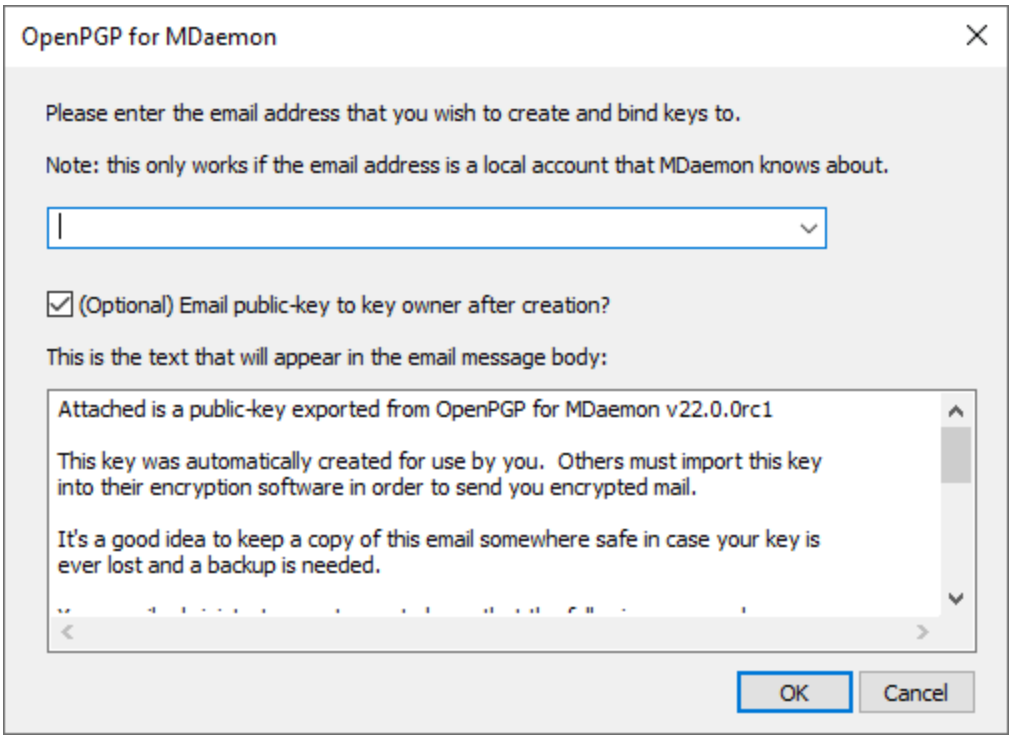
Key size
Use this option to specify the key size for keys that MDPGP generates. You can set the key size to 1024, 2048, or 4096. The default setting is 2048 bit keys.

Expires in [xx] days (0=never)
Use this option to specify the number of days from creation date that a key generated by MDPGP will be valid before it expires. Set the option to "0" if you do not want keys to expire. The default setting is 0.

Create keys for a specific user
To manually generate a key pair for an account:

1. Click **Create keys for a specific user**.
2. Select the account from the drop-down list. If you wish to create a single key to apply to all of a domain's accounts, choose the "_Domain Key (domain.tld)_ <anybody@domain.tld>" option from the list.
3. **Optional:** Check the box **Email public key to key owner...** if you wish to send the key to the user as an email attachment.
4. Click **Ok**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Encrypt outbound mail based on receiving IP
If you wish to use a specific encryption key to encrypt all messages destined for a certain IP address, enable this option and click **Setup** to open the MDaemon Message Transport Encryption file, in which you can list the IP address and associated key ID. Any outbound SMTP session delivering a message to one of the listed IPs will encrypt the message using the associated key just prior to transmission. If the message is already encrypted by some other key then this step will be skipped.

Import keys
If you wish to import a key file into MDPGP manually, click this button, locate the key file, and click **Open**. When importing a private key file, you do not need to import the corresponding public key, as it is included in the private key. If you are importing a private key protected by a passphrase then MDPGP will prompt you to enter the passphrase. Without the passphrase you cannot import the private key. After importing a private key, MDaemon will change that key's passphrase to whichever passphrase MDPGP is currently using.

Import Domain's key
If a public encryption key has been provided to you to encrypt all messages being sent to a certain domain, click this button, enter the domain name, click **OK**, and then navigate the domain's `public.asc` file and click **Open**. This will add the domain's public key to the list and create a Content Filter rule to encrypt all outbound messages for that domain, regardless of the sender.

Change passphrase
Private keys are protected at all times by a passphrase. When attempting to import a private key, you must enter its passphrase. When exporting a private key, that

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

exported key will still be protected by the passphrase, and it cannot be used or imported elsewhere without it. MDPGP's default passphrase is **MDaemon**. For security reasons you should change this passphrase after you begin using MDPGP, because until you do so, every key created by or successfully imported into MDPGP will have its passphrase set (or changed) to **MDaemon**. You can change the passphrase at any time by clicking **Change passphrase** on the MDPGP screen. When you change the passphrase, every private key on the keyring is updated to the new passphrase.

Backup data files
Click this button to make a backup of your current `Keyring.private` and `Keyring.public` keyring files. By default the backup files will be copied to: "`\MDaemon\Pem\_mdpgp\backups`" and have a date and `.bak` extension appended to the filenames.

- Forwarded messages are not encrypted.
- Autoresponder messages are not encrypted.
- Key servers and key revocation are not supported, except as outlined in the "*Collect public-keys from DNS (pka1) and cache for [xx] hours*" and "*Send public-keys over HTTP (Webmail)*" options above.
- The Content Filter encrypt action does not act on messages already encrypted, and the encrypt and decrypt actions are subject to all MDPGP configuration requirements.
- The drop-down lists that display MDaemon accounts show the first 500 accounts by default. You can set `MaxUsersShown=0` in `plugins.dat` to view all accounts. This may take longer to load for very large user lists.
- `MDPGPUtil.exe` is a tool that can encrypt and decrypt via command line options. Run MDPGPUtil with no arguments from a command line shell for help.

4.5 Outbreak Protection

Outbreak Protection is part of the optional MDaemon AntiVirus 653 feature. Enabling MDaemon AntiVirus for the first time will start a 30-day trial. If you wish to purchase this feature, contact your authorized MDaemon reseller or visit: www.mdaemon.com.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

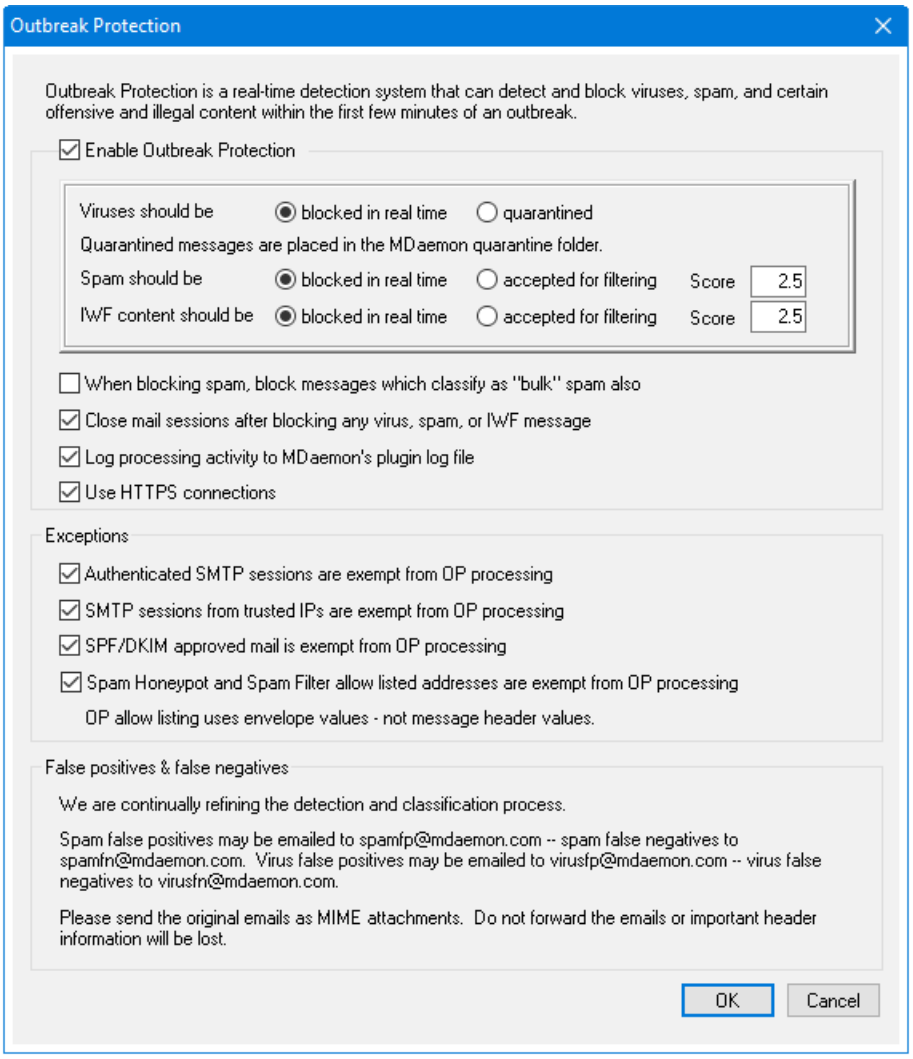
Outbreak Protection (OP) is accessible from MDaemon's Security menu (Security » Outbreak protection..., or Ctrl+Shift+1). It is a revolutionary real time anti-spam, anti-virus, and anti-phishing technology capable of proactively protecting an MDaemon email infrastructure automatically and within minutes of an outbreak.

Outbreak Protection is completely content agnostic, meaning that it doesn't rely on strict lexical analysis of message content. Thus, it doesn't require heuristic rules, content filtering, or signature updates. Further, that means it is not fooled by the addition of seed text, clever spelling changes, social engineering tactics, language barriers, or differences in encoding techniques. Instead, OP is based on Recurrent Pattern Detection and Zero-hour technologies. It relies on the mathematical analysis of message structure and message distribution characteristics over SMTP—it analyzes "patterns" associated with an email transmission and compares them to similar patterns collected from millions of email messages worldwide, which are sampled and compared in real time. **Note:** OP never transmits the actual content of messages, nor can message content be derived from the extracted patterns.

Because messages are being analyzed worldwide in real time, protection is provided within minutes—often seconds—of a new outbreak. For viruses, this level of protection is critical since it is often hours after an outbreak before a traditional antivirus vendor can verify and submit a virus signature update, and it can then be even longer before that update is put into production use. During that interval, servers without Outbreak Protection are vulnerable to that particular outbreak. Similarly, for spam messages it will often take time and effort to analyze the spam and create a safe filtering rule before it will be recognized by traditional heuristic and content based systems.

It is important to note, however, that the Outbreak Protection feature is not a replacement for traditional anti-virus, anti-spam, and anti-phishing techniques. In fact, OP provides another specialized layer of protection on top of the existing heuristics, signature, and content based tools found within MDaemon. Specifically, OP is designed to deal with large-scale outbreaks rather than old, unique, or specifically targeted messages that can be more readily caught by the traditional tools.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Outbreak Protection

Enable Outbreak Protection

Click this checkbox to enable Outbreak Protection for your server. Incoming messages will be analyzed to see if they are part of an ongoing virus, spam, or phishing outbreak. The remaining options on this dialog are used to determine what will be done with messages found to be part of an outbreak, and to designate the senders that will be exempt from OP processing.

Viruses should be...

blocked in real time

Select this option if you wish to block messages during the SMTP process when they are determined to be part of a virus outbreak. These messages will not be quarantined or delivered to their intended recipients—they will be rejected by the server.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

quarantined
Select this option if you wish to accept messages that OP determines are part of a virus outbreak. Although these messages will not be rejected by the server, they will be quarantined instead of delivered to their intended recipients. Quarantined messages are placed in the quarantine folder.

Spam should be...

blocked in real time
Select this option if you wish to block messages during the SMTP process when OP confirms that they are part of a spam outbreak. These messages will not be flagged as spam and delivered to their intended recipients—they will be rejected by the server. Messages classified by OP as "bulk" mail will not be blocked by this option unless you activate the *When blocking spam, block messages which classify as "bulk" spam also* option below. Messages classified as "bulk" by OP could simply be a part of certain very large mailing lists or other similar widely distributed content, so you may or may not consider those types of messages to be spam. For that reason, those types of messages generally shouldn't be scored negatively or blocked by OP.

accepted for filtering
Select this option if you wish to accept messages that OP confirms to be part of a spam outbreak, so that they can then be subjected to spam filtering and content filter processing. These messages will not be blocked by OP, but they will have their Spam Filter scores adjusted according to the *Score* option below.

When using the *accepted for filtering* option, OP will not directly cause a confirmed spam message to be blocked, but a message may still be blocked by MDaemon during the SMTP process if you have configured the Spam Filter to use the *SMTP rejects messages with scores greater than or equal to [xx]* option, located on the Spam Filter 661 screen.

For example, if the scoring option below caused a message's Spam Filter score to be 15.0, then the message would still be rejected as spam if you had also configured the Spam Filter's "*SMTP rejects...*" option to reject messages that have a score of 15.0 or greater.

Score
When using the *accepted for filtering* option above, this amount will be added to a message's Spam Filter score when OP confirms that the message is part of a spam outbreak.

IWF Content

The following option applies to content identified by the Internet Watch Foundation (IWF) as referring to child abuse image sites (i.e. child pornography sites). It enables OP to use an integrated URL list provided by the IWF to detect and tag messages that refer to that content. The IWF operates an independent internet "hotline" for reporting potentially illegal online content, including child abuse content

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

hosted anywhere in the world. They work in partnership with the police, governments, the wider online industry and the public to combat the availability of illegal online content. The Foundation's URL list is updated daily with new sites hosting child abuse images.

Many organizations have internal compliance rules governing the content of email sent or received by its employees, especially with regard to obscene or illegal material. In addition, many countries have outlawed the sending or receipt of such content. This feature can assist in your efforts to ensure compliance.

For more on the IWF, see:

http://www.iwf.org.uk/

IWF content should be...

blocked in real time
Choose this option if you wish to reject incoming messages during the SMTP process when they have IWF restricted content.

accepted for filtering
Choose this option if you wish to increase a message's Spam Filter score instead of rejecting it when it has IWF restricted content. The Spam Filter score will be increased by the amount specified in the *Score* option below.

Score
When the *accepted for filtering* option above is selected, this is the amount that will be added to a message's Spam Filter score when it contains IWF restricted content.

When blocking spam, block messages which classify as "bulk" spam also
Sometimes OP will identify certain messages that could be considered spam but aren't being sent from a known spammer or bot-net—as is sometimes the case with legitimate bulk mailings and newsletters. OP classifies these types of messages as "*Spam (bulk)*" rather than *"Spam (confirmed)*." Click this checkbox if you wish to apply OP's spam blocking features to "*Spam (bulk)*" mail as well. If this option is disabled, only messages classified as "*Spam (confirmed)*" will be affected by OP's spam blocking features above. Accepting this type of spam for later processing may be necessary for sites that want to receive bulk mailings but for some reason cannot exempt the source or recipient.

Log processing activity to MDaemon's plugin log file
Enable this checkbox if you wish to log all OP processing activity into MDaemon's plugin log file.

Use HTTPS connections
By default Outbreak Protection uses HTTPS connections when connecting to the Outbreak Protection service.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Exceptions

Authenticated SMTP sessions are exempt from OP processing
When this option is enabled, authenticated SMTP sessions are exempt from OP processing. This means that messages sent during that session will not be subjected to Outbreak Protection checks.

SMTP sessions from trusted IPs are exempt from OP processing
Enable this option if you wish to exempt trusted IP addresses from Outbreak Protection—messages arriving from a server at a trusted IP address not be subjected to OP checks.

SPF/DKIM approved mail is exempt from OP processing
Click this checkbox if you wish to exempt a message from OP processing when the sending domain appears on the Approved List 544 and it is validated by SPF or DKIM.

Spam Honeypots and Spam Filter allowed addresses are exempt from OP processing
Click this option if you wish to exempt the Spam Honeypots 690 and Spam Filter allow lists from Outbreak Protection. The allow list applies to the recipient, or RCPT value given during the SMTP session. The "Allow List (from)" applies to the sender, or MAIL value given during the SMTP session. These operations are not based on message header values.

False Positives and False Negatives

False positives, or classifying a legitimate message improperly as part of an outbreak, should rarely if ever happen. Should a false positive occur, however, you can send that message to us at **spamfp@mdaemon.com** for spam/phishing false positives or **virusfp@mdaemon.com** for virus false positives, so that we can use it to help refine and improve our detection and classification processes.

False negatives, or classifying a message as not part of an outbreak even though it is still spam or an attack, will happen more often than false positives. However, it worth noting that OP is not designed to catch all spam, virus attacks, and the like—it is simply one layer of protection that specifically targets outbreaks. Old messages, specifically targeted messages and the like, which are not part of a currently ongoing outbreak, might pass the OP check. Those sorts of messages should then be caught by the other AntiVirus and MDaemon features further down the processing chain. Should a false negative occur, however, you can send that message to us at **spamfn@mdaemon.com** for spam/phishing false negatives or **virusfn@mdaemon.com** for virus false negatives, so that we can use it to help refine and improve our detection and classification processes.

When sending improperly classified messages to us, the original email should be sent as a MIME email attachment rather than forwarded. Otherwise, headers and other information critical to the classification process will be lost.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6 Content Filter and AntiVirus

Content Filter

The Content Filter[631] (Security » Content Filter) can be used for a large number of purposes such as: preventing spam email, intercepting messages containing viruses before they reach their final destination, copying certain emails to one or more additional users, appending a note or disclaimer to the bottom of messages, adding, and deleting headers, stripping email attachments, deleting messages, and more. Because individual Content Filter rules are created by the administrator, and because of their diversity, they can be used in many situations and are limited for the most part only be the creativity of the person creating them. With a little bit of thought and experimentation, this feature can be very useful.

MDaemon AntiVirus (MDAV)

When utilizing MDaemon's optional AntiVirus feature, you will have access to two additional screens on the Content Filter dialog: Virus Scanning[653] and AV Updater[657]. These screens are used to directly control the AntiVirus features and designate what actions MDaemon will take when a virus is detected. MDAV is equipped with two virus scanning engines: IKARUS Anti-Virus and ClamAV. You can scan messages with either engine or both, for an extra layer of security. MDAV also includes Outbreak Protection[624], which is not heuristics-based or signature dependent like the traditional protection tools, but is designed to catch spam, phishing and virus attacks that are part of an ongoing outbreak, and which can sometimes be missed by the traditional tools.

Enabling MDaemon AntiVirus[653] for the first time will start a 30-day trial. If you wish to purchase this feature, contact your authorized MDaemon reseller or visit: www.mdaemon.com.

See:

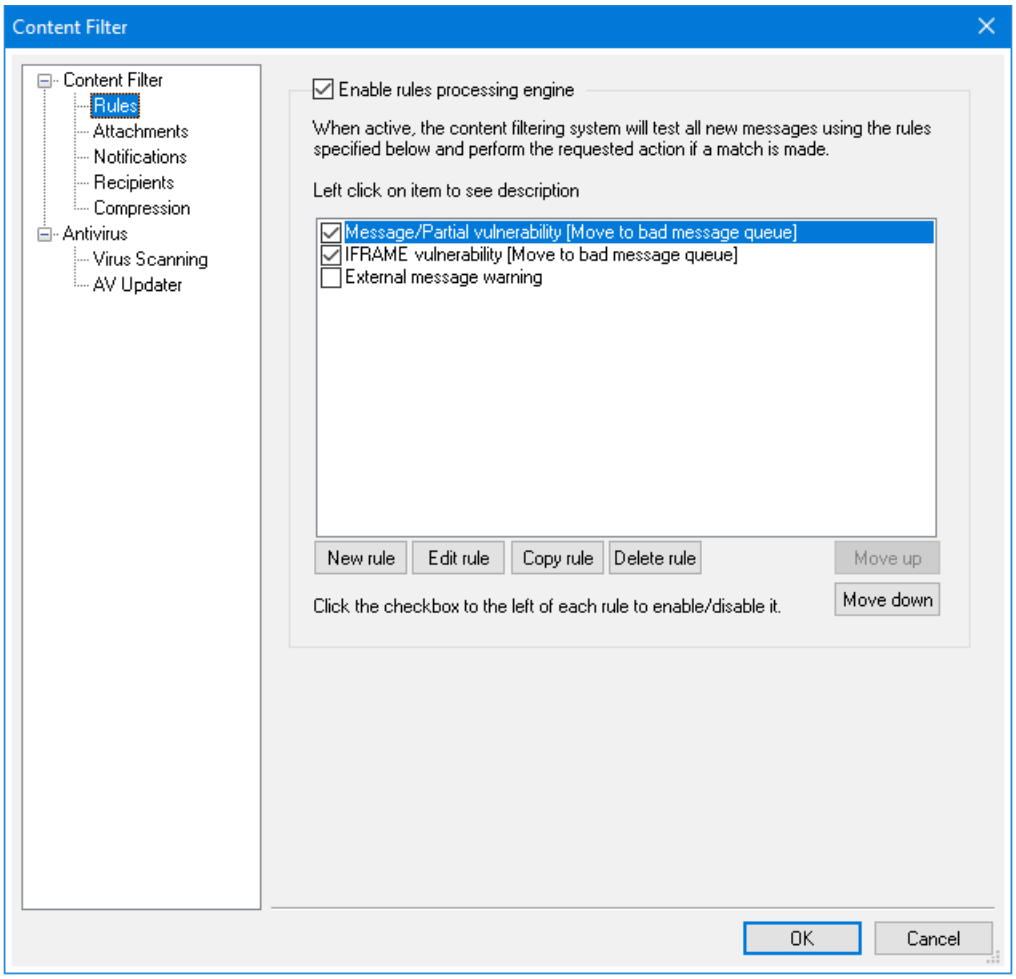
Content Filter Editor[631]
Creating a New Content Filter Rule[633]
Modifying an Existing Content Filter Rule[638]
Using Regular Expressions in Your Filter Rules[638]

Virus Scanning[653]
AntiVirus Updater[657]
Outbreak Protection[624]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.1 Content Filter Editor

4.6.1.1 Rules



All messages processed by MDaemon will at some point reside temporarily in one of the message queues. When Content Filtering is enabled, before any message is allowed to leave the queue it will first be processed through the Content Filter rules. The result of this procedure will determine what is done with the message.

Messages that have a filename beginning with the letter "P" will be ignored by the content filtering process. Every other message will be processed through the content filter system. Once processed, MDaemon will change the first character of the filename to a "P". In this way a message will only be processed through the content filtering system once.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Content Filtering Rules

Enable rules processing engine
Click this checkbox to enable content filtering. All messages processed by MDaemon will be filtered through the content filter rules before being delivered.

Existing Content Filtering Rules

This box lists all of your Content Filter rules, with a checkbox beside each one so that you can enable/disable them at will. To see a description of any given rule in its internal script format, click that rule and pause your mouse-cursor over it (moving your mouse will cause the description to disappear). Whenever a message is processed through the Content Filter, these rules will be applied in the order in which they are listed. This makes it possible for you to arrange your rules to achieve a greater level of versatility.

For example: If you have a rule that deletes all messages containing the words, "This is Spam!" and a similar rule that sends those messages to the Postmaster, then putting them in the right order will enable both rules to be applied to the message. This assumes that there isn't a "Stop Processing Rules" rule that applies to the message higher up in the list. If so, then you would use the *Move Up*/*Move Down* buttons to move the "Stop" rule below the other two. Then, any message containing "This is Spam!" would be copied to the Postmaster and then deleted.

MDaemon has the capability to create rules that will perform multiple tasks and use `and/or` logic. Considering the example above, instead of using multiple rules you could create a single rule that would accomplish all of those tasks and more.

New rule
Click this button to create a new content filter rule. This will open the Create Rule 633 dialog.

Edit rule
Click this button to open the selected rule in the Modify Rule 638 editor.

Copy rule
Click this button to clone the selected content filter rule. An identical rule will be created and added to the list. The new rule will be given a default name of "Copy of [Original Rule Name]". This is useful if you wish to create multiple similar rules. You can create a single rule, clone it several times, and then modify the copies as needed.

Delete rule
Click this button to delete the selected content filter rule. You will be asked to confirm your decision to delete the Rule before MDaemon will do so.

Move up
Click this button to move the selected rule up.

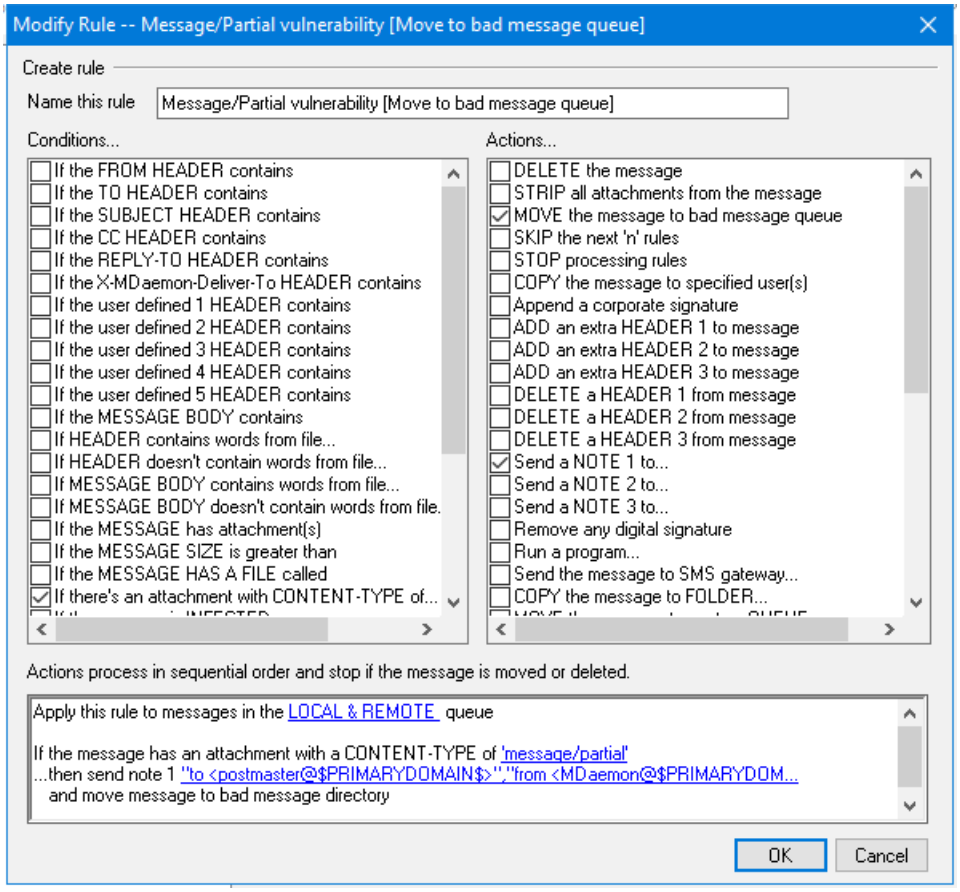
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Move down
Click this button to move the selected rule down.

See:

[Creating a New Content Filter Rule](#) 633
[Modifying an Existing Content Filter Rule](#) 638
[Using Regular Expressions in Your Filter Rules](#) 638

4.6.1.1.1 Creating a New Content Filter Rule



This dialog is used for creating Content Filter Rules. It is reached by clicking the *New Rule* button on the Content Filter dialog.

Create Rule

Name this rule
Type a descriptive name for your new rule here. By default it will be called "New Rule #n".

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Conditions...

This box lists the conditions that may be applied to your new rule. Click the checkbox corresponding to any condition that you want to be applied to the new rule. Each enabled condition will appear in the Rule Description box below. Most Conditions will require additional information that you will specify by clicking on the Condition's hyperlink in the Rule Description box.

If the [HEADER] contains—Click any of these options to base your rule on the content of those particular message headers. You must specify the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 638.

If the user defined [# HEADER] contains—Click one or more of these options to base the rule on message headers that you will define. You must specify the new header, and the text for which to scan. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 638.

If the MESSAGE BODY contains—This option makes the contents of the message body one of the conditions. This condition requires you to specify a text string for which to search. This condition now supports regular expressions. See Using Regular Expressions in Your Filter Rules 638.

If the MESSAGE has Attachment(s)—When this option is selected, the rule will be contingent upon the presence of one or more message attachments. No additional information is required.

If the MESSAGE SIZE is greater than—Click this option if you want the rule to be based upon the size of the message. The size must be specified in *KB*. Default is 10KB.

If the MESSAGE HAS A FILE called—This option will scan for a file attachment with a particular name. The filename must be specified. Wildcards such as *.exe and file *.* are permitted.

If message is INFECTED...—This condition is `TRUE` when MDaemon determines that a message is infected with a virus.

If the EXIT CODE from a previous run process is equal to—If a previous rule in your list utilizes the *Run Process* action, you can use this condition to look for a specific exit code from that process.

If the MESSAGE IS DIGITALLY SIGNED—The condition applies to messages that have been digitally signed. No further information is required by this condition.

If SENDER is a member of GROUP...—This condition applies to a message when it is sent by an account that is a member of the account Group designated in the rule.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If RECIPIENT is a member of GROUP...— This condition applies to a message when its recipient is a member of the account Group designated in the rule.

If ALL MESSAGES—Click this option if you want the rule to be applied to all messages. No further information is required; this rule will affect every message except those to which a "Stop Processing Rules" or "Delete Message" action has been applied in a previous rule.

Actions...

MDaemon can perform these actions if a message matches the rule's conditions. A few Actions will require additional information that you will specify by clicking on the Action's hyperlink in the Rule Description box.

Delete Message—Selecting this action will cause the message to be deleted.

Strip All Attachments From Message—This action causes all attachments to be stripped from the message.

Move Message To Bad Message Queue—Click this action to cause a message to be moved to the bad message queue. An `X-MDBadQueue-Reason` header will be added to the message.

Skip n Rules—Selecting this action will cause a specified number of rules to be skipped. This is useful in situations where you may want a rule to be applied in certain circumstances but not in others.

For example: you may wish to delete messages that contain the word "Spam", but not those that contain "Good Spam". To accomplish this you could create a rule that deletes messages containing "Spam" and then place above it another rule that states "if the message contains "Good Spam" then Skip 1 Rule".

Stop Processing Rules—This action will skip all remaining rules.

Copy Message To Specified User(s)—Causes a copy of the message to be sent to one or more recipients. You must specify which recipients are to receive the message.

Append a corporate signature—This action makes it possible for you to create a small amount of text that will be appended as a footer to the message. Alternatively, it can add the contents of a text file. There is a *Use HTML* checkbox available if you wish to include HTML code in your signature's text. This Action supports the `$CONTACT...$` signature macros 128.

For example: you could use this rule to include a statement that says "This email originated from my company, please direct any complaints or questions to user01@example.com".

Add Extra Header Item To Message—This action will add an additional header to the message. You must specify the name of the new header and its value.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete A Header Item From Message—This action will remove a header from a message. You must specify the header that you wish to delete.

Send Note To... —This action will send an email to a particular address. You will be able to specify the recipient, sender, subject, and a small amount of text. You can also configure this action to attach the original message to the note. **Note:** This action skips all messages that do not have a return-path. Therefore it cannot be triggered by, for example, Delivery Status Notification (DSN) messages.

For example: you might wish to create a rule that will move all messages containing "This is Spam!" to the bad message directory and create another rule that will send a note to someone letting them know that this has been done.

Remove Digital Signature—Click this action to cause a digital signature to be removed from the message.

Run Process...—This action can be used to run a particular program when a message meets the rule's conditions. You must specify the path to the program that you wish to run. You can use the `$MESSAGEFILENAME$` macro to pass the name of the message to the process, and you can specify whether or not MDaemon should suspend its operations temporarily or indefinitely while it waits for the process to terminate. Further, you can force the process to terminate and/or run it in a hidden window.

Send Message Through SMS Gateway Server...—Click this option to send the message through an SMS Gateway Server. You must supply the Host or IP Address and the SMS phone number.

Copy Message to Folder...—Use this option to place a copy of the message into a specific folder.

MOVE the messages to custom QUEUE...—Use this action to move the message into one or more previously created custom mail queues. When moving messages to custom remote mail queues you can use the custom scheduling options on the Event Scheduler to control when those messages will be processed.

Add Line To Text File—This option will cause a line of text to be added to a specific text file. When choosing this action you will have to specify the path to the file and the text that you want to be appended to it. You may use certain MDaemon macros in your text to cause the content filter to dynamically include information about the message such as the sender, recipient, message ID, and so on. Click the Macros button on the "Add line to text file" dialog to display a list of permitted macros.

[Copy|Move] Message to Public Folders...—Use this action to cause the message to be copied (or moved) to one or more Public Folders.

Search and Replace Words in a Header—Use this option to scan a specified header for certain words and then delete or replace them. When creating this rule, click the "specify information" link in the Rule Description to open the "Header – Search and Replace" dialog on which you will designate the header and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

words to replace or delete. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 638.

Search and Replace Words in the Message Body—Use this option to scan the message body and replace any desired text. This action now supports regular expressions. See Using Regular Expressions in Your Filter Rules 638.

Jump to Rule...—Use this action to jump immediately to a rule further down in the list, skipping over all rules between the two.

Send an instant message...—This action sends an instant message to someone when the message matches the rule's criteria. You will specify the **To:** email address, the **From:** address, and content of the message.

Add to Windows Event Log...—Use this action to log a text string to the Windows Event Log. You can use macros in the string, and there is a button to display the permitted macros.

Extract attachments to folder...—Use this action to extract attachments from a message. You will specify the folder to which the attachments will be copied, and you can choose to remove the attachment from the message after extraction. You can also set conditions to determine which attachments will be extracted, based on the file name, content type, and size of the attachments.

Change message processing priority...—This action is used to set the processing priority of the message, from "10 (Urgent)" to "90 (Retry)". The default settings is "50 (normal)."

Sign with DKIM selector...—Use this action if you want the rule to cause a message to contain a DKIM signature 518. You can also use it if you wish to sign some messages using a selector other than the one designated on the DKIM dialog.

Flag message for REQUIRETLS...—Indicates that the message should use REQUIRETLS 576.

[Sign|Encrypt|Decrypt] message with the user's [Private| Public] key...—Use these actions to sign, encrypt, or decrypt a message using a private or public key. See: MDPGP 614 for more information. **Note:** these actions will be performed even when MDPGP is disabled.

Add a warning to the top of the message...—Use this action if you wish to add some sort of warning to the top of a message. You enter a string of plain text or enter HTML code and check the "Use HTML" box. Alternatively, you can load the text from a file.

Add an attachment...—Use this action if you wish to attach a file to a message that meets the rule's criteria. The file must be contained in the `./MDaemon/CFilter/Attachments/` folder.

Extract attachment and add link...—Use this action if you wish to extract attachments from messages that meet the rule's criteria, and add a link to them. See: Attachment Linking 357.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Rule description

This box displays the new rule's internal script format. Click any of the rule's conditions or actions (listed as hyperlinks) and the appropriate editor will be opened for specifying any needed information.

See:

Content Filter Editor 631
Modifying an Existing Content Filter Rule 638
Using Regular Expressions in Your Filter Rules 638

4.6.1.1.2 Modifying an Existing Content Filter Rule

To modify an existing content filter rule, select the rule and then click the *Edit Rule* button on the Content Filter dialog. The rule will be opened for editing in the Modify Rule editor. The controls on this editor are identical to the Create Rule Dialog 633.

See:

Content Filter Editor 631
Creating a New Content Filter Rule 633
Using Regular Expressions in Your Filter Rules 638

4.6.1.1.3 Using Regular Expressions in Your Filter Rules

The Content Filtering system supports *regular expression* searches, which is a versatile system that makes it possible for you to search not only for specific text strings, but also for text *patterns*. Regular expressions contain a mix of plain text and special characters that indicate what kind of matching to do, and can thus make your Content Filter rules more powerful and better targeted.

What are Regular Expressions?
A regular expression (regexp) is a text pattern consisting of a combination of special characters known as *metacharacters* and alphanumeric text characters, or "*literals*" (abc, 123, and so on). The pattern is used to match against text strings—with the result of the match being either successful or not. Regexps are used primarily for regular text matches and for search and replace.

Metacharacters are special characters that have specific functions and uses within regular expressions. The regexp implementation within the MDaemon Content Filtering system allows the following metacharacters:

```
\ | () [] ^ $ * + ? . <>
```

Metacharacter	Description

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

**** When used before a metacharacter, the backslash ("\") causes the metacharacter to be treated as a literal character. This is necessary if you want the regular expression to search for one of the special characters that are used as metacharacters. For example, to search for "+" your expressions must include "\+".

| The *alternation* character (also called "*or*" or "*bar*") is used when you want either expression on the side of the character to match the target string. The regexp "abc|xyz" will match any occurrence of either "abc" or "xyz" when searching a text string.

[...] A set of characters contained in brackets ("[" and "]") means that any character in the set may match the searched text string. A dash ("-") between characters in the brackets denotes a range of characters. For example, searching the string "abc" with the regexp "[a-z]" will yield three matches: "*a*," "*b*, " and "*c*. " Using the expression "[az]" will yield only one match: "*a*."

^ Denotes the beginning of the line. In the target string, "abc ab a" the expression "^a" will yield one match—the first character in the target string. The regexp "^ab" will also yield one match—the first *two* characters in the target string.

[^...] The caret ("^") immediately following the left-bracket ("[") has a different meaning. It is used to exclude the remaining characters within brackets from matching the target string. The expression "[^0-9]" indicates that the target character should not be a digit.

(...) The parenthesis affects the order of pattern evaluation, and also serves as a *tagged* expression that can be used in *search and replace* expressions.

The results of a search with a regular expression are kept temporarily and can be used in the *replace* expression to build a new expression. In the *replace* expression, you can include a "$0" character, which will be replaced by the sub-string found by the regular expression during the search. So, if the *search* expression "a(bcd)e" finds a sub-string match, then a *replace* expression of "123-$0-123" will replace the matched text with "123-abcde-123".

Similarly, you can also use the special characters "$1," "$2," "$3," and so on in the *replace* expression. These characters will be replaced only be the results of the *tagged* expression instead of the entire sub-string match. The number following the backslash denotes which tagged expression you wish to reference (in the case of a regexp

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

containing more than one tagged expression). For example, if your *search* expression is "(123)(456)" and your *replace* expression is "a-$2-b-$1" then a matching sub-string will be replaced with "a-456-b-123" whereas a *replace* expression of "a-$0-b" will be replaced with "a-123456-b"

**$** The dollar sign ("$") denotes the end of the line. In the text string, "13 321 123" the expression "3$" will yield one match —the last character in the string. The regexp "123$" will also yield one match—the last *three* characters in the target string.

***** The asterisk ("*") quantifier indicates that the character to its left must match *zero or more* occurrences of the character in a row. Thus, "1*abc" will match the text "111abc" and "abc."

+ Similar to the asterisk quantifier, the "+" quantifier indicates that the character to its left must match *one or more* occurrences of the character in a row. Thus, "1+abc" will match the text "111abc" but not "abc."

? The question mark ("?") quantifier indicates that the character to its left must match *zero or one* times. Thus, "1?abc" will match the text "abc," and it will match the "1abc" portion of "111abc."

. The period or dot (".") metacharacter will match any other character. Thus ".+abc" will match "123456abc," and "a.c" will match "aac," abc," acc," and so on.

Eligible Conditions and Actions
Regular expressions may be used in any *Header* filter rule *Condition*. For example, any rule using the "`if the FROM HEADER contains`" condition. Regular expressions may also be used in the "`if the MESSAGE BODY contains`" condition.

Regular expressions may be used in two Content Filter rule *Actions*: "`Search and Replace Words in a Header`" and "`Search and Replace Words in the Message Body`."

Regular expressions used in Content Filter rule *conditions* are case insensitive. Case will not be considered.

Case sensitivity in regular expressions used in Content Filter rule *actions* is optional. When creating the regexp within the rule's action you will have the option to enable/disable case sensitivity.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Configuring a Regexp in a Rule's Condition

To configure a header or message body condition to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the header or message body condition that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**contains specific strings**" link that corresponds to the condition that you selected in step 1. This will open the Specify Search Text dialog.

3. Click the "**contains**" link in the "Currently specified strings..." area.

4. Choose "**Matches Regular Expression**" from the drop-down list box, and click **OK**.

5. If you need help creating your regexp or want to test it then click "**Test regular expression**." If you do not need to use the Test Regular Expression dialog then type your regexp into the text box provided, click **Add**, and then go to step 8.

6. Type your regular expression into the "Search expression" text box. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu. When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

7. Type any text that you wish to use to test your expression in the text area provided, and click **Test**. When you are finished testing your expression, click **OK**.

8. Click **OK**.

9. Continue creating your rule normally.

Configuring a Regexp in a Rule's Action

To configure a "Search and Replace Words in…" action to use a regular expression:

1. On the Create Rule dialog, click the checkbox that corresponds to the "*Search and Replace Words in...*" action that you wish to insert into your rule.

2. In the summary area at the bottom of the Create Rule dialog, click the "**specify information**" link that corresponds to the action that you selected in step 1. This will open the Search and Replace dialog.

3. If you chose the "*Search...header*" action in step 1, then use the drop-down list box provided to choose the header that you wish to search, or type a header into the box if the desired header isn't listed. If you did not choose the "*Search...header*" action in step 1 then skip this step.

4. Type the *search* expression that you wish to use in this action. To simplify the process we have provided a shortcut menu that can be used to easily insert the desired metacharacters into your regexp. Click the ">" button to access this menu.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

When you choose an option from this menu its corresponding metacharacter will be inserted into the expression and the text insertion point will be moved to the appropriate place required by the character.

5. Type the *replace* expression that you wish to use in this action. As with the *search* expression we have provided a metacharacter shortcut menu for this option as well. Leave this text box blank if you wish to delete a matched sub-string instead of replace it with more text.

6. Click "**Match case**" if you want the expression to be case sensitive.

7. Click Regular expression if you want the search and replace strings to be treated as regular expressions. Otherwise each will be treated as a simple sub-string search and replace—it will look for an exact literal match of the text rather than process it as a regular expression.

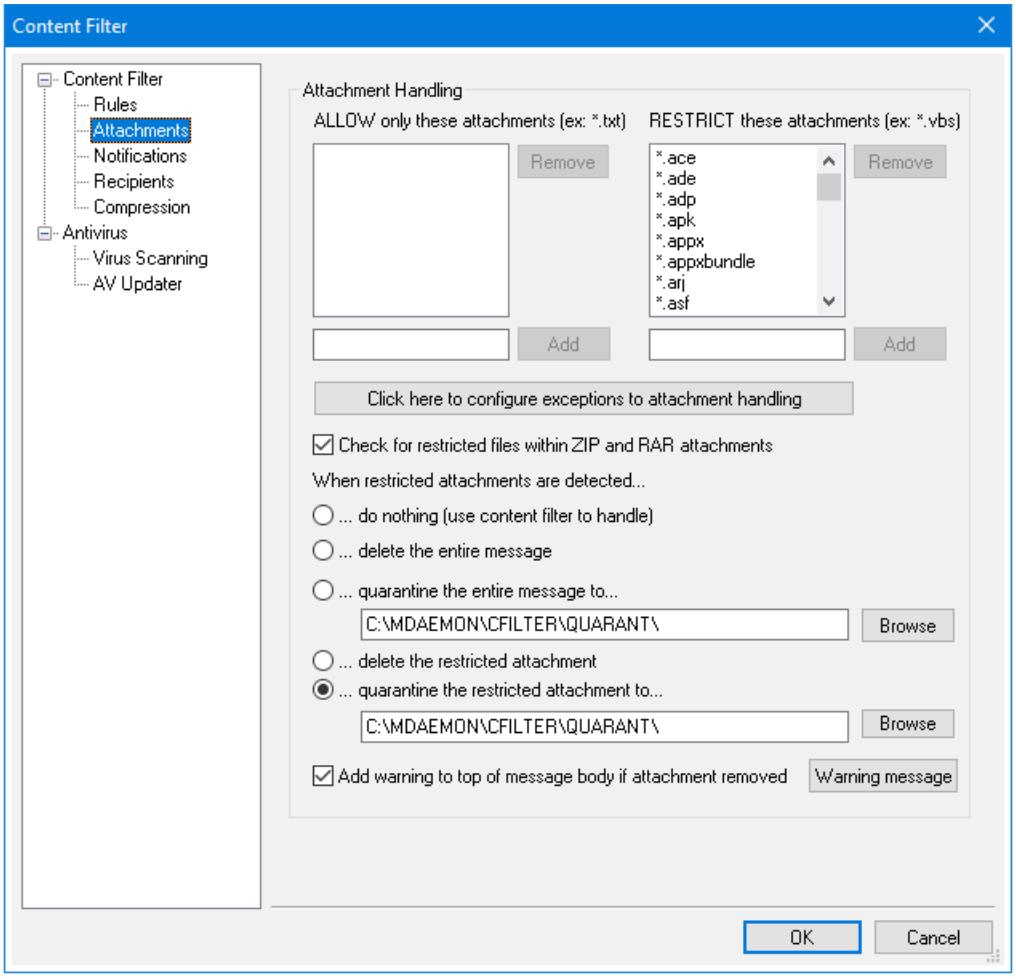
8. If you do not need to test your expression then skip this step. If you do need to test your expression then click "**Run Test**." On the Search and Replace Tester dialog, type your search and replace expressions and the text that you wish to test with, then click **Test**. When you are finished testing your regexps click **OK**.

9. Click **OK**.

10. Continue creating your rule normally.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.1.2 Attachments



Use this tab to specify attachments that you wish to classify as allowed or restricted. Attachments that are not allowed will be automatically removed from messages.

Attachment Handling

Filenames specified in *RESTRICT these attachments* list will be stripped from messages automatically when MDaemon encounters them. If you list any files in the *ALLOW only these attachments* list, then only those files listed will be permitted — all other attachments will be stripped from messages. After the attachment is stripped, MDaemon will continue normally and delivery the message without it. You can use the options on the Notifications tab to cause a notification message to be sent to various addresses when one of these restricted attachments is encountered.

Wildcards are permitted in list entries. An entry of "`*.exe`", for example, would cause all attachments ending with the `EXE` file extension to be allowed or removed. To add an entry to either of the lists, type the filename in the space provided and the click Add.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Click here to configure exceptions to attachment handling
Click this button to specify addresses that you wish to exclude from attachment restriction monitoring. When a message is directed to one of these addresses MDaemon will allow the message to pass even if it contains a restricted attachment.

Check for restricted files within ZIP and RAR attachments
Click this option if you wish to scan the contents of Zip, 7-Zip, and RAR compressed files for restricted attachments. Additionally, any Content Filter rule set to look for a particular filename will be triggered if a matching file is found within a compressed attachment.

When restricted attachments are detected...
Click the desired action to be taken when a message includes a restricted attachment.

...do nothing (use content filter to handle)
Choose this option if you do not wish to take a specific action based on the Attachments settings, but instead wish to base the actions on the Content Filter rules 631.

...delete the entire message
This option will delete the entire message when it contains a restricted attachment.

...quarantine the entire message to...
This option will cause messages with restricted attachments to be quarantined to the specified location.

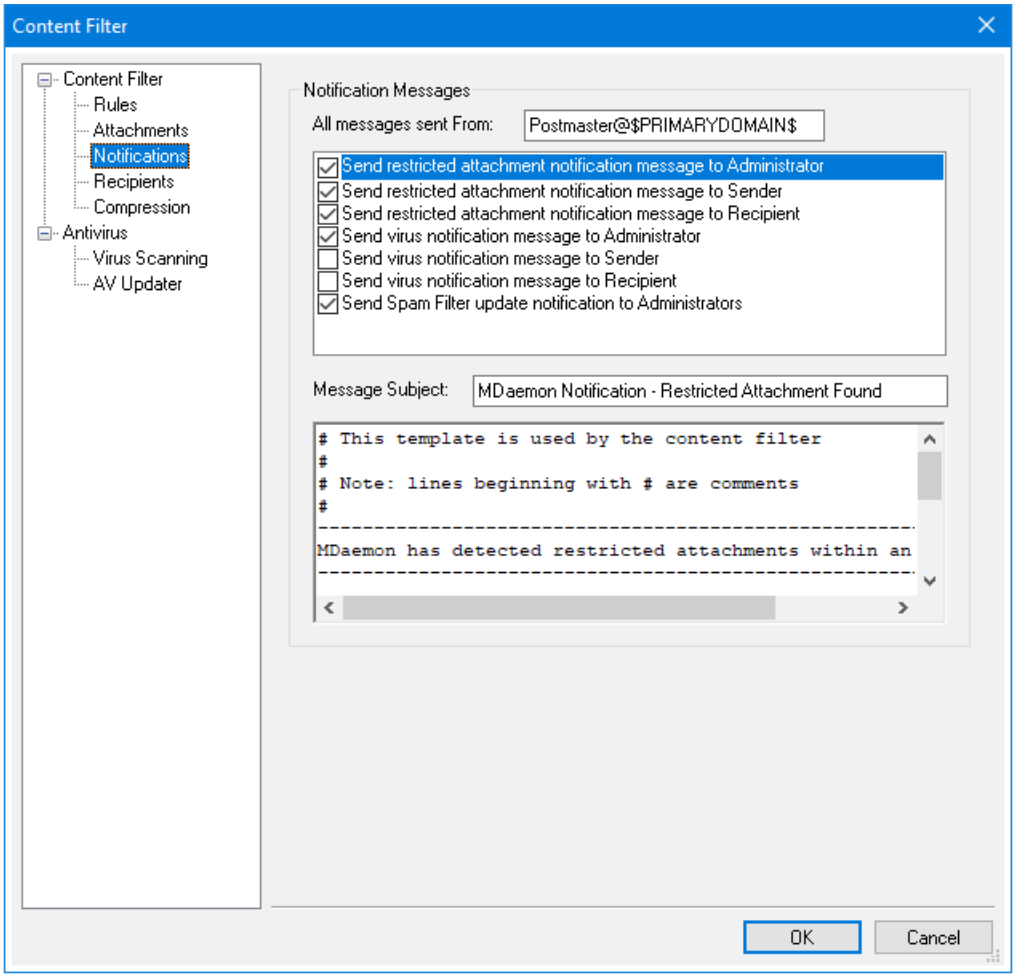
...delete the restricted attachment
Choose this option if you wish to delete any restricted attachments rather than delete the entire message.

...quarantine the restricted attachment to...
Click this option and specify a location if you wish to quarantine restricted attachments to a specific location rather than simply delete them. This is the default setting.

Add warning to top of message body if attachment is removed
When MDaemon removes an attachment from a message, for example because a virus was detected, it will add a warning message to the top of the message body. Click the **Warning** button if you wish to review or modify that message's template. This option is enabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.1.3 Notifications



Use this screen to designate those who should receive notification messages when a virus or restricted attachment is detected, or when the antivirus or Spam Filter files are updated.

Notification Messages

All messages sent From:
Use this box for specifying the address from which you wish the notification messages to be sent.

Send virus notification message to...
When a message arrives with a file attachment containing a virus, a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients 649 screen. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this screen. Each entry has its own message, though by default this isn't obvious since some are identical.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Send restricted attachment notification message to...
When a message arrives with a file attachment matching a restricted attachment entry (listed on the Attachments tab) a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Recipients tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

Send Spam Filter update notification to Administrators
Use this option if you wish to send an email to the administrators whenever the Spam Filter is updated, containing the results of the update. This option is the same as the "*Send notification email with results of update*" option located at: `Spam Filter » Updates`.

Message Subject:
This text will be displayed in the "Subject:" header of the notification message that is sent.

Message
This is the message that will be sent to the entry selected in the list above when the checkbox corresponding to that entry is enabled. You can directly edit this message from the box in which it is displayed.

The actual files containing this text are located in the `MDaemon\app\` directory. They are:

`cfattrem[adm].dat` – Restricted attachment message – Admins
`cfattrem[rec].dat` – Restricted attachment message – Recipient
`cfattrem[snd].dat` – Restricted attachment message – Sender
`cfvirfnd[adm].dat` – Virus found message – Admins
`cfvirfnd[rec].dat` – Virus found message – Recipient
`cfvirfnd[snd].dat` – Virus found message – Sender

Should you desire to restore one of these messages to its original appearance, simply delete the relevant file and MDaemon will recreate it in its default state.

4.6.1.3.1 Message Macros

For your convenience, certain macros may be used in the notification messages and other messages that the Content Filters generate. You may use any of the following macros:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

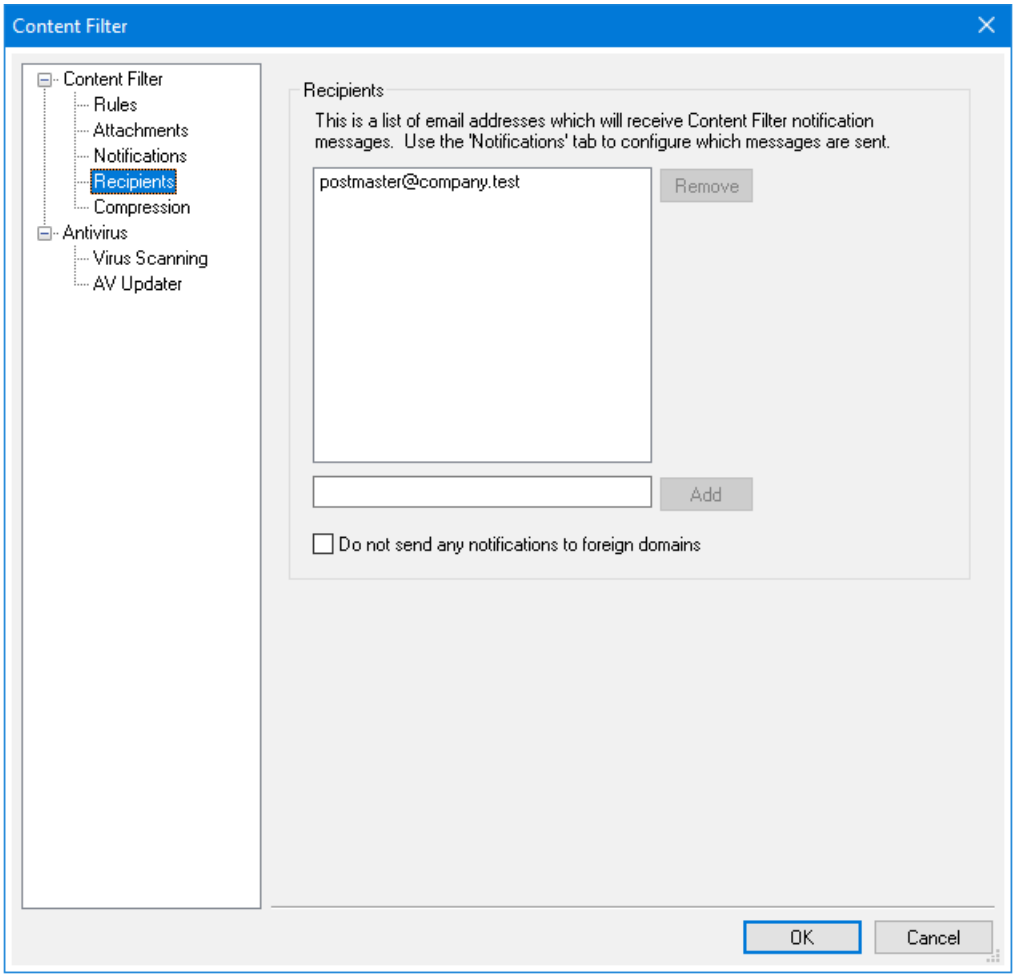
$ACTUALTO$	Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro is replaced with that value.
$AV_VERSION$	Lists the version of AntiVirus that you are using.
$CURRENTTIME$	This macro is replaced with the current time when the message is being processed.
$ACTUALFROM$	Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro is replaced with that value.
$FILTERRULENAME$	This macro is replaced by the name of the rule whose criteria the message matched.
$FROM$	Expands to the full address contained in the message's "From:" header.
$FROMDOMAIN$	This macro will insert the domain name contained in the address found in the message's "From:" header (the value to the right of "@" in the email address).
$FROMMAILBOX$	Lists the mailbox portion of the address found in the message's "From:" header (the value to the left of "@" in the email address).
GEN_GUID	Generates a unique ID with 11 alpha-numeric characters. Example: 0XVBASADTZC
$HEADER:XX$	This macro will cause the value of the header specified in place of the "xx" to be expanded in the reformatted message. For example: If the original message has "TO: user01@example.com" then the $HEADER:TO$ macro will expand to "user01@example.com". If the original message has "Subject: This is the subject" then the $HEADER:SUBJECT$ macro would be replaced with the text "This is the subject"
$HEADER:MESSAGE-ID$	As with $HEADER:XX$ above, this macro will expand to the value of the Message-ID header.
$LIST_ATTACHMENTS_REMOVED$	When one or more attachments are removed from the message, this macro will list them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$LIST_VIRUSES_FOUND$	When one or more viruses is found in a message, this macro will list them.
$MESSAGEFILENAME$	This macro expands to the file name of the current message being processed.
$MESSAGEID$	As $HEADER:MESSAGE-ID$ above, except this macro strips "<>" from the value of the message ID.
$PRIMARYDOMAIN$	Expands to MDaemon's Default Domain name, which is designated on the Domain Manager 174.
$PRIMARYIP$	This macro expands to the IPv4 address 177 of your Default Domain 174.
$PRIMARYIP6$	This macro expands to the IPv6 address 177 of your Default Domain 174.
$RECIPIENT$	This macro resolves to the full address of the message recipient.
$RECIPIENTDOMAIN$	This macro will insert the domain name of the message recipient.
$RECIPIENTMAILBOX$	Lists the recipient's mailbox (the value to the left of "@" in the email address).
$REPLYTO$	This macro expands to the value of the message's "Reply-to" header.
$SENDER$	Expands to the full address from which the message was sent.
$SENDERDOMAIN$	This macro will insert the domain name of the message's sender (the value to the right of "@" in the email address).
$SENDERMAILBOX$	Lists the sender's mailbox (the value to the left of "@" in the email address).
$SUBJECT$	Displays the text contained in the message's subject.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.1.4 Recipients



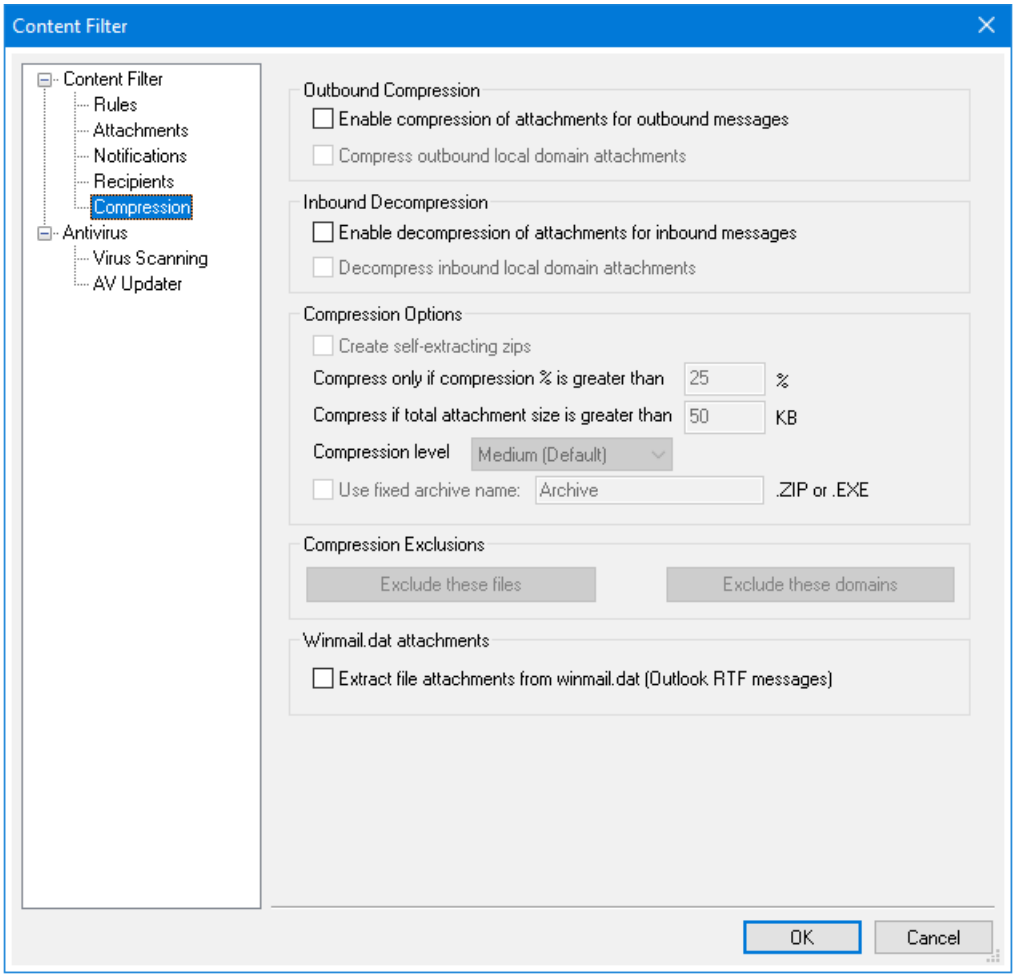
Recipients

This list of recipients corresponds to the various "*send...to administrator*" options located on the Notifications tab. These addresses will receive notification messages when one of the Administrator options is selected on that tab. To add an address to this section, type it into the space provided and then click *Add*. To remove an address, select it from the list and then click *Remove*.

Do not send any notifications to foreign domains
Check this box if you wish to restrict Content Filter notification messages to local domain recipients. This option is disabled by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.1.5 Compression



With the controls on this tab you can cause message attachments to be automatically compressed or decompressed before the message is delivered. The level of compression can be controlled as well as several other parameters and exclusions. This feature could significantly reduce the amount of bandwidth and throughput required to deliver your outbound messages.

Outbound Compression

Enable compression of attachments for outbound messages
Click this checkbox if you want to enable automatic message attachment compression for outbound remote mail messages. Enabling this control will not cause all message attachments to be compressed; it simply turns the feature on. Whether an outbound message's files are compressed or not is determined by the remaining settings on this tab.

Compress outbound local domain attachments
Enabling this control will cause the file compression settings to be applied to all outbound mail – even those messages whose destination is another local address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Inbound Compression

Enable decompression of attachments for inbound messages
Click this checkbox if you want to enable automatic decompression of inbound remote mail message attachments. When a message arrives with a zipped attachment, MDaemon will decompress it before delivering it to the local user's mailbox.

Decompress inbound local domain attachments
Enable this control if you want automatic decompression to apply to local mail as well.

Compression Options

Create self-extracting zips
Click this checkbox if you want the compression files that MDaemon creates to be self-extracting zip files with an `EXE` file extension. This is useful if you are concerned that the message recipients may not have access to a decompression utility. Self-extracting zip files can be decompressed simply by double-clicking on them.

Compress only if compression % is greater than XX%
MDaemon will not compress a message's attachments before sending it unless they can be compressed by a percentage greater than the value specified in this control. For example, if you designate a value of 20 and a given attachment can't be compressed by at least 21% then MDaemon will not compress it before sending the message.

MDaemon must first compress a file to determine by what percentage it can be compressed. Thus, this feature does not prevent files from being compressed – it simply prevents file attachments from being sent in a compressed format when they cannot be compressed beyond the designated value. In other words, if after compressing the file MDaemon finds that it couldn't be compressed by more than this value, the compression will be disregarded and the message will be delivered with its attachments unchanged.

Compress if total attachment size is greater than XX KB
When automatic attachment compression is enabled, MDaemon will only attempt to compress a message's attachments when their total size exceeds the value specified here. Messages with total attachment sizes below this threshold will be delivered normally with the attachments unchanged.

Compression level
Use the drop-down list box to choose the degree of compression that you want MDaemon to apply to automatically compressed attachments. You can choose three levels of compression: minimum (fastest compression process with least compression), medium (default value), or maximum (slowest compression process but highest degree of compression).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use fixed archive name: [archive name]
Click this checkbox and choose a name if you want the automatically compressed attachments to have a specific filename.

Compression exclusions

Exclude these attachments...
Click this button to specify files that you want to exclude from the automatic compression features. When a message attachment matches one of these filenames it will not be compressed, regardless of the compression settings. Wildcards are permitted in these entries. Therefore, you could specify "*.exe", for example, and all files ending with ".exe" would remain uncompressed.

Exclude these domains...
Click this button to specify recipient domains whose messages you wish to exclude from automatic compression. Messages bound for these domains will not have their file attachments compressed, regardless of your compression settings.

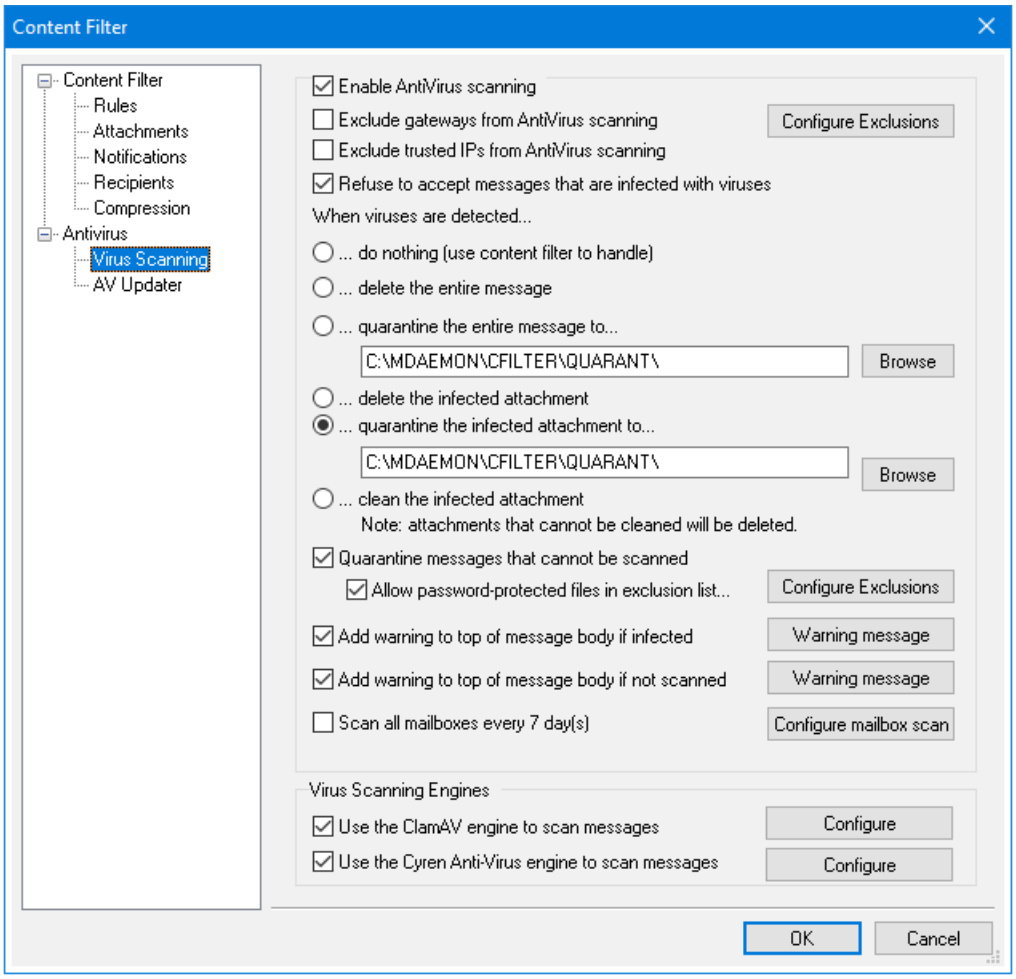
Winmail.dat attachments

Extract file attachments from winmail.dat (Outlook RTF messages)
Enable this option if you wish to extract files from inside winmail.dat attachments and turn them into standard MIME message attachments.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.6.2 AntiVirus

4.6.2.1 Virus Scanning



The options on this screen will only be available when using the optional MDaemon AntiVirus 653 feature. Enabling MDaemon AntiVirus for the first time will start a 30-day trial. If you wish to purchase this feature, contact your authorized MDaemon reseller or visit: www.mdaemon.com.

Enable AntiVirus scanning

Click this checkbox to enable AntiVirus scanning of messages. When MDaemon receives a message with attachments, it will scan them for viruses before delivering the message to its final destination.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Exclude gateways from AntiVirus scanning
Click this checkbox if you want messages bound for one of MDaemon's domain gateways to be excluded from virus scanning. This may be desirable for those who wish to leave the scanning of those messages to the domain's own mail server. For more information on domain gateways, see Gateway Manager 239.

Configure Exclusions
Click the Configure Exclusions button to specify recipient addresses to exclude from virus scanning. Messages bound for these addresses will not be scanned for viruses. Wildcards are allowed in these addresses. You could therefore use this feature to exclude entire domains or specific mailboxes across all domains. For example, "*@example.com or "VirusArchive@*".

Exclude Trusted IPs from AntiVirus scanning
Click this checkbox if you wish to exempt messages from AntiVirus scanning when coming from one of your Trusted IP addresses 506.

Refuse to accept messages that are infected with viruses
Click this option is you wish to scan incoming messages for viruses during the SMTP session rather than after the session is concluded, and then reject those messages found to contain viruses. Because each incoming message is scanned before MDaemon officially accepts the message and concludes the session, the sending server is still responsible for it—the message hasn't technically been delivered yet. Thus the message can be rejected outright when a virus is found. Further, because the message was rejected, no further AntiVirus related actions listed on this dialog will be taken. No quarantine or cleaning procedures will be taken, and no notification messages will be sent. This can greatly reduce the number of infected messages and virus notification messages that you and your users receive.

The SMTP-(in) log will show the result of AV processing. The possible results you might see are:

- the message was scanned and found infected with a virus
- the message was scanned and no virus was found
- the message could not be scanned (usually because a ZIP or other type or attachment could not be opened/accessed)
- the message could not be scanned (it exceeds the max size limit)
- an error occurred during the scan

When viruses are detected...
Click one of the options in this section to designate the action that MDaemon will take when AntiVirus detects a virus.

...do nothing (use content filter to handle)
Choose this option if you wish to take none of the above actions, and have set up content filter rules to take some alternative actions instead.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...delete the entire message
This option will delete the entire message rather than just the attachment when a virus is found. Because this deletes the whole message, the "*Add a warning...*" option doesn't apply. However, you can still send a notification message to the recipient by using the controls on the Notifications tab.

...quarantine the entire message to...
This option is like the "*Delete the entire message*" option above, but the message will be quarantined in the specified location rather than deleted.

...delete the infected attachment
This option will delete the infected attachment. The message will still be delivered to the recipient but without the infected attachment. You can use the "*Add a warning...*" control on the bottom of this dialog to add text to the message informing the user that an infected attachment was deleted.

...quarantine the infected attachment to...
Choose this option and specify a location in the space provided if you want infected attachments to be quarantined to that location rather than deleted or cleaned. Like the "*Delete the infected attachment*" option, the message will still be delivered to the recipient but without the infected attachment.

...clean the infected attachment
When this option is chosen, AntiVirus will attempt to clean (i.e. disable) the infected attachment. If the attachment cannot be cleaned, it will be deleted.

Quarantine messages that cannot be scanned
When this option is enabled, MDaemon will quarantine any messages it is unable to scan, such as some containing password-protected files.

Allow password-protected files in exclusion list...
Use this option if you wish to allow a message with a password-protected, non-scannable file to pass through the AntiVirus scanner if the file name or type is in the exclusion list.

Configure Exclusions
Click this button to open and manage the file exclusion list. File name and types included on this list will not be scanned.

Add warning to top of message body if infected
When one of the "*...attachment*" options is chosen above, click this option if you want to add some warning text to the top of the previously infected message before it is delivered to the recipient. Thus you can inform the recipient that the attachment was stripped and why.

Warning message...
Click this button to display the warning text that will be added to messages when the "*Add a warning message...*" feature is used. After making any desired changes to the text, click **OK** to close the dialog and save the changes.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Add warning to top of message body if not scanned
When this option is enabled, MDaemon will add some warning text to the top of any message it is unable to scan.

Warning message...
Click this button to display the warning text that will be added to messages that cannot be scanned. After making any desired changes to the text, click **OK** to close the dialog and save the changes.

Scan all mailboxes every *n* day(s)
Check this box if you wish to scan all stored messages periodically, to detect any infected message that may have passed through the system before a virus definition update was available to catch it. Infected messages will be moved to the quarantine folder and have the `X-MDBadQueue-Reason` header added, so that you can see an explanation when viewed in MDaemon. Messages that cannot be scanned will not be quarantined.

Configure mailbox scan.
Click this button to specify how often you wish to scan the mailboxes and whether you wish to scan all message or only those that are less than a certain number of days old. You can also manually run a mailbox scan immediately.

Virus Scanning Engines

MDaemon AntiVirus is equipped with two virus scanning engines: ClamAV and IKARUS Anti-Virus. When both are enabled, messages will be scanned by both engines; first by IKARUS Anti-Virus and then by ClamAV. This provides an extra layer of protection, since a virus could potentially be identified by one engine before the virus definitions of the other engine have been updated.

Use the ClamAV engine to scan messages
Click this checkbox if you wish to use the ClamAV engine to scan messages for viruses.

Configure
Click this button to access an option to activate debug logging for ClamAV. The log file will be located in MDaemon's log folder.

Use the IKARUS Anti-Virus engine to scan messages
Click this checkbox if you wish to use the IKARUS Anti-virus engine to scan messages for viruses.

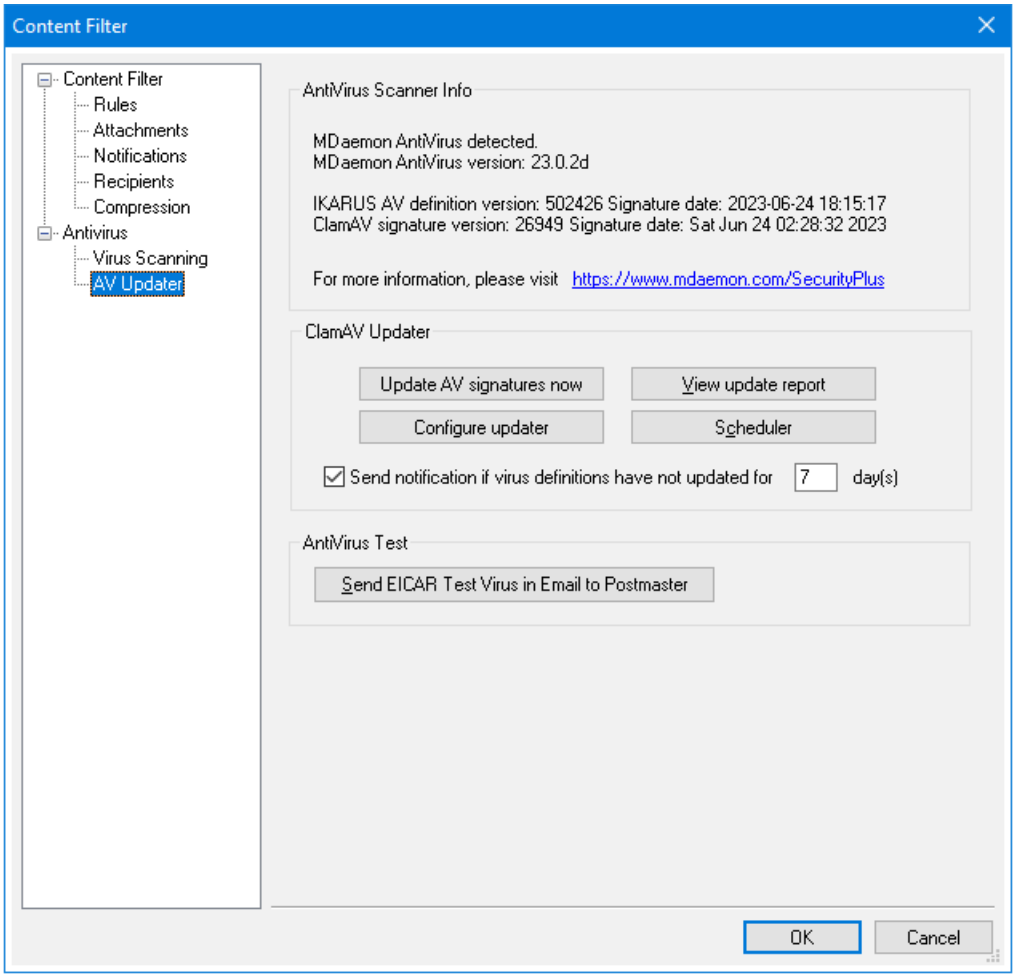
Configure
Use this option if you wish to flag as a virus, attachments with documents that contain macros. You can set a heuristics level from -1 to 5. "-1" is auto, "0" is disabled, and 1-5 is lowest to highest heuristics level.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

AV Updater 657
Content Filter and AntiVirus 630

4.6.2.2 AV Updater



Some of the options on this screen will only be available when using the optional MDaemon AntiVirus 653 feature. Enabling MDaemon AntiVirus for the first time will start a 30-day trial. If you wish to purchase this feature, contact your authorized MDaemon reseller or visit: www.mdaemon.com.

Use the controls on this screen to manually or automatically update your virus definitions. There is a scheduler for automatic updating, a report viewer so that you can review when and which updates have been downloaded, and a test feature used for confirming that virus scanning is working properly.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

AntiVirus Scanner Info

This section tells you whether AntiVirus is available and what version you are running. It also lists the date of your last virus definition update.

ClamAV Updater

Update AV signatures now

Click this button to update the virus definitions manually. The updater will connect immediately after the button is pressed.

Configure updater

Click this button to open the Updater Configuration dialog 659. This dialog contains four tabs: Update URLs, Connection, Proxy, and Misc.

View update report

The AntiVirus Log Viewer is opened by clicking the *View update report* button. The viewer lists the times, actions taken, and other information about each update.

Scheduler

Click this button to open the AntiVirus Scheduling 370 screen, used for scheduling checks for virus signature updates at specific times on specific days or at regular intervals.

Send notification if virus definitions have not updated for xx day(s)

By default the administrator will be notified if the ClamAV virus definitions have not been updated for the specified number of days.

AntiVirus Test

Send EICAR Test Virus in Email to Postmaster

Click this button to send a test message to the postmaster, with the EICAR virus file attached. This attachment is harmless – it is merely used for an antivirus test. By watching the Content Filter's log window on MDaemon's main interface you can see what MDaemon does with this message when it is received. For example, depending upon your settings, you might see a log excerpt that looks something like the following:

```
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)
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
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)
```

See:

Updater Configuration Dialog 659
AntiVirus 653
Content Filter and AntiVirus 630

4.6.2.2.1 Updater Configuration Dialog

Click the *Configure updater* button on the AV Updater 657 screen to open the Updater Configuration dialog. It contains the following four tabs:

Update URLs
The Update URLs tab is used to designate the servers that AntiVirus will check for updates. You can set the order in which the servers will be checked or cause them to be checked in random order.

Connection
The Connection tab is used to designate the Internet Connection Profile that AntiVirus will use when connecting to the update sites. The "*Use Internet Settings from Control Panel*" option uses your default Internet settings. The "*Setup Internet settings manually*" option and subsequent controls can be used to manually choose a Connection Profile and designate its user name and password settings.

Proxy
The Proxy tab contains options for configuring any HTTP or FTP proxy settings that your current network configuration may require in order to connect to the update sites.

Misc
The Misc tab contains options governing updater logging. You can choose to log updater actions in a log file, and you can specify a maximum size for the file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

AV Updater 657
AntiVirus 653
Content Filter and AntiVirus 630

4.7 Spam Filter

4.7.1 Spam Filter

The Spam Filter is one of the main features in MDaemon's extensive suite of spam prevention tools. It incorporates heuristics to examine incoming email messages in order to compute a "score" based on a complex system of rules. The score is then used to determine the likelihood of a message being spam, and certain actions can be taken based on that score — you can refuse the message, flag it as possible spam, and so on.

Addresses can be allowed or blocked, or designated as completely exempt from Spam Filter examination. You can have a spam report inserted into messages, showing their spam scores and how those scores were achieved, or you can generate the report as a separate email and have the original spam message included with it as an attachment. Further, you can even use Bayesian 664 learning to help the Spam Filter learn to identify spam more accurately over time, thus increasing its reliability.

Finally, by examining many thousands of known spam messages, the rules have been optimized over time and are very reliable in detecting the fingerprint of a spam message. You can, however, customize or add new rules by editing the Spam Filter's configuration files to meet your specific needs.

MDaemon's Spam Filter uses an integrated, popular open-source heuristic technology. The homepage for the open-source project is:

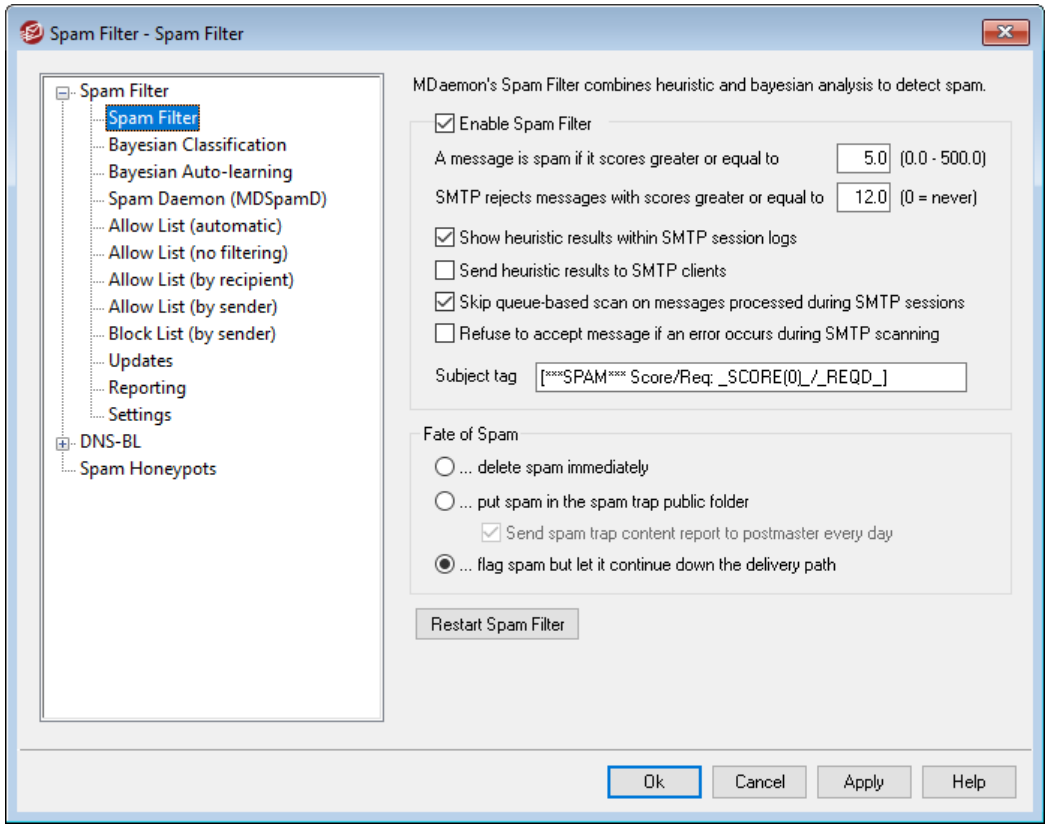
```
http://www.spamassassin.org
```

See:

Spam Filter 661
DNS Block Lists 683

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.7.1.1 Spam Filter



Enable Spam Filter

Check this box to activate the heuristic message-scoring, spam filtering system. None of the other Spam Filter options on this screen will be available until this option is enabled.

A message is spam if its score is greater or equal to [XX] (0.0-500.0)
The value that you specify here is the required spam threshold that MDaemon will compare to each message's spam score. Any message with a spam score greater than or equal to this amount will be considered spam, and then the appropriate actions will be taken based on your other Spam Filter settings.

SMTP rejects messages with scores greater or equal to XX (0=never)
Use this option to designate a spam score rejection threshold. When a message's spam score is greater than or equal to this score it will be rejected completely rather than proceed through the rest of the options and possibly be delivered. The value of this option should always be greater than the value of the "*A message is spam if its score...*" option above. Otherwise, a message would never be considered spam and have the rest of the Spam Filter's options applied to it—it would simply be rejected during delivery. Use "0" in this option if wish to disable scanning during the SMTP process, and if you do not want MDaemon to reject any messages regardless of their scores. If SMTP scanning is disabled then a queue-based scan will still be performed on the messages after they are accepted. The default setting for this option is "12.0".

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Example,

If you have the spam score threshold set to 5.0 and the rejection threshold set to 10.0, then any message with a spam score that is greater than or equal to 5.0 but less than 10.0 will be considered spam and handled according to the rest of your Spam Filter settings. Any message with a spam score greater than or equal to 10.0 will be rejected by MDaemon during the delivery process.

You should monitor the spam filter's performance over time and refine both the spam and rejection thresholds to suit your need. For most people, however, a spam score threshold of 5.0 will catch most spam, with relatively few false negatives (spam that slips through unrecognized) and rarely any false positives (messages flagged as spam that are not). A rejection threshold of 10-15 will cause only messages that are almost certainly spam to be rejected. It is extremely rare that a legitimate message will have a score that high. The default rejection threshold is 12.

Show heuristic results within SMTP session logs
Click this option to log the results of heuristic processing during SMTP sessions to the SMTP session logs 168.

Send heuristic results to SMTP clients
Click this option to display heuristic processing results inline with SMTP session transcripts. This option is not available when you have your Spam Score rejection threshold set to "0", meaning that spam will never be rejected because of its score. For more information see, "*SMTP rejects messages with scores greater or equal to XX (0=never)*" above.

Skip queue-based scan on messages processed during SMTP sessions
By default, MDaemon scans messages during the SMTP session to determine whether or not they should be rejected for having a spam score above the rejection threshold. For messages that are accepted MDaemon will then perform another, queue-based, scan and treat the messages accordingly, based on their scores and your spam filter configuration. Click this option if you want MDaemon to omit the queue-based scan and treat the results of the initial Spam Filter scan as definitive. This can potentially significantly decrease CPU usage and increase the efficiency of the AntiSpam system. However, only the default SpamAssassin headers will be added to messages when the queue-based scan is omitted. If you have made any changes to the default SpamAssassin headers or specified custom headers in your `local.cf` file, those changes and additions will be ignored.

Refuse to accept message if an error occurs during SMTP scanning
Click this option if you want a message to be refused when an error is encountered while it is being scanned during the SMTP process.

Subject tag
This tag will be inserted at the beginning of the Subject header of all messages that meet or exceed the required spam score threshold. It can contain information about

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the spam score, and you can use your IMAP message filters to search for it and filter the message accordingly (assuming that you have the Spam Filter configured to continue delivering spam messages). This is a simple method for automatically routing spam messages to a designated "spam" folder. If you want to dynamically insert the message's spam score and the value of the required spam threshold then use the tag "_HITS_" for the message's score and "_REQD_" for the required threshold. Alternatively, you can use "_SCORE(0)_" instead of "_HITS_"— this will insert a leading zero into lower scores, which can help ensure the proper sort-order when sorting messages by subject in some email clients.

Example,

A subject tag set to: `***SPAM*** Score/Req: _HITS_/_REQD_ -`
will cause a spam message with a score of 6.2 and the subject: "Hey, here's some spam!" to be changed to "***SPAM*** Score/Req: 6.2/5.0 – Hey, here's some spam!"

If "_SCORE(0)_" is substituted for "_HITS_" then it would be changed to "***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"

If you do not wish to alter the subject header then leave this option blank. No subject tag will be inserted.

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. The Subject tag configuration will be determined by the other server's settings. See: Spam Daemon 670, for more information.

Fate of Spam

The Spam Filter will perform the action chosen below if a message's spam score is greater than or equal to the spam score specified above.

...delete spam immediately
Choose this option if you wish simply to delete any incoming message whose spam score is equal to or exceeds the designated limit.

...put spam in the spam trap public folder
Choose this option if you want to flag messages as spam and then move them to the spam public folder rather than allow them to be delivered.

Send spam trap content report to postmaster every day
When using the *...put spam in the spam trap public folder* option above, check this box if you would like the postmaster to receive a daily message with a summary of the folder's contents.

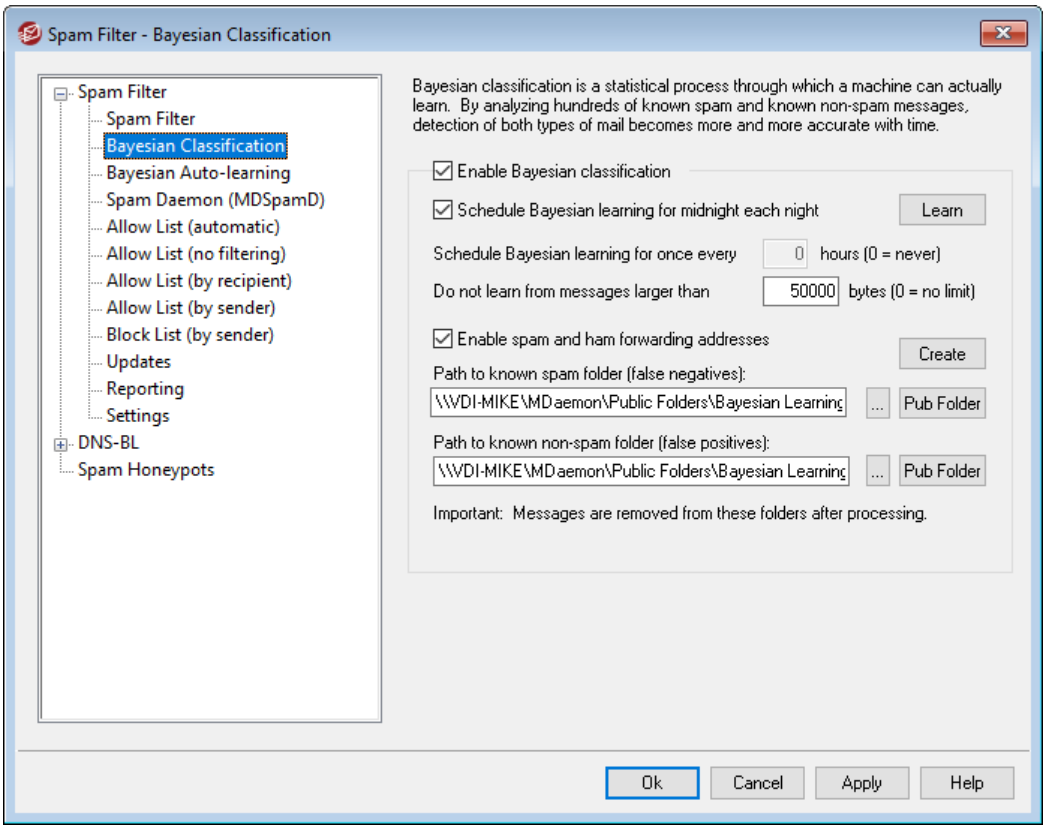
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...flag spam but let it continue down the delivery path
Choose this option if you want to go ahead and deliver each spam message to its intended recipient, but flag it as spam by inserting various spam headers and/or tags designated above and on the Reporting 680 screen. This is the default option, which allows users to take advantage of options such as filtering mail into a spam folder for their review and thus avoid losing messages that may be erroneously labeled as spam (i.e. false positives).

Restart Spam Filter

Click this button to restart the Spam Filter engine.

4.7.1.2 Bayesian Classification



Bayesian Classification is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 670 screen for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The Spam Filter supports Bayesian learning, which is a statistical process that can optionally be used to analyze spam and non-spam messages in order to increase the reliability of spam recognition over time. You can designate a folder for spam messages and non-spam message that will can be scanned manually or automatically at regular intervals. All of the messages in those folders will be analyzed and indexed so that new messages can be compared to them statistically in order to determine the likelihood that they are spam. The Spam Filter can then increase or decrease a message's spam score based upon the results of its Bayesian comparison.

The Spam Filter will not apply a Bayesian classification to messages until a Bayesian analysis has been performed on the number of spam and non-spam messages designated on the Bayesian Auto-learning 668 screen. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

Bayesian Classification

Enable Bayesian classification
Click this check box if you want each message's spam score to be adjusted based on a comparison to the currently known Bayesian statistics.

Schedule Bayesian learning for midnight each night
When this option is active, once each day at midnight the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you wish to schedule Bayesian learning for some other time interval then clear this option and use the *Schedule Bayesian learning for once every XX hours* option below. If you do not wish Bayesian learning to ever occur automatically, then clear this option and specify "0" hours in the option below.

Schedule Bayesian learning for once every XX hours (0=never)
If you wish Bayesian learning to occur at some time interval other than once each night at midnight, then clear the above option and specify a number of hours in this option instead. Each time that number of hours has elapsed, the Spam Filter will analyze and then delete all messages contained in the spam and non-spam folders specified below. If you do not wish Bayesian learning to ever occur automatically, then clear the above option and specify "0" hours in this option.

If for some reason you do not want the messages to be deleted after they are analyzed then you can prevent that by copying `LEARN.BAT` to `MYLEARN.BAT` in the `\MDaemon\App\` subfolder and then deleting the two lines that begin with "`if exist`" near the bottom in that file. When the `MYLEARN.BAT` file is present in that folder MDaemon will

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

use it instead of LEARN.BAT. See SA-Learn.txt in your \MDaemon\SpamAssassin\ subfolder for more information.

For more detailed information on heuristic spam filtering technology and Bayesian learning, visit:

http://www.spamassassin.org/doc/sa-learn.html

Don't learn from messages larger than XX bytes (0=no limit)
Use this option to designate a maximum message size for Bayesian analysis. Messages larger this value will not be analyzed. Specify "0" in this option if you do not wish to implement any size restriction.

Learn
Click this button to initiate a manual Bayesian analysis of the designated folders rather than waiting for the automatic analysis.

Enable spam and ham forwarding addresses
Click this check box if you wish to allow users to forward spam and non-spam (ham) messages to designated addresses so that the Bayesian system can learn from them. The default addresses that MDaemon will use are "SpamLearn@<domain>" and "HamLearn@<domain>". Messages sent to these addresses must be received via SMTP from a session that is authenticated using SMTP AUTH. Further, MDaemon expects the messages to be forwarded to the above addresses as attachments of type "message/rfc822". Any message of another type that is sent to these email addresses will not be processed.

You can change the addresses MDaemon uses by adding the following key to the CFilter.INI file:

```
[SpamFilter]
SpamLearnAddress=MySpamLearnAddress@
HamLearnAddress=MyNonSpamLearnAddress@
```

Note: the last character of these values must be "@".

Create
Click this button to create spam and non-spam Public IMAP Folders automatically, and to configure MDaemon to use them. The following folders will be created:

\Bayesian Learning.IMAP\	Root IMAP folder
\Bayesian Learning.IMAP\Spam.IMAP\	This folder is for false negatives (spam that doesn't score high enough to get flagged as such).
\Bayesian Learning.IMAP\Non-Spam.IMAP\	This folder is for false positives (non-spam messages that

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

erroneously score high enough to get flagged as spam).

By default, access permission to these folders is only granted to local users of local domains and is limited to Lookup and Insert. The postmaster's default permissions are Lookup, Read, Insert, and Delete.

Path to known spam folder (false negatives):
This is the path to the folder that will be used for Bayesian analysis of known spam messages. Only copy messages to this folder which you consider to be spam. You should not automate the process of copying messages to this folder unless doing so via the Bayesian Auto-learning 668 or Spam Honeypots 690 options. Automating this process by some other means could potentially cause non-spam messages to be analyzed as spam, which would decrease the reliability of the Bayesian statistics.

Path to known non-spam folder (false positives):
This is the path to the folder that will be used for Bayesian analysis of messages that are definitely **not** spam. Only messages that you do **not** consider to be spam should be copied to this folder. You should not automate the process of copying messages to this folder unless doing so via the Bayesian Auto-learning 668 options. Automating this process by some other means could potentially cause spam messages to be analyzed as non-spam, which would decrease the reliability of the Bayesian statistics.

Pub Folder
Click one of these buttons to designate one of your existing Public Folders as the Bayesian directory. This is an easy way for your users to place their messages incorrectly categorized as spam or non-spam into your Bayesian directories for analysis. Note, however, that giving access to more people increases the likelihood that some messages will be put into the wrong folders thus skewing the statistics and decreasing reliability.

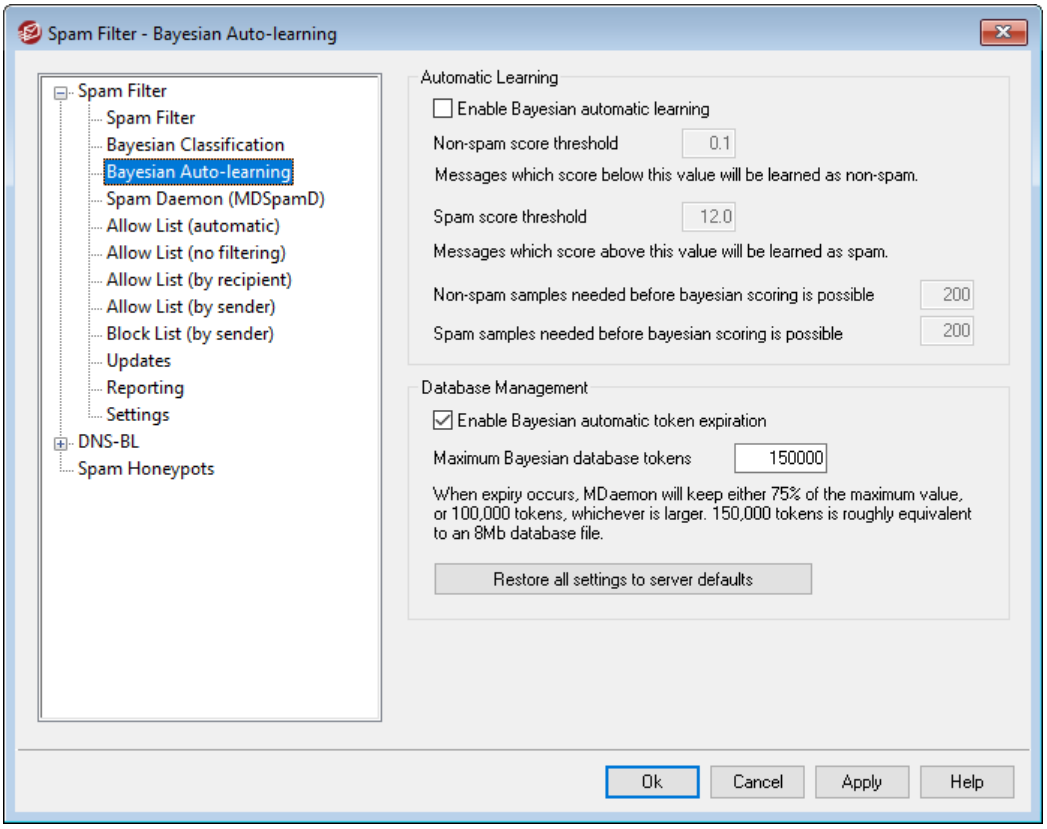
If you rename a Public folder via a mail client, Windows Explorer, or some other means, then you must manually reset this path to the appropriate new folder name. If you rename a folder but do not change its path here, the Spam Filter will continue to use this path for the Bayesian folder instead of the new one.

See:

Bayesian Auto-learning 668
Spam Honeypots 690

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.7.1.3 Bayesian Auto-learning



Bayesian Auto-learning is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning will be performed on the other server. See the Spam Daemon 670 screen for more information.

Automatic Learning

Enable Bayesian automatic learning
With automatic Bayesian learning you can designate spam and non-spam scoring thresholds, which make it possible for the Bayesian learning system to learn from messages automatically rather than requiring you to manually place those messages in the spam and non-spam folders. Any message scoring below the non-spam threshold will be treated by automatic learning as non-spam, and any message scoring above the spam threshold will be treated as spam. With automatic learning, old expired tokens that are removed from the database (see *Database Management* below) can be replaced automatically. This prevents the need for manual retraining to recover expired tokens. Automatic Learning can be useful and beneficial as long if

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

you are careful in setting your thresholds, to avoid placing improperly classified messages in the folders.

Non-spam score threshold
Messages with a spam score below this value will be treated as non-spam messages by the Bayesian Classification system.

Spam score threshold
Messages with a spam score above this value will be treated as spam messages by the Bayesian Classification system.

Non-spam samples needed before Bayesian scoring is possible
The Spam Filter will not apply a Bayesian classification to messages until this number of non-spam messages (and spam messages specified in the next option) has been analyzed by the Bayesian system. This is necessary in order for the Spam Filter to have a sufficient pool of statistics to draw from when making the Bayesian comparison. Once you have given the system these messages to analyze, it will be sufficiently equipped to begin applying the results of a Bayesian comparison to each incoming message's spam score. By continuing to analyze even more messages the Bayesian classifications will become more accurate over time.

Spam samples needed before Bayesian scoring is possible
Just as the previous option applies to non-spam messages, this option is for designating the number of *spam* messages that must be analyzed before the Spam Filter will begin applying a Bayesian classification to messages.

Database Management

Enable Bayesian automatic token expiration
Click this option if you want the Bayesian system to automatically expire database tokens whenever the number of tokens specified below is reached. Setting a token limit can prevent your Bayesian database from getting excessively large.

Maximum Bayesian database tokens
This is the maximum number of Bayesian database tokens allowed. When this number of tokens is reached, the Bayesian system removes the oldest, reducing the number to 75% of this value, or to 100,000 tokens, whichever is higher. The number of tokens will never fall below the larger of those two values regardless of how many tokens are expired. Note: 150,000 database tokens is approximately 8Mb.

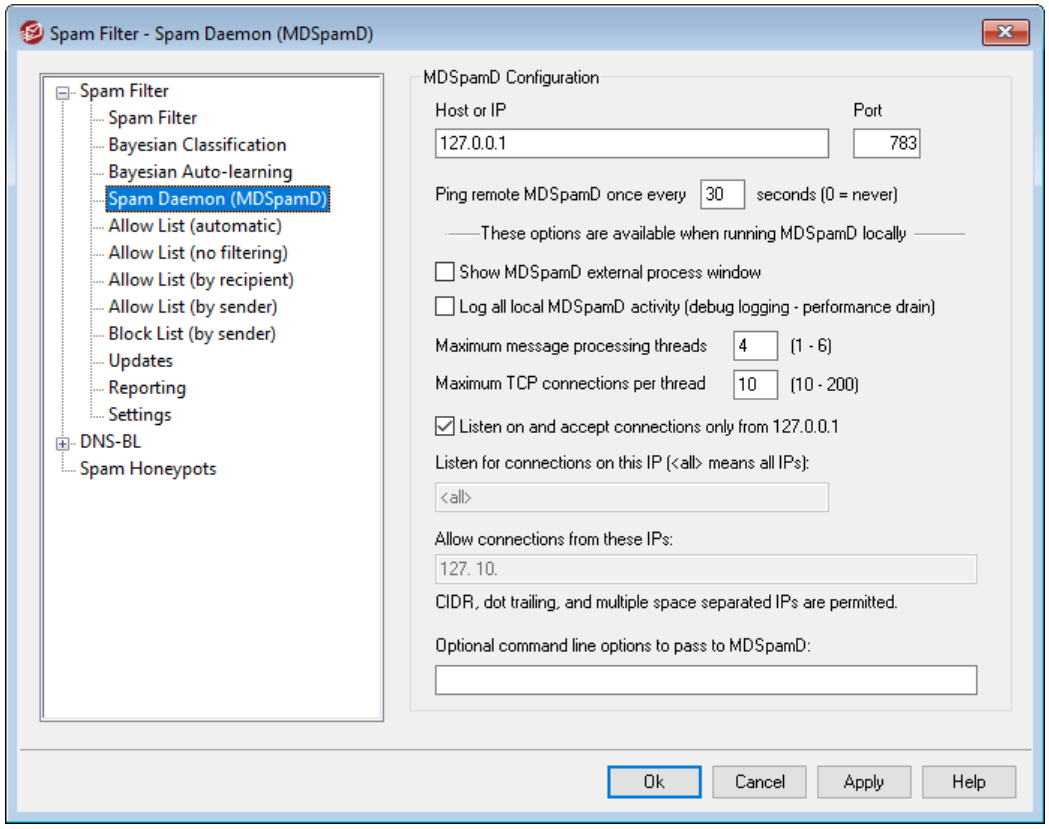
Restore all settings to server defaults
Click this button to restore all of the Bayesian advanced options to their default values.

See:

Bayesian Classification 664
Spam Honeypots 690

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.7.1.4 Spam Daemon (MDSpamD)



MDaemon's spam filtering system runs as a separate daemon—the MDaemon Spam Daemon (MDSpamD), which is fed messages via TCP/IP for scanning. This greatly increases the Spam Filter's performance and makes it possible for you to run MDSpamD locally, on a separate computer, or have MDaemon use another MDSpamD (or any other Spam Daemon enabled product) running at some other location. By default MDSpamD runs locally and receives messages on port 783 at 127.0.0.1, but you can configure a different port and IP address if wish to send the messages to some other spam daemon running at a different location or on a different port.

MDSpamD Configuration

Host or IP
This is the host or IP address to which MDaemon will send messages to be scanned by MDSpamD. Use `127.0.0.1` if MDSpamD is running locally.

Port
This is the port on which the messages will be sent. The default MDSpamD port is 783.

Ping remote MDSpamD once every XX seconds (0=never)
If you are using a spam daemon that is running at a remote location, you can use this option to ping its location periodically. Use "0" if you do not wish to ping that location.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

These options are available when running MDSpamD locally

Show MDSpamD external process window
When MDSpamD is running locally, enable this option if you would like it to run in an external process window. This option will cause the output from MDSpamD to be piped to the external process window rather than to MDaemon's internal UI or logging system. Using this option could increase performance since MDSpamD's data will not have to be piped into and logged by MDaemon. However, no log file will be created and as such this feature cannot be used with the logging option below, nor will MDSpamD data appear in the *Security»MDSpamD* tab of MDaemon's main GUI.

Log all local MDSpamD activity (debug logging—performance drain)
Click this option if you wish to log all MDSpamD activity. This option is unavailable if you are using the *Show MDSpamD external process window* option above. Further, if using user credentials on the Windows Service 399 dialog rather than running MDaemon under the SYSTEM account, no MDSpamD activity will be logged.

When using this logging option, you may see decreased performance in your mail system, depending on your system and the level of activity. Generally you should only use this option for debugging purposes.

Maximum message processing threads (1-6)
This is the maximum number of threads that MDaemon will use for internal processing. You can set this value from 1 to 6.

Maximum TCP connections per thread (10-200)
This is the maximum number of TCP connections accepted by an MDSpamD thread before it branches into another thread. You can set this value from 10 to 200.

Listen on and accept connections only from 127.0.0.1
Click this option if do not you wish to allow your local MDSpamD to accept connections from any external source. Only connections from the same machine on which it is running will be allowed.

Listen for connections on this IP
If the previous option is disabled, you can use this option to bind or restrict connections to a specific IP address. Only connections to the designated IP address will be allowed. Use "`<all>`" if you do not wish to restrict MDSpamD to any particular IP address.

Allow connections from these IPs
These are the IP addresses from which MDSpamD will accept incoming connections. Connections from other IP addresses will be rejected. This is useful if you wish to allow connections from another server in order to share Spam Filter processing.

Optional command line options to pass to MDSpamD:

MDSpamD can accept many command line options, documented at:

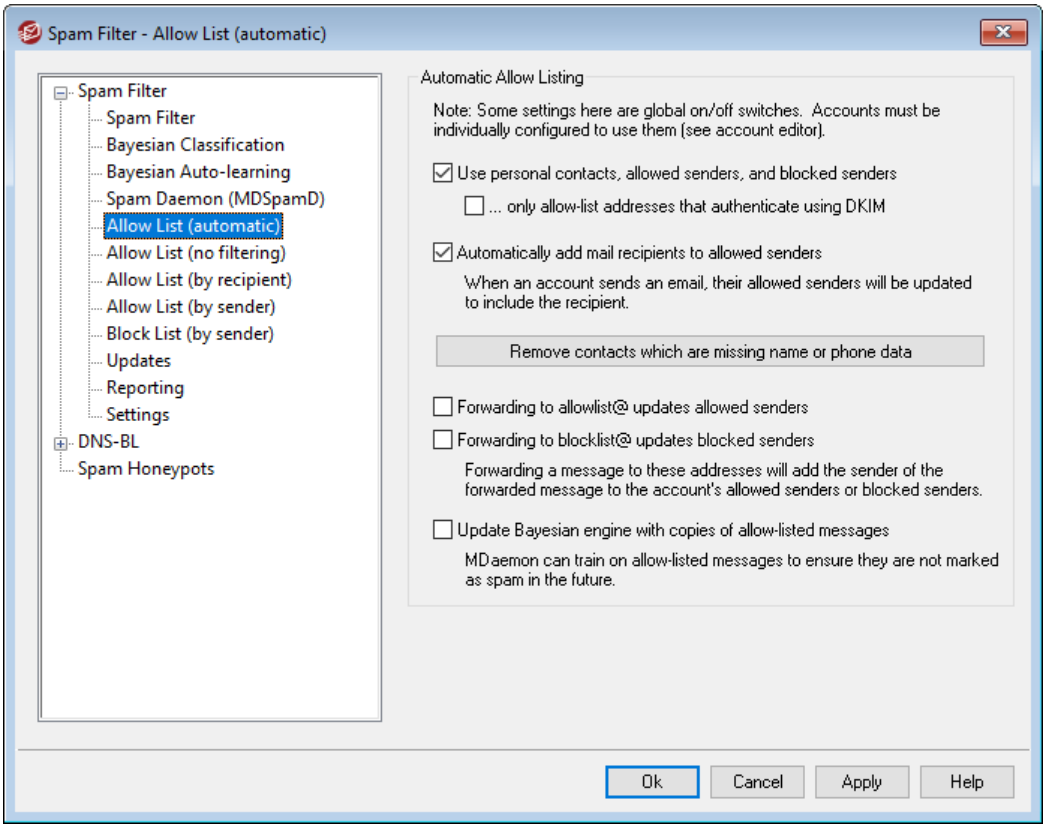
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

http://spamassassin.apache.org/

If you wish to use any of those options, construct a string containing the desired options and place it here.

Some of those options can be configured via the settings on this dialog and therefore do not need to be set up manually using command line options.

4.7.1.5 Allow List (automatic)



Automatic Allow Listing

Use personal contacts, allowed senders, and blocked senders
Click this option to use each user's personal contacts, and allowed and blocked senders for spam filtering for that user. For each incoming message, MDaemon will search for the sender of the message in the recipient account's contacts and lists of allowed and blocked senders. If the sender is found then the message will be allowed or blocked automatically. If you do not wish to apply automatic allow and block listing to every MDaemon user, then you can disable it for individual users by clearing the *Spam Filter uses personal contacts, allowed senders, and blocked senders* option on the Allow List 742 screen of the Account Editor.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...only allow-list addresses that authenticate using DKIM
When this option is enabled, MDaemon will not allow-list the message unless the sender was authenticated via DomainKeys Identified Mail 514 (DKIM). This option helps to avoid allow-listing messages with spoofed addresses. This option is disabled by default.

Automatically add mail recipients to allowed senders
When this option is enabled, whenever a user sends mail to any non-local email address, MDaemon will automatically add that recipient to the user's list of allowed senders. When used in conjunction with "*Use personal contacts, allowed senders, and blocked senders*" option above, the number of Spam Filter false positives can be drastically reduced.

If you do not wish to apply this option to every MDaemon user, you can disable it for individual users by clearing the "*Automatically add mail recipients to allowed senders*" check box on the Allow List 742 screen of the Account Editor.

This option is disabled for accounts using autoresponders.

Remove contacts which are missing name or phone data
Click this button if you wish to remove every contact that contains only an email address from every user's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who have been using MDaemon's automatic allow-listing option prior to version 11 to purge contacts that were added purely as a function of the allow list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated allowed senders folder. This could result in users having many entries in their contacts that they would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

Forwarding to allowlist@ updates allowed senders
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, allowed senders, and blocked senders*" on the Account Editor's Settings screen can forward messages to `allowlist@<domain>` and have MDaemon add the sender of the original message to the account's allowed senders. The allowed address is taken from the forwarded message's `From` header.

Messages forwarded to `allowlist@<domain>` must be forwarded as attachments of the type `message/rfc822`, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

You can change the address MDaemon uses by editing the following key in the `CFILTER.INI` file:

```
[SpamFilter]
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
WhiteListAddress=MyAllowListAddress@
```

Note: the last character must be "@".

Forwarding to blocklist@ updates blocked senders
When this option is enabled, accounts using the "*Spam Filter uses personal contacts, allowed senders, and blocked senders*" on the Account Editor's Settings screen can forward messages to `blocklist@<domain>` and have MDaemon add the sender of the original message to the account's blocked senders. The blocked address is taken from the forwarded message's `From` header.

Messages forwarded to `blocklist@<domain>` must be forwarded as attachments of the type `message/rfc822`, and they must be received by MDaemon via SMTP from a session that is authenticated. Forwarded messages not meeting these requirements will not be processed.

Update Bayesian engine with copies of allow-listed messages
Check this box to cause qualified messages to be copied automatically into the Bayesian non-spam learning folder (designated on the Bayesian 664 screen). This helps to automate the process of providing the Bayesian engine with samples of non-spam messages. Regularly providing the Bayesian engine with new examples of non-spam to learn from will increase its reliability over time and help to reduce the number of false positives (i.e. messages that are erroneously classified as spam).

To qualify for this feature, an incoming message must be addressed to a local user and the sender must be someone in his address book or allowed senders folder. If the message is outgoing, then it must be the recipient who is in the address book or allowed senders. If you do not want any outgoing messages to qualify, then use Notepad to edit the following setting in the `CFILTER.INI` file:

```
[SpamFilter]
UpdateHamFolderOutbound=No (default = Yes)
```

When a message qualifies, it is copied into the Bayesian non-spam learning folder even if Bayesian scheduled learning is disabled on the Bayesian screen. Thus, when scheduled learning is later enabled, or when learning is manually activated, a set of non-spam messages will be ready for analysis. Not every message that qualifies, however, is copied into the learning folder. When the feature is activated, MDaemon will copy qualified messages until a designated number is reached. Subsequently it will copy single messages at designated intervals. By default, the first 200 qualifying messages will be copied and then every tenth qualifying message after that. The initial number copied is equal to the number designated in the option, "*Non-spam samples needed before Bayesian scoring is possible*" located on the Bayesian Auto-learning 668 screen. Changing that setting will also change this value. If you wish to change the interval by which subsequent messages are copied, you can do so by editing the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
HamSkipCount=10 (default = 10)
```

Finally, once a designated total number of messages has been copied, the entire process will be begin again — 200 will be copied and then every tenth (or an alternate value if you have changed these settings). By default, the process will be

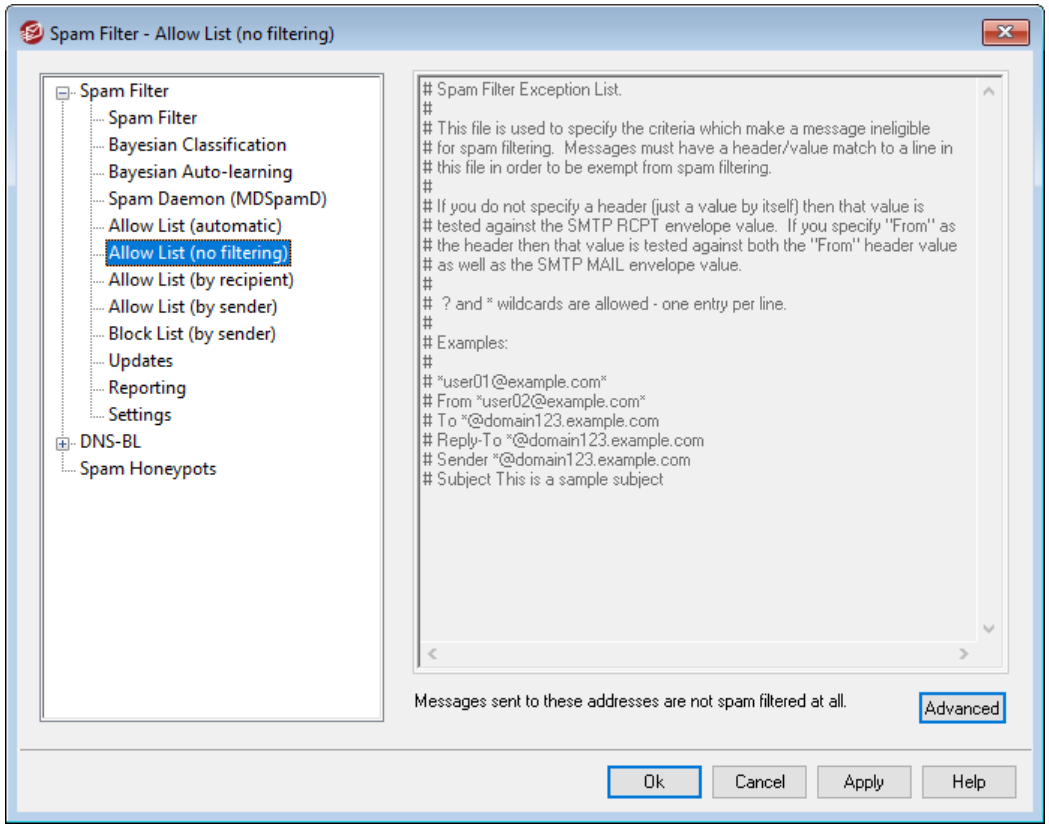
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

restarted after 500 qualifying messages have been copied. You can change this value by editing the following setting in the `MDaemon.ini` file:

```
[SpamFilter]
HamMaxCount=500 (default = 500)
```

This option is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. All Bayesian learning functions are determined by the other server's settings and are performed on the other server. See Spam Daemon 670 for more information.

4.7.1.6 Allow List (no filtering)



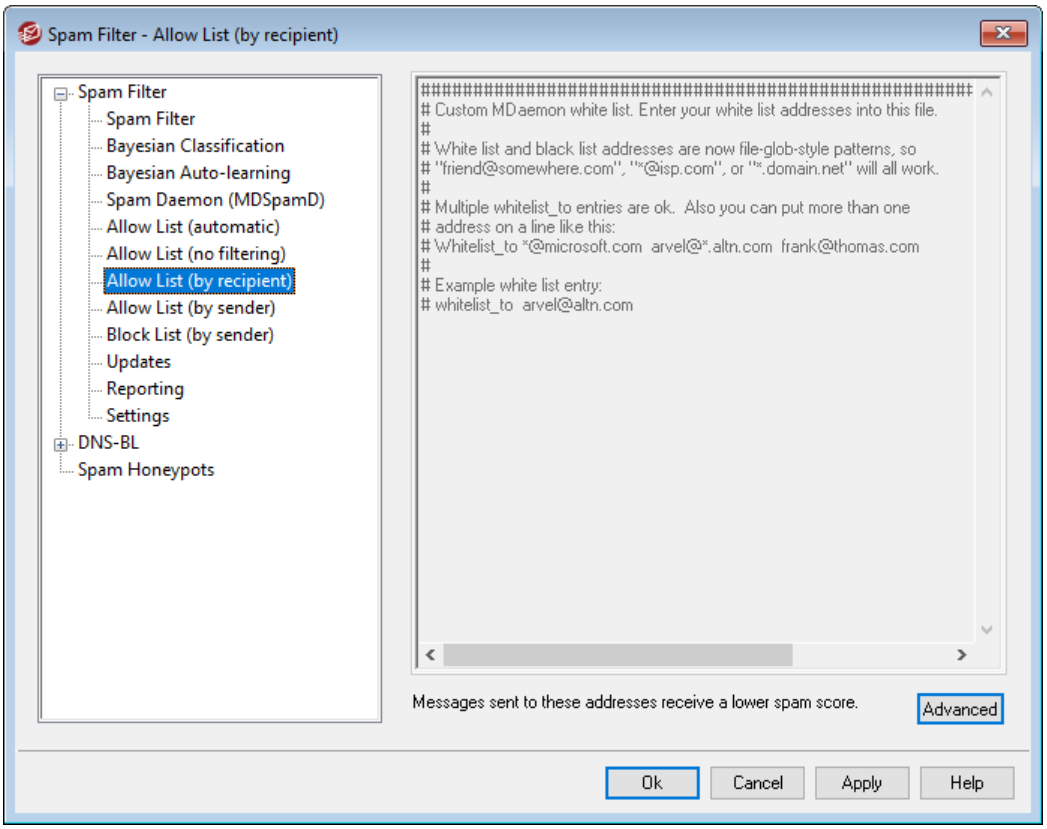
Messages sent to these addresses are not filtered at all
Click **Advanced** on this screen to designate recipient addresses that you wish to be exempt from spam filtering. Messages destined for these addresses will not be processed through the spam filter.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 670 for more information.

4.7.1.7 Allow List (by recipient)

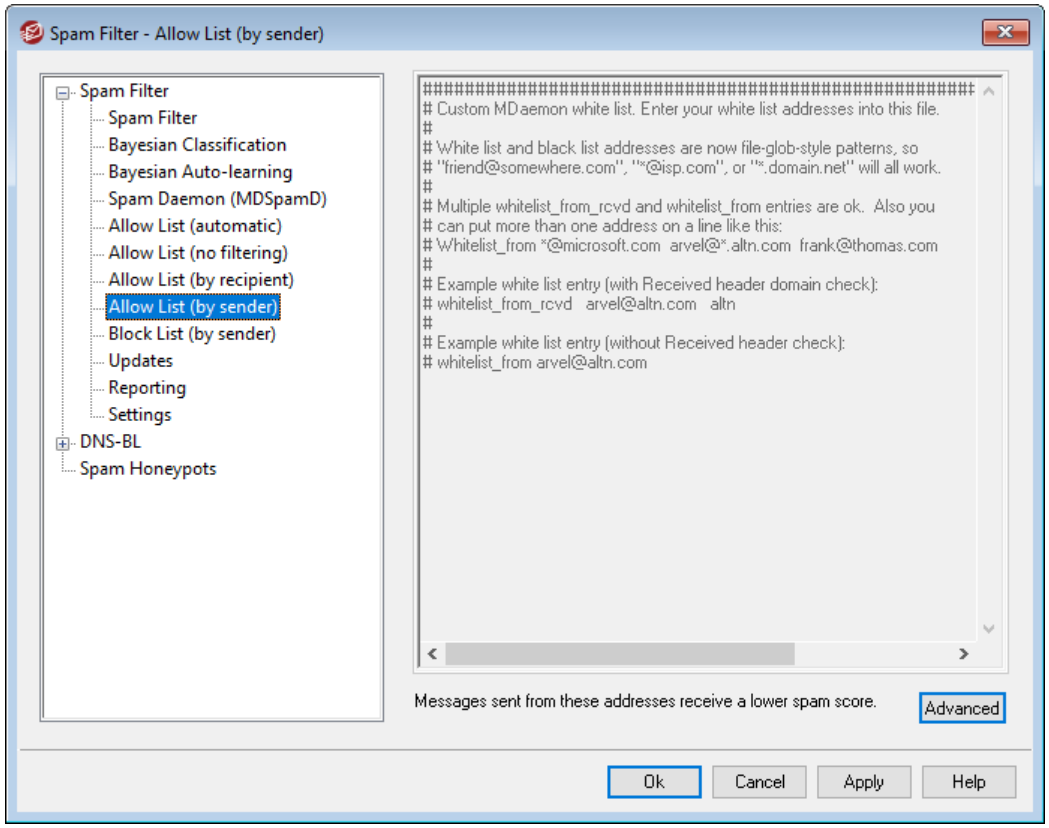


Messages sent to these addresses receive a beneficial score
Click **Advanced** to add addresses to this list. This list is similar to *Allow List (no filtering)* 675, except that rather than exempting messages for the recipient from Spam Filter processing, they will be processed but have their Spam Filter score 661 reduced by the amount specified on the Spam Filter Settings 681 screen. Therefore including an address on this allow list does not automatically guarantee that a message to that address will not be considered spam. For example, if you have the spam score threshold set to 5.0 and the allow list value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the allow list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This is highly unlikely, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blocked address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 670 for more information.

4.7.1.8 Allow List (by sender)

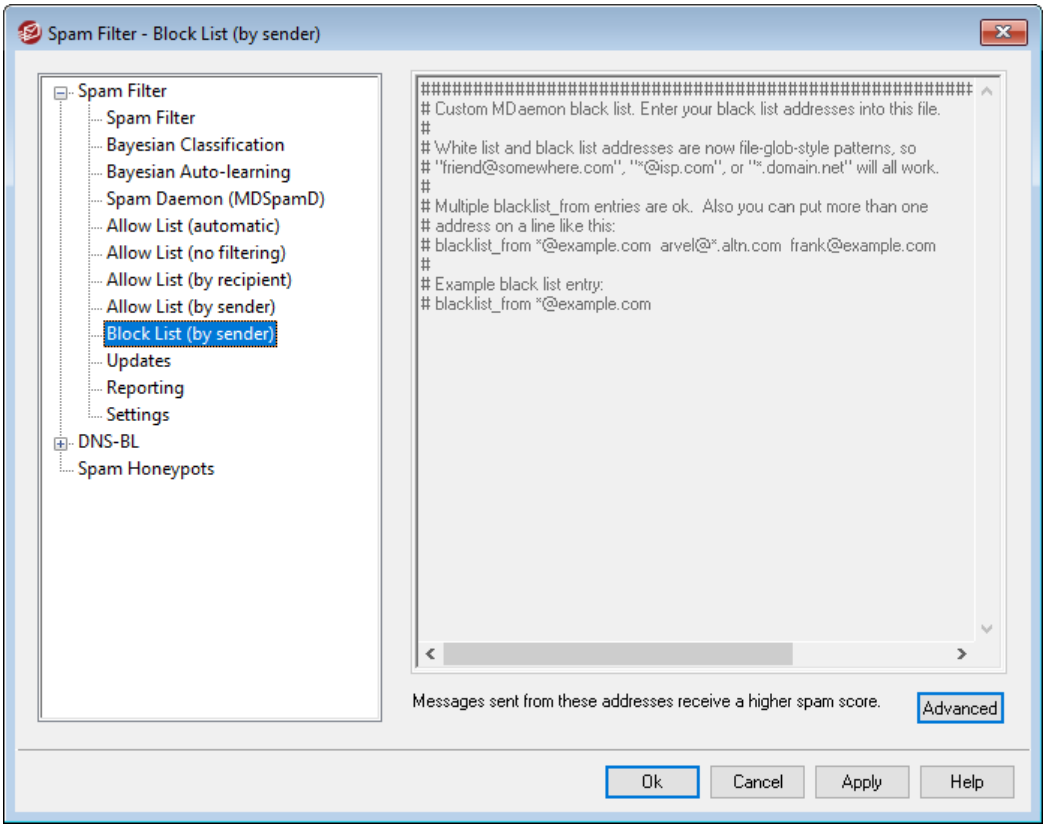


Messages sent from these addresses receive a beneficial score
Click **Advanced** to add addresses to this list. This allow list is similar to *Allow List (by recipient)* 676, except that spam score reduction is based on who the message is *from* rather than based on the recipient. Messages from these senders will have their Spam Filter score 661 reduced by the amount specified on the Spam Filter Settings 681 screen. Therefore including an address on this allow list does not automatically guarantee that a message to that address will not be considered spam. For example, if you have the spam score threshold set to 5.0 and the allow list value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the allow list value is subtracted, then the final spam score of the message will be at least 5.0, thus denoting it as spam. This is highly unlikely, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as a blocked address.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 670 for more information.

4.7.1.9 Block List (by sender)



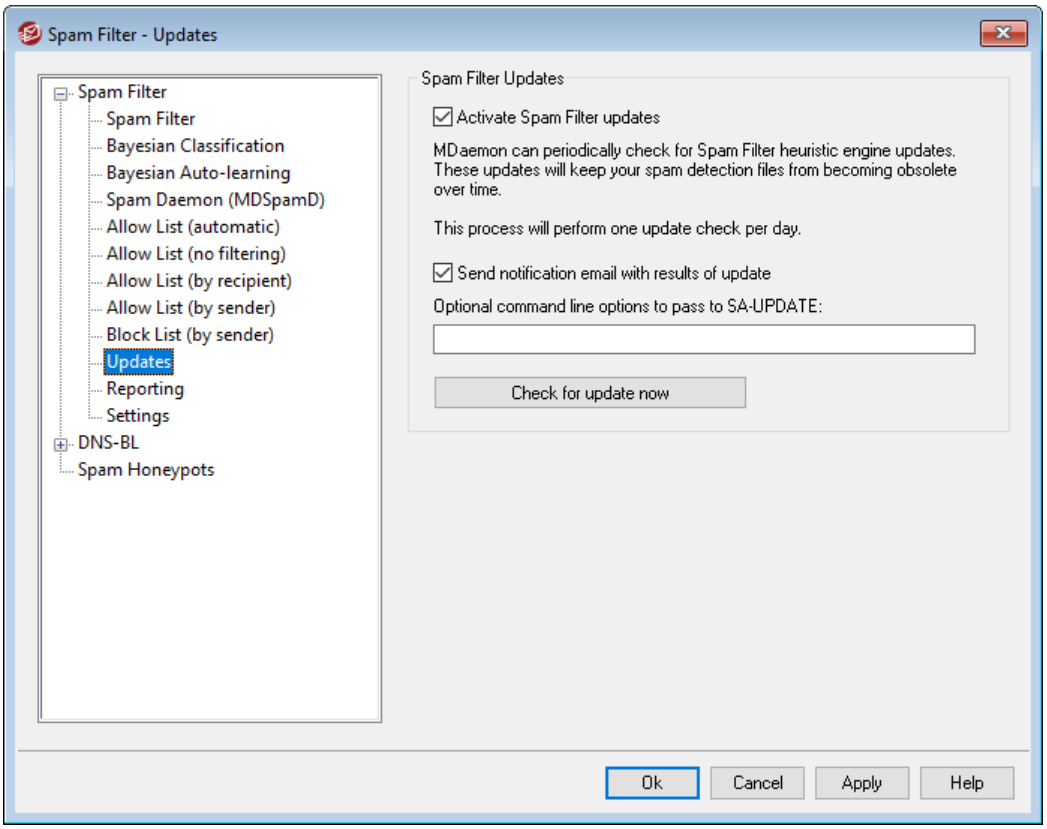
Messages sent from these addresses receive a detrimental score
Click **Advanced** to add addresses to this list. Messages from addresses on this block list will have their Spam Filter score 661 increased by the amount specified on the Spam Filter Settings 681 screen, typically causing them to be marked as spam. However, including an address on this list does not automatically guarantee that a message from that address will always be considered spam. For example, if a message comes from a blocked sender but is addressed to an allowed recipient, then the score modifiers may offset each other and cause the message to have a final score that is below the spam score threshold. This could also happen if you have the block list score modifier set particularly low.

This screen is unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

for Spam Filter processing. This Spam Filter list will be maintained on the other server. See Spam Daemon 670 for more information.

4.7.1.10 Updates



Spam Filter Updates

Activate Spam Filter updates
Click this check box if you want the Spam Filter be updated automatically. Once per day MDaemon will to see if there are any updates available for the Spam Filter heuristics engine, and if so it will download and install them automatically.

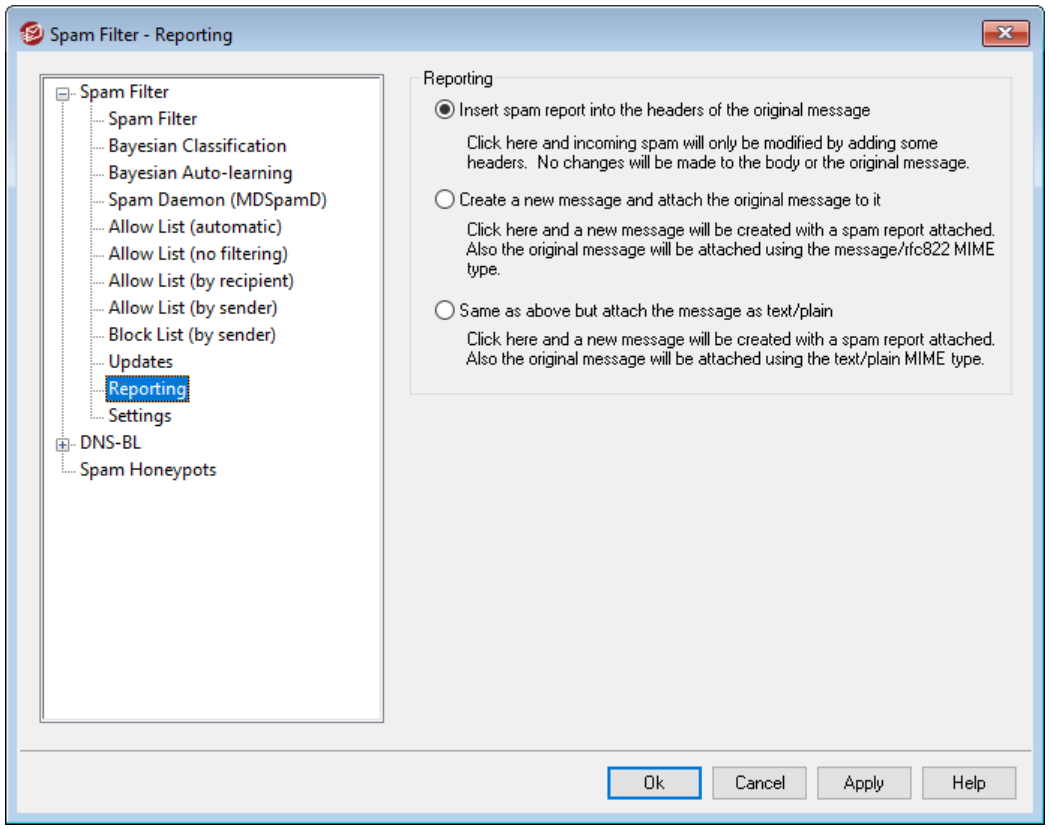
Send notification email with results of update
Use this option if you wish to send an email to the administrators whenever the Spam Filter is updated, containing the results of the update. This option is the same as the "*Send Spam Filter update notification to Administrators*" option located at: Content Filter » Notifications.

Optional command line options to pass to SA-UPDATE
Use this advanced option if you wish to pass any command line options to SA-UPDATE.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Check for update now
Click this button to check immediately for a Spam Filter rules update.

4.7.1.11 Reporting



The Spam Filter Reporting options are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. Spam Filter Reporting will be controlled by the other server's settings. See the Spam Daemon 670 screen for more information.

Reporting

Insert spam report into the headers of the original message
This is the default reporting option. Use this option if you want the Spam Filter to insert a spam report into each spam message's headers. The following is an example of a simple spam report:

```
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
```

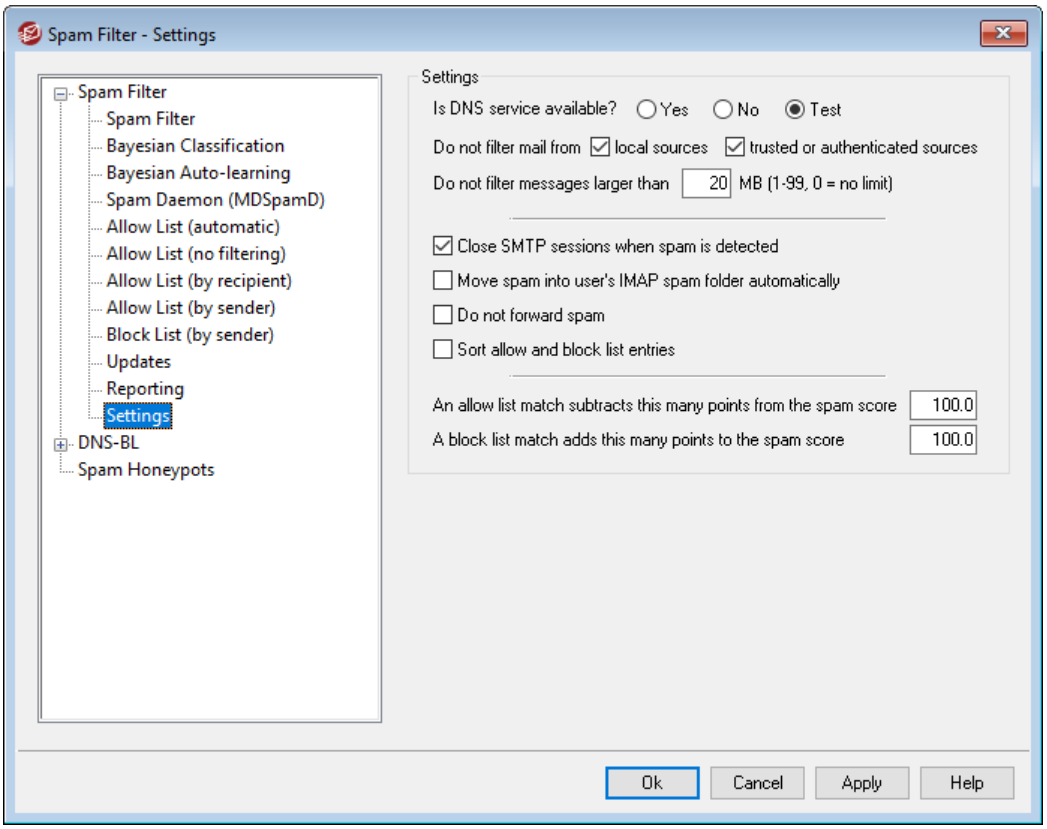
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
  *  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
```

Create a new message and attach the original message to it
Choose this reporting option if you want spam to cause a new email message to be created containing the spam report. The original spam message will be included with it as a file attachment.

Same as above but attach the message as text/plain
Like the previous reporting option, this option will generate the spam report as a new message that includes the original spam message as a file attachment. The difference is that the original message will be attached using the text/plain MIME type. Because spam sometimes contains HTML code that is unique for each message and can potentially reveal to the spammer which email and IP address opened it, this method can prevent that from happening by converting the HTML code to plain text.

4.7.1.12 Settings



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Settings

Is DNS service available?
These options allow you to choose whether or not DNS is available to the Spam Filter when processing messages. You may choose one of the following options:

Yes - DNS is available. SURBL/RBL and other rules that require DNS connectivity will therefore be utilized.

No - DNS is not available. Spam filtering rules that require DNS will not be utilized.

Test - DNS availability will be tested and if present it will be used. This is the default setting.

Don't filter mail from...

local sources
Click this check box if you want messages from local users and domains to be exempt from filtering.

trusted or authenticated sources
Enable this option if you want messages sent from trusted domains or authenticated senders to be exempt from spam filtering.

Don't filter messages larger than [XX] MB MB (1-99, 0 = no limit)
It is typical for spam messages to be fairly small since the usual goal of the spammers is to deliver as many messages as possible in the shortest amount of time. If you want messages over a certain size to be exempt from spam filtering then specify the size (in MB) here. Use "0" if you do not wish to set a message size limit on spam filtering.

Close SMTP sessions when spam is detected
This option is enabled by default and will close an SMTP session if an inline scan detects a spam message.

Move spam into user's IMAP spam folder automatically
Click this option and MDaemon will automatically place each message that the Spam Filter determines to be spam into each user's "Spam" IMAP folder (if such a folder exists). It will also automatically create the folder for each new user account that is added.

When you click this option you will also be asked whether or not you would like MDaemon to create this folder for each of your already existing user accounts. If you choose "Yes" then a folder will be created for all users. If you choose "No" then a folder will only be created when each new user is added. Any folders that already exist for some or all of your users will not be altered or affected in any way.

Do not forward spam
Click this check box if you do not wish to allow spam messages to be forwarded.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Sort allow and block list entries
Use this option if you wish to keep the Spam Filter allow and block list entries in sorted sequence. **Note:** if you have added your own comments to the file (lines starting with #), enabling this option will sort these lines to the top of the file. This feature is disabled by default. If you enable the option, the sort will take place upon the next change to the allow or block list file.

The remaining options on this screen are unavailable when you have configured MDaemon to use another server's MDaemon Spam Daemon (MDSpamD) for Spam Filter processing. See the Spam Daemon 670 screen for more information.

An allow list match subtracts this many points from the spam score
Placing an address on the Spam Filter's Allow List (by recipient) 676 or Allow List (by sender) 677 screens does not automatically guarantee that a message to or from that address will not be considered spam. Instead, those addresses will simply have the amount specified in this control subtracted from their spam scores. For example, if you have the spam score threshold set to 5.0 and this value set to 100, and then a particularly excessive spam message arrives that gets a spam score of 105.0 or higher before the allow list value is subtracted, then the final spam score of the message will be at least 5.0 — thus denoting it as spam. This would rarely happen, however, because spam rarely has a value that high unless it contains some other exceptionally high-scoring element, such as an address on the block list. Of course, if you set the allow list subtraction value to a much lower amount then it would occur much more frequently.

If you wish to cause messages addressed to certain recipients to bypass the Spam Filter completely rather than simply adjust their scores, include those recipient addresses on the Allow List (no filtering) 675 screen. You can also exclude messages from Spam Filter scoring based on the sender by using the options on the Allow List (automatic) 672 screen.

A block list match adds this many points to the spam score
This value is added to the spam score of messages from addresses found on the Block List (by sender) 678 screen. As with the allow list option above, including an address on the Spam Filter's block list doesn't guarantee that a message from that address will be considered spam. Instead, the value specified in this option will be added to the message's spam score, which will then be used to determine whether or not the message is spam.

4.7.2 DNS Block Lists (DNS-BL)

DNS Block Lists (DNS-BL) can be used to help prevent spam email from reaching your users. This security feature allows you to specify several DNS block list services (which

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

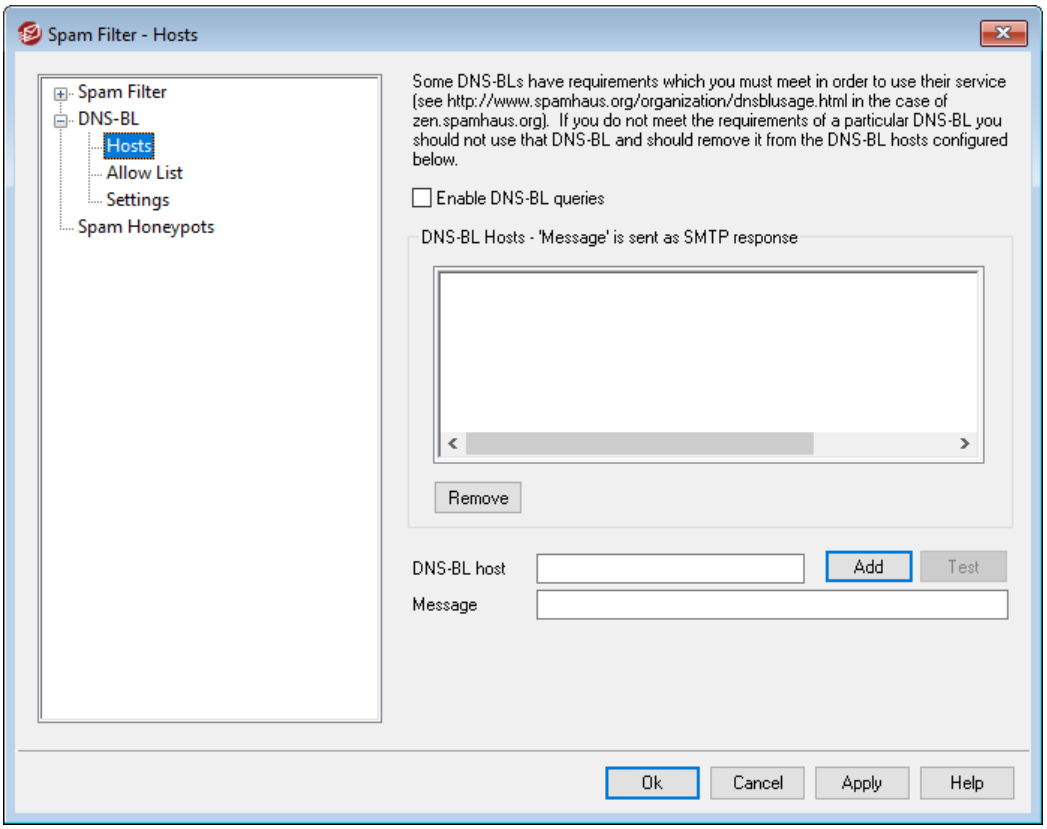
maintain lists of servers known to relay spam) that will be checked each time someone tries to send a message to your server. If the connecting IP has been listed by any one of these services, the message(s) will be refused or flagged according to the settings on the Settings 687 screen.

DNS Block Lists includes an Allow List for designating IP addresses that you wish to make exempt from DNS-BL queries. Before activating DNS-BL, you should make sure that your local IP address range is on the Allow List to prevent lookups on those addresses. "127.0.0.1" is exempt and therefore doesn't need to be added to the list.

See:

DNS-BL Hosts 684
DNS-BL Settings 687
DNS-BL Allow List 686

4.7.2.1 Hosts



DNS-BL Hosts

Enable DNS-BL queries
Activate this option if you wish to check incoming mail against DNS Block Lists. MDaemon will query each listed host when performing a DNS-BL lookup on the sending IP address. If a host replies to the query with a positive result, MDaemon

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

can flag the message or refuse to accept it, depending on which options you have enabled on the DNS-BL Settings 687 screen.

Remove
Select an entry from the DNS-BL service list and click this button to remove it from the list.

DNS-BL host
If you wish to add a new host to be queried for block listed IP addresses, enter it here.

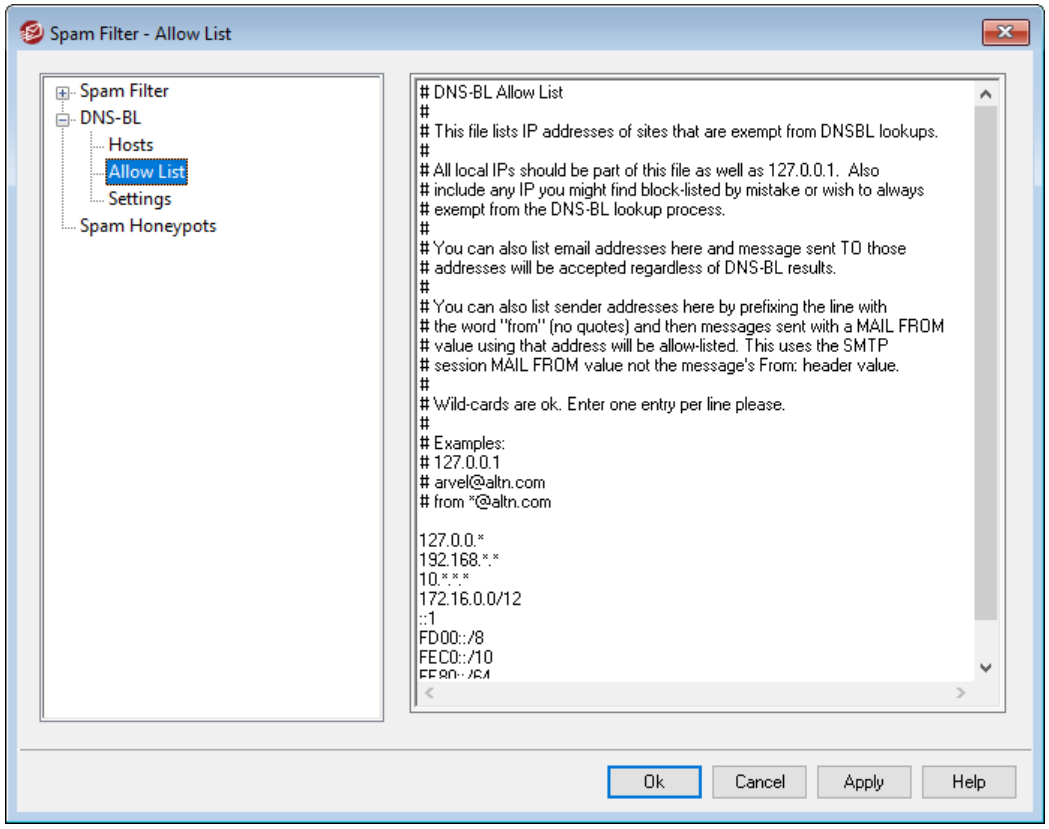
Test
Enter a host into the *DNS-BL host* option and click this button to test it by looking up 127.0.0.2.

Message
This is the message that can be sent during the SMTP session when an IP address has been listed by the corresponding DNS-BL host listed above. This message corresponds to the *...and respond with 'Message' rather than 'user unknown'* option located on the DNS-BL Settings 687 screen.

Add
After entering a host and return message, click this button to add it to the DNS-BL hosts list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.7.2.2 Allow List

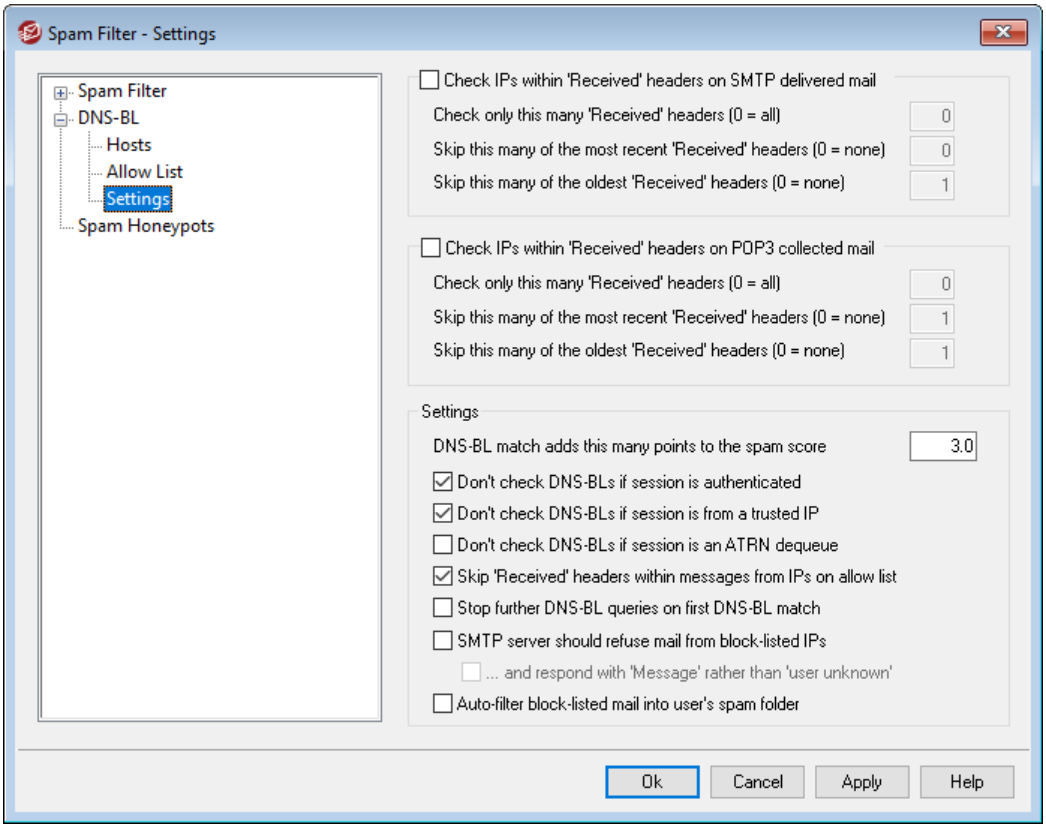


Use this screen to designate IP addresses that will be exempt from DNS Block List queries. You should always include your local IP address range to prevent DNS-BL from looking up messages originating from local users and domains (i.e. `127.0.0.*`, `192.168.*.*`, and so on). You can also include email addresses on the list. When a message is addressed to one of them then that message will be accepted regardless of the DNS-BL lookups results. Finally, you can also exempt specific senders from DNS-BL results by entering "from *sender@example.com*" on the list. This address must match the SMTP session's "MAIL FROM" value, not the messages "From:" header.

Place only one entry on each line. Wildcards are permitted.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

4.7.2.3 Settings



Check IPs within 'Received' headers on SMTP delivered mail
Click this switch if you want DNS Block Lists to check the IP address stamped in the "Received" headers of messages received via SMTP.

Check only this many 'Received' headers (0 = all)
Specify the number of "Received" headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all "Received" headers will be checked.

Skip this many of the most recent 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the most recent Received headers when checking SMTP messages.

Skip this many of the oldest 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of oldest Received headers when checking SMTP messages.

Check IPs within 'Received' headers on POP3 collected mail
When this switch is enabled DNS-BL will check the IP address stamped in the "Received" headers of messages collected via DomainPOP and MultiPOP.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Check only this many 'Received' headers (0 = all)
Specify the number of 'Received' headers that you want DNS-BL to check, starting with the most recent. A value of "0" means that all 'Received' headers will be checked.

Skip this many of the most recent 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the most recent Received headers when checking DomainPOP and MultiPOP messages. Since it is often necessary to skip the most recent Received header on POP3 collected mail such as DomainPOP, this option has a default setting of "1".

Skip this many of the oldest 'Received' headers (0 =none)
Use this option if you want DNS-BL to skip over one or more of the oldest Received headers when checking DomainPOP and MultiPOP messages.

Settings

DNS-BL match adds this many points to the spam score
Use this option to specify a value that will be added to a message's spam score 661 when a DNS-BL match is found. Sometimes the Spam Filter's heuristic examination of a message may not score it high enough to be considered spam, but a DNS-BL lookup may indicate that it is. Thus adding this value to the spam score could help catch some spam messages that might otherwise slip through undetected. By default a DNS-BL match adds 3.0 points to the spam score.

Don't check DNS-BLs if session is...

authenticated
Click this checkbox if you want those sessions that were authenticated using the AUTH command to be exempt from DNS-BL queries.

from a trusted IPs
Click this checkbox if you want addresses that are listed on the Trusted Hosts 505 screen to be exempt from DNS-BL queries.

an ATRN dequeue
Enable this option if you do not wish to do DNS-BL lookups on mail collected over ATRN dequeue sessions. This setting is disabled by default but you can enable it if, for example, your smart-host is already doing DNS-BL checks on your stored mail..

Skip 'Received' headers within messages from IPs on the allow list
When this option is enabled, DNS-BL will not check the "Received" headers within messages coming from IP addresses that you have listed on the DNS-BL Allow List 686 .

Stop further DNS-BL queries on first DNS-BL match
Oftentimes there are multiple hosts contained in the headers of each message that DNS-BL processes, and multiple DNS-BL services that are queried. By default, DNS-BL will continue to query these services for all hosts in the message regardless of

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

the number of matches found. Click this option if you want DNS-BL to stop querying the services for any given message as soon as a match is found.

SMTP server should refuse mail from block-listed IPs
By default this box is unchecked, meaning that messages from block-listed IP addresses will not be refused during the SMTP session, but will have an X-MDDNSBL-Result header inserted. You can then use the Content Filter to search for messages with this header and do with them as you please. You can also use the "*Auto-filter block-listed mail into user's spam folder*" option below to filter messages automatically into each user's spam folder. Check this box if you wish MDaemon to refuse messages from block-listed IP addresses rather than flag them.

Because some IP addresses can be block-listed by mistake, you should exercise caution before choosing to refuse messages rather than simply flagging them. It is also worth noting that in addition to flagging a message, you can adjust its spam score based on the DNS-BL results via the *DNS-BL match adds this many points to the spam score* option located on the Spam Filter 661.

...and respond with 'Message' rather than 'user unknown'
Click this option if you want the specific Message you have assigned to the DNS-BL Host 684 to be passed during the SMTP session whenever an IP address is found to be listed. Otherwise, a "user unknown" message will be passed instead. This option is only available if you have elected to use the "*SMTP server should refuse mail from block-listed IPs*" option above.

Auto-filter block-listed mail into user's spam folder
Click this option and a "Junk E-mail" IMAP folder will be created for all future user accounts that you add to MDaemon. MDaemon will also create a mail filter for each of those users, which will search for the X-MDDNSBL-Result header and then place messages containing that header into the user's spam folder. When you click this option you will also be asked whether or not you would like MDaemon to create this folder and filter for each of your already existing user accounts. See *Auto-generating a Spam Folder and Filter for Each Account* below.

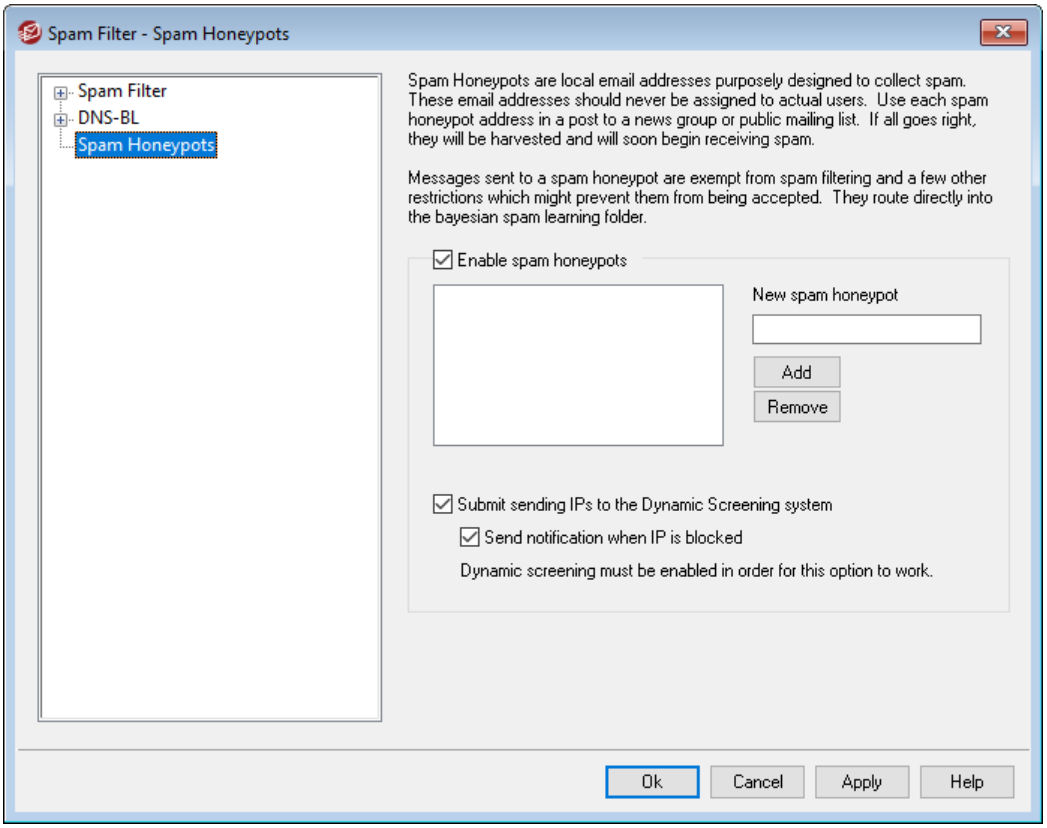
Auto-generating a Spam Folder and Filter for Each Account

MDaemon can automatically create a "Junk E-mail" IMAP mail folder for each account and generate a mail filter that will move messages into that folder whenever if finds the X-MDDNSBL-Result header. Whenever you click the *Auto-filter block-listed mail into user's spam folder* option, you will be presented with the option to create the folder and accompanying filter for all accounts. Simply choose "yes" on the dialog to create the folders and filters. Although not foolproof, this is an easy and generally reliable way to help your users quickly identify spam email messages—it can effectively prevent spam email from being mixed in with all of their legitimate email. They will only occasionally need to review the contents of their spam folder just to make sure that an important message doesn't accidentally get put there (which may sometimes occur). When creating the folders and filters for your accounts, if MDaemon finds that an account already has a filter that checks for the existence of the X-MDDNSBL-Result

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

header then no action will be taken and no filter will be created for that account. If you want the name of the IMAP folder to be something other than "Junk E-mail", you can change the default setting by editing the *Default spam folder name* option located on the System 480 screen under Setup » Preferences.

4.7.3 Spam Honeypots



Spam Honeypots (located at Security » Spam Filter » Spam Honeypots) is for designating local email addresses purposely designed to collect spam. These spam honeypots are not valid MDaemon accounts or address aliases and should never be used for sending or receiving legitimate email. But, by posting a honeypot address to a news group, public mailing list, or other source from which spammers often farm addresses, you should begin to see incoming messages addressed to the spam honeypots — you could also pull addresses from other spam that you have received addressed to other invalid local addresses. Because honeypots will never receive legitimate email, all incoming messages addressed to them will always be routed directly to your Bayesian spam learning folder 664 for processing. Further, the IP addresses of the sending servers can optionally be added to the Dynamic Screening 552 system, banning future connections from those addresses for a designated period of time. All of this helps increase the probability of identifying and blocking spam in the future.

Spam Honeypots

This list contains all addresses that you have designated as Spam Honeypots.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Enable spam honeypots
This option is enabled by default. Uncheck this box if you wish to disable the spam honeypots feature.

New spam honeypot
To add a spam honeypot, enter the address here and click *Add*.

Remove
To remove a spam honeypot, select the desired address and then click Remove.

Submit sending IPs to the Dynamic Screening system
Check this box if you wish to submit to the Dynamic Screening 552 system all IP addresses from which a Spam Honeypots message arrives. The Dynamic Screen (located at Security » Security Settings » Screening » Dynamic Screen) must be enabled on your server before this feature will be available.

Send notification when IP is blocked
By default, when a submitted IP addresses is blocked by the Dynamic Screening system, the Dynamic Screening *IP Address Blocking Reports* 604 options will be used to notify you of that action. Clear this checkbox if you do not wish to be notified when an IP address is blocked due to Spam Honeypots submission feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

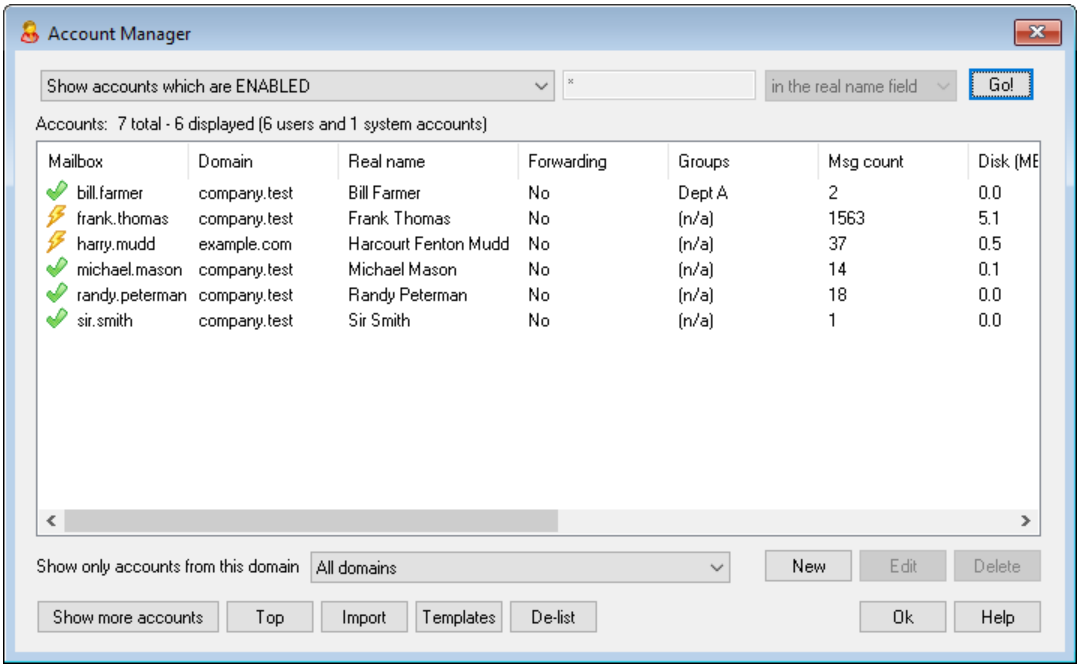
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section V

5 Accounts Menu

5.1 Account Manager

To better manage the selection, addition, deletion, or modification of your accounts, MDaemon contains the Account Manager. This dialog provides access to account information and can be used to sort accounts by mailbox, domain, real name, or mail folder. The Account Manager is located under the Accounts menu at: Accounts » Account Manager...



Account Management

Above the list of accounts you will see two statistics regarding the list. The first number is the total number of MDaemon user accounts that currently exist on your system. The second number is the number of those accounts currently displayed in the list. The accounts that will be displayed is contingent upon what you have chosen in the *Show only accounts from this domain* option below the list. If you have selected "All Domains" then all of your MDaemon accounts will be displayed in the list. There is a search option at the top of this dialog that you can use to define exactly which accounts will be displayed beyond simply the domain to which they belong.

Each entry in the list contains an Account Status Icon (see below), the mailbox, the domain to which it belongs, the "real name" of the account holder, any groups to which the account belongs, the message count, the disk space used (in MB), the last time the account was accessed, and the mail folder in which the account's messages are stored. This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

By default, only 500 accounts at a time will be displayed in this list. If you want to see more accounts from the currently selected domain (or All Domains, if you have selected that option) then you must click the *Show more accounts* button to display the next 500. If you want to be able to display more than 500 accounts at a time then open the `MDaemon.ini` file and change the `MaxAccountManagerEntries=500` key to whatever value that you prefer.

Account Status Icons

Account is a global or domain administrator.

Full access account. Both POP and IMAP access are enabled.

Restricted access account. Either POP, IMAP, or both are disabled.

Account is frozen. MDaemon will still accept mail for the account, but the user cannot send or check mail.

Disabled account. All access to the account is disabled.

New
Click this button to open the Account Editor 697 in order to create a new account.

Edit
Select an account from the list and then click this button to open it in the Account Editor 697. You can also double-click the account to open it.

Delete
Select an account from the list and then click this button to delete it. You will be asked to confirm your decision to delete the account before MDaemon will proceed.

Show only accounts from this domain
Choose "All Domains" from this drop-down list box to display all MDaemon accounts. Choose a specific domain to show only that domain's accounts.

Show more accounts
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500. See the note above for instructions on how to increase the maximum number of accounts that may be displayed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Top
Click this button to quickly move to the top of the account list.

Import
Click this button if you wish to import accounts from a comma delimited text file. This button is identical to the Accounts » Importing » Import accounts from a comma delimited text file menu selection.

Templates
Click this button to open the Groups & Templates 764 dialog, from which you can manage the default settings for New Accounts 775 and control account group membership.

De-list
Select one or more accounts and then click this button if you wish to unsubscribe them from all Mailing Lists 265 hosted on the server. A box will open asking you to confirm the decision to remove the addresses from the lists.

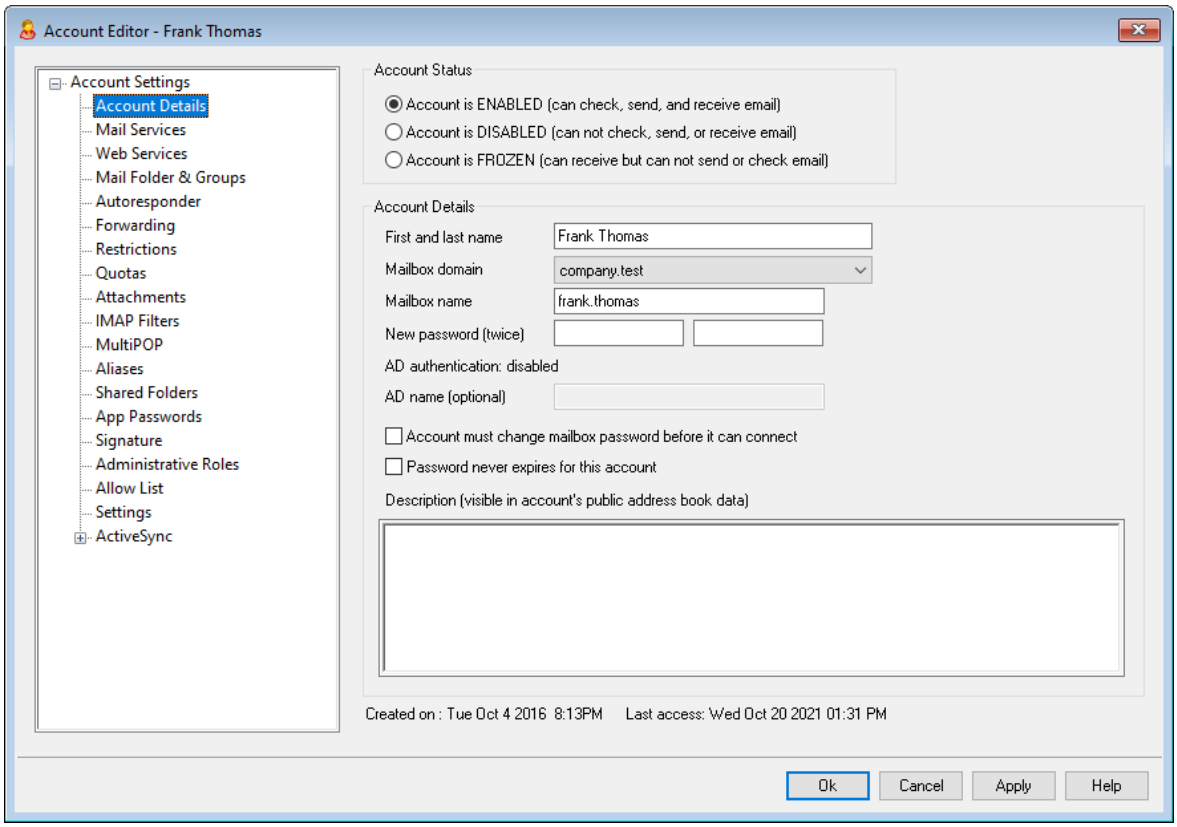
See:

Account Editor 697
New Accounts Template 775

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1 Account Editor

5.1.1.1 Account Details



Account Status

Account is ENABLED (can check, send, and receive email)
This is the default option; the account can check, send, and receive email.

Account is DISABLED (can not check, send, and receive email)
Select this options if you wish to disable all access to the account. The user will not be able to access the account by any means, nor will MDaemon accept mail for it. It will not be deleted, and it will still count toward the number of accounts used in your license's account limit, but MDaemon will operate as if the account doesn't exist, with one exception—any of the account's folders that have been shared with other users can still be accessed by those users, according to the folder's ACL permissions 302.

Account is FROZEN (can receive but can not send or check email)
Select this options if you wish to allow the account to receive incoming messages but prevent it from being able to check or send messages. This is useful when, for example, you suspect the account has been hijacked. Freezing the account would prevent the malicious user from accessing its messages or using the account to send messages, but it would still be able to receive its incoming email.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Account Details

First and last name
Enter the user's first and last name here. When creating a new account, some of the fields on the various screens of the Account Editor (for example, *Mailbox name* and *Mail Folder*) will be automatically filled in while typing the first and last name and choosing the *Mailbox domain*. You can, however, change any of those default values. The first and last name field cannot contain " ! " or " | ".

Mailbox domain
Use this drop-down list box to specify the domain to which this account will belong and that will be used in its email address. MDaemon's Default Domain 174 will appear in the drop-down list by default.

Mailbox name
This is the portion of the account's email address that sets it apart from other accounts on the domain. The complete email address (i.e. [*Mailbox name*]@[*Mailbox domain*]) is used as the unique identifier for the account and as its login for POP3, IMAP, Webmail, and so on. Email addresses cannot contain spaces or " ! " or "|" characters. Do not use "@" in this option. For example, use "frank.thomas" not "frank.thomas@".

New password (twice)
If you wish to change the account's password, type a new one here, once in each box. This is the password that the account will use when connecting to MDaemon to send or receive email via POP3 or IMAP, when authenticating during the SMTP process, or when using Webmail, Remote Administration, or MDaemon Connector. Both of these boxes will be highlighted in red if the passwords do not match or they violate the password restrictions 840. Otherwise they will be green.

If you are using Active Directory Authentication 851 for this account then you must enter two backslashes followed by the Windows domain to which the user belongs, rather than entering a password (for example, `\\ALTN` rather than `123Password`). Below the password fields there is a short statement to indicate whether AD authentication is enabled or disable for the account.

The account should have a password even if you do not wish to allow POP3/IMAP access to the mail account. In addition to mail session verification, the email address and *Mailbox password* values are used to allow remote account configuration and remote file retrieval. If you wish to prevent POP/IMAP access, use the options located on the Mail Services 701 screen. If you wish to prevent all access, then use the *Account is DISABLED* or *Account is FROZEN* options above.

AD name (optional)
Use this setting if you wish to specify an optional Active Directory account name to access the account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Account must change mailbox password before it can connect
Check this box if you wish to require the account to change its *Mailbox password* before it can access POP, IMAP, SMTP, Webmail, or Remote Administration. The user can connect to Webmail or Remote Administration but will be required to change his or her password before proceeding. Note, however, that in order for users to be able to change their passwords via Webmail or Remote Administration they must first be granted the "*...edit password*" web access permission on the Web Services 703 screen. After the password is changed this option will be deactivated.

Because changing the password may not be easy or possible for some users, you should exercise caution before activating this option.

Password never expires for this account
Check this box if you wish to exempt the account from the password expiration option located on the Passwords 840 dialog.

Description
Use this text area if you wish to add a public description of the account.

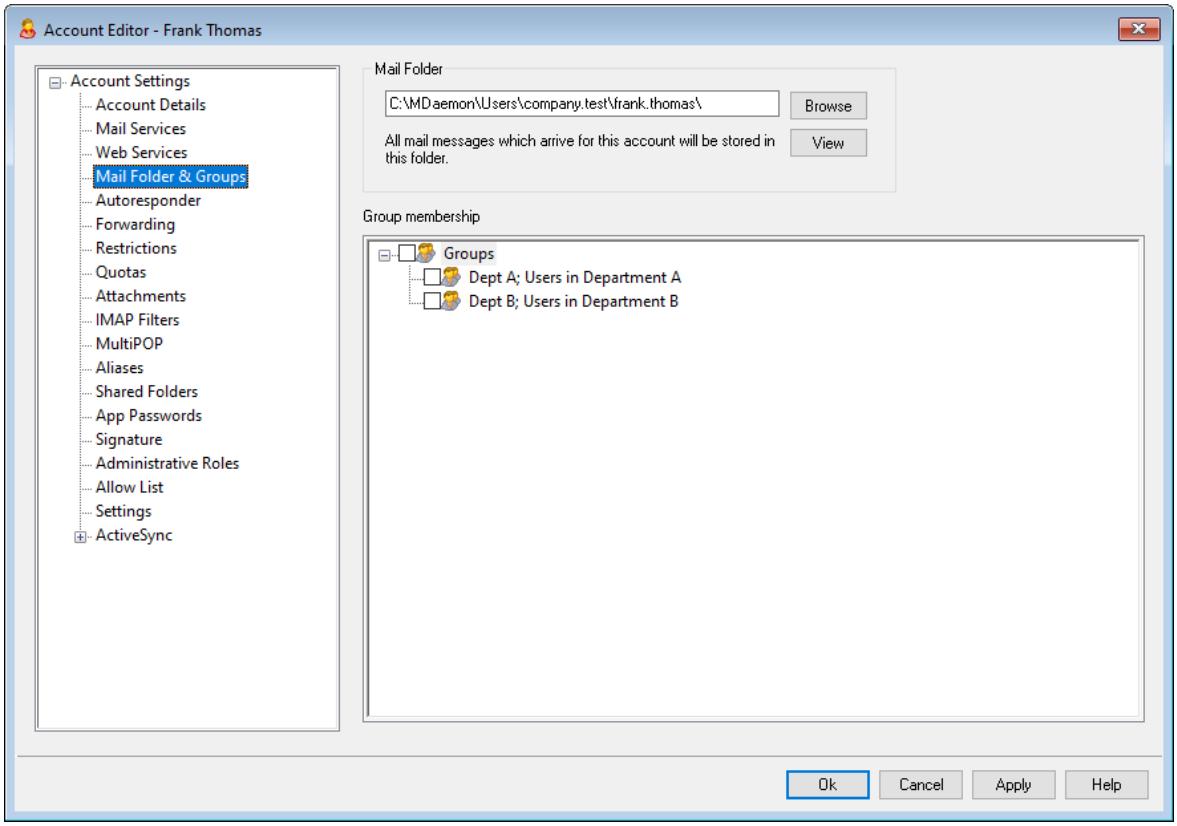
This description is included in the account's public contact record and is viewable by others. Do not include private or sensitive information in this field. For private notes or comments regarding this account, use the space provided on the Administrator Roles 741 screen.

See:

AD Authentication 851
Passwords 840
Account Editor » Web Services 703

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.2 Mail Folder & Groups



Mail Folder

Enter the folder where you wish to store this account's email messages. When creating a new account, the default location of this folder is based on the *Mail folder* setting designated on the New Accounts template 776.

View

Click this button to open the Queue/Stats Manager 868 to the user's *Mail Folder*.

Groups Membership

Use this box to add the account to one or more Groups 764. Check the box next to each group that you wish the account to join.

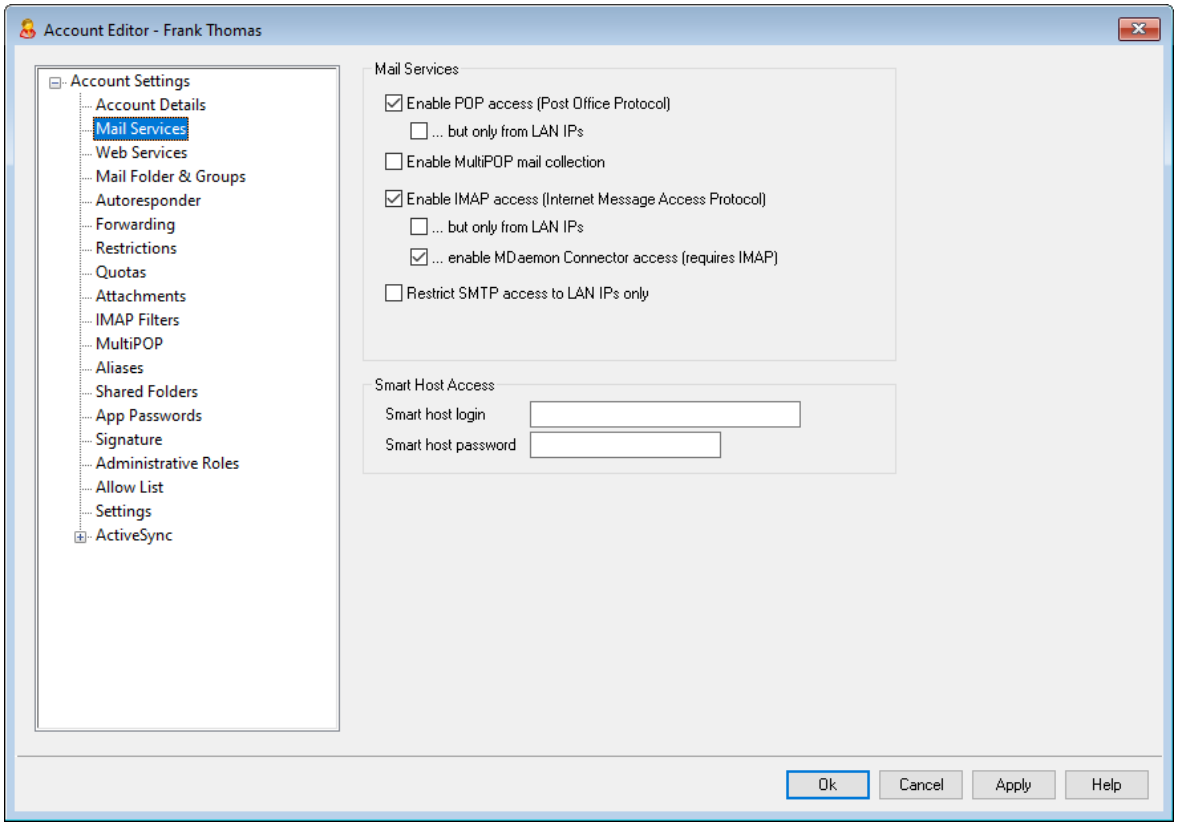
See:

New Accounts Template 776

Groups 764

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.3 Mail Services



The options on this screen govern which mail services the account is allowed to use: POP, IMAP, MultiPOP, and MDaemon Connector. Email access via Webmail is controlled from the Web Services 703 screen. It also contains options for specifying optional Smart Host Access credentials for the account.

Mail Services

Enable POP access (Post Office Protocol)
When this box is checked, the account's mail can be accessed via Post Office Protocol (POP). Virtually all email client software supports this protocol.

...but only from LAN IPs
Check this box if you wish to allow the account to be accessed via POP only when the user is connecting from a LAN IP address 594.

Enable MultiPOP mail collection
Check this box if you wish to allow the account to use MultiPOP 723. MultiPOP allows the user to collect mail from other email accounts, maintained on other mail servers.

Enable IMAP access (Internet Message Access Protocol)
When this box is checked, the account's mail can be accessed via Internet Message Access Protocol (IMAP). IMAP is more versatile than POP3, allowing email to be managed on the server and accessed using multiple clients. Most email client software supports this protocol.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...but only from LAN IPs
Check this box if you wish to allow the account to be accessed via IMAP only when the user is connecting from a LAN IP address[594].

...enable MDaemon Connector access (requires IMAP)
Click this option if you wish to allow the account to connect using MDaemon Connector[379]. **Note:** this option will only be available when support for MDaemon Connector is activated on your server.

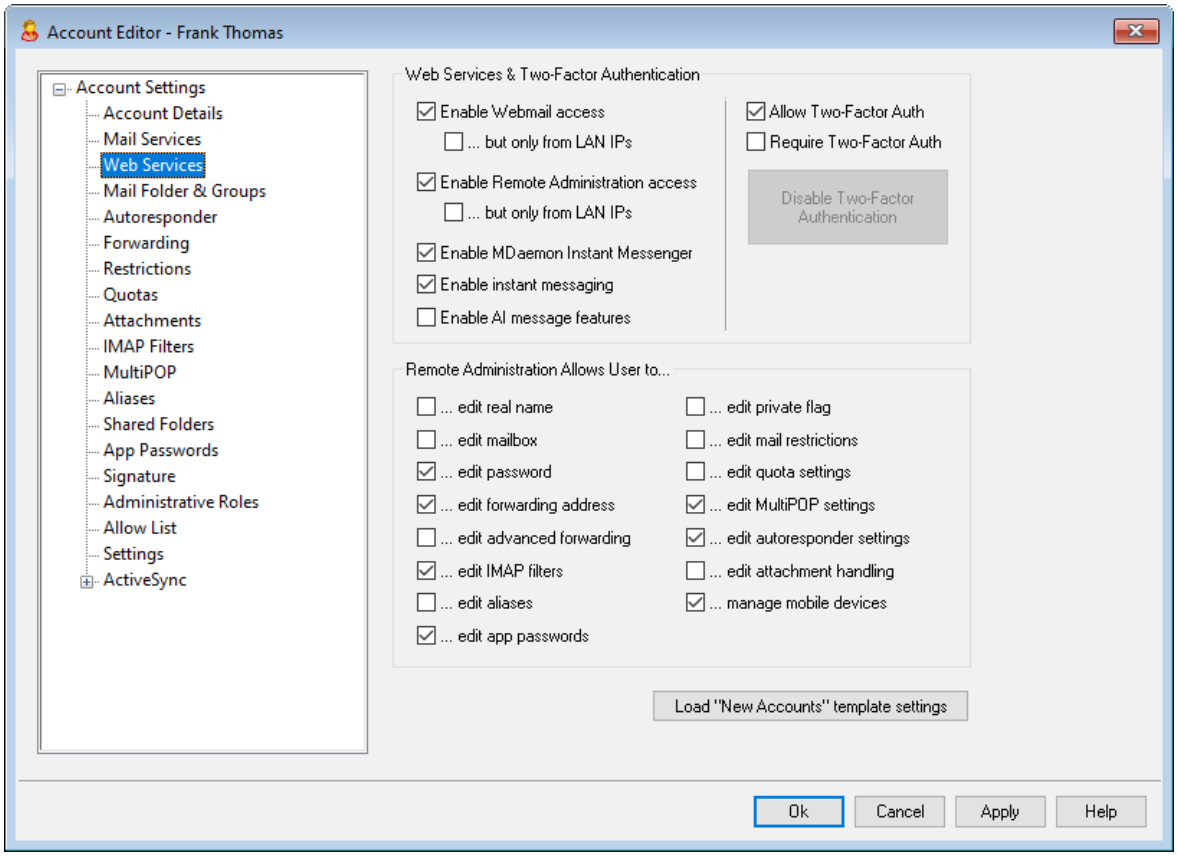
Restrict SMTP access to LAN IPs only
Check this box if you wish to restrict SMTP access to LAN IPs only. This will prevent accounts from sending mail unless they are connected to your network. If the account tries to send mail from an outside IP address the connection will be refused and dropped.

Smart Host Access

Smart host login/password
If the *Allow per-account authentication* option is enabled on the Delivery[89] screen at Setup » Server Settings, and you wish to use per-account authentication with this account instead of using the credentials specified on that screen, then specify the account's optional smart host credentials here. If you do not wish to use per-account authentication for this account then leave these options blank.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.4 Web Services



Web Service

Enable Webmail access
Enable this checkbox if you want the account to be able to access Webmail[308], which enables users to access their email, calendars, and other features using a web browser.

...but only from LAN IPs
Check this box if you wish to allow the account access to Webmail only when connecting from a LAN IP address[594].

Enable Remote Administration access
Check this box if you wish to grant the user permission to modify his or her account settings via Remote Administration[341]. The user will only be able to edit those settings that you designate below.

When this feature is enabled and the Remote Administration server is active, the user will be able to log in to Remote Administration by pointing a browser to the designated MDaemon domain and port assigned to Remote Administration[343] (e.g. `http://example.com:1000`). He will first be presented with a sign-in screen and then a screen that contains the settings that he has been given permission to edit. All he needs to do is edit whatever settings he chooses and then click the *Save changes* button. He can then sign out and close the browser. If he has access to

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Webmail then he can also access Remote Administration from the Advanced Options menu within Webmail.

If the user is a Global or Domain Administrator (designated on the Account Editor's Administrative Roles 741 screen) he will see a different screen after he logs in to Remote Administration.

...but only from LAN IPs
Check this box if you wish to allow the account access to Remote Administration only when connecting from a LAN IP address 594.

Enable MDaemon Instant Messenger
Click this box if you wish to enable MDIM 309 support for this account.

Enable Instant Messaging
When MDIM support is enabled for the account, click this option is you also wish to enable support for MDIM's instant messaging system. When this checkbox is cleared, you will be able to access MDIM's other features, but not instant messaging.

User can edit categories
Check this box if you wish to allow this Webmail user to edit categories. This is enabled by default. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Skip IP persistence check for Webmail sessions
When the Webmail Web Server 313 option to "Require IP persistence throughout Webmail session" is enabled, you can check this box if you wish to exempt this user from the IP persistence requirement. **Note:** This option is only available in the MDaemon Remote Administration (MDRA) 341 web-interface.

Enable AI message features
If the *Enable AI message features* option is enabled on this account domain's Webmail 187 dialog, check this box if you wish to allow this account to use those features in MDaemon Webmail; the features will only be available to the user when the domain-level option is enabled. **Note:** You can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features. See: "Webmail's AI Message Features 707" below for important information and cautions about using these features.

Two-Factor Authentication

MDaemon supports Two-Factor Authentication (2FA) for users signing into Webmail or MDaemon's Remote Administration web-interface. Accounts that sign into Webmail via HTTPS can activate Two-Factor Authentication for that account on the **Options » Security** screen in Webmail. From then on the user must enter a verification code when signing into Webmail or Remote Administration. The code is obtained at sign-in from an authenticator app installed on the user's mobile device or tablet. This feature is designed for any client that supports Google Authenticator. See the Webmail help file for more information on setting up 2FA for an account.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow Two-Factor Authentication
By default new accounts[782] are allowed to setup and use Webmail's Two-Factor Authentication (2FA) feature. Clear this checkbox if you so not wish to allow this account to use 2FA.

Require Two-Factor Authentication
Enable this option if you wish to force the account to use Two-Factor Authentication (2FA) when signing in to Webmail. If 2FA hasn't yet been configured for the account, the next time the account signs in to Webmail the user will be redirected to a page to set it up. See the Webmail help file for more information on setting up 2FA for an account.

Disable Two-Factor Authentication
Click this button if you need to disable Two-Factor Authentication for the account. This could be necessary if, for example, the user loses his device and can't otherwise access his authenticator data.

Remote Administration Allows User to...

...edit real name
Enabling this feature will allow the user to modify the account's *First and last name*[697] setting.

...edit mailbox
Enabling this feature will allow the user to modify the account's *Mailbox name*[697].

Because the *Mailbox name* is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

...edit password
Click this checkbox if you wish to allow the user to modify the account's *Mailbox password*. For more on password requirements, see: Passwords[840].

...edit forwarding address
When this feature is enabled, the user will be able to modify the forwarding[711] address settings.

...edit advanced forwarding
When this feature is enabled, the user will be able to modify the *Advanced Forwarding Settings*[711].

...edit IMAP filters
Use this control to enable the user to create and manage his own IMAP Filters[720].

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...edit aliases
Enable this option if you wish to allow the account holder to use Remote Administration to edit Aliases[725] associated with his or her account.

...edit app passwords
By default users can edit their App Passwords[734]. Clear this checkbox if you do not wish to allow the user to edit them.

...edit private flag
This option governs whether or not the user will be permitted to use Remote Administration to edit the *"Account hidden from "Everyone" lists, shared calendars, and VRFY"* option located on the Account Editor's Settings[744] screen.

...edit mail restrictions
This checkbox controls whether or not the account will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions[713] screen.

...edit quota settings
Click this checkbox if you wish to allow the account to modify the Quota[715] settings.

...edit MultiPOP settings
Click this checkbox if you wish to give the account permission to add new MultiPOP[723] entries and to enable/disable MultiPOP collection for those entries in MDRA[341]. When this option and the account's *Enable MultiPOP*[723] option are both turned on, a Mailboxes page will be available in Webmail[308] for the user to manage his MultiPOP mailbox settings. Finally, the global option for enabling/disabling the MultiPOP server is located at: Setup » Server Settings » MultiPOP[137].

...edit autoresponder settings
Click this checkbox if you wish to give the user permission to add, edit, or delete Autoresponders[708] for his account.

...edit attachment handling
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Attachments[718] screen.

...manage mobile device
Click this option if you wish to allow the account holder to use Remote Administration to manage his or her device-specific settings, such as for ActiveSync devices.

Load "New Accounts" template settings

Click this button to return the settings on this screen to the default values designated on the Web Services[782] screen of the *New Accounts* template.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Webmail's AI Message Features

As of MDaemon 23.5.0, the Pro theme in MDaemon's Webmail client includes various Artificial Intelligence (AI) features to help assist your users in managing their email and increasing productivity. These features are optional and disabled by default, but can be enabled for any user you choose.

With these features, in MDaemon Webmail you can use AI to:

- Give you a summary of the contents of an email message.
- Suggest a reply to the message, according to several guidelines that you can instruct the AI to use. You can set the *Tone* of the reply to be professional, respectful or casual. The *Position*, or stance, to take in the reply can be set to interested or not interested, agree or disagree, or skeptical. The *Attitude* the reply should convey can be set to confident, excited, calm, or apologetic. Last, you can designate the *Length* of the reply, ranging from very brief to detailed.
- Assist you in composing a new email message, based on some text you have already included. As with the *Suggest a Reply* option above, you can also designate the Tone, Position, Attitude, and Length for the AI to use when composing the message.

The *Enable AI message features* option on the main Webmail Settings 333 dialog controls whether or not support for the AI features is enabled by default for your domains. There is an option of the same name located on the Domain Manager's Webmail 187 dialog that can be used to override that main setting for specific domains. **Note:** enabling AI Message Features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services 703 screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates 774 and Groups 764 features to assign users to a group that has access to the AI message features.

Enabling accounts to use MDaemon's AI message features allows them to submit and receive information to and from third-party generative AI services, specifically ChatGPT by OpenAI. Administrators and users should therefore be aware that this introduces several potential privacy concerns due to the feature's ability to process personal data and generate potentially sensitive information. To address privacy concerns, it's vital for organizations to train their employees to use AI responsibly. **Note:** Data submitted to/from Open AI is not stored on the local server or on our network.

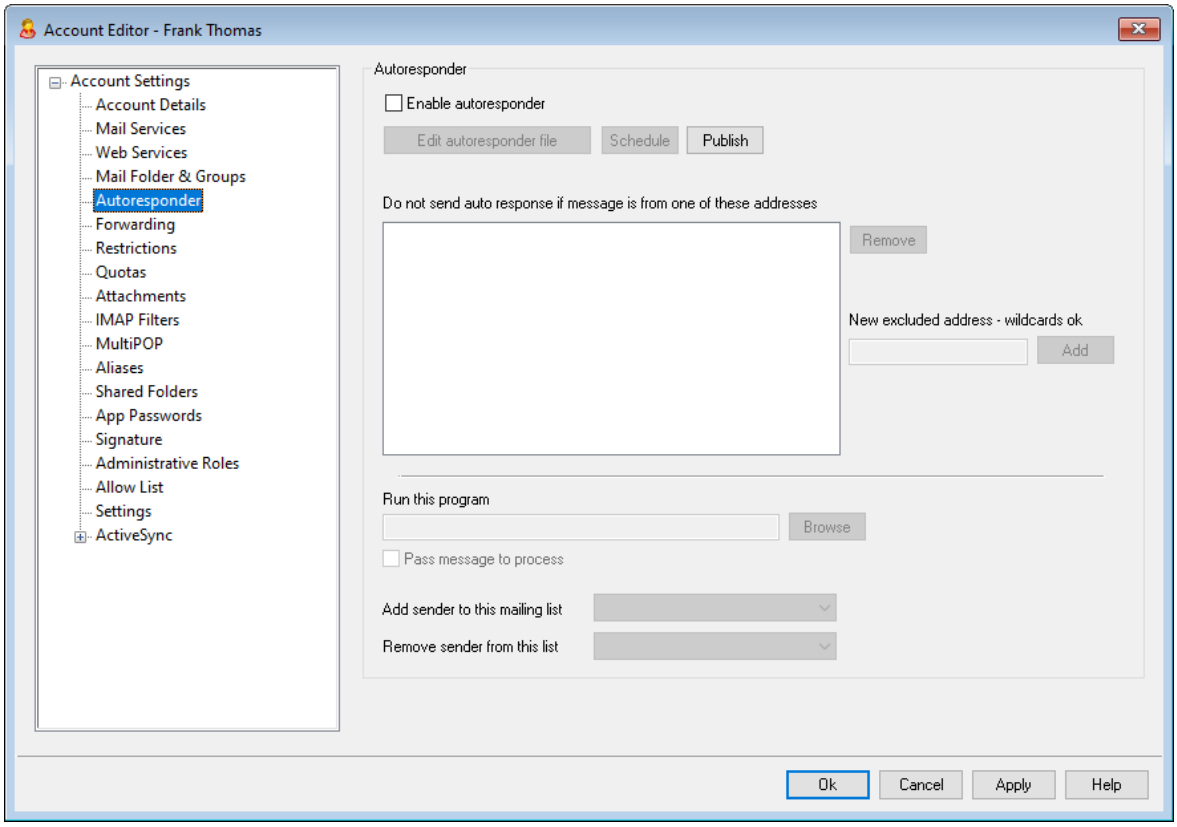
You can find MDaemon Technologies' AI Usage Policy at our Artifical Intelligence (AI) Information Page. On that same page there is also a link to OpenAI's Terms of Use.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Webmail 308
Remote Administration 341
Template Manager » Web Services 782

5.1.1.5 Autoresponder



Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with web access 703 to Webmail 308 or Remote Administration 341 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response messages are based on the contents of the `OOF.mrk` file, found in each user's root `\data\` folder. This file supports a large number of macros, which can be used to cause much of the message's content to be generated dynamically, making autoresponders quite versatile.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating from a user's same domain, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 827 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

Autoresponder

Enable autoresponder

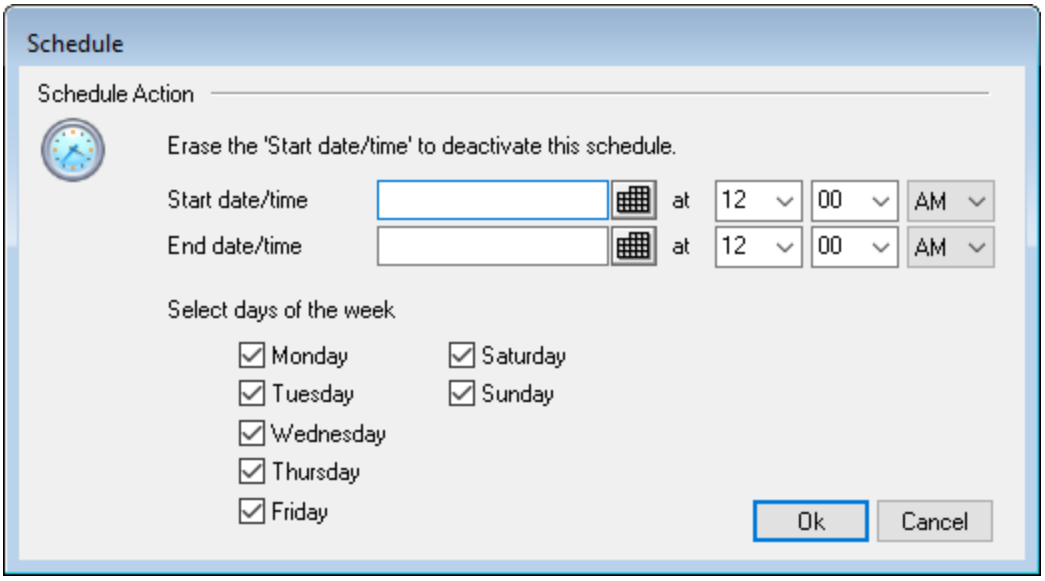
Enable this control to activate an autoresponder for the account. For more information on autoresponders see: Autoresponders 823.

Edit autoresponse file

Click this button to edit the account's autoresponse file. This file is the `oof.mrk` file, located in the account's `\data\` folder.

Schedule

Click this button to open the Schedule dialog on which you can set a start and end date and time for the Autoresponder, and set the days of the week for it to be active. Leave the Schedule blank if you want the Autoresponder to be active continually.



Publish

Click this button if you wish to copy this account's auto responder file and settings to one or more other accounts. Select the accounts to which you wish to copy the autoresponder and then click **Ok**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this autoresponder.

Occasionally auto response messages may be sent to an address that returns an auto response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. If you encounter one of those addresses, enter it here to prevent that from happening. There is also an option located on the Autoresponders » Settings 827 screen, which can be used to limit auto response messages to one response per sender per day.

Remove
Click this button to delete any selected entries from the list of excluded addresses.

New excluded address—wildcards okay
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Run a Program

Run this program
Use this field to specify the path and filename to a program that you wish to run when new mail arrives for this account. Care must be taken to ensure that this program terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run this Program* field will be passed the name of the triggering message as the first available command line parameter. When the autoresponder is set for an account that is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see Forwarding 711) then this function will be disabled.

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible:
`logmail /e /j /message=$MESSAGE$ /q`.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailing Lists

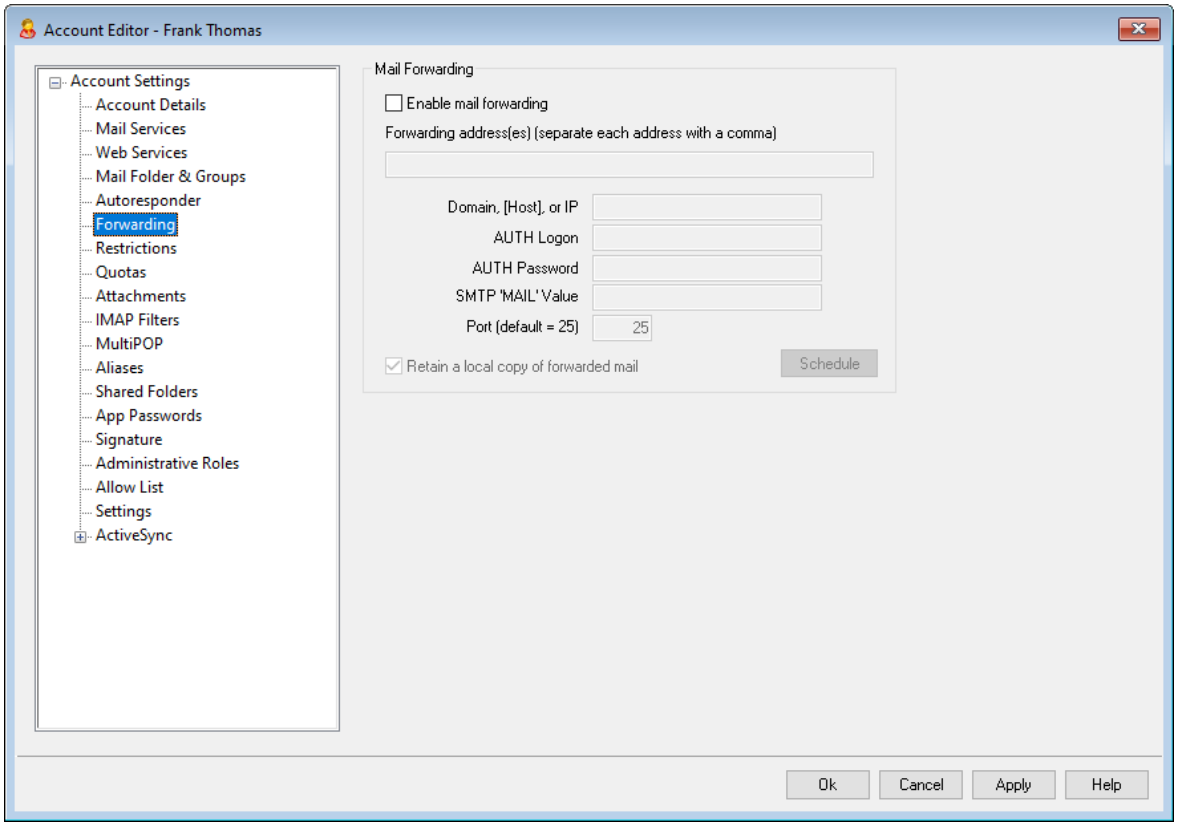
Add sender to this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically added as a member of that mailing list. This is a handy feature for building lists automatically.

Remove sender from this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically removed from the specified mailing list.

See:

Autoresponders » Accounts 823
Autoresponders » Exempt List 826
Autoresponders » Settings 827
Creating Auto Response Messages 828

5.1.1.6 Forwarding



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mail Forwarding

Enable mail forwarding
Check this box if you wish to forward this account's incoming messages to the address or addresses specified in the *Forwarding addresses* option below. MDaemon users with web access 703 to Webmail 308 or Remote Administration 341 can use the options provided to set the forwarding options for themselves rather than requiring an administrator to do so.

Forwarding addresses (separate each address with a comma)
Use this field to designate any email addresses to which you wish to forward copies of this account's incoming messages as they arrive. A copy of each new message arriving at the server will be automatically generated and forwarded to the addresses specified in this field, provided the *Enable mail forwarding* option above is checked. When forwarding to multiple addresses, separate each one with a comma.

Domain, [Host], or IP
If you wish to route the forwarded messages through another server, such as a particular domain's MX servers, then specify the domain or IP address here. If you wish to route the messages to a specific host, then enclose the value in brackets (e.g. `[host1.example.com]`).

AUTH Logon/Password
Enter any required login/password credentials here for the server to which you are forwarding the user's mail.

SMTP 'MAIL' Value
If an address is specified here, it will be used in the "`MAIL From`" statement sent during the SMTP session with the accepting host, instead of using the actual sender of the message. If you require an empty SMTP "`MAIL From`" statement (i.e. "`MAIL FROM <>`") then enter "[trash]" into this option.

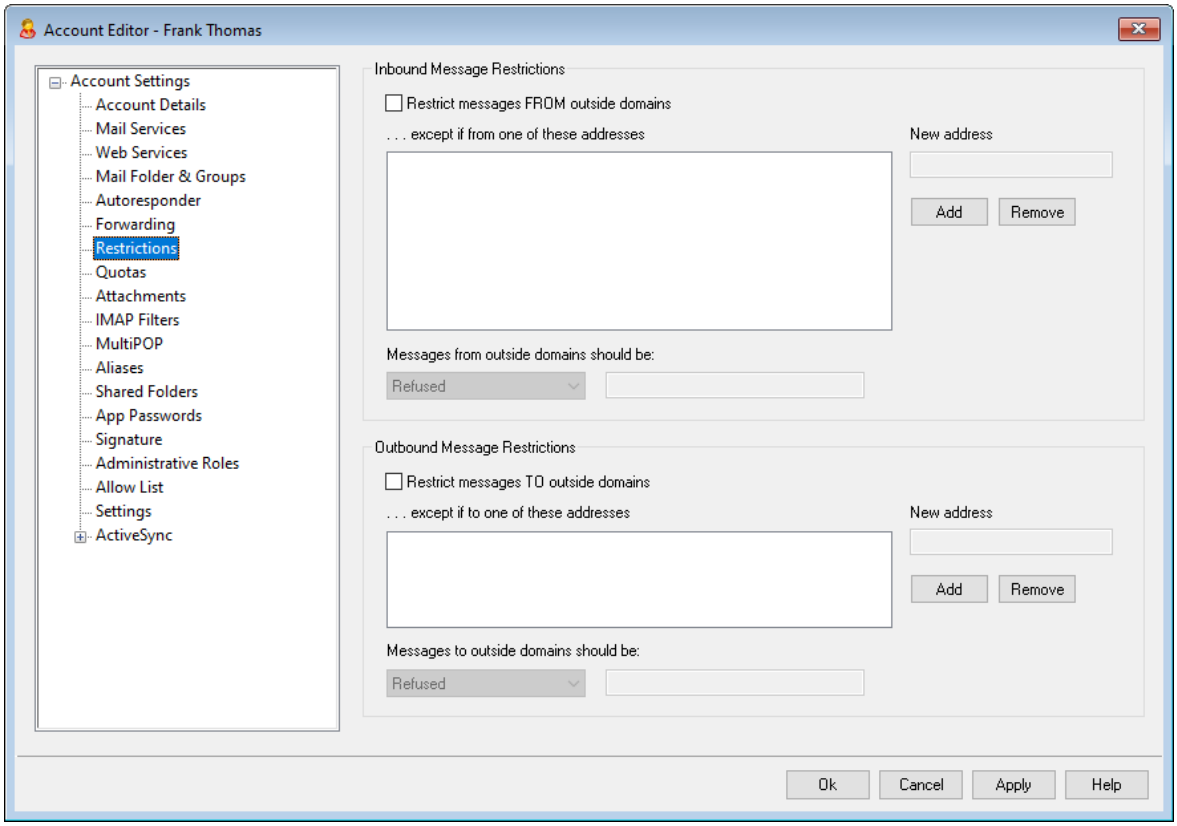
Port (default = 25)
MDaemon will send the forwarded messages using the TCP port specified here. The default SMTP port is 25.

Retain a local copy of forwarded mail
By default, a copy of each forwarded message is delivered normally to the local user's mailbox. If you uncheck this box then no local copy will be retained.

Schedule
Click this button to create a schedule for when the account's email will be forwarded. You can set a start date and time, an end date and time, and specify the days of the week on which mail will be forwarded.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.7 Restrictions



Use the options on this screen to govern whether or not the account will be able to send or receive mail to or from non-local domains.

Inbound Message Restrictions

Restrict messages FROM outside domains
Click this checkbox to prevent this account from receiving email messages from non-local domains.

...except if from one of these addresses
Addresses specified in this area are exceptions to the Inbound Message Restrictions. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then no inbound messages from any address at altn.com would be restricted.

New address
If you wish to add an address exception to the Inbound Message Restrictions list then type it here and click the *Add* button.

Add
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages from outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that are destined for this account but originate from a non-local domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

Returned to sender – Messages from restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of this account.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

Outbound Message Restrictions

Restrict messages TO outside domains
Click this checkbox to prevent this account from sending email messages to non-local domains.

...except if to one of these addresses
Addresses specified in this area are exceptions to the Outbound Message restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then outbound messages to any address at altn.com would not be restricted.

New address
If you wish to add an address exception to the Outbound Message Restrictions list then type it here and click the *Add* button.

Add
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages to outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that originate from this account but are destined for a non-local domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

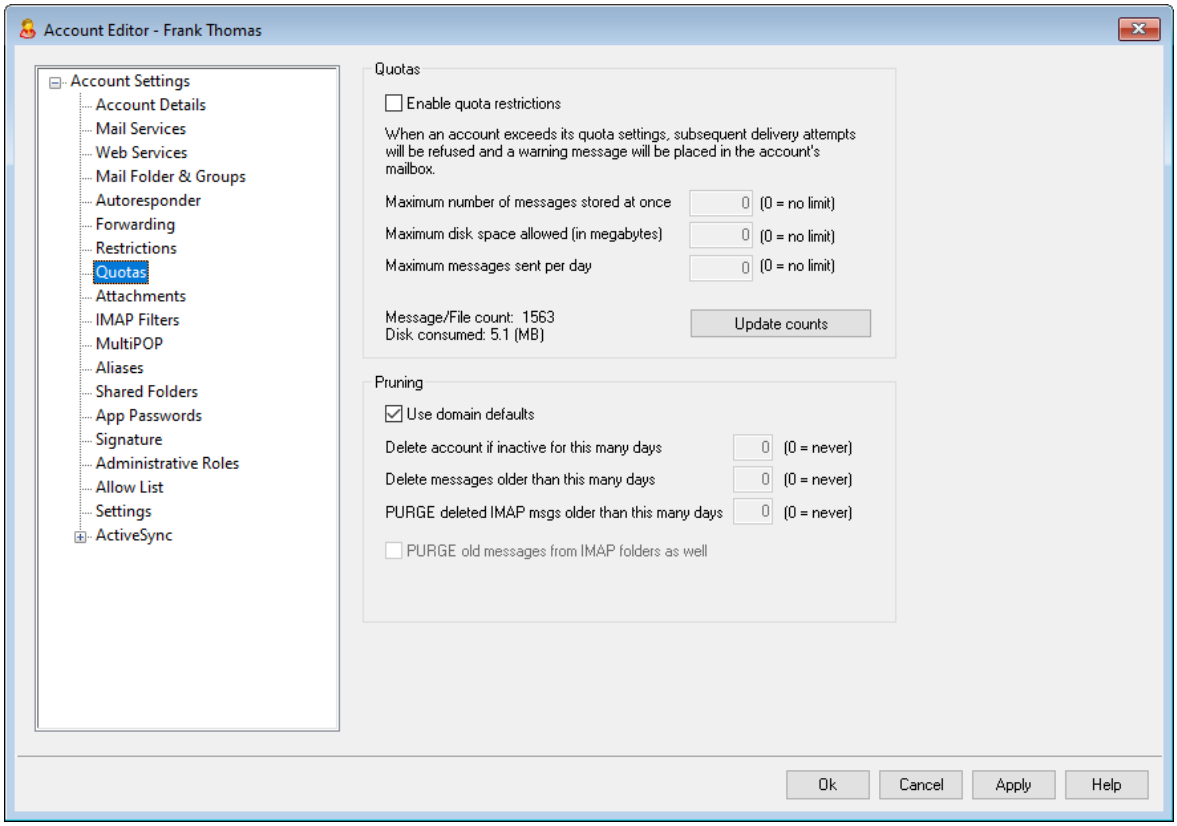
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Returned to sender – Messages to restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of the designated recipient.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

5.1.1.8 Quotas



Quotas

Enable quota restrictions
Check this box if you wish to specify a maximum number of messages that the account can store, set a maximum amount of disk space that the account can use (including any file attachments in the account's Documents folder), or designate a maximum number of messages that the account can send via SMTP per day. If a mail delivery is attempted that would exceed the maximum message or disk space limitations, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP 723 collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use the *Email a warning to user if this percent of their quota is reached* option at "Accounts » Account Settings » Quotas 796 " to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message.

Maximum number of messages stored at once
Use this option to designate the maximum number of messages that can be stored for the account. Using "0" in the option means there will be no limit to the number of messages permitted.

Maximum disk space allowed (in megabytes)
Use this option to designate the maximum amount of disk space that the account can use, including any file attachments that may be stored in the account's Documents folder. Using "0" in the option mean there will be no limit to the amount of disk space that the account can use.

Maximum messages sent per day
Use this option to designate the maximum number of messages that the account can send per day via SMTP. If the account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages the account can send.

Update counts
Click this button to update the *Message/File count* and *Disk consumed* statistics displayed to the left.

Pruning

The options in this section are used to designate when or if this account will be deleted by MDaemon if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain amount of time. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit.

Use domain defaults
The default Pruning settings are domain-specific and located on the Domain Manager's Settings 205 screen. If you wish to override the domain defaults for this account, clear this checkbox and set the desired values in the options below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
This is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age. **Note:** This option's setting does not apply to messages contained in IMAP folders unless you also enable the "*PURGE old messages from IMAP folders as well*" option below.

PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

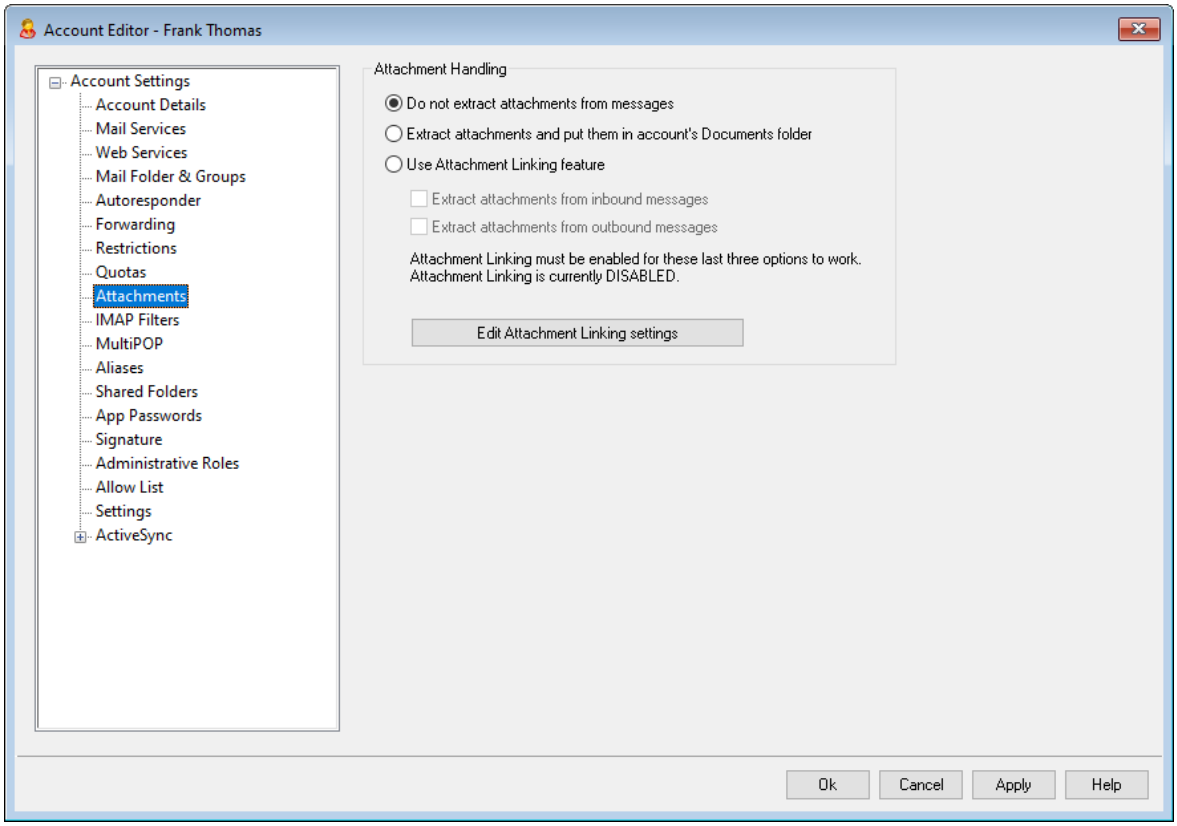
PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than this many days*" option above to apply to messages in IMAP folders as well. When this control is disabled, regular messages contained in IMAP folders will not be deleted due to their age.

See:

Template Manager » Quotas 796
Account Settings » Quotas 844

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.9 Attachments



Attachment Handling

This screen is used to control whether or not MDaemon will extract attachments from this account's email messages. You can use the Template Manager 799 to designate the default settings for these options.

Do not extract attachments from messages
If this option is selected, attachments will not be extracted from the account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

Extract attachments and put them in account's Documents folder
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages for this account. Extracted files are removed from the incoming message, decoded, and placed in the account's Documents folder. A note is then placed within the body of the message, stating the names of the files that were extracted. This option does not provide a link to the stored attachments, but users can use Webmail 308 to access their Documents folder.

Use Attachment Linking feature
Select this option if you wish to use the Attachment Linking feature for inbound or outbound messages with attachments.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If this option is selected but the Attachment Linking feature is disabled on the Attachment Linking 357 dialog, then attachments will not be extracted.

Extract attachments from inbound messages
When this option is enabled, attachments will be extracted from the account's incoming messages and stored in the location designated on the Attachment Linking 357 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file. This option is enabled by default.

Extract attachments from outbound messages
Check this box if you wish to use the Attachment Linking feature to extract attachments from the account's outbound messages. When the account sends an email, Attachment Linking will extract the file, store it, and replace it with a URL to download the file.

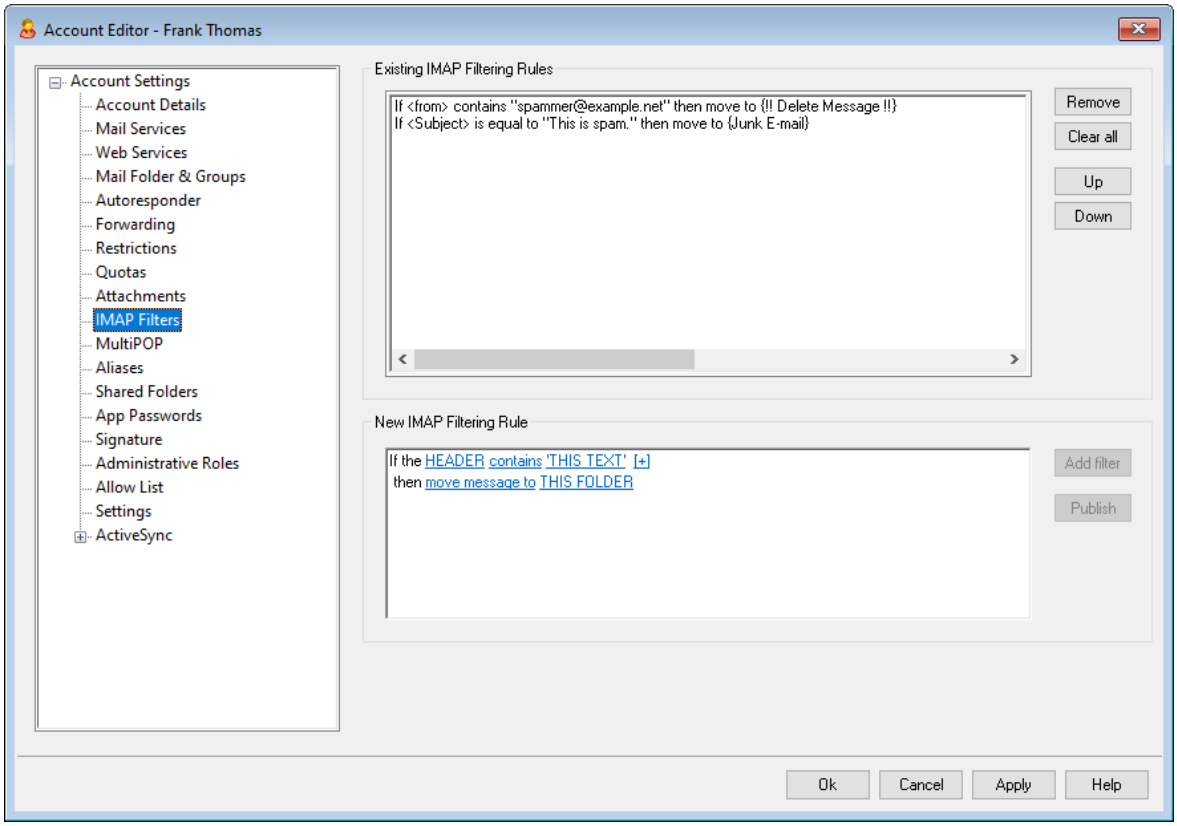
Edit Attachment Linking settings
Click this button to open the Attachment Linking 357 dialog.

See:

Attachment Linking 700
Template Manager » Attachments 799

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.10 IMAP Filters



IMAP and Webmail[308] users can have their mail routed automatically to specific folders on the server by using filters. Similar to the Content Filters[631], MDaemon will examine the headers of each of the account's incoming messages and then compare them to the account's filters. When a message for the account matches one of its filters, MDaemon will move it to the folder specified in that filter, delete the message, or redirect or forward it to the email address of your choosing. This method is much more efficient (for both the client and server) than attempting to filter the messages at the client, and since some mail clients do not even support local message rules or filtering, IMAP Filters provide this option to them.

Administrators can create filters via the IMAP Filters screen of the Account Editor, or by using Remote Administration[341]. However, you can also grant your users permission to create and manage filters for themselves within Webmail or Remote Administration. These permissions are set on the Web Services[703] screen.

Existing IMAP Filtering Rules

This box displays the list of all filter rules that have been created for the user's account. Filters are processed in the order in which they are listed until a match is found. Therefore, as soon as a message matches one of the filters it will be moved to the folder specified in that filter and then filter processing for that message will cease. Use the *Up* and *Down* buttons to move filters to different positions in the list.

Remove
Click a filter in the list and then click *Remove* to delete it from the list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Clear all
Click this button to delete all of the user's filters.

Up
Click a filter in the list and then click this button to move it to a higher position in the list.

Down
Click a filter in the list and then click this button to move it to a lower position in the list.

New IMAP Filtering Rule

Use the links in this area to construct a new filter rule. When your rule is complete, click **Add filter** to add it to the *Existing IMAP Filtering Rules*.

Filter Conditions

Click the links in the first section of the filtering rule to set the filter's conditions. When a message matches the filter's conditions then the Filter Action will be performed.

HEADER
Click "**HEADER"** to choose the header or other message component that you wish to examine as part of the filter rule. You can choose: **TO**, **CC**, **FROM**, **SUBJECT**, **SENDER**, **LIST-ID**, **X-MDMAILING-LIST**, **X-MDRCPT-TO**, **X-MDDNSBL-RESULT**, **X-SPAM-FLAG**, **MESSAGE SIZE**, **MESSAGE BODY**, or **Other...** If you choose "Other..." then a Filter Condition box will open for you to specify a header name not listed. If you click MESSAGE SIZE, the "contains" and 'THIS TEXT' links will be replaced by "is greater than" and "0 KB" respectively.

contains / is greater than
Click "**contains**" or **is greater than** to choose what type of condition to set when the header is examined. For example, does the header exist or not exist, contain or not contain certain text, start or end with certain text, or the like. You can choose from the following conditions: **starts with**, **ends with**, **is equal to**, **is not equal to**, **contains**, **does not contain**, **exists**, **does not exist**, **is greater than**, or **is less than**. The "is greater than" and "is less than" options are only available when the HEADER link is set to "MESSAGE SIZE."

THIS TEXT / 0 KB
Enter the text that you want MDaemon to search for when scanning the header that you selected for the filter. When the HEADER option is set to MESSAGE SIZE, the link will say "0 KB" and the Filter Condition dialog will have a box for stating the "Message size in KB."

[+] [x] and
Click **[+]** if you wish to set two or more conditions for the filter rule. This will add another line containing the "HEADER," "contains," and "THIS TEXT" components for expanding the filter. When testing a message against a filter rule with multiple conditions, by default the message must pass each of the conditions for it to match the rule. Click "**and**" and then select "**or**" if you want the message to

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

match the rule when it passes any of the conditions. When a filter rule has multiple lines, you can click **[x]** next to any line that you wish to delete.

Filter Actions

Click the links in the bottom section of the filtering rule to designate the action to take when a message matches the filter's conditions.

move message to
Click "**move message to**" to designate the filter action. You can choose: **move message to**, **delete message**, **redirect message to**, or **forward message to**.

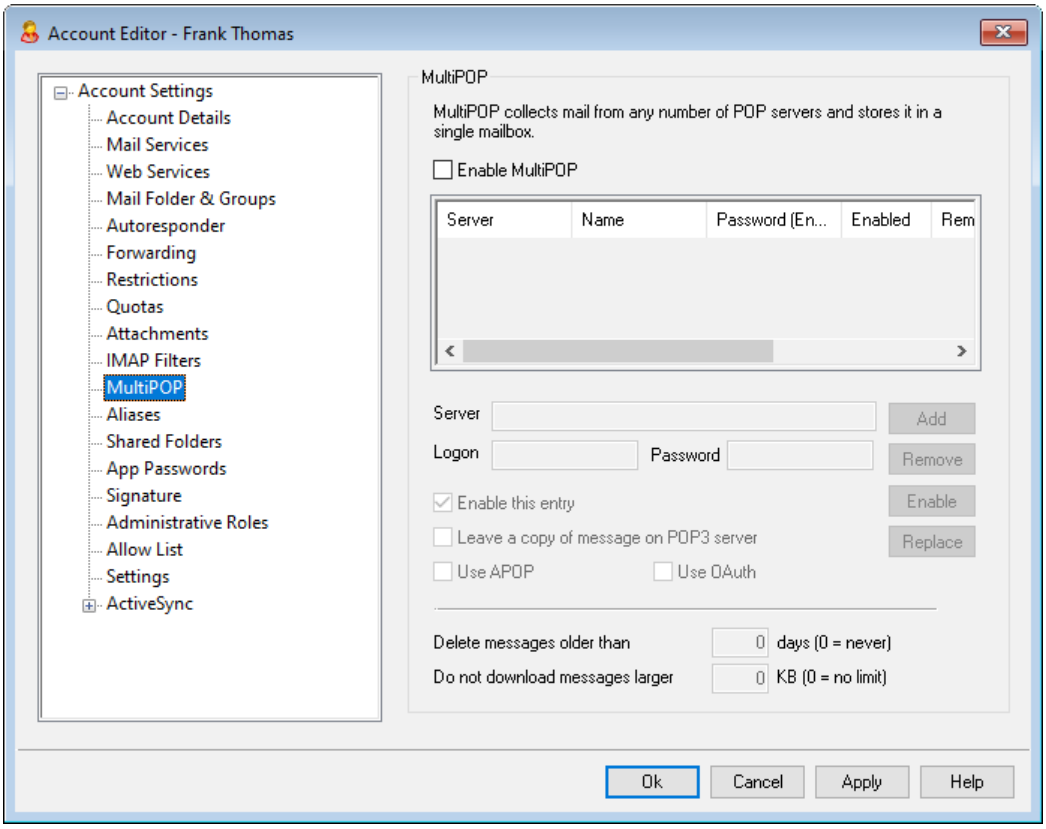
THIS FOLDER / EMAIL
If you selected the "move message to" action, then click **THIS FOLDER** to designate the folder to which the message should be moved. If you chose to redirect or forward the message, then click **EMAIL** and enter the recipient's email address. For redirected messages, no changes to the message headers or body are made. The only thing changed is the SMTP envelope recipient. For forwarded messages, a new message will be created and sent, with the Subject header and body content taken from the original message.

Add filter
When you are finished creating your new filter, click this button to add it to the *Existing IMAP Filtering Rules*.

Publish
After creating a rule, click **Publish** if you wish to copy that rule to every other user account belonging to this account's domain. You will be asked to confirm your decision to copy the rule to the other accounts.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.11 MultiPOP



The MultiPOP feature allows you to create an unlimited number of POP3 host/user/password combinations for collection of mail messages from multiple sources. This is useful for your users who have mail accounts on multiple servers but would prefer to collect and pool all their email together in one place. Before being placed in the user's mailbox, MultiPOP collected mail is first placed in the local queue so that it can be processed like other mail having Autoresponders and Content filters applied to it. The scheduling options for MultiPOP are located at: Setup » Event Scheduling » Mail Scheduling » MultiPOP Collection 375.

Enable MultiPOP
Check this box to enable MultiPOP processing for this account. If you wish to allow the user to edit his own MultiPOP settings in MDRA 341, then enable the "*...edit MultiPOP settings*" option on the account's Web Services 703 page. When this option and the web services option are both enabled, a Mailboxes page will be available in Webmail 308 for the user to manage his MultiPOP mailbox settings. The global option for enabling/disabling the MultiPOP server is located at: Setup » Server Settings » MultiPOP 137. If that option is off, MultiPOP cannot be used, even if this account option is on.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Creating or Editing a MultiPOP Entry

Server
Enter the POP3 server from which you wish to collect mail. If this server requires you to connect on a specific port other than the standard POP3 ports, then append ":[port]" to the server name. For example, "mail.example.com:1000". When collecting from Gmail or Microsoft (Office) 365, use "pop.gmail.com:995" or "outlook.office365.com:995", respectively.

Logon
Enter the POP3 username or login name that is associated with the mail account on the server specified above.

Password
Enter the POP3 or APOP password used for accessing the mail account on the specified server.

Use APOP
Click this checkbox if you want the MultiPOP entry to use the APOP method of authentication when retrieving mail from its corresponding host.

Use OAuth
Choose this authentication method when collecting mail from Gmail or Office365. See the MultiPOP OAuth 2.0 instructions 137 on the Server Settings » MultiPOP page for more information. **Note:** the "*...edit MultiPOP settings*" option on the account's Web Services 703 page must also be enabled for the user to be able to use OAuth with Gmail or Office 365, because he or she must sign in to Webmail and go to the **Mailboxes** page in order to authenticate the Gmail or Office 365 mailbox entry.

Leave a copy of message on POP3 server
Click this checkbox if you want to leave a copy of collected messages on the server. This is useful when you plan to retrieve these messages again at a later time from a different location. If you wish to override this option for all users, meaning that the messages will always be deleted from the POP server after they are downloaded to MDaemon, you can do so by enabling the "*MultiPOP always deletes mail from all servers after collection*" option at Setup » Server Settings » MultiPOP 137.

Add
After entering all of the information for the new MultiPOP entry, click this button to add it to the list.

Remove
If you wish to delete one of your MultiPOP entries, select the desired entry and then click this button.

Enable/disable
Clicking this button toggles the state of the selected MultiPOP entries, giving you control over whether MDaemon will collect mail for this entry or skip over it when it performs its MultiPOP processing.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Replace
To edit an entry, click the entry in the list, make any desired changes, and click this button to save the changes to the entry.

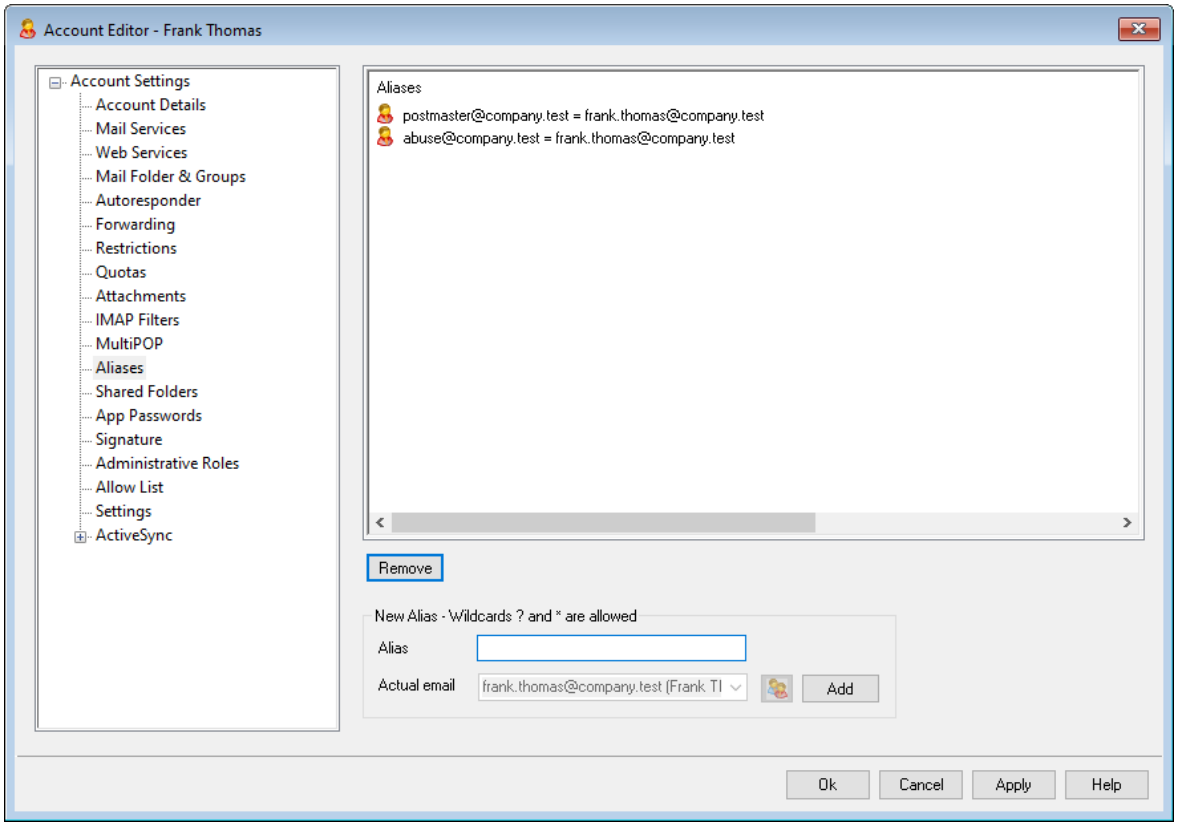
Delete messages older than [XX] days (0 = never)
This is the number of days that a message can remain on the MultiPOP host before it will be deleted. Use "0" if you do not wish to delete older messages.

Don't download messages larger than [XX] KB (0 = no limit)
Enter a value here if you wish to limit the size of messages that may be downloaded.

See:

Server Settings » MultiPOP 137
Scheduling MultiPOP Collection 375

5.1.1.12 Aliases



This screen lists all address aliases 818 associated with the account, and can be used to add or remove them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Removing an Alias

To remove an alias from the account, select the alias in the list and then click **Remove**.

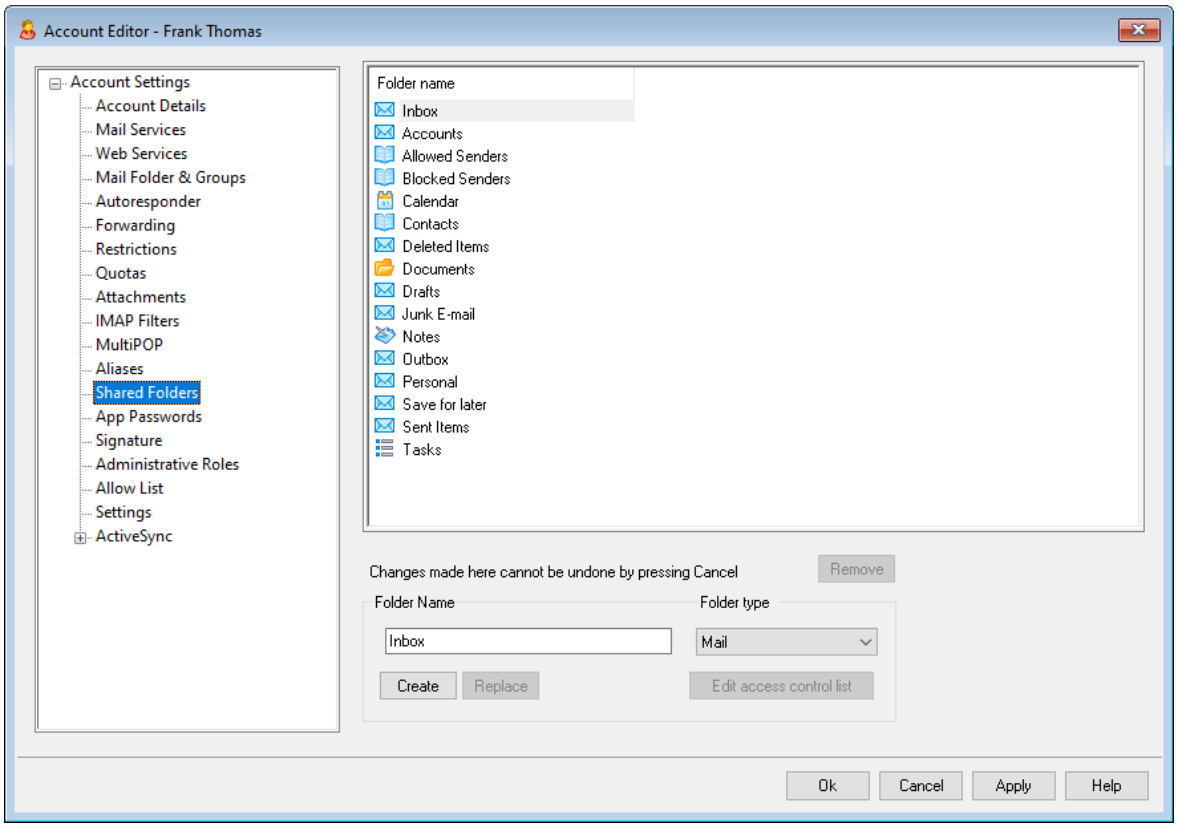
Adding an Alias

To add a new alias to the account, in the *Alias* box type the address that you wish to associate with the account and then click **Add**. The wildcards "?" and "*" are permitted, representing single characters and single words, respectively.

See:

Account Settings » Aliases 818

5.1.1.13 Shared Folders



This screen is only available when the *Enable public folders* option is enabled on the Public & Shared Folders 113 screen, located at Setup » Server Settings » Public & Shared folders.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

> Public Folders can be managed from the Public Folder Manager 300.

This top section displays all of the user's IMAP Folders and can be used to share access to them with other MDaemon users or Groups 764. When the account is first created, this area will only have the Inbox listed until you use the *Folder name* and *Create* options (or the options on IMAP Filters 720) to add folders to it. Subfolders in this list will have the folder and subfolder names separated by a slash.

Remove
To remove a Shared IMAP folder from the list, select the desired folder and then click the *Remove* button.

Folder name
To add a new folder to the list, specify a name for it in this option and click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, then prefix the new folder's name with the parent folder's name and a slash. For example, if the parent folder is "My Folder" then the new subfolder name would be "My Folder/My New Folder". If you don't want it to be a subfolder then name the new folder "My New Folder" without the prefix.

Nest under
Use the drop-down list to choose the parent folder under which this shared folder will nest. **Note:** This option is only available in the MDRA 341 web-interface.

Folder type
Use this drop-down list to choose the type of folder you wish to create: Mail, Calendar, Contacts, and so on.

Create
After specifying a folder's name click this button to add the folder to the list.

Replace
If you wish to edit one of the Shared Folders, click the entry, make the desired change, and then click *Replace.*

Edit access control list
Choose a folder and then click this button to open the Access Control List 302 dialog for that folder. Use the Access Control List to designate the users or groups that will be able to access the folder and the permissions for each user or group.

See:

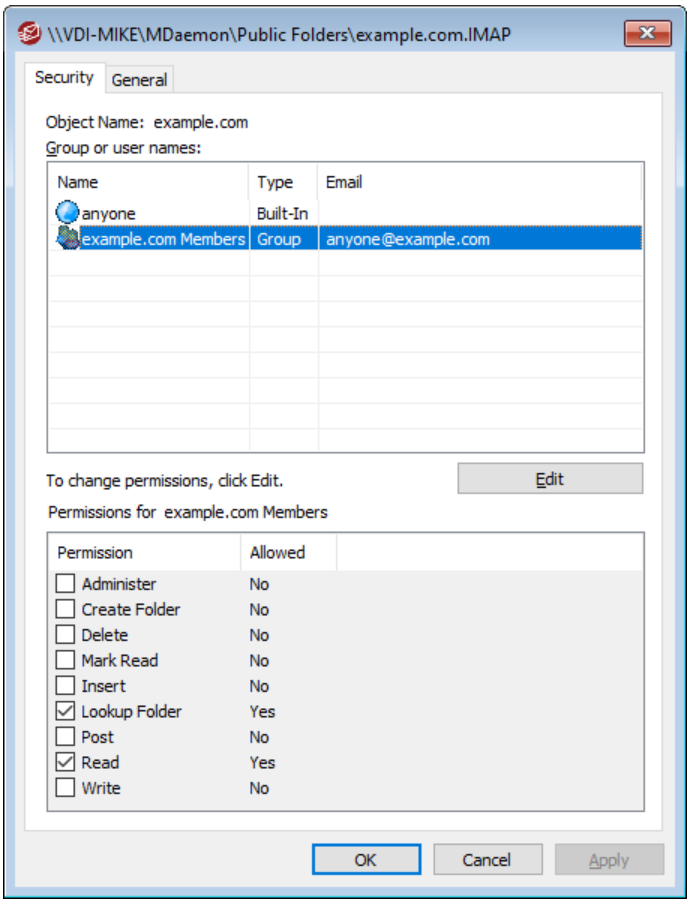
Access Control List 302
Public Folder Manager 300

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

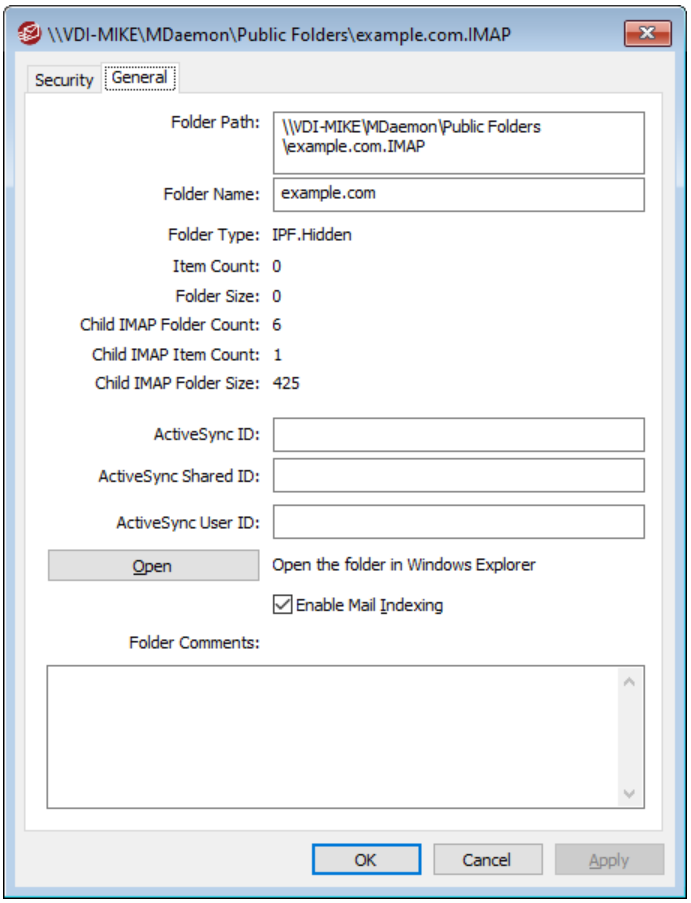
5.1.1.13.1 Access Control List

The Access Control List (ACL) is used for setting user or group access permissions for your public and shared folders[110]. It is accessed from the *Edit ACLs* button on the Public Folder Manager[300] or the *Edit access control list* button on Account Editor's Shared Folders[726] screen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Security

This tab displays the list of groups or users associated with the folder and the specific access permissions granted to each. Select a group or user in the list to display its permissions 305 for review in the Permissions window below. To edit the permissions, click **Edit** 304.

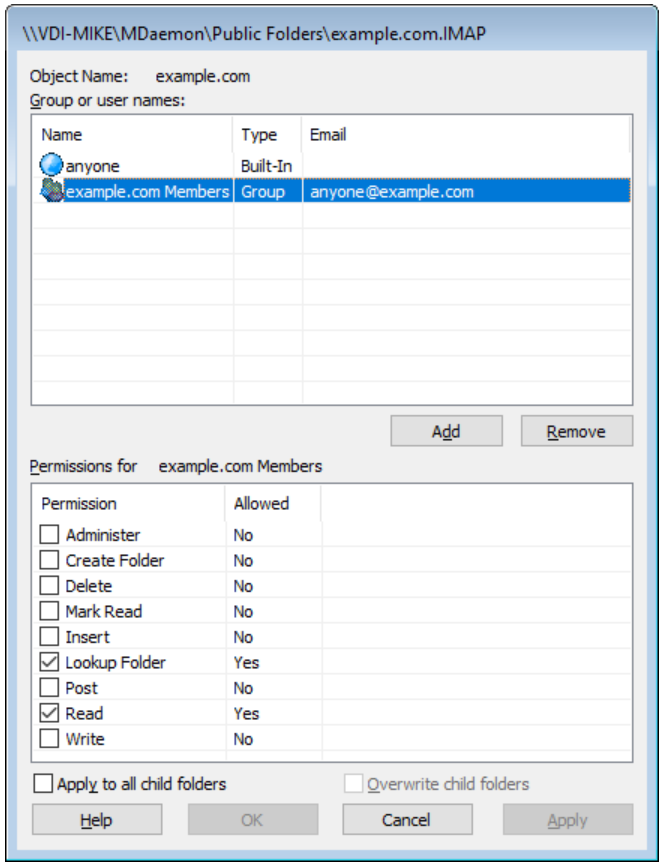
General

This tab displays the folder's properties, such as its path, name, type, size, and so on.

ACL Editor

Click **Edit** on the ACL's Security tab to open the ACL Editor for modifying access permissions.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Object Name
This is the name of the object or folder to which the ACL permissions will apply.

Group or user names
These are the groups or users to which some level of access permissions may have been granted. Select a group or user to display its permissions in the *Permissions for <group or user>* window below. Check the box next to any access permission that you wish to grant to the group or user.

Add
To grant access permissions to a group or user not listed above, click **Add** 306.

Remove
To remove a group or user, select its entry in the list above and click **Remove**.

Permissions for <group or user>
Check the box next to any access permission that you wish to grant to the group or user selected above.

You can grant the following access control permissions:

Administer – user can administer the ACL for this folder.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Create – user can create sub-folders within this folder.

Delete – user can delete items from this folder.

Mark Read – user can change the read/unread status of messages in this folder.

Insert – user can append and copy items into this folder.

Lookup Folder – user can see this folder in his personal list of IMAP folders.

Post – user can send mail directly to this folder (if folder allows).

Read – user can open this folder and view its contents.

Write – user can change flags on messages in this folder.

Apply to all child folders
Check this box if you wish to apply this folder's access control permissions to any sub-folders it currently contains. This will add the folder's user and group permissions to the child folders, replacing them when there are any conflicts. It will not, however, delete any other user or group permissions that currently have access to those folders.

Example,

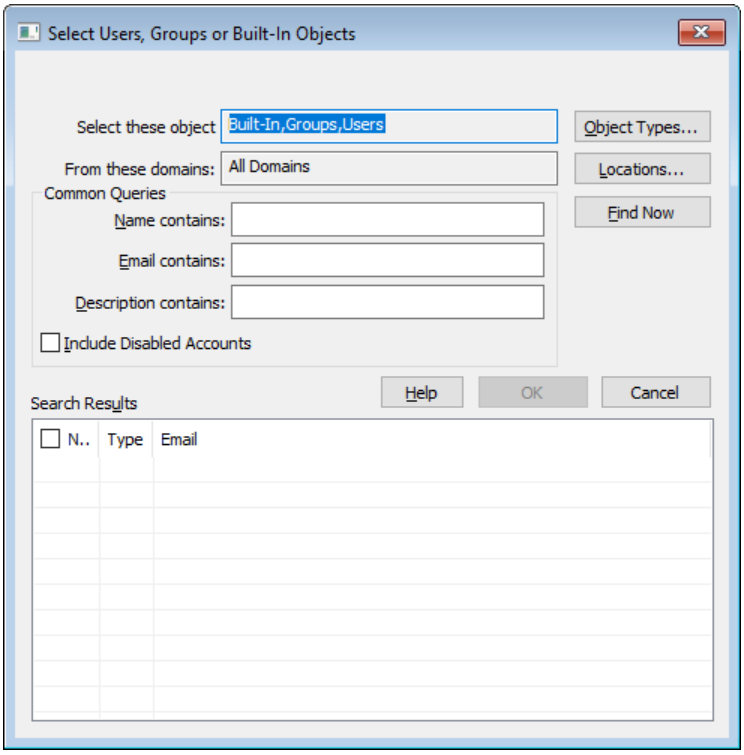
The parent folder grants certain permissions to `User_A` and `User_B`. The child folder grants permissions to `User_B` and `User_C`. This option will add `User_A` permissions to the child folder, replace the child folder's `User_B` permissions with those from the parent folder, and do nothing to the `User_C` permissions. Therefore the child folder will then have `User_A`, `User_B`, and `User_C` permissions.

Overwrite child folders
Check this box if you wish to replace all child folder access permissions with the parent folder's current permissions. The child folder permissions will then be identical to the parent folder.

Adding a Group or User

Click **Add** on the ACL Editor if you wish to add another group or user to the Access Control List. This opens the Add Group or User screen that you can use to search for them and then add them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Select these object types
Click **Object Types...** to select the object types that you wish to search for the groups or users you wish to add. You can select: Built-In, Groups, and Users.

From these locations
Click **Locations...** to select the domains that you wish to search. You can select all of your MDaemon domains or specific domains.

Common Queries
Use the options in this section to narrow your search by specifying all or part of the user's name, email address, or the contents of the account's Description 697. Leave these fields blank if you want the search results to contain every group and user that matches the Object Types and Locations specified above.

Include Disabled Accounts
Check this box if you wish to include disabled accounts 697 in your search.

Find Now
After you have specified all of your search criteria, click **Find Now** to perform the search.

Search Results
After performing the search, select any desired groups or users in the Search Results and click **OK** to add them to the ACL.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

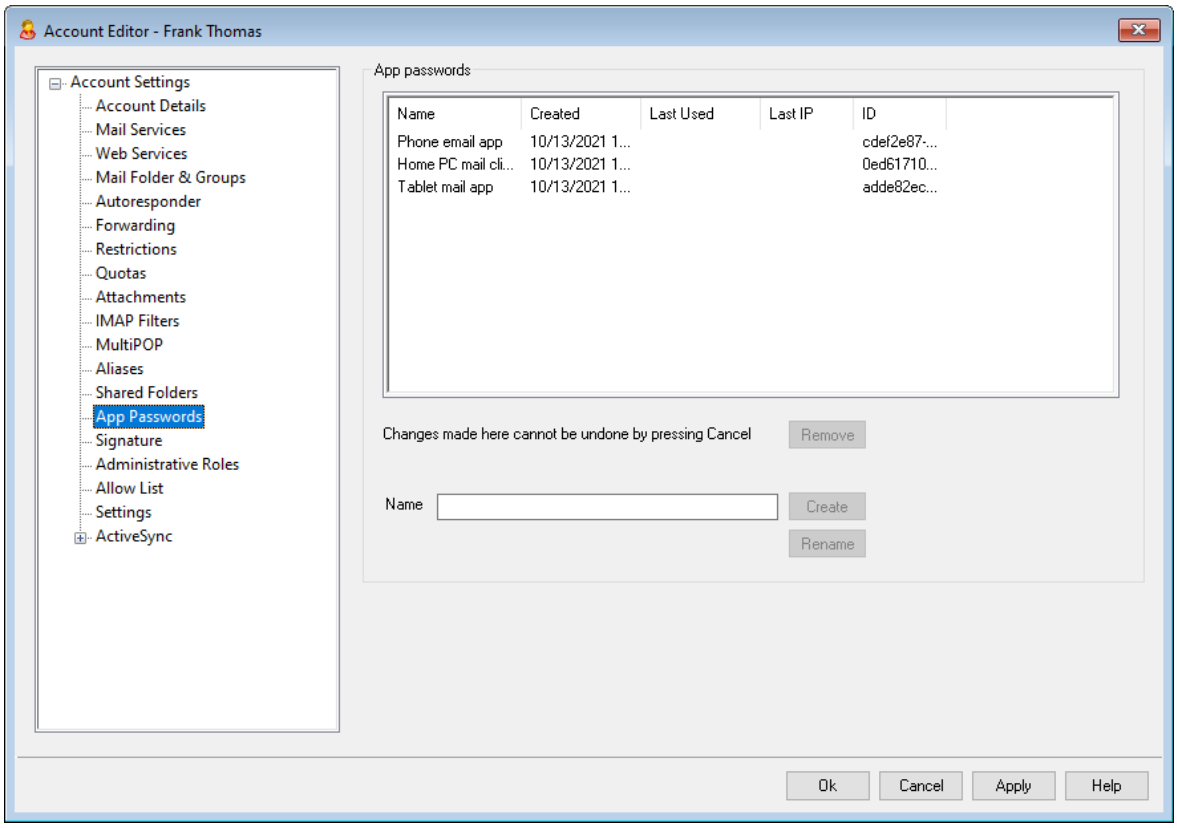
Access rights are controlled through MDaemon's support for Access Control Lists (ACL). ACL is an extension to the Internet Message Access Protocol (IMAP4), which makes it possible for you to create an access list for each of your IMAP message folders, thus granting folder access rights to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog.

ACL is fully discussed in RFC 2086, which can be viewed at: http://www.rfc-editor.org/rfc/rfc2086.txt.

See:

Public Folder Manager 300
Public Folders Overview 110
Public & Shared Folders 113
Account Editor » Shared Folders 726
Mailing List » Public Folders 289

5.1.1.14 App Passwords



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

App Passwords

App Passwords are very strong, randomly-generated passwords for use in email clients and apps, to help make your email apps more secure since they can't be protected by Two-Factor Authentication 703 (2FA). 2FA is a secure way for a user to sign in to Webmail or MDaemon Remote Administration (MDRA), but an email app can't use it, because the app must be able to access your email in the background without you having to enter a code from your authenticator app. The App Passwords feature allows you to create strong, secure passwords for use in your apps, while still keeping your account password secured by 2FA. App Passwords can only be used in email apps, they cannot be used to sign in to Webmail or MDRA. This means that even if an App Password were somehow compromised, the unauthorized user still wouldn't be able to get into your account to change your password or other settings, but you, however, would still be able to sign in to your account with your account password and 2FA, to delete the compromised App Password and create a new one if needed.

If you do not wish to allow a user to use App Passwords, you can do so by disabling the *...edit app passwords* 703 option on the user's Web Services page. If you wish to disable support for App Passwords for all users, you can do so using the *Enable app passwords* 840 option on the Passwords page.

App Password requirements and recommendations

- In order to create App Passwords, 2FA must be enabled for the account (although you can turn off this requirement 840 if you choose).
- App Passwords can only be used in email apps—they cannot be used to sign in to Webmail or MDRA.
- Each App Password is displayed only once, when it is created. There is no way to retrieve it later, so users should be ready to enter it into their app when it is created.
- Users should use a different App Password for each email app, and they should revoke (delete) its password whenever they stop using an app or when a device is lost or stolen.
- Each App Password lists when it was created, when it was last used, and the IP address from which it last accessed the account's email. If a user finds something suspicious about the Last Used or Last IP data, the user should revoke that App Password and create a new one for his or her app.
- When an account password is changed, all App Passwords are automatically deleted—a user cannot continue using old App Passwords.

Creating and using App Passwords

User's will typically create and manage their own App Passwords from within Webmail following the steps outlined below (this information is included in the Webmail help file). Before the user begins, he should have his email app or client ready to enter the password, because the App Password will only be displayed once while creating it.

1. Have the app or email client ready to enter the App Password.
2. Sign in to Webmail and click **Options » Security**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

3. Enter the account password in **Current Password**.
4. Click **New App Password**.
5. Enter the name of the app that will use this password (e.g. "Phone email app"), and click **OK**.
6. Copy/paste or manually enter the displayed password into the email app, or paste it into a text file or write it down if necessary. If one copies the password to use later then he should delete the copy after entering it into his email client. When finished, click **OK**.

If for some reason you need to create or delete an App Password for one of your users, you can do so using the options on this page. Just as in Webmail, the App Password will only be displayed once when it is created, so it should immediately be entered into the app or copied somewhere to give to the user later.

There is an account option on the Account Editor's Settings 744 page that you can use to "*Require app password to log in to SMTP, IMAP, ActiveSync, etc.*"

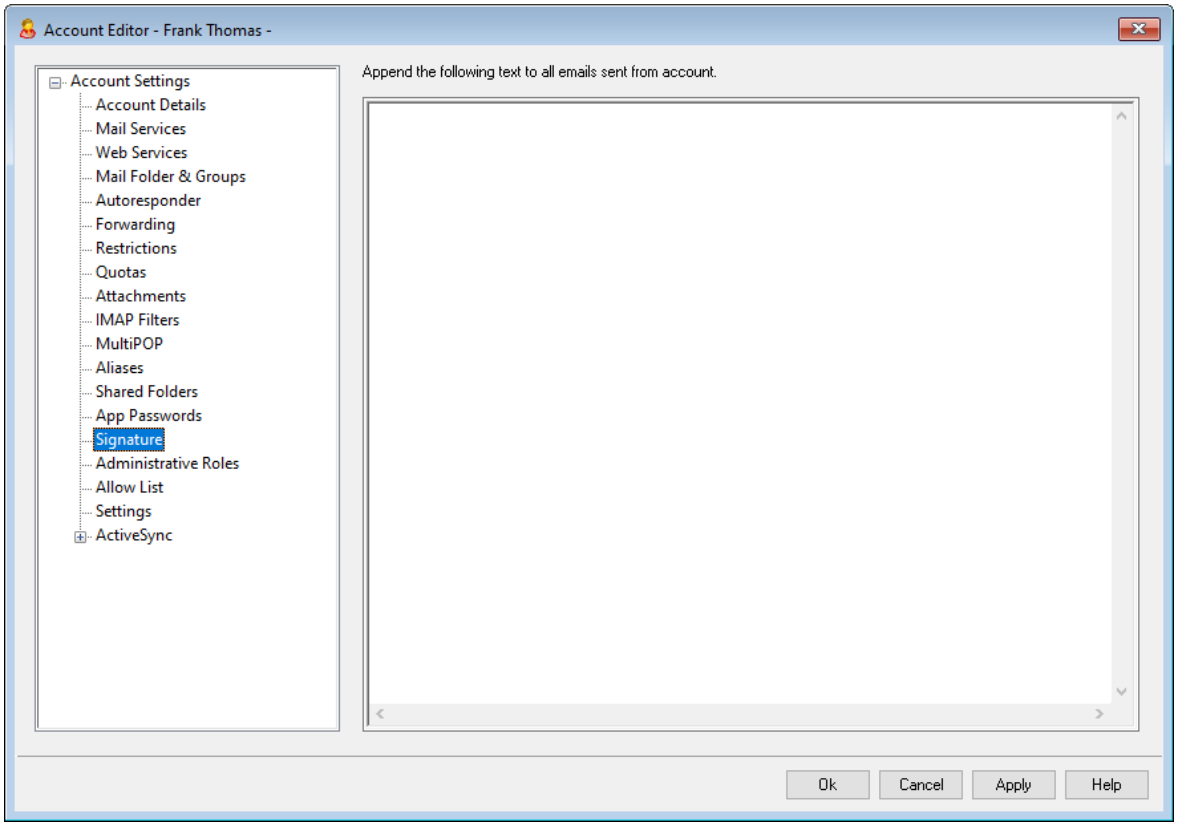
Requiring App Passwords can help protect an account's password from dictionary and brute force attacks via SMTP, IMAP, etc. This is more secure because even if an attack of this sort were to guess an account's actual password, it wouldn't work and the attacker wouldn't know, because MDaemon would only accept a correct App Password. Additionally, if your accounts in MDaemon are using Active Directory 806 authentication and Active Directory locks an account after a number of failed attempts, this option can help prevent accounts from being locked out, because MDaemon will only check the App Passwords, not try to authenticate to Active Directory.

See:

Passwords 840
Account Editor » Settings 744

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.15 Signature



Account Signature

Use this screen to designate a signature that will be appended to the bottom of every email that the account sends. This signature is added in addition to any other signatures or footers added by other options, such as the signature option included in Webmail and other mail clients, the Default 127 and Domain 195 signature options, and Mailing List footers 287. Default/Domain Signatures and Mailing List footers are always added below Account Signatures.

Users with access to Webmail or Remote Administration 341 can edit their own signatures from there.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Users can control the placement of MDaemon signatures in their emails by placing any of the **Signature Selector** macros into a message wherever they want the signature to appear.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**
Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
Instant Messaging and Web	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
Address	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
Business Related	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**
Business main phone	**$CONTACTBUSINESSMAINPHONE$**
Business phone	**$CONTACTBUSINESSPHONE$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

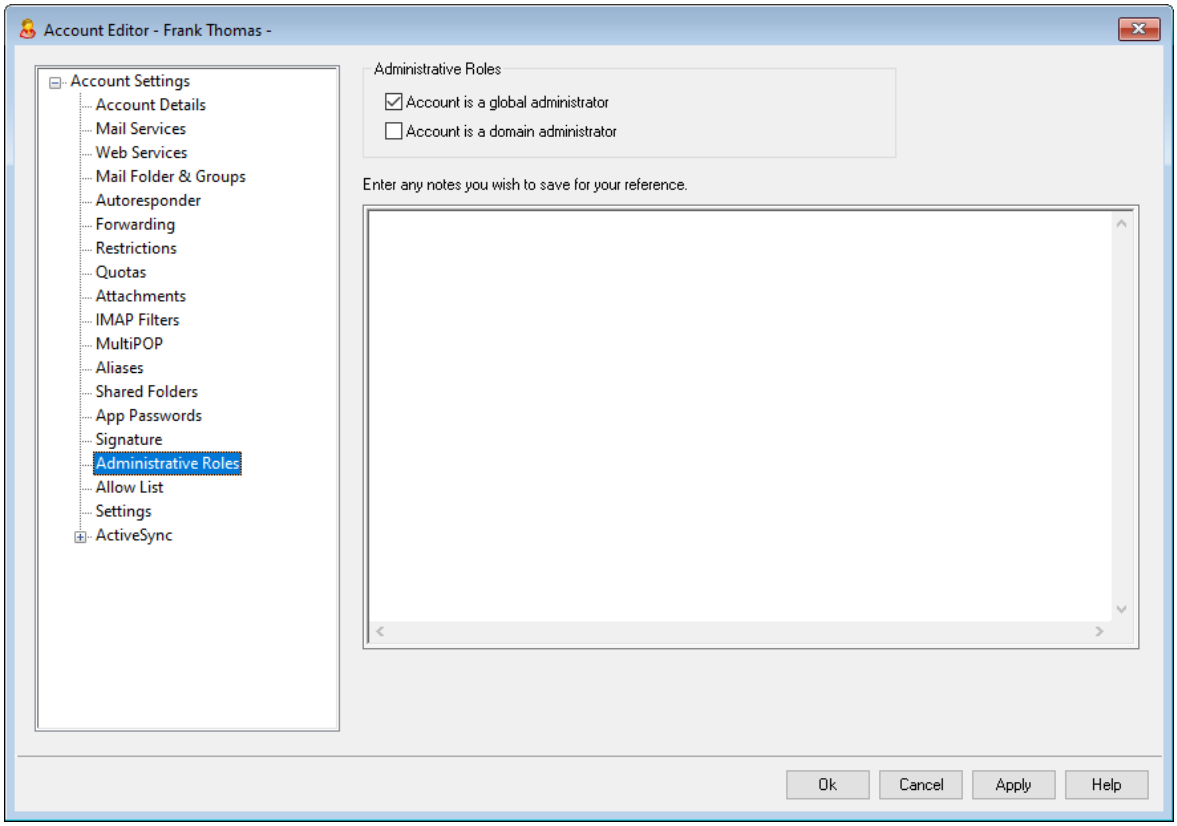
Business phone 2	$CONTACTBUSINESSPHONE2$
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Default Signatures 127
Domain Signature 195
Mailing List Footers 287

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.16 Administrative Roles



Administrative Roles

Account is a global administrator
Enable this checkbox to grant the user server-level administrative access. Global administrators have:

- Full access to server configuration, all users, and all domains via Remote Administration
- Access to all MDaemon users of all MDaemon domains as Instant Messaging buddies.
- The ability to post to all mailing lists even if flagged as "Read Only".
- The ability to post to all mailing lists even if not a member.

The user will have complete access to MDaemon's files and options. For more on the administrative options within the Remote Administration web-interface, see Remote Administration 341.

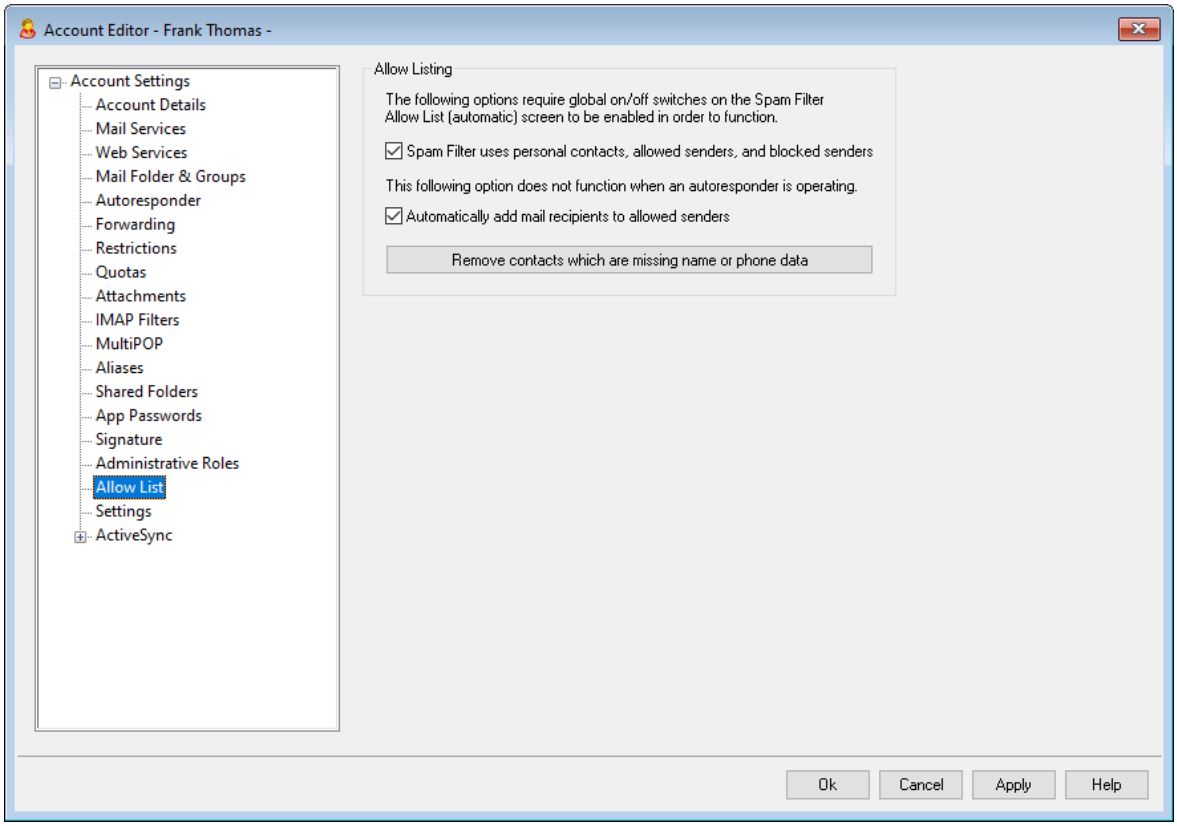
Account is a domain administrator
Click this checkbox to designate the user as a Domain Administrator. Domain administrators are similar to global administrators except that their administrative access is limited to this domain and to the permissions granted on the Web Services 703 page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If you wish to allow this account to administer a different domain, you can do so from within the Remote Administration 341 web interface, on the Domain Manager » Admins page.

Enter any notes you wish to save for your reference
Use this space for any notes or other information you wish to save for your own reference regarding this account. Unlike the *Description* field on the Account Details 697 screen, this note will not be synchronized to the public contacts or mapped to any field in Active Directory.

5.1.1.17 Allow List



Allow Listing

Spam Filter uses personal contacts, allowed senders, and blocked senders
The Spam Filter's Allow List (automatic) 672 screen contains a global option that can be used to cause the Spam Filter allow a message automatically when the sender of the message is found in the local recipient's personal contacts or allowed senders folder. It will also automatically block a message when the sender is found in the user's blocked senders folder. If you have enabled the Spam Filter's global option but do not wish to apply it to this account, clear this check box to override the global setting. If the global option is disabled then this option will not be available.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Automatically add mail recipients to allowed senders
Click this option if you wish to update this account's allowed senders folder each time it sends an outgoing message to a non-local email addresses. When used in conjunction with the above option, *Spam Filter uses personal contacts, allowed senders, and blocked senders*, the number of Spam Filter false positives can be drastically reduced. The *Automatically add mail recipients to allowed senders* option located on the Allow List (automatic) 672 screen must be enabled before you can use this feature.

This option is disabled when the account is using an autoresponder.

Remove contacts which are missing name or phone data
Click this button if you wish to remove every contact that contains only an email address from the account's default Contacts folder. If a contact doesn't have at least a name or phone data it will be removed. The option is primarily to help those who were using MDaemon's automatic allow listing option prior to version 11 purge contacts that were added purely as a function of the allow list feature. In previous versions of MDaemon the addresses were added to the main contacts instead of to a dedicated allow list folder. This could result in the account having many entries in the contacts folder that the user would rather not have there.

Consider this option carefully before using it, because contacts containing only an email address could still be legitimate.

Setting the Default Values for New Accounts and Groups

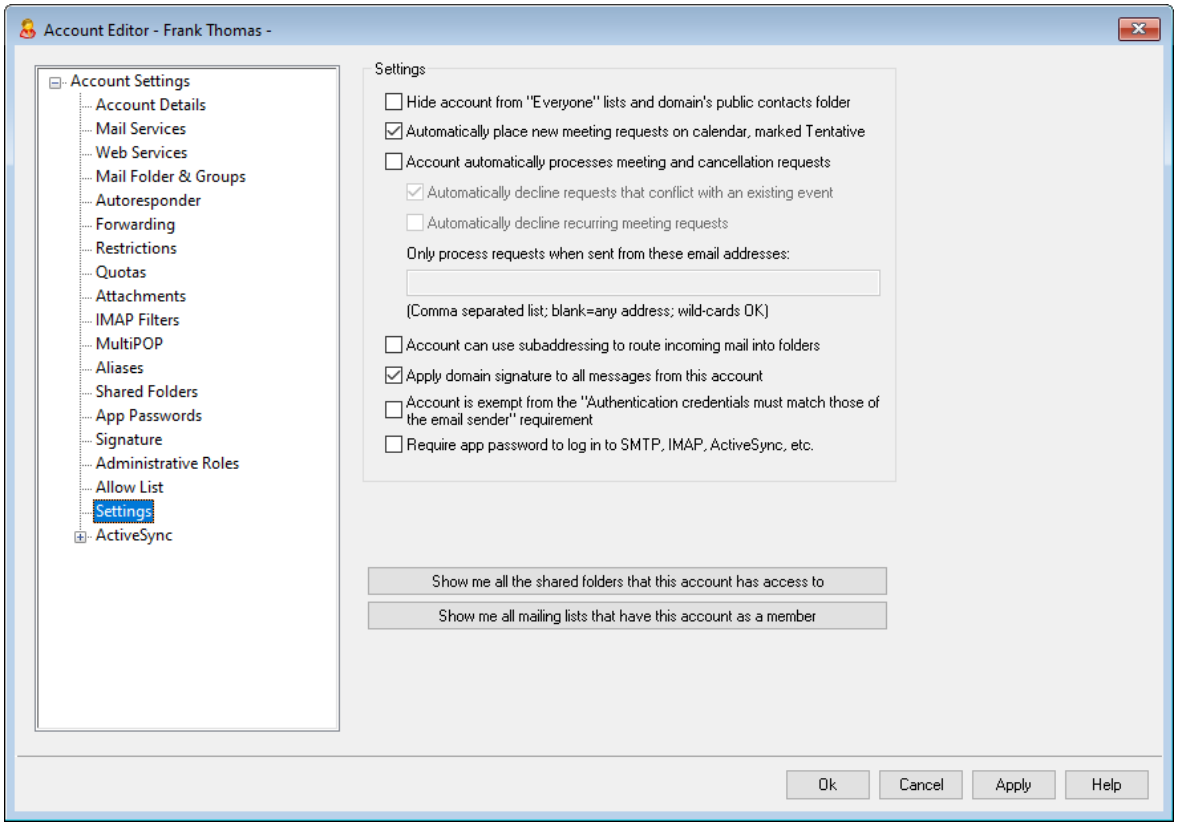
The options on this screen correspond to those located on the Template Properties » Allow List 802 screen, which can be used to set the default values for new accounts 775 and values for accounts belonging to certain groups 764.

See:

Allow List (automatic) 672
Template Manager 774
Template Properties » Allow List 802

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.18 Settings



Settings

Hide account from "Everyone" lists and domain's public contacts folder
MDaemon can automatically create and maintain "Everyone@" and "MasterEveryone@" mailing lists 262, which can be used to send a message to all of a domain's users and all MDaemon users, respectively. By default these lists include all accounts of each domain, but you can check this box if you wish to hide this account from those lists—messages to those lists will not be sent to the account. This will also hide the account from the domain's public contacts folder.

Automatically place new meeting requests on calendar, marked Tentative
By default when an account receives a new meeting request, the meeting is placed on the user's calendar and marked as *Tentative*.

Account automatically processes meeting and cancellation requests
Click this checkbox if you wish to cause automatic processing of meeting requests, changes, and cancellations for this account. When the account receives a message that contains a meeting request, the account's calendar will be updated automatically. This option is disabled for all accounts by default.

Automatically decline requests that conflict with an existing event
If automatic processing of meeting requests and cancellations is enabled for this account, those meeting requests will be automatically declined by default when

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

they conflict with an existing event. Clear this checkbox if you wish to allow the conflicting event to be created.

Automatically decline recurring meeting requests
Click this box if automatic processing of meeting requests and cancellations is enabled for this account but you wish to decline those requests when they are for recurring meetings.

Only process requests when sent from these email addresses
If you wish to automatically process requests only from certain email addresses, list those addresses here. Separate each address with a comma. Wildcards in addresses are permitted (e.g. *@example.com). If you leave this box blank then any address is allowed.

Account can use subaddressing to route incoming mail into folders
Click this checkbox if you wish to permit subaddressing 746 for this account.

Apply domain signature to all messages from this account
When there is a Domain Signature 195 for the domain to which this account belongs, this option causes it to be added to all emails sent by the account. It is enabled by default.

Account is exempt from the "Authentication credentials must match those of the email sender" requirement
Use this option if you wish to exempt the account from the "*Authentication credentials must match those of the email sender*" global option located on the SMTP Authentication 509 screen. This option is disabled by default.

Require app password to log in to SMTP, IMAP, ActiveSync, etc.
Check this box if you wish to require that the account use App Passwords 734 in mail clients, to log in to SMTP, IMAP, ActiveSync, or other mail service protocols. The account's regular password 840, however, must still be used to sign in to Webmail or Remote Admin.

Requiring App Passwords can help protect an account's password from dictionary and brute force attacks via SMTP, IMAP, etc. This is more secure because even if an attack of this sort were to guess an account's actual password, it wouldn't work and the attacker wouldn't know, because MDaemon would only accept a correct App Password. Additionally, if your accounts in MDaemon are using Active Directory 806 authentication and Active Directory is set to lock an account after a number of failed attempts, this option can help prevent accounts from being locked out, because MDaemon will only check the App Passwords, not try to authenticate to Active Directory.

Show me all shared folders that this account has access to
Click this button to display all shared folders to which the account has been given access.

Show me all mailing lists that have this account as a member
Click this button to open a list of all Mailing Lists 259 that have this account as a member.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Subaddressing

Subaddressing is a system for including a folder name in the mailbox portion of an account's email address. Using this system, messages addressed to the *mailbox+folder* name combination will be routed automatically to the account's folder included in the address (assuming that folder actually exists), without the need to create specific filtering rules to make that happen.

For example, if bill.farmer@example.com has an IMAP mail folder called "stuff," then mail arriving addressed to "bill.farmer+stuff@example.com" would be routed automatically to that folder. Subfolders can be designated by including the folder and subfolder names separated by an additional "+" character, and underscores are used to replace spaces in folder names. So, using the example above, if Bill's "stuff" folder had a subfolder called "my older stuff," then messages addressed to "bill.farmer+stuff+my_older_stuff@example.com" would be routed automatically to Bill's "\stuff\my older stuff\" mail folder.

Since subaddressing requires the use of the "+" character, mailboxes that contain "+" cannot be subaddressed. So, in the example above, if the actual address were "bill+farmer@example.com" instead of "bill.farmer@example.com" then it could not be subaddressed. Further, you cannot use an address alias in a subaddress. You can, however, create an alias that refers to an entire subaddressed form. So, even though "alias+stuff@example.com" is not permitted, using "alias@example.com" to point to "bill.farmer+stuff@example.com" would be fine.

To prevent exploits or abuse, the IMAP folder included in the subaddress **must** be valid. If a subaddressed message arrives for an account that does not have a folder matching the name of the folder defined in the subaddress, then the subaddress will be treated as an unknown email address and handled accordingly, based on your other MDaemon settings. For example, if bill.farmer@example.com does not have a folder named "stuff" and yet a message arrives for "bill.farmer+stuff@example.com" then that message will be treated as if were addressed to an unknown user, and it will most likely be rejected.

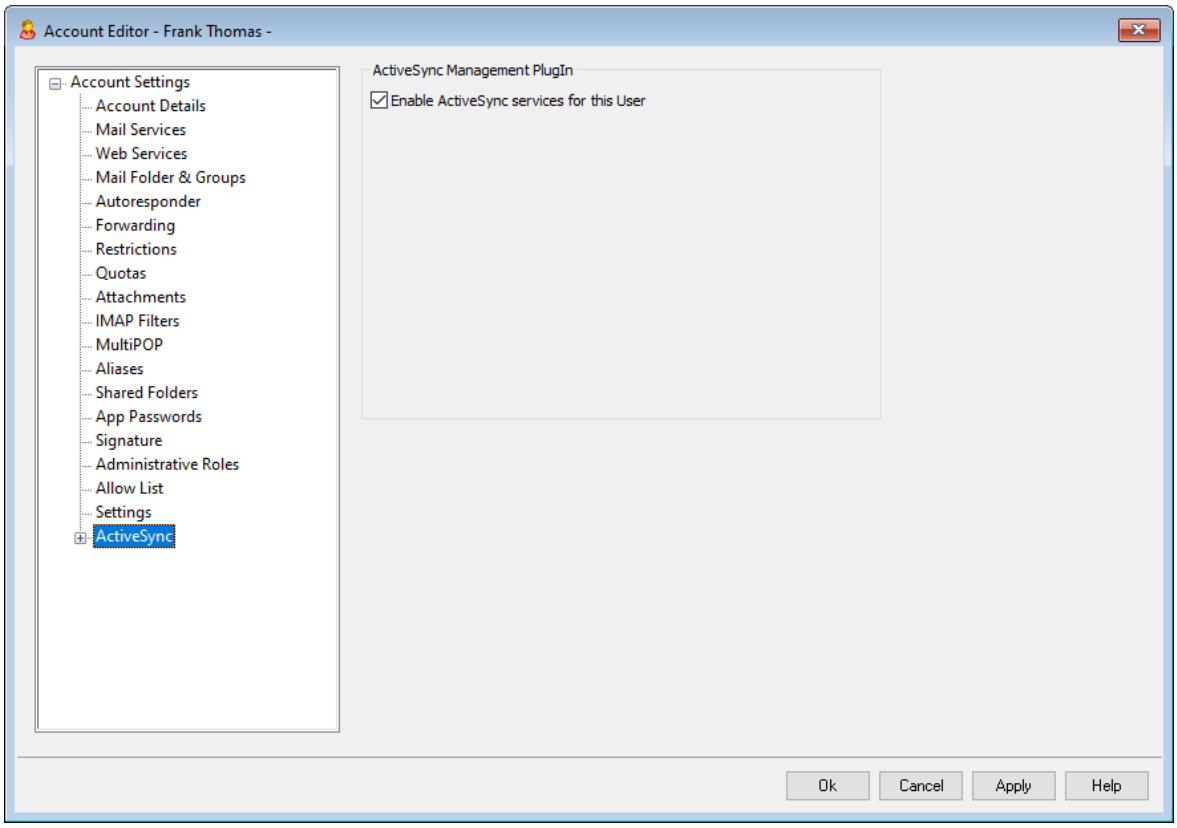
By default, each account has the subaddressing feature disabled. You can, however, disable this feature globally via the *Disable subaddressing feature for all accounts* option located on the Miscellaneous 489 screen of the Preferences dialog. If Subaddressing is disabled via that option, it will not be permitted for any account, regardless of the individual account settings.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Allow List (automatic) 672
Remote Administration 341
Template Manager 774
Passwords 840

5.1.1.19 ActiveSync for MDaemon



The ActiveSync for MDaemon screens in the Account Editor are used to enable or disable ActiveSync for the account, configure account-specific settings 748, assign a default policy 754, and manage the account's ActiveSync clients 755.

Enabling/Disabling ActiveSync for the Account

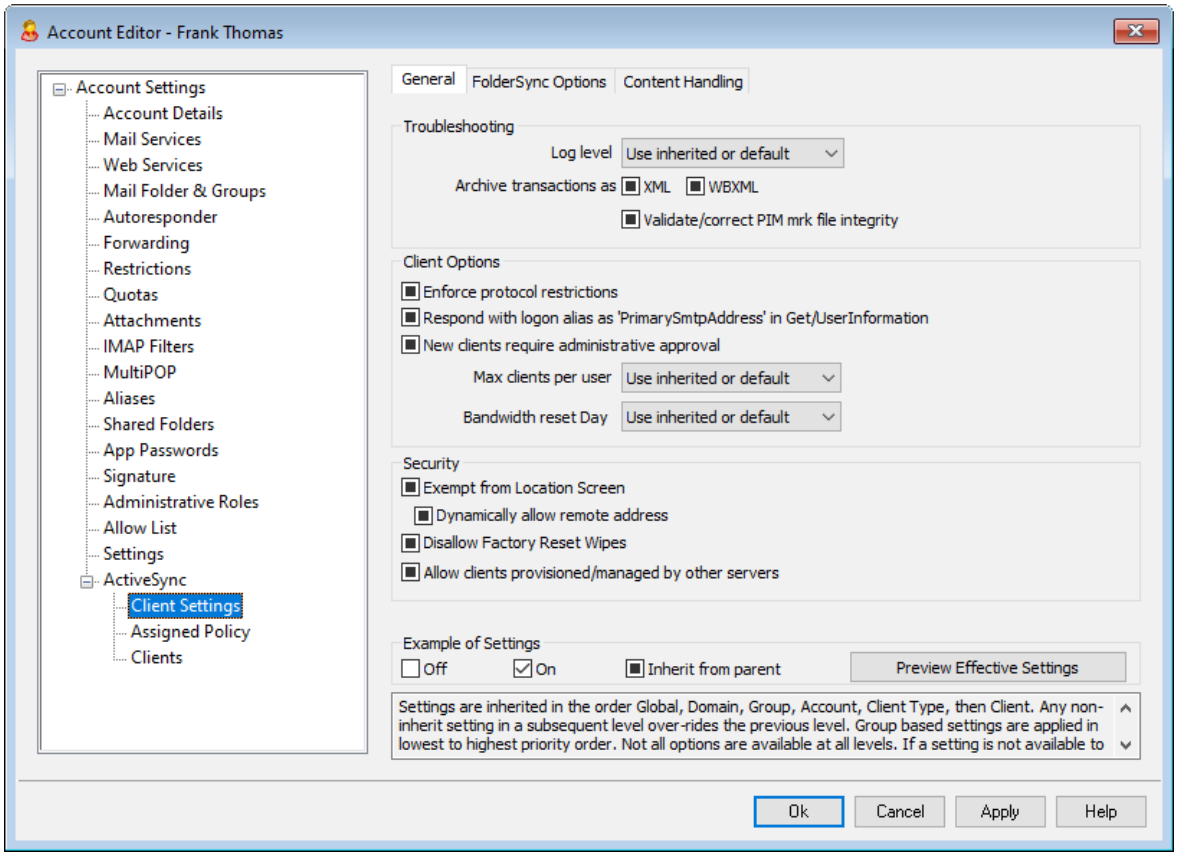
If you wish to allow the account to use an ActiveSync client to access its email and PIM data, enable this option.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

[Accout Editor » ActiveSync » Client Settings](#) 748
[Accout Editor » ActiveSync » Assigned Policy](#) 754
[Accout Editor » ActiveSync » Clients](#) 755

5.1.1.19.1 Client Settings



The options on this screen are used to control ActiveSync client settings for clients associated with this account. By default each of these options is configured to inherit its setting from the corresponding domain to which the account belongs. Changing any setting on this screen will override the domain setting 426 for this account. Further, you can use the *Settings* option on the Clients 755 screen if you wish to override these account-level settings for specific clients.

General

Troubleshooting

Log level
ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Info Moderate logging. Logs general operations without details. This is the default log level.

Warning Warnings, errors, critical errors, and startup/shutdown events are logged.

Error Errors, critical errors, and startup/shutdown events are logged.

Critical Critical errors and startup/shutdown event are logged.

None Only startup and shutdown events are logged.

Inherit By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder
By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders
By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders
By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy
Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)
By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders
Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

limit set.

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

copied to the user's contacts folder. This can be useful on clients that do not support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

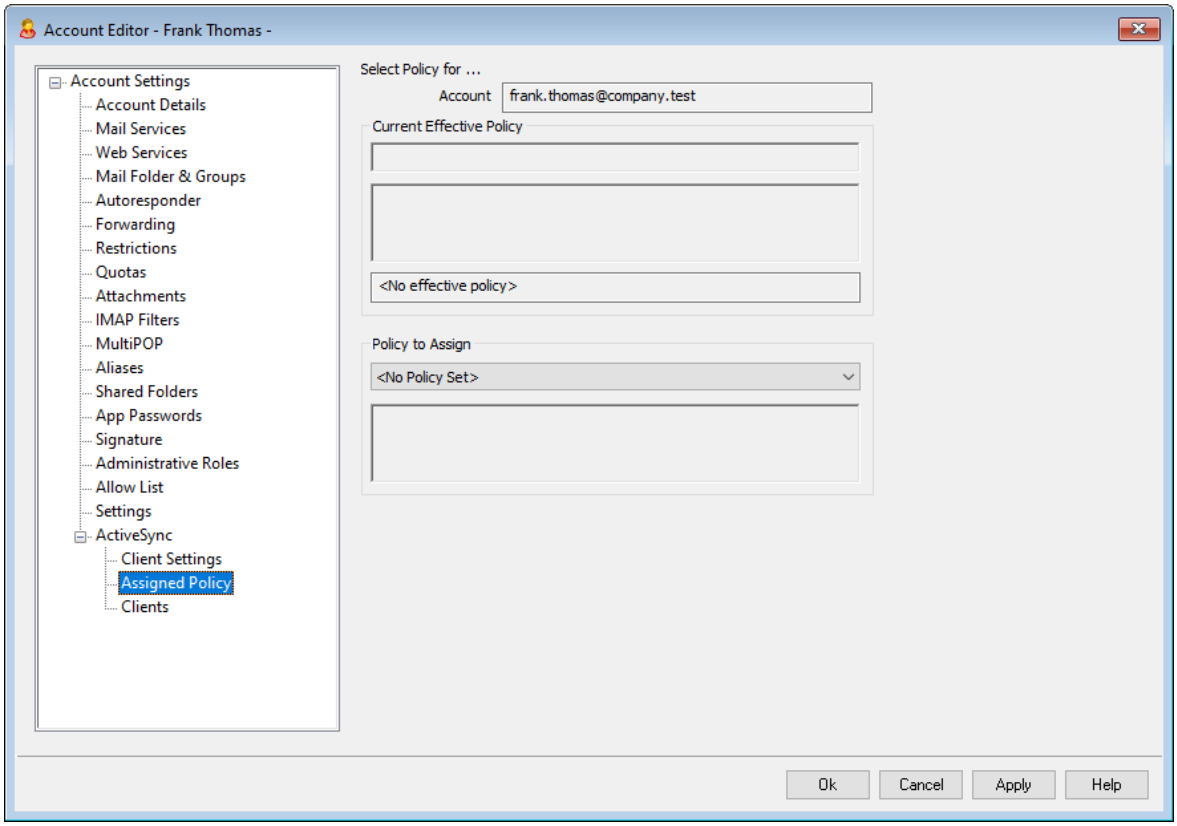
This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

See:

ActiveSync » Domains 426
Accout Editor » ActiveSync » Clients 755

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.1.1.19.2 Assigned Policy



Use this screen to designate the default ActiveSync Policy 434 that will be used for any ActiveSync client that connects using this account. By default this policy setting is inherited from the domain's policy 222 setting, but you can change it here to override that setting for this account. Further, you can also override this account-specific setting and assign a different policy to specific Clients 755.

Assigning an ActiveSync Policy

To assign a policy to the account, click the **Policy to Assign** drop-down list, choose the policy, and click **Ok** or **Apply**.

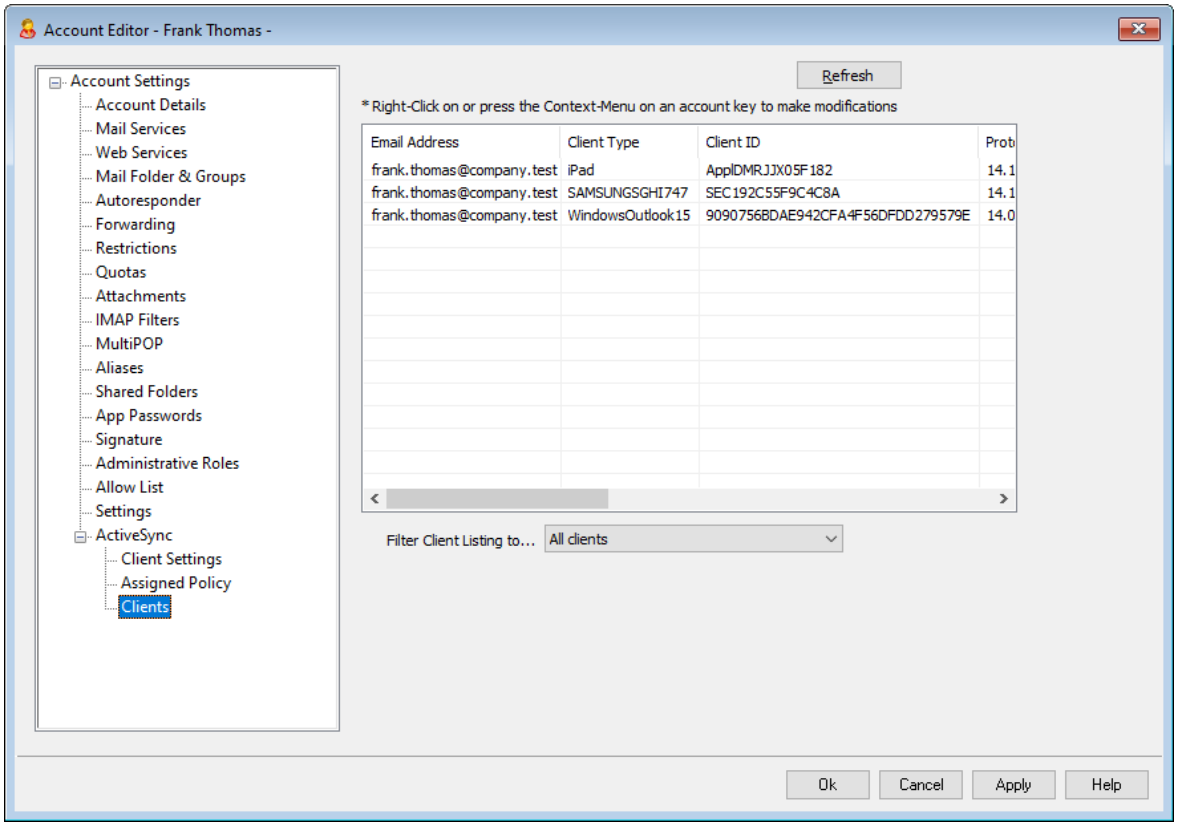
Not all ActiveSync devices recognize or apply policies consistently. Some may ignore policies or certain policy elements altogether, and others may require a device reboot before changes take effect. Further, when attempting to assign a new policy, it will not be applied to a device until the next time the device connects on its own to the ActiveSync server; policies cannot be "pushed" to devices until they connect.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

ActiveSync » Policy Manager 434
ActiveSync » Domains 426
Accout Editor » ActiveSync » Clients 755

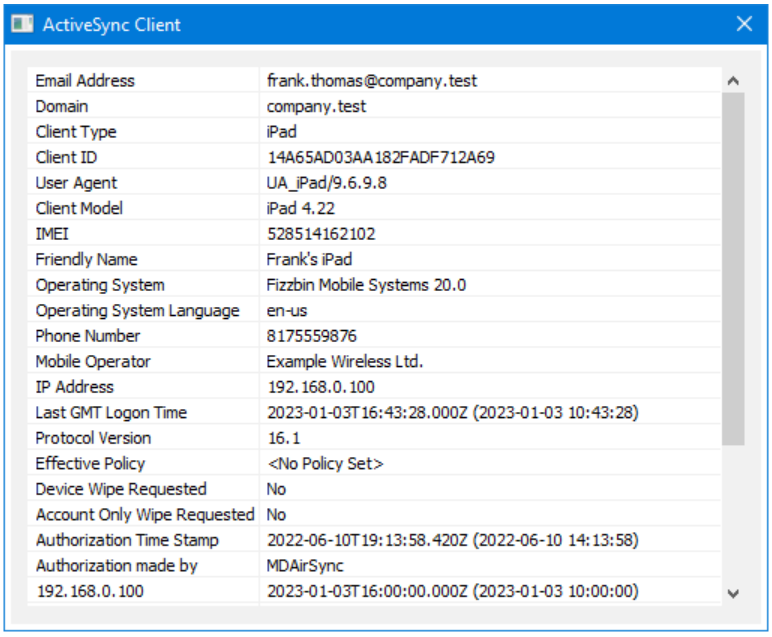
5.1.1.19.3 Clients



This screen displays information about any ActiveSync clients associated with the user's account. From here you can assign an ActiveSync Policy 754 for each client, control various client settings, remove clients, remotely wipe them, and reset the client statistics within MDaemon.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ActiveSync Client Details



Double-click an entry, or right-click the entry and click **View Client Details**, to open the Client Details dialog. This screen contains information about the client, such as its Client Type, Client ID, last login time, and the like.

Client Settings

Right-click a client and click **Customize Client Settings** to manage its Client Settings. By default these settings are inherited from the Client Type settings, but they can be adjusted however you like. See Managing a Device's Client Settings 757 below.

Assigning an ActiveSync Policy

To assign a Policy 434 to the device:

1. Right-click a device in the list.
2. Click **Apply Policy**. This opens the Apply Policy dialog.
3. Click the **Policy to Assign** drop-down list and choose the desired policy.
4. Click **OK**.

Statistics

Right-click an entry and then click **View Statistics** to open the Client Statistics dialog, containing various usage stats for the client.

Reset Statistics

If you wish to reset a client's statistics, right-click the client, click **Reset Statistics**, and then **OK** to confirm the action.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Removing an ActiveSync Client

To remove an ActiveSync client, right-click the client and click **Delete**, and then **Yes**. This will remove the client from the list and delete all synchronization information related to it in MDaemon. Therefore if in the future the account uses ActiveSync to synchronize the same client, MDaemon will treat the client as if it had never before been used on the server; all client data will have to be re-synchronized with MDaemon.

Full Wiping an ActiveSync Client

When a policy 434 has been applied to a selected ActiveSync client, and the client has applied it and responded, then there will be a Full Wipe option available for that client. To do a Full Wipe, right-click the client (or select it if you are using MDRA) and click **Full Wipe**. The next time the client connects, MDaemon will tell it to erase all data, or restore itself to its factory default state. Depending on the client, this may remove everything on it, including downloaded apps. Further, as long as the client's ActiveSync entry exists, MDaemon will continue to send the wipe request any time that device connects in the future. If at some point you wish to delete the client, make sure you add it to the Block List 420 first, so that it cannot connect again in the future. Finally, if a wiped device is recovered and you wish to allow it to connect again, you should select the device and click **Cancel Wipe Actions**. You must also remove it from the Block List.

Account Wiping an ActiveSync Client

To wipe the account's mail and PIM data from the client or device, right-click and click **Account Wipe Account Mail and PIM from client**. The *Account Wipe* option is similar to the *Full Wipe* option explained above, but instead of wiping all data, it will wipe only the account's data, such as its emails, calendar entries, contacts, and the like. The rest, such as apps, photos or music is left alone.

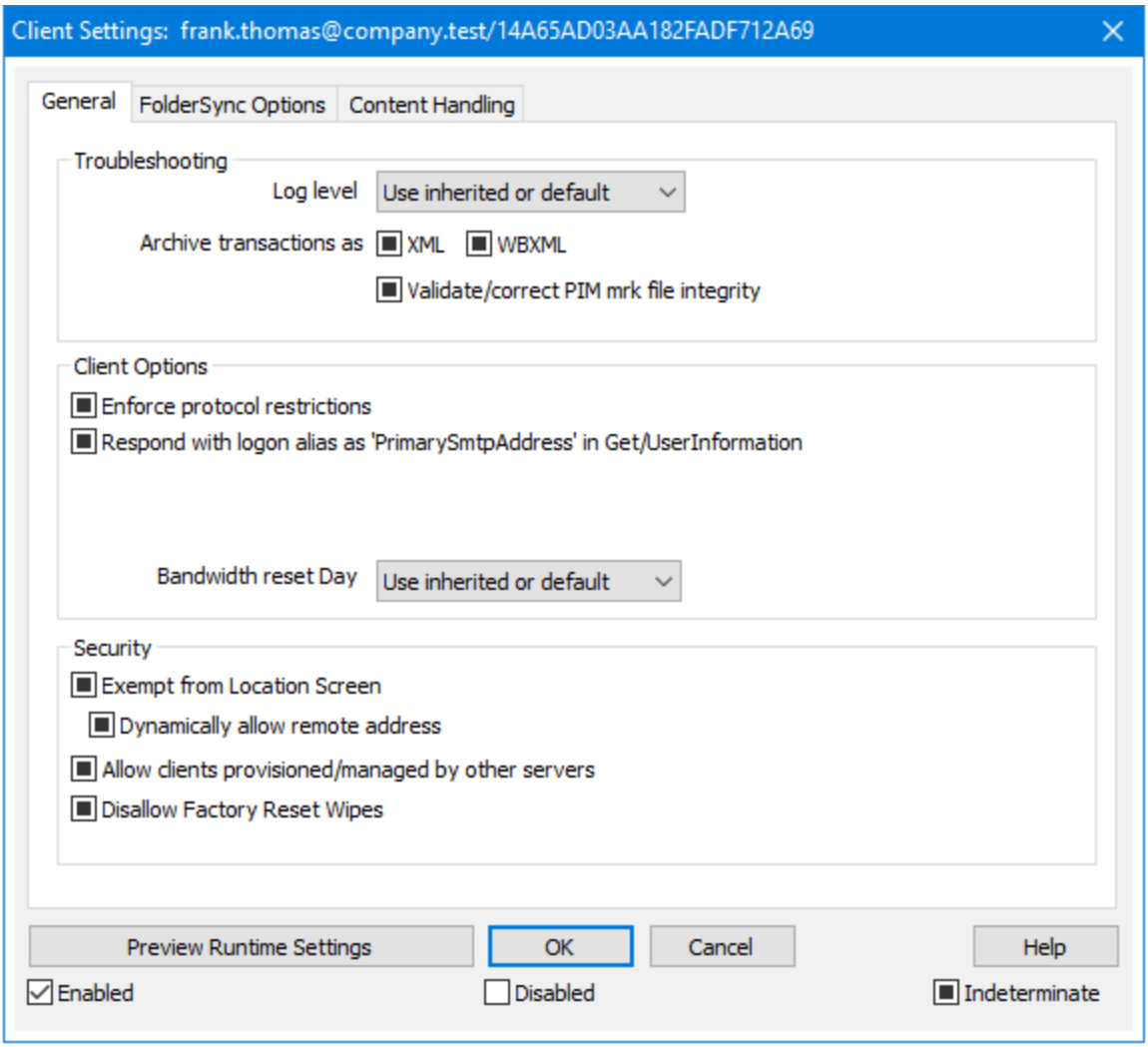
Authorizing Client

If the "*New clients require administrative approval*" option on the ActiveSync Client Settings 413 screen is set to require approval, select a client and click Approve client to sync, to authorize it for synchronization with the server.

Managing a Device's Client Settings

The device-level Client Settings screen allows you to manage settings for a specific device.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



By default all of the options on this screen are set to "Use inherited or default," which means that each option will take its setting from the corresponding option on the Client-Types Client Settings 466 screen. Any changes made to the settings on that screen will be reflected on this screen. Conversely, any changes you make to this screen will override the client-type-level setting for this device.

General

Troubleshooting

Log level

ActiveSync for MDaemon supports six levels of logging, from the highest to lowest amount of data logged:

Debug This is the most extensive log level. Logs all available entries, and is typically only used when diagnosing a problem.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Info	Moderate logging. Logs general operations without details. This is the default log level.
Warning	Warnings, errors, critical errors, and startup/shutdown events are logged.
Error	Errors, critical errors, and startup/shutdown events are logged.
Critical	Critical errors and startup/shutdown event are logged.
None	Only startup and shutdown events are logged.
Inherit	By default, the Log Level setting is inherited from the Client Settings hierarchy. So, Clients inherit their setting from Client Types, Client Types from Accounts, Accounts from Groups, and so on. The Global Client Setting for this option is determined by the Log Level setting on the Diagnostics 422 dialog.

Archive transactions as [XML | WBXML]
Use the *Archive XML...* and *WBXML* options if you wish to save this data, which can sometimes be useful for debugging purposes. The global options are disabled by default.

Validate/correct PIM mrk file integrity
This option runs a validation and correction process on the client's PIM data to look for known issues that could prevent it from syncing correctly, such as duplicate iCal UIDs or empty required fields. The global option is disabled by default.

Client Options

Enforce protocol restrictions
Enable this option if you wish to deny connections from any client that attempts to use a protocol other than the the *Allowed Protocol Versions* specified for the client. By default this option is disabled, which means that protocol restrictions do not prevent a client from using a different protocol; they simply tell the client which protocols to use. If a client attempts to use a restricted protocol anyway, MDaemon will still allow the connection. See: Protocol Restrictions 424 for more information.

Respond with logon alias as 'PrimarySmtpAddress' in Get/UserInformation
This allows the service to return an alias/secondary address as the primary address in response to a Settings/Get/UserInformation request. This works around an issue caused by a post iOS9.x update that resulted in clients not being able to send mail using an alias. Using this option results in a non-specification compliant response to Settings/Get/UserInformation.

New clients require administrative approval
Enable this option if you wish to require new clients to be authorized by an administrator before they can begin synchronizing with an account. The Clients 451 list indicates any clients awaiting authorization, and the administrator can authorize

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

them from the same screen. This setting it is Off by default.

Max clients per user
If you wish to limit the number of ActiveSync clients or devices that can be associated with an MDaemon account, specify the desired number in this option. The global option is set to "unlimited" by default. This option is available on the Global, Domain, and Account client settings screens, not the individual Clients screens.

Bandwidth reset day
Use this option if you wish to reset the bandwidth usage statistics for ActiveSync devices on a specific day of each month. The reset event takes place as part of the normal nightly maintenance process and is logged to the System log like other maintenance routines. The global option is set to "0 (Never)" by default, meaning the usage stats will never be reset. Set the child options to a different day if, for example, you want the reset day to coincide with a user or client's wireless carrier billing reset date.

Security

Exempt from Location Screen
Enable this option on an ActiveSync client's settings screen if you want the device to be able to bypass Location Screening 558. This makes it possible for a valid user to continue to access his or her account via ActiveSync when, for example, traveling to a location that is otherwise blocked from authentication attempts. In order to exempt the device it must have connected and authenticated using ActiveSync within the time-frame configured in the Remove inactive clients after this many days 410 setting located on the Tuning screen.

Dynamically allow remote address
When exempting a device from Location Screening, enable this option if you also wish to allow the remote IP address from which it is connecting. This can be useful for allowing other clients that might be connecting from the same IP address.

Allow clients provisioned/managed by other servers
By default, when the ActiveSync server sends provisioning data/policy specifics to a client and it reports that it is also managed by another ActiveSync server, the client will still be allowed to connect to MDaemon. In this circumstance, however, there is no way to ensure that your policy specifics will be applied where they conflict with the other ActiveSync server's policy. Generally clients default to using the most restrictive option where policies conflict. Disable this option if you do not wish to allows those clients to connect.

Disallow Factory Reset Wipes
If set to On/Yes, the ability to **Full Wipe** an ActiveSync Client will not be available. If you wish to be able to do a full remote wipe on a client, you must first disable this option. The option is disabled by default. For more information, see: **Full Wiping an ActiveSync Client** 451 on the Clients page.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

FolderSync Options

FolderSync Options

Exclude

Allowed/Blocked Senders folder

By default the user's Allowed Senders and Blocked Senders contact folders are not synced with devices. They are generally only used by MDaemon to help with automatic spam prevention. For that reason they do not need to be displayed on devices as contacts.

Non-default mail folders

By default all user-created and default mail folders can be synced with the device. Enable this option if you wish to allow only the default mail folders to be synced, i.e. the Inbox, Sent Items, Deleted Items, Drafts, and so on. No user-created folders will be included. This option is disabled by default.

Non-default PIM folders

By default all of the user's PIM folders (i.e. contacts, calendar, notes, tasks, etc.) will be synced with the device. Enable this option if you wish to allow only the default PIM folders to be synced. For example, if this option is enabled and a user has multiple calendar folders, only the default calendar will be synced. This option is disabled by default.

Include

Public Folder hierarchy

Check this box if you want the public folders 300 to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching

Allows the client to search the Public Folders 300 to which it has access. This is allowed by default.

Public Folder traversal (exposes folder names)

By default, in order for a client to sync/access a public subfolder, the account must have Lookup permission 302 for both the subfolder (i.e. child folder) and all parent public folders 300 above it. If the account does not have permission to see the parent folders then it cannot see the child folder either, even if the account has permission to do so. Enable this option if you wish to allow the client to access these child folders. **Note:** enabling this option must necessarily reveal the names of the parent folders to the client, which could be deemed a security risk. This option is disabled by default.

Maximum number of Public folders

Use this option if you wish to limit the number of Public Folders allowed on the device. When a limit is set, the server iterates through the list of folders until the limit is reached, and then no more are sent to the device. There is no way to ensure the order in which folders will be processed. By default there is no global limit set.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Shared folders
Check this box if you want the shared folders[113] to which a user has access to be included in the user's folder list on ActiveSync devices. This is enabled by default.

Allow searching
Allows the client to search the Shared Folders[726] to which it has access. This is allowed by default.

Content Handling

Content Handling Options

Create tasks/reminders for mail items when flagged by client
This option makes it possible for MDaemon to remind the user about flagged items, by creating a task item for each flagged email when the client requests it. The global option for this control is enabled by default.

Always send meeting updates when event modified
Some clients do not properly send meeting update emails when modifying a meeting. This instructs the ActiveSync Service to send out a meeting update when a meeting item is updated by the organizer. This should only be set on clients[451] and client types[466] that fail to send out meeting updates properly, otherwise, it will result in duplicate meeting updates being sent. Consequently, this option is only available on the settings pages for Clients and Client-Types.

Request Read Receipts on all sent mail
Enable this option if you want the server to request read confirmation for all mail sent by a client. This is disabled by default.

Send Read Receipt from Server when mail marked as read and when requested by sender
Enable this option if you want the server to support read confirmation requests and issue a read receipt when a message is flagged as read by a client. This is disabled by default.

Send as Alias specified in ReplyTo Address
Some clients may not allow a sender to send mail using an Alias. This feature was added to the Exchange ActiveSync (EAS) protocol[424] 16.x, but some clients do not support 16.x. For instance, Outlook for Windows only uses EAS 14.0, and while it does allow a user to specify an alternate address to send as, the message generated does not reflect the user's choices correctly. This option allows the use of the ReplyTo field to send the email, as long as that ReplyTo address is a valid alias[818] for that user. The global option is enabled by default.

Virtually merge public contacts into default contacts
Enable this option if you wish to merge the public contacts with the user's default contacts on the device. This is only a virtual merge, that is they are not actually copied to the user's contacts folder. This can be useful on clients that do not

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

support Global Address List (GAL) searches. This is disabled by default.

Block Sender when moving mail into Junk-Email folder
When enabled, upon a client moving an email to the account's Junk Email folder, the service will add the Sender or From address of that email to the Blocked Senders Contacts folder.

Force sending meeting responses when a meeting request is accepted/declined, etc.
When enabled, upon a client accepting, declining or otherwise choosing an action in response to a meeting request, the service will send a meeting response to the meeting organizer. This is for specific clients that don't properly send those updates themselves.

Preview Effective Settings

This button is available on all of the child Client Settings screens (i.e. domains 426, accounts 442, and clients 451). Since by default the options on those screens are set to inherit their settings from a parent screen, use this feature to see what settings are currently being applied to the displayed screen.

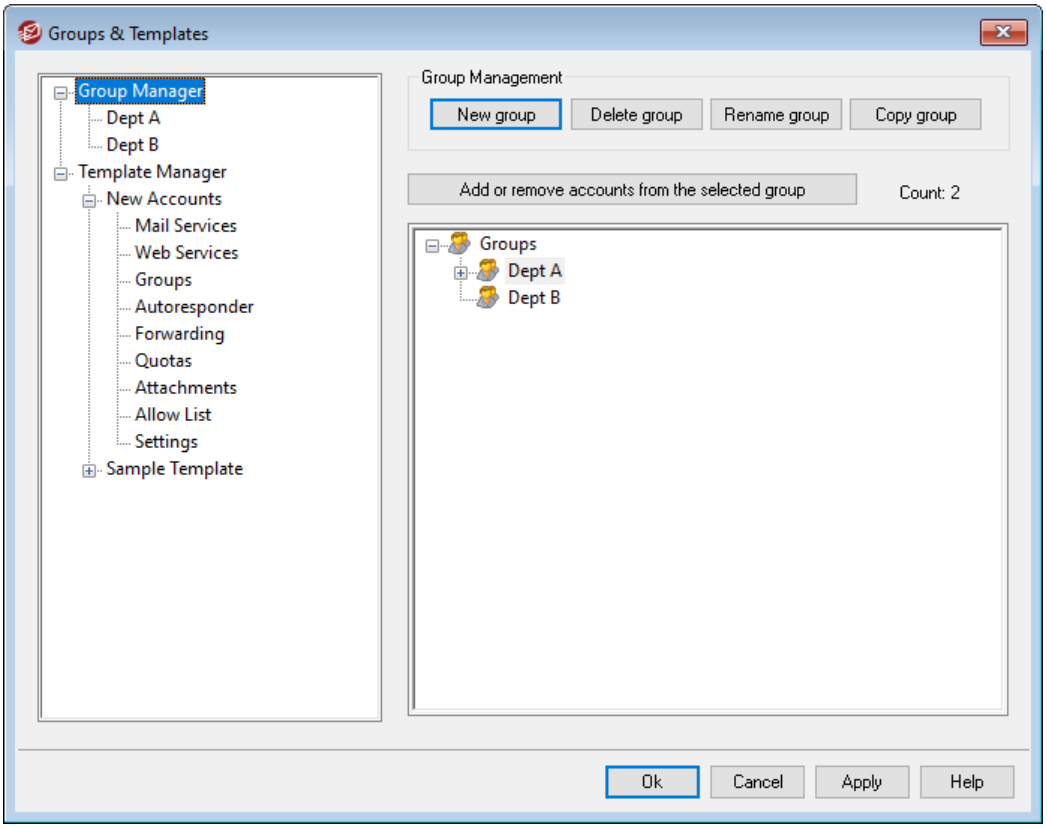
See:

ActiveSync » Client Settings 413
ActiveSync » Domains 426
ActiveSync » Accounts 442

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2 Groups & Templates

5.2.1 Group Manager



The Group Manager (Accounts » Groups & Templates... » Group Manager) is used to create account Groups and manage which accounts belong to them. Groups have a number of different uses and functions. For example, using the Group Properties 766 screen you can assign an account template 774 to a Group, allowing you to control a variety of account settings for group members. You can also control whether or not group members have access to MDaemon Instant Messenger 309 and instant messaging. Further, the Content Filter supports groups, allowing you to create rule conditions 633 based on whether or not a message sender or recipient is a member of a specific Group. Finally, for Shared Folders 110 you can assign Access Control List 302 rights to specific Groups, meaning all members of that Group will share those access rights.

You can add accounts to a Group by selecting the Group from the list below and then clicking the "*Add or remove accounts...*" button. You can also add users to Groups from each user's Mail Folder & Groups 700 screen.

Group Management

New group

To create a new Account Group, click *New group*, type a name and description for the group, and click *OK*. The new group will appear in the list of groups below and in the left pane.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Delete group
To delete a group, select the group in the list below, click *Delete group*, and click *Yes* to confirm your decision to delete the group.

Rename group
To rename a group, select the group in the list below and click *Rename group*. Type a new name for the group and click *OK*.

Copy group
If you wish to create a group with settings that match another group, select a group from the list, click this button, and then specify a name and description for the new group.

Add or remove accounts from the selected group

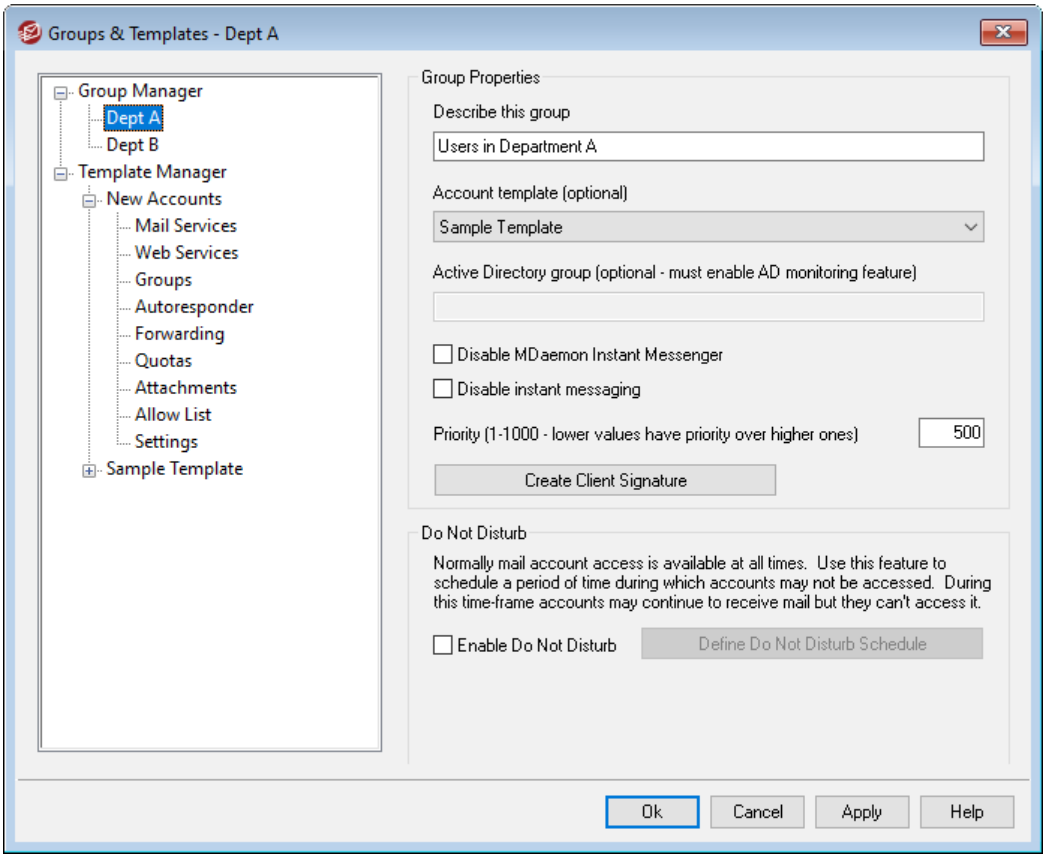
To manage a group's membership, select a group from the list below and click this button. Click the checkbox next to any accounts you wish to add to the group and clear the checkbox next to any members you wish to remove. Click *Ok*.

See:

Mail Folder & Groups 700
Creating a New Content Filter Rule 633
Shared Folders 110

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.1.1 Group Properties



The Group Properties screen (Accounts » Groups & Templates... » [group name]) is used to configure the settings for each group you have created using the Group Manager 764. To open Group Properties from the Group Manager, double-click the group you wish to edit, or click the name of the group in the left pane. On this screen you can assign an Account Template 774 to a group, allowing you to control a variety of account settings for group members. You can also link the group to an Active Directory group, control whether or not group members have access to MDaemon Instant Messenger (MDIM) 309 and instant messaging, and set a priority level for the group. To control group membership, use the Group Manager and Mail Folder & Groups 700 screen on the Account Editor.

Group Properties

Describe this group
Enter a description of the group here, for your own reference. This information is typically entered when you create the group but can be edited from this screen at any time.

Account template (optional)
If you have created an Account Template 774 that you would like to use to control some of the account settings for group members, use this drop-down list to select the desired template. When an account template is linked to a group, any category of account settings designated on Template Properties 776 will be used for all

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

accounts belonging to the group. The template will be used to control those settings rather than using the individual account settings on the Account Editor. If an account is removed from a group that was controlling its account settings, the settings will revert to the values designated by the New Accounts template 775.

If an account belongs to multiple groups linked to different templates, then all of the templates will be used wherever there are no conflicts in the designated Template Properties 776. If multiple templates are set to control the same properties, then the first template listed is the one that will be used.

Active Directory group (optional - requires AD monitoring)
Use this option if you wish to link the group to a specific Active Directory group. Members of the Active Directory group will added to the account group automatically. But for this to work you must be using the Active Directory Monitoring 812 feature.

You can map any Active Directory attribute you want to use as a trigger for adding accounts to Groups, although the "`memberOf`" attribute will most likely be the one to use. You can configure this by editing `ActiveDS.dat` in notepad. This feature is disabled by default. To enable it, edit `ActiveDS.dat` and specify which attribute to use for your group trigger, or uncomment the "`Groups=%memberOf%`" line in `ActiveDS.dat` to use it.

Disable MDaemon Instant Messenger
Click this box if you wish to disable MDIM support for all members of the group.

Disable Instant Messaging
Click this box if you wish to allow support for MDIM but not its Instant Messaging feature.

Priority (1-1000 - lower values have priority over higher ones)
Use this option to set a priority level (1-1000) for your groups, which allows accounts to be members of multiple groups and avoid possible conflicts between group settings. For example, when an account is a member of multiple groups that each have a linked account template controlling the same settings, the settings for the group with the first Priority will be used. In other words, a group with a Priority value of "1" will be over a group with a value of "10". When there is no conflict the settings for each group are collectively applied. In the case of a tie the first group found wins. When an account is removed from a group linked an account template, the account settings previously controlled by the account template will change to the account settings designated by the next Priority group. If there isn't another group controlling those settings, then they will revert to settings designated by the New Accounts template 775.

Create Client Signature
Click this button if you wish to add a client signature to be used for members of the group. See: Group Client Signature 769

Do Not Disturb

Use the Do Not Disturb feature to schedule a time frame during which an account may not send mail or be accessed by its users. Access during a Do Not Disturb period is not

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

allowed and returns an appropriate error response to IMAP, POP, SMTP, ActiveSync, and Webmail access requests. MDaemon will still accept incoming mail for accounts in this state, but those accounts may not send mail or be accessed by mail clients.

To apply Do Not Disturb to one or more accounts:

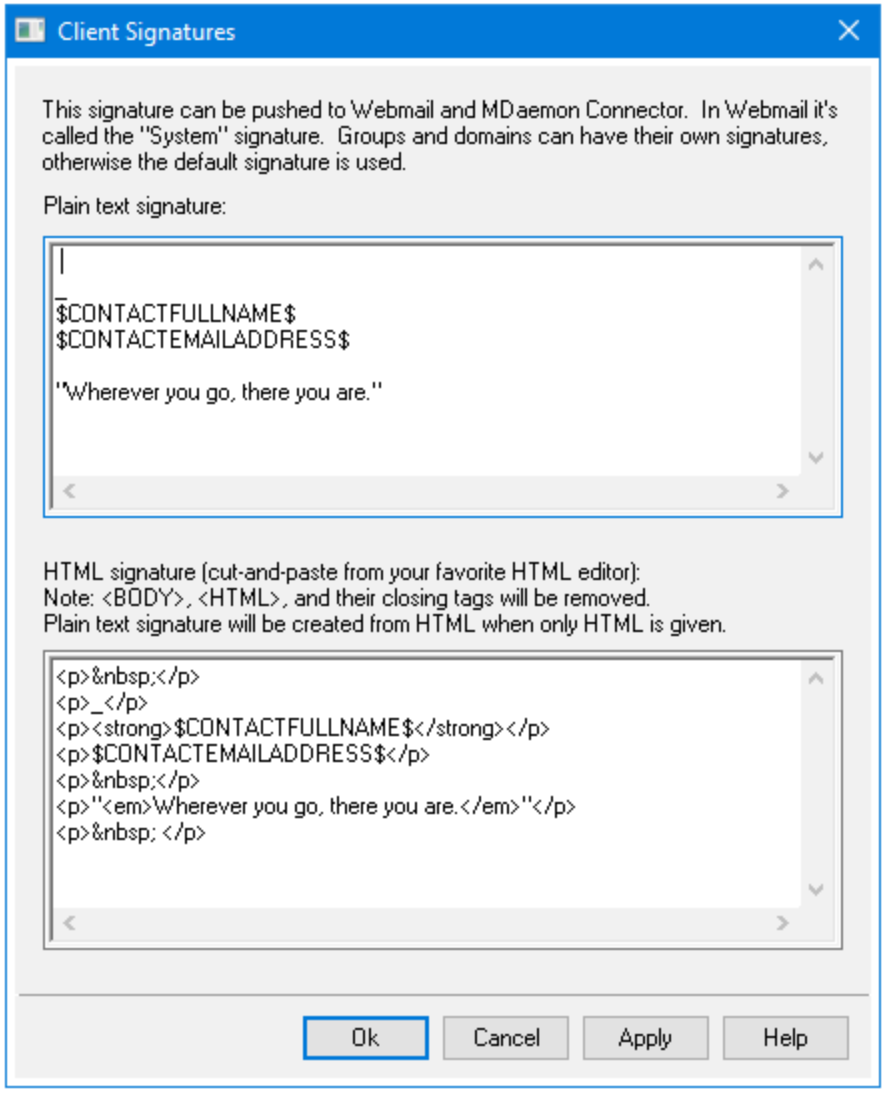
1. Click **Enable Do Not Disturb**.
2. Click **Define Do Not Disturb Schedule**.
3. Set the start/end dates, the start/end times, and the days of the week to use it.
4. Click **Ok**.
5. Use the Group Manager 764 to assign any accounts to this group that you wish to use it.

See:

Group Manager 764
Mail Folder & Groups 700
Template Manager 774
Template Properties 776

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.1.1.1 Client Signature



Use this screen to create a client signature for this group that you can push to MDaemon Webmail[333] and MDaemon Connector[397], to be utilized by your users when composing email messages. You can use the macros[770] listed below to personalize the signature, so that it will be unique for each user, including elements like the user's name, email address, phone number, and the like. If you have created a Default Client Signature[132] or Domain Client Signature[200], this signature will be used instead of either of those for group members. Use the *Push client signature*[333] option if you wish to push the client signature to Webmail and the *Push client signature to Outlook*[397] option if you wish to push it to MDaemon Connector. In Webmail's Compose options, the pushed client signature is called "System." For MDaemon Connector you can designate a name for the signature that will appear in Outlook.

Plain text signature

This area is for inserting a plain text signature. If you wish to designate a corresponding html signature to be used in the text/html part of multipart messages,

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

use the *HTML signature* area below. If a signature is included in both places then MDaemon will use the appropriate one for each part of the multipart message. If no html signature is specified then the plain text signature will be used in both parts.

HTML signature (cut-and-paste from your favorite HTML editor)

This area is for inserting an HTML signature to be used in the text/html part of multipart messages. If a signature is included both here and in the *Plain text signature* area above, MDaemon will use the appropriate one for each part of the multipart message. If no plain text signature is specified then the html will be used to create one.

To create your html signature, either type the html code here manually or cut-and-paste it directly from your favorite HTML editor. If you wish to include inline images in your HTML signature, you can do so by using the `$ATTACH_INLINE:path_to_image_file$` macro.

For example:

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

There are also several ways you can insert inline images into signatures from within MDaemon's Remote Administration 341 web interface:

- On the Client Signature screen in Remote Administration, click the "Image" toolbar button in the HTML editor and select the upload tab
- On the Client Signature screen in Remote Administration, click the "Add image" toolbar button in the HTML editor.
- Drag and drop an image into the Client Signature screen's HTML editor with Chrome, FireFox, Safari, or MSIE 10+
- Copy and paste an image from the clipboard into the Client Signature screen's HTML editor with Chrome, FireFox, MSIE 11+

<body></body> and <html></html> tags are not allowed in signatures and will be removed when found.

Signature Macros

MDaemon signatures support macros that insert the sender's contact information into the signature, taken from the sender's contact located in its domain's Public Contacts folder. This allows default and domain signatures to be personalized with the sender's information. `$CONTACTFULLNAME$`, for example, inserts the sender's full name, and `$CONTACTEMAILADDRESS$` inserts the sender's email address. Use Webmail, MDaemon Connector, or ActiveSync to edit the public contacts. Blank values are used if no contact exists for the sender. Available macros are listed below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Users can control the placement of MDaemon signatures in their emails by placing any of the **Signature Selector** macros into a message wherever they want the signature to appear.

Signature Selector	
$SYSTEMSIGNATURE$	Places the Default Signature 127 or Domain Signature 195 in a message. If both exist, the Domain Signature is used.
$CLIENTSIGNATURE$	Places the Default Client Signature 132 or Domain Client Signature 200 in a message. If both exist, the Domain Client Signature is used.
$ACCOUNTSIGNATURE$	Places the Account Signature 737 in the message.
Names and IDs	
Full name	**$CONTACTFULLNAME$**
First name	**$CONTACTFIRSTNAME$**
Middle name	**$CONTACTMIDDLENAME$,**
Last name	**$CONTACTLASTNAME$**
Title	**$CONTACTTITLE$**
Suffix	**$CONTACTSUFFIX$**
Nickname	**$CONTACTNICKNAME$**
Yomi First Name	**$CONTACTYOMIFIRSTNAME$**
Yomi Last Name	**$CONTACTYOMILASTNAME$**
Account name	**$CONTACTACCOUNTNAME$**
Customer ID	**$CONTACTCUSTOMERID$**
Government ID	**$CONTACTGOVERNMENTID$**
File as	**$CONTACTFILEAS$**
Email Addresses	
Email address	**$CONTACTEMAILADDRESS$**
Email address 2	**$CONTACTEMAILADDRESS2$**
Email address 3	**$CONTACTEMAILADDRESS3$**
Phone and Fax Numbers	
Mobile phone	**$CONTACTHOMEMOBILE$**
Mobile phone 2	**$CONTACTMOBILE2$**
Car phone	**$CONTACTCARPHONENUMBER$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Home phone	**$CONTACTHOMEPHONE$**
Home phone 2	**$CONTACTHOMEPHONE2$**
Home fax	**$CONTACTHOMEFAX$**
Other phone	**$CONTACTOTHERPHONE$**
Instant Messaging and Web	
IM Address	**$CONTACTIMADDRESS$**
IM Address 2	**$CONTACTIMADDRESS2$**
IM Address 3	**$CONTACTIMADDRESS3$**
MMS Address	**$CONTACTMMSADDRESS$**
Home web address	**$CONTACTHOMEWEBADDRESS$**
Address	
Home address	**$CONTACTHOMEADDRESS$**
Home city	**$CONTACTHOMECITY$**
Home state	**$CONTACTHOMESTATE$**
Home zip code	**$CONTACTHOMEZIPCODE$**
Home country	**$CONTACTHOMECOUNTRY$**
Other address	**$CONTACTOTHERADDRESS$**
Other city	**$CONTACTOTHERCITY$**
Other state	**$CONTACTOTHERSTATE$**
Other zip code	**$CONTACTOTHERZIPCODE$**
Other country	**$CONTACTOTHERCOUNTRY$**
Business Related	
Business Name	**$CONTACTBUSINESSCOMPANY$**
Yomi Business Name	**$CONTACTYOMICOMPANYNAME$**
Business title	**$CONTACTBUSINESSTITLE$**
Business office	**$CONTACTBUSINESSOFFICE$**
Business department	**$CONTACTBUSINESSDEPARTMENT$**
Business manager	**$CONTACTBUSINESSMANAGER$**
Business assistant	**$CONTACTBUSINESSASSISTANT$**
Business assistant phone	**$CONTACTBUSINESSASSISTANTPHONE$**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

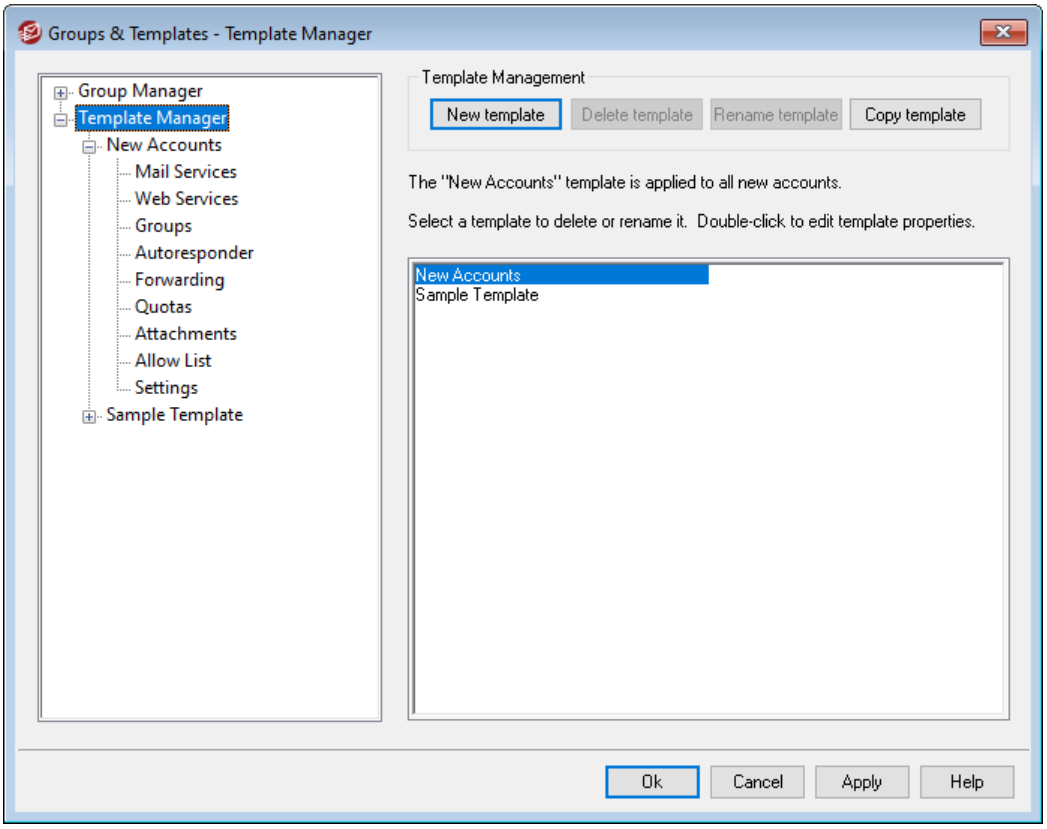
Business main phone	$CONTACTBUSINESSMAINPHONE$
Business phone	$CONTACTBUSINESSPHONE$
Business phone 2	$CONTACTBUSINESSPHONE2$
Business IP phone	$CONTACTBUSINESSIPPHONE$
Business fax	$CONTACTBUSINESSFAX$
Business pager	$CONTACTBUSINESSPAGER$
Business radio	$CONTACTBUSINESSRADIO$
Business address	$CONTACTBUSINESSADDRESS$
Business city	$CONTACTBUSINESSCITY$
Business state	$CONTACTBUSINESSSTATE$
Business zip code	$CONTACTBUSINESSZIPCODE$
Business country	$CONTACTBUSINESSCOUNTRY$
Business web address	$CONTACTBUSINESSWEBADDRESS$
Other	
Spouse	$CONTACTSPOUSE$
Children	$CONTACTCHILDREN$
Categories	$CONTACTCATEGORIES$
Comment	$CONTACTCOMMENT$

See:

Default Client Signatures 132
Default Signatures 127
Domain Manager » Signatures 195
Account Editor » Signature 737
Domain Manager » Webmail Settings 187
MC Client Settings » Signature 397

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2 Template Manager



With the Template Manager (Accounts » Groups & Templates... » Template Manager) you can create and manage Account Templates, which are named sets of account settings that can be assigned to specific Groups 764. Any account belonging to one or more of those groups will have the designated account settings locked, being controlled only by the assigned templates rather than by the Account Editor. The categories of account settings that a template will control are designated on each template's properties 776 screen, which is reached by double-clicking the template's name in the list below, or by clicking the template in the left pane.

Template Management

New template

To create a new Account Template, click *New template*, type a name for the template, and click *OK*. The new template will appear in the list of templates below and in the left pane.

Delete template

To delete a template, select the template in the list below, click *Delete template*, and click *Yes* to confirm your decision to delete the template.

Rename template

To rename a template, select the template in the list below and click *Rename template*. Type a new name for the template and click *OK*.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Copy template
If you wish to create a template with settings that match another template, select a template from the list, click this button, and then specify a name for the new template.

Template List

The list on the bottom of the Template Manager contains all your templates. Click a template and then use the buttons at the top of the screen to delete or rename it. Double-click a template to open its properties 776 screen from which you can designate the categories of account settings that it will control. You can jump directly to any template and its account settings using the controls in the left pane. The *New Accounts* template is a special template that always appears first in the list.

New Accounts Template

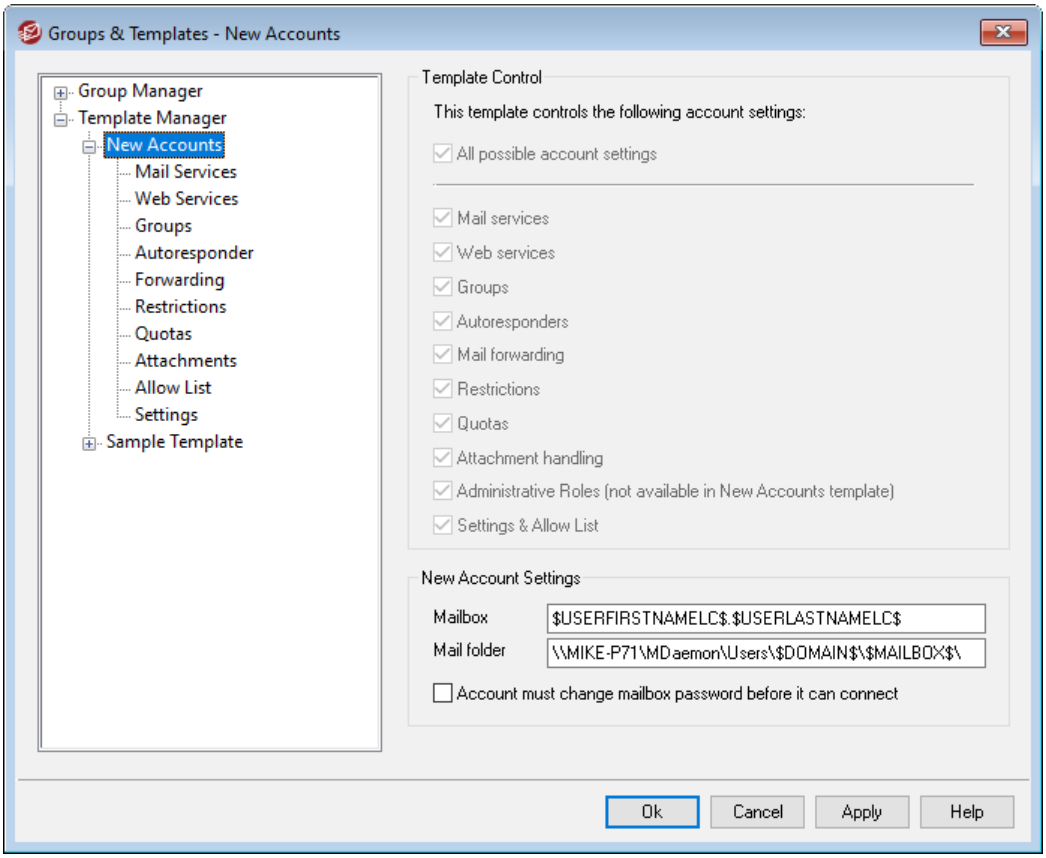
The *New Accounts* template is a special template that is applied to all new accounts when they are created. Rather than locking and controlling certain account settings like other templates, *New Accounts* is used simply to designate the initial settings for new accounts. Those initial settings can then be changed normally by using the Account Editor to edit individual accounts. Some template settings, such as the options located on the Administrative Roles 801 screen, are not available to the New Accounts template.

See:

Template Properties 776
Group Manager 764

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1 Template Properties



To access a template's properties screen, open the Template Manager[774] and click the template's name in the left pane. Use each template's properties screen to designate the categories of account settings that the template will control. Any account belonging to a Group[764] that utilizes an account template will have the corresponding Account Editor screens locked, since those settings will be controlled by the template. If an account belongs to multiple groups linked to different templates, then all of the templates will be used wherever there are no conflicts in the designated template properties. If multiple templates are set to control the same properties, then the first template listed is the one that will be used.

Template Control

All possible account settings
Click this checkbox if you would like this template to control all available account settings for Groups[764] using the template. All of the template screens will be used for each group member's account settings instead of the corresponding screens of the same name on the Account Editor. Clear this check box if you wish to use the *Account Settings* options below to pick specific account settings to control.

Account Settings
This section lists all of the categories of account settings that the template may control for Groups utilizing the template. Each option corresponds to the template screen of the same name. When an option is selected, the settings on that template

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

screen will be used instead of the settings on the corresponding Account Editor screen for associated group members.

New Account Settings

These options are only available on the New Accounts template[775]. They use a variety of special macros[778] to automatically generate the mail storage folder and the mailbox portion of the email address for new accounts.

Mailbox
Use this field to control the default *Mailbox name*[697] portion of the email address that will be generated for new accounts. See Template Macros[778] below for a list of the Macros that can be used in this template string. "`$USERFIRSTNAMELC$.$USERLASTNAMELC$`" is the default template for this option. Therefore creating an account for "Michael Mason" under the example.com domain would result in his address being set to "`michael.mason@example.com`".

Mail folder
Use this field to control the default *Mail folder*[700] that will be used for new accounts. Each account's *Mail folder* is where its email messages will be stored on the server. For example, "`...\$DOMAIN$\$MAILBOX$\`" would create the path, "`...\example.com\michael.mason\`" for the user, "michael.mason@example.com".

MDaemon supports a basic system for folder hashing. Under NTFS, keeping many folders under the same root can sometimes cause performance problems. If you have large numbers of users and wish to subdivide the user folders beyond the default `$DOMAIN$\$MAILBOX$\` setup, you can use the macro `$MAILBOXFIRSTCHARSn$` to do so. Using this macro, "`n`" is a number between 1 and 10 and will expand to the first "`n`" characters of the mailbox name. Changing your default *Mail folder* path to something like the following will achieve a decent folder hashing system:

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\.
```

Account must change mailbox password before it can connect
This option controls whether or not the new account must change its *Mailbox password* before it can access POP, IMAP, SMTP, Webmail, or Remote Administration. The user can connect to Webmail or Remote Administration but will be required to change his or her password before proceeding. Note, however, that in order for users to be able to change their passwords via Webmail or Remote Administration they must first be granted the "*...edit password*" web access permission on the Web Services[782] screen. After the password is changed this option will be deactivated on the account's Account Details[697] screen.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Because changing the password may not be easy or possible for some users, you should exercise caution before activating this option.

Template Macros

Below is a quick reference to the macros available for automating your account setup.

$DOMAIN$	This variable will resolve to the domain name selected for the account.
$DOMAINIP$	This variable will resolve to the IPv4 address associated with the domain currently selected for the account.
$DOMAINIP6$	This variable will resolve to the IPv6 address associated with the domain currently selected for the account.
$MACHINENAME$	This macro returns the host name of the Default Domain, from the Host Name & IP screen of the Domain Manager. The macro is now used in the default account information script (NEWUSERHELP.DAT) for new installations.
$USERNAME$	This variable resolves to the full first and last name of the account holder. This field is equivalent to "$USERFIRSTNAME$ $USERLASTNAME$"
$USERFIRSTNAME$	This variable resolves to the first name of the account holder.
$USERFIRSTNAMELC$	This variable resolves to the first name of the account holder, in lower case letters.
$USERLASTNAME$	This variable resolves to the last name of the account holder.
$USERLASTNAMELC$	This variable resolves to the last name of the account holder, in lower case letters.
$USERFIRSTINITIAL$	This variable resolves to the first letter of the account holder's first name.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

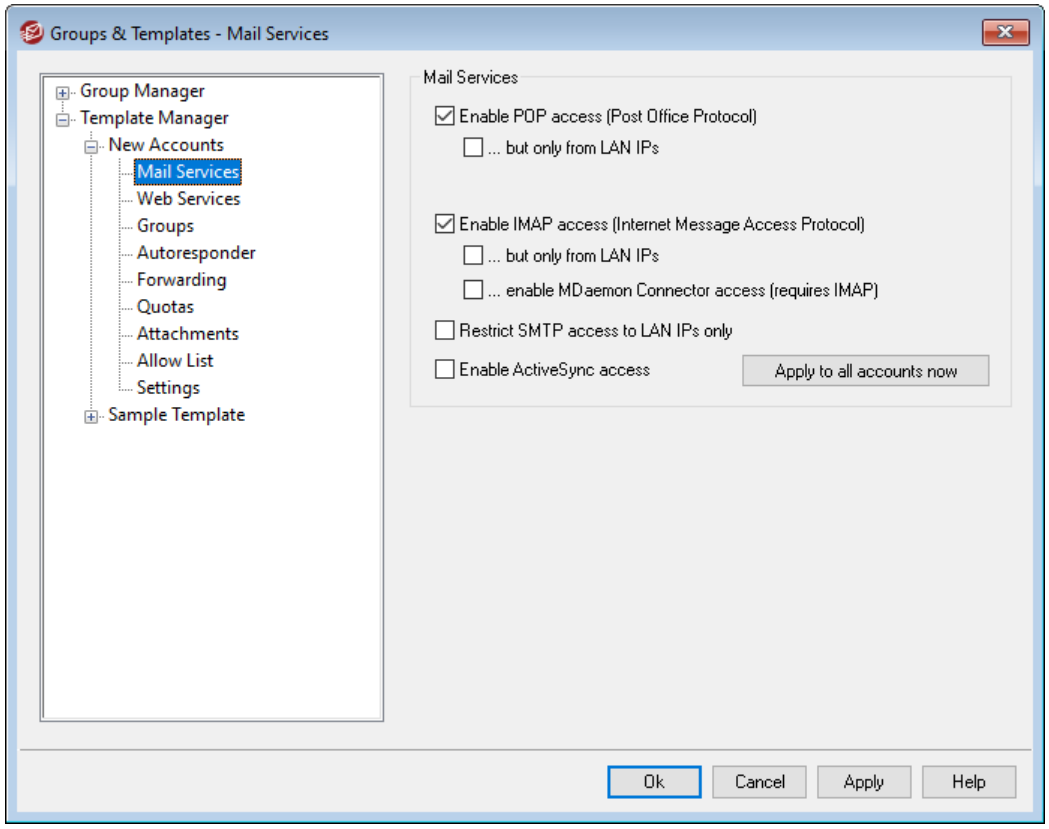
$USERFIRSTINITIALLC$	This variable resolves to the first letter of the account holder's first name, in lower case.
$USERLASTINITIAL$	This variable resolves to the first letter of the account holder's last name.
$USERLASTINITIALLC$	This variable resolves to the first letter of the account holder's last name, in lower case.
$MAILBOX$	This variable resolves to the mailbox name of the current account. The value will also be used as the value of the USER command passed during POP3 mail sessions.
$MAILBOXFIRSTCHARSn$	Where "n" is a number between 1 and 10. This will expand to the first "n" characters of the mailbox name.

See:

Template Manager 774
Group Manager 764

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.1 Mail Services



The options on this template screen correspond to the options located on the Account Editor's Mail Services 701 screen. When a template is set to control this screen 776, it will control the Mail Services options for any account belonging to a Group 766 that utilizes the template.

Mail Services

Enable POP access (Post Office Protocol)
When this box is checked, accounts with settings controlled by this template can be accessed via Post Office Protocol (POP). Virtually all email client software supports this protocol. Clear this checkbox if you do not wish to allow POP access.

...but only from LAN IPs
Check this box if you wish to allow accounts to be accessed via POP only when the user is connecting from a LAN IP address 594.

Enable IMAP access (Internet Message Access Protocol)
When this box is checked, accounts with settings controlled by this template can be accessed via Internet Message Access Protocol (IMAP). IMAP is more versatile than POP, allowing email to be managed on the server and accessed using multiple clients. Most email client software supports this protocol.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...but only from LAN IPs
Check this box if you wish to allow accounts to be accessed via IMAP only when the user is connecting from a LAN IP address 594.

...enable MDaemon Connector access (requires IMAP)
This option is only available on the New Accounts template. Click this option if you wish to allow the account to connect using MDaemon Connector 379. **Note:** this option will only be available when support for MDaemon Connector is activated on your server.

Restrict SMTP access to LAN IPs only
Check this box if you wish to restrict SMTP access to LAN IPs only. This will prevent accounts from sending mail unless they are connected to your network. If the account tries to send mail from an outside IP address the connection will be refused and dropped.

Enable ActiveSync access
This option is only available on the New Accounts template. Check this box if you wish to allow new accounts to use ActiveSync on a mobile device to synchronize email, contacts, calendar, and other data with MDaemon/Webmail. This setting corresponds to the *Enable ActiveSync services for this user* option located on the Account Editor's ActiveSync for MDaemon 747 screen.

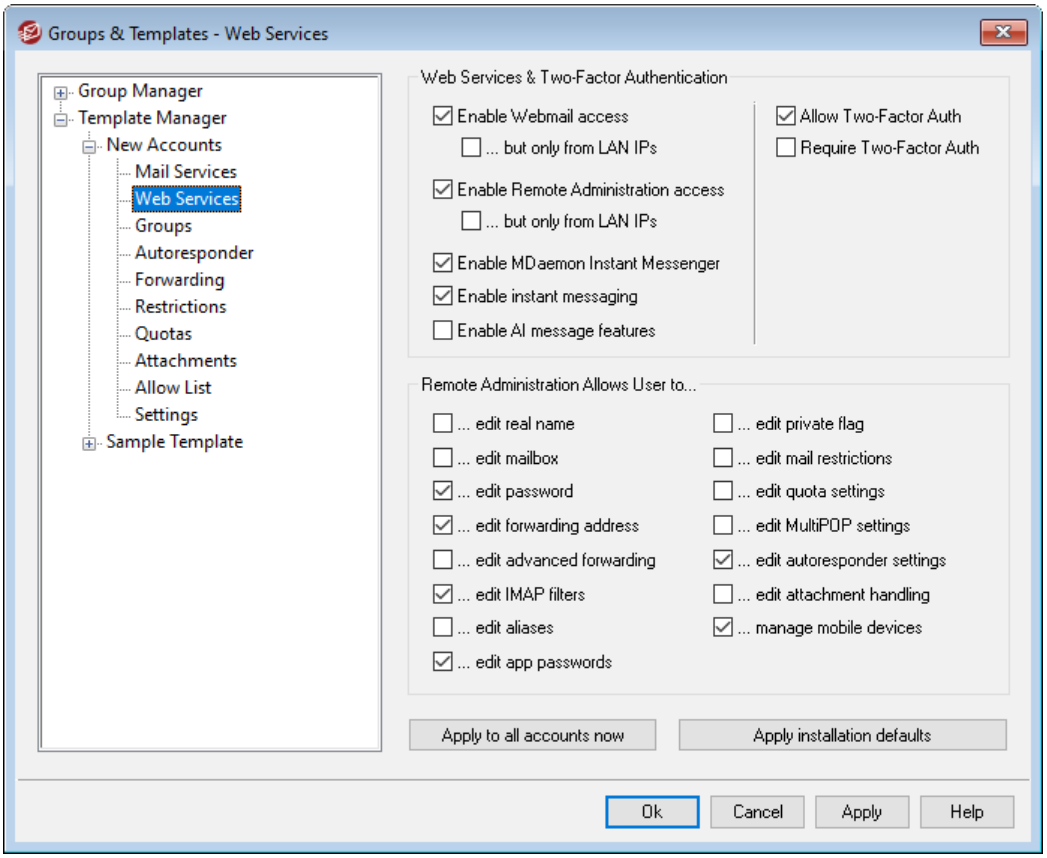
Apply to all accounts now
This option is only available on the New Accounts template. Click this button to apply this screen's settings immediately to the Mail Services 701 and ActiveSync for MDaemon 747 screens of all existing MDaemon accounts.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Mail Services 701

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.2 Web Services



The options on this template screen correspond to the options located on the Account Editor's Web Services 703 screen. When a template is set to control this screen 776, it will control the Web Services options for any account belonging to a Group 766 that utilizes the template.

Web Service & Two-Factor Authentication

Enable Webmail access
Enable this checkbox if you want accounts controlled by this template to be able to access Webmail 308, which enables users to access their email, calendars, and other features using a web browser.

...but only from LAN IPs
Check this box if you wish to allow associated accounts access to Webmail only when connecting from a LAN IP address 594.

Enable Remote Administration access
Check this box if you wish to allow accounts controlled by this template to modify some of their account settings via Remote Administration 341. The accounts will only be able to edit those settings that you designate below.

When this feature is enabled and the Remote Administration server is active, the user will be able to log in to Remote Administration by pointing a browser to the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

designated MDaemon domain and port assigned to Remote Administration 343 (e.g. `http://example.com:1000`). He will first be presented with a sign-in screen and then a screen that contains the settings that he has been given permission to edit. All he needs to do is edit whatever settings he chooses and then click the *Save changes* button. He can then sign out and close the browser. If he has access to Webmail then he can also access Remote Administration from the Advanced Options menu within Webmail.

If the user is a Global or Domain Administrator (designated on the Account Editor's Administrative Roles 741 screen) he will see a different screen after he logs in to Remote Administration.

...but only from LAN IPs
Check this box if you wish to allow the account access to Remote Administration only when connecting from a LAN IP address 594.

Enable MDaemon Instant Messenger
Click this box if you wish to enable MDIM 309 support by default for new accounts. This option is only available on the New Accounts Template 775. There is a similar option on Group Properties 766 that can be used to control group member access to MDIM.

Enable Instant Messaging
Click this option is you wish to enable support for MDIM's instant messaging system by default for new accounts. This option is only available on the New Accounts Template 775. There is a similar option on Group Properties 766 that can be used to control group member access to Instant Messaging.

User can edit categories
Check this box if you wish to allow new Webmail users to edit categories. This is disabled by default for new users. **Note:** This option is only available in MDaemon's Remote Administration web-interface.

Skip IP persistence check for Webmail sessions
When the Webmail Web Server 313 option to "Require IP persistence throughout Webmail session" is enabled, you can check this box if you wish to exempt new users from the IP persistence requirement. **Note:** This option is only available in MDaemon's Remote Administration web-interface.

Enable AI message features
If the *Enable AI message features* option is enabled on an account domain's Webmail 187 dialog, check this box if you wish to allow accounts controlled by this template to use those features in MDaemon Webmail; the features will only be available to the user when the domain-level option is enabled. **See:** "Webmail's AI Message Features 786" below for important information and cautions about using these features.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Two-Factor Authentication

MDaemon supports Two-Factor Authentication (2FA) for users signing into Webmail or MDaemon's Remote Administration web-interface. Accounts that sign into Webmail via HTTPS can activate Two-Factor Authentication for that account on the **Options » Security** screen in Webmail. From then on the user must enter a verification code when signing into Webmail or Remote Administration. The code is obtained at sign-in from an authenticator app installed on the user's mobile device or tablet. This feature is designed for any client that supports Google Authenticator. See the Webmail help file for more information on setting up 2FA for an account.

Allow Two-Factor Authentication

By default new accounts are allowed to setup and use Webmail's Two-Factor Authentication (2FA) feature. Clear this checkbox if you so not wish to allow 2FA by default for new accounts. You can control this setting for specific accounts on each account's Web Services 703 page.

Require Two-Factor Authentication

Enable this option if you wish to force all new accounts to use Two-Factor Authentication (2FA) when signing in to Webmail or MDaemon's remote administration web-interface. When 2FA is required, any account that has not yet been configured to use it will be redirected to a page to set it up the next time the account signs in to Webmail. See the Webmail help file for more information on setting up 2FA for an account.

Remote Administration Allows User to...

...edit real name

Enabling this feature will allow accounts associated with this template to modify the *First and last name* 697 setting.

...edit mailbox

Enabling this feature will allow users to modify the *Mailbox name* 697.

Because the *Mailbox name* is part of the account's email address, which is the unique identifier and login value for the account, changing it means that the user will be changing his or her actual email address. This could result in any future messages directed to the old address being rejected, deleted, or the like.

...edit password

Click this checkbox if you wish to allow accounts to modify the *Mailbox password*. For more on password requirements, see: Passwords 840.

...edit forwarding address

When this feature is enabled, accounts associated with the template will be able to modify the forwarding 711 address settings.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

...edit advanced forwarding
When this feature is enabled, users will be able to modify the *Advanced Forwarding Settings*[711].

...edit IMAP filters
Use this control to allow each user to create and manage his own IMAP Filters[720].

...edit aliases
Enable this option if you wish to allow the account holders to use Remote Administration to edit Aliases[725] associated with their accounts.

...edit app passwords
By default users can edit their App Passwords[734]. Clear this checkbox if you do not wish to allow the user to edit them.

...edit private flag
This option governs whether or not each will be permitted to use Remote Administration to edit the *"Account hidden from "Everyone" lists, shared calendars, and VRFY"* option located on the Account Editor's Settings[744] screen.

...edit mail restrictions
This checkbox controls whether or not the account will be able to edit the Inbound/Outbound mail restriction, located on the Restrictions[713] screen.

...edit quota settings
Click this checkbox if you wish to allow the account to modify the Quota[715] settings.

...edit MultiPOP settings
Click this checkbox if you wish to give the account permission to add new MultiPOP[723] entries and to enable/disable MultiPOP collection for those entries.

...edit autoresponder settings
Click this checkbox if you wish to give the user permission to add, edit, or delete Autoresponders[708] for his account.

...edit attachment handling
Check this box if you wish to allow the user to edit the account's attachment handling options, located on the Attachments[718] screen.

...manage mobile device
Click this option if you wish to allow the account holder to use Remote Administration to manage his or her device-specific settings, such as for ActiveSync devices.

Apply to all accounts now

This option is only available on the New Accounts Template[775]. Click it to apply the settings on this screen to all existing MDaemon accounts that are not specifically controlled by a Web Services Account Template.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Apply installation defaults

This option is only available on the New Accounts Template[775]. Click it to reset the New Accounts template to the installation defaults. It will only change the template's settings, it will not change any existing accounts.

Load "New Accounts" template settings

This option is only available for custom templates. Click it to set the options on this screen to the default values designated on the Web Services screen of the New Accounts Template[775].

Webmail's AI Message Features

As of MDaemon 23.5.0, the Pro theme in MDaemon's Webmail client includes various Artificial Intelligence (AI) features to help assist your users in managing their email and increasing productivity. These features are optional and disabled by default, but can be enabled for any user you choose.

With these features, in MDaemon Webmail you can use AI to:

- Give you a summary of the contents of an email message.
- Suggest a reply to the message, according to several guidelines that you can instruct the AI to use. You can set the *Tone* of the reply to be professional, respectful or casual. The *Position*, or stance, to take in the reply can be set to interested or not interested, agree or disagree, or skeptical. The *Attitude* the reply should convey can be set to confident, excited, calm, or apologetic. Last, you can designate the *Length* of the reply, ranging from very brief to detailed.
- Assist you in composing a new email message, based on some text you have already included. As with the *Suggest a Reply* option above, you can also designate the Tone, Position, Attitude, and Length for the AI to use when composing the message.

The *Enable AI message features* option on the main Webmail Settings[333] dialog controls whether or not support for the AI features is enabled by default for your domains. There is an option of the same name located on the Domain Manager's Webmail[187] dialog that can be used to override that main setting for specific domains. **Note:** enabling AI Message Features support for a domain does not grant all of that domain's users access to the features. You must activate the *Enable AI message features* option on the Account Editor's Web Services[703] screen for any user you wish to allow to use them. Alternatively, you can use the Account Templates[774] and Groups[764] features to assign users to a group that has access to the AI message features.

Enabling accounts to use MDaemon's AI message features allows them to submit and receive information to and from third-party generative AI services, specifically ChatGPT by OpenAI. Administrators and users should therefore be aware that this introduces several potential privacy concerns due to the feature's ability to process personal data and generate

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

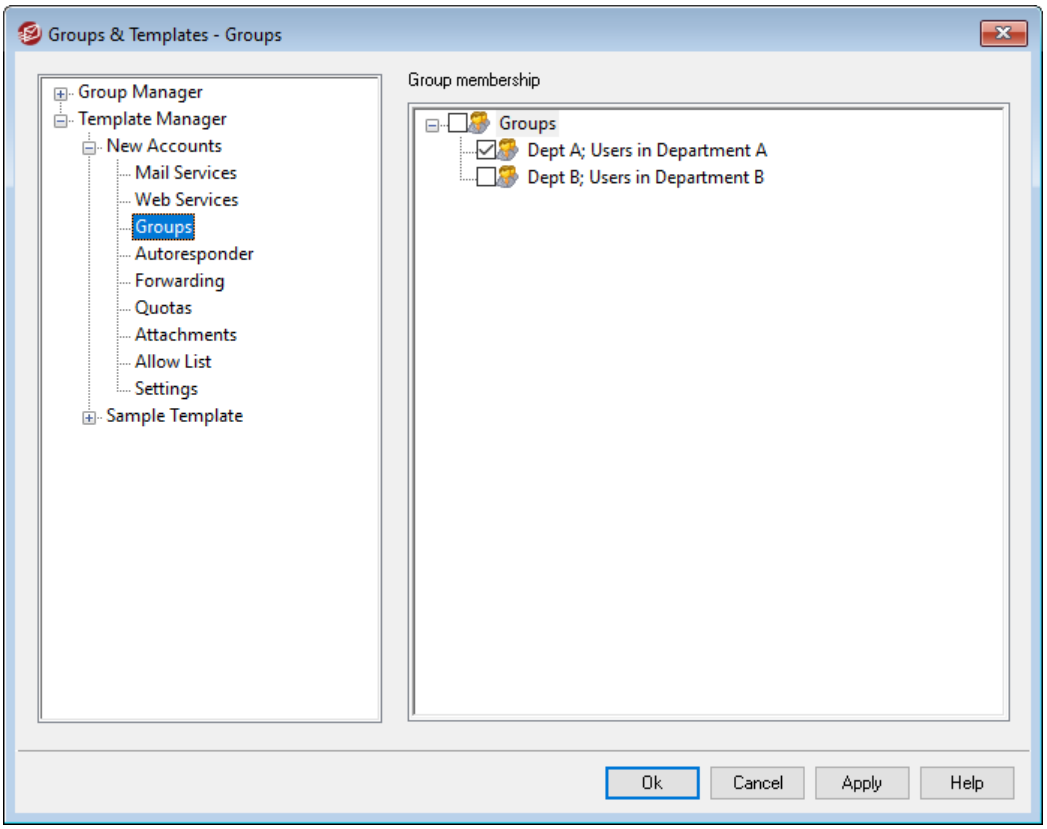
potentially sensitive information. To address privacy concerns, it's vital for organizations to train their employees to use AI responsibly. **Note:** Data submitted to/from Open AI is not stored on the local server or on our network.

You can find MDaemon Technologies' AI Usage Policy at our Artifical Intelligence (AI) Information Page. On that same page there is also a link to OpenAI's Terms of Use.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Web Services 703

5.2.2.1.3 Groups



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

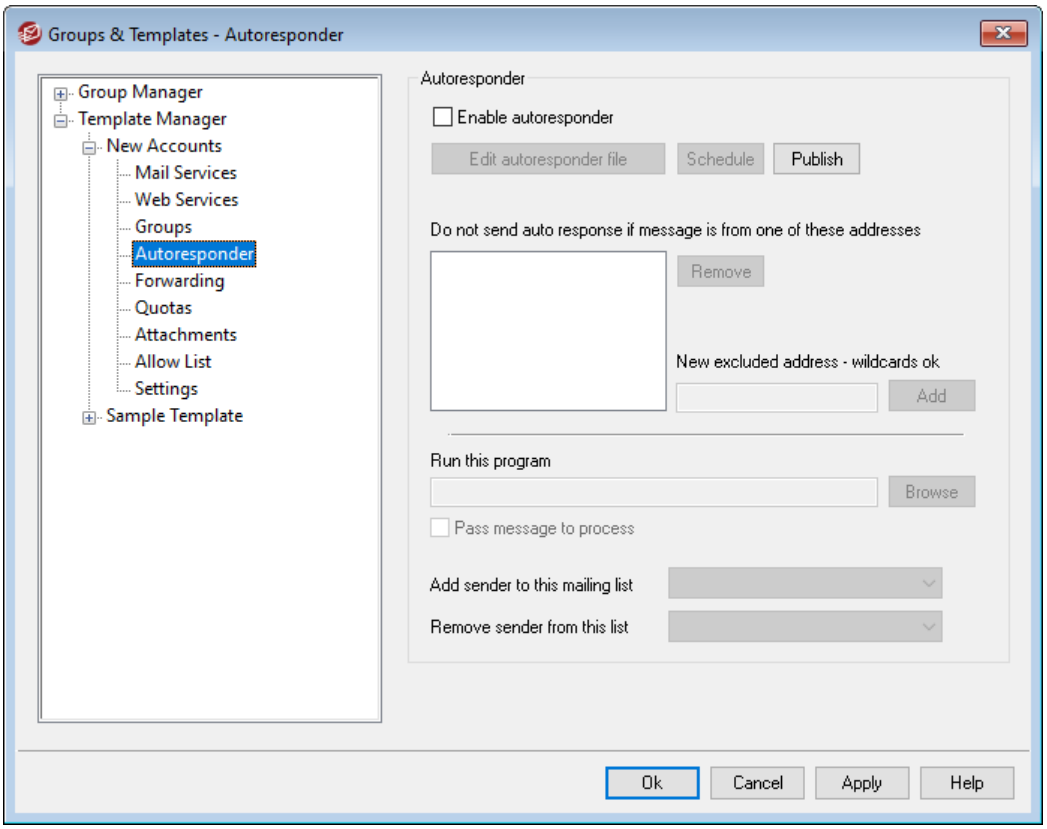
Group Membership

This screen is only available in the New Accounts template[775] and corresponds to the Group Membership section of the Account Editor's Mail Folder & Groups[700] screen. When you select one or more groups on this screen, new accounts will be automatically added to those groups.

See:

New Accounts template[775]
Group Manager[764]
Group Properties[766]

5.2.2.1.4 Autoresponder



The options on this template screen correspond to the options located on the Account Editor's Autoresponder[708] screen. When a template is set to control this screen[776], it will control the Autoresponder options for any account belonging to a Group[766] that utilizes the template.

Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

possible, or the like. MDaemon users with Web Access 703 to Webmail 308 or Remote Administration 341 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response messages are based on the contents of the `OOF.mrk` file, found in each user's root `\data\` folder. This file supports a large number of macros, which can be used to cause much of the message's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for messages originating from a user's same domain, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 827 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

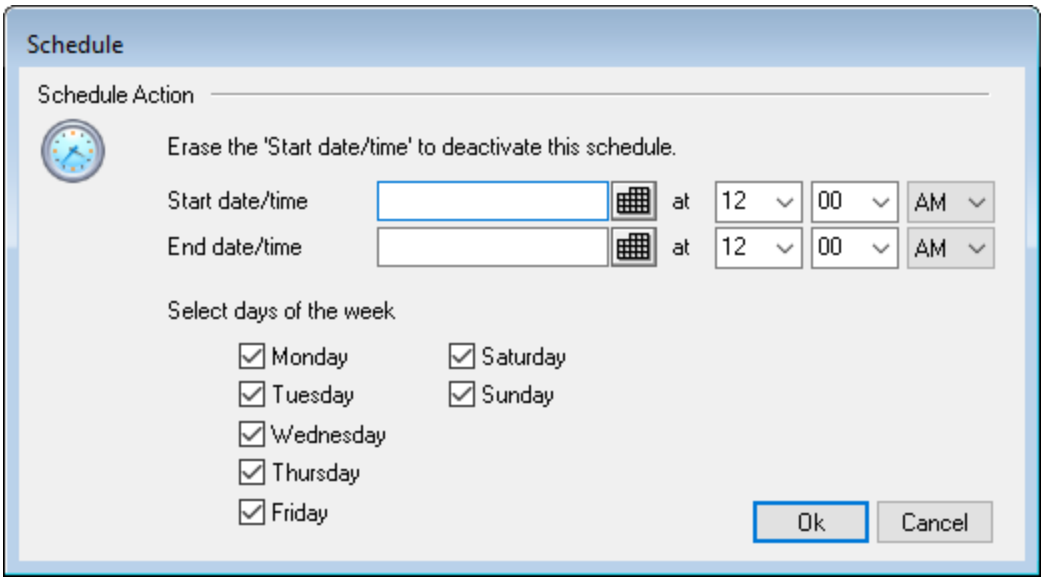
Autoresponder

Enable autoresponder
Enable this control to activate an autoresponder for all groups controlled by this template. For more information on autoresponders see: Autoresponders 823.

Edit autoresponse file
Click this button to edit the autoresponse file that will be used for those associated with this template.

Schedule
Click this button to open the Schedule dialog on which you can set a start and end date and time for the Autoresponder, and set the days of the week for it to be active. Leave the Schedule blank if you want the Autoresponder to be active continually.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



Publish
Click this button if you wish to copy this template's auto responder file and settings to one or more other accounts. Select the accounts to which you wish to copy the autoresponder and then click **Ok**.

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this autoresponder.

> Occasionally auto response messages may be sent to an address that returns an auto response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. If you encounter one of those addresses, enter it here to prevent that from happening. There is also an option located on the Autoresponders » Settings 827 screen, which can be used to limit auto response messages to one response per sender per day.

Remove
Click this button to delete any selected entries from the list of excluded addresses.

New excluded address—wildcards okay
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Run a Program

Run this program
Use this field to specify the path and filename to a program that you wish to run when new mail arrives for a group member controlled by this template. Care must be

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

taken to ensure that this program terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run this Program* field will be passed the name of the triggering message as the first available command line parameter. When the autoresponder is set for an account that is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see Forwarding 711) then this function will be disabled.

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible:
`logmail /e /j /message=$MESSAGE$ /q`.

Mailing Lists

Add sender to this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically added as a member of that mailing list. This is a handy feature for building lists automatically.

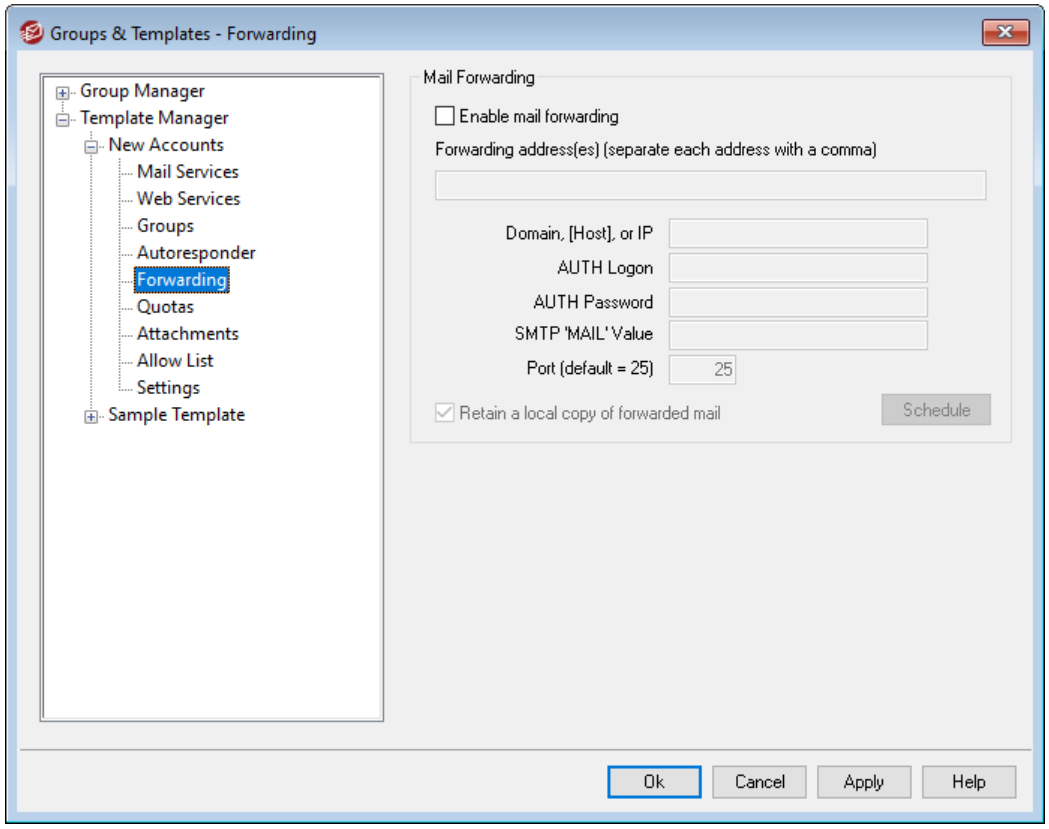
Remove sender from this mailing list
If a mailing list is entered in this field then the sender of the incoming message will be automatically removed from the specified mailing list.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Autoresponder 708

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.5 Forwarding



The options on this template screen correspond to the options located on the Account Editor's Forwarding 711 screen. When a template is set to control this screen 776, it will control the Forwarding options for any account belonging to a Group 766 that utilizes the template.

Mail Forwarding

Enable mail forwarding
Check this box if you wish to forward associated accounts' incoming messages to the address or addresses specified in the *Forwarding addresses* option below. MDaemon users with web access 703 to Webmail 308 or Remote Administration 341 can use the options provided to set the forwarding options for themselves rather than requiring an administrator to do so.

Forwarding addresses (separate each address with a comma)
Use this field to designate any email addresses to which you wish to forward copies of the associated account's incoming messages as they arrive. A copy of each new message arriving at the server will be automatically generated and forwarded to the addresses specified in this field, provided the *Enable mail forwarding* option above is checked. When forwarding to multiple addresses, separate each one with a comma.

Domain, [Host], or IP
If you wish to route the forwarded messages through another server, such as a particular domain's MX servers, then specify the domain or IP address here. If you

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

wish to route the messages to a specific host, then enclose the value in brackets (e.g. [host1.example.com]).

AUTH Logon/Password
Enter any required login/password credentials here for the server to which you are forwarding the associated users' mail.

SMTP 'MAIL' Value
If an address is specified here, it will be used in the "MAIL From" statement sent during the SMTP session with the accepting host, instead of using the actual sender of the message. If you require an empty SMTP "MAIL From" statement (i.e. "MAIL FROM <>") then enter "[trash]" into this option.

Port (default = 25)
MDaemon will send the forwarded messages using the TCP port specified here. The default SMTP port is 25.

Retain a local copy of forwarded mail
By default, a copy of each forwarded message is delivered normally to the local user's mailbox. If you uncheck this box then no local copy will be retained.

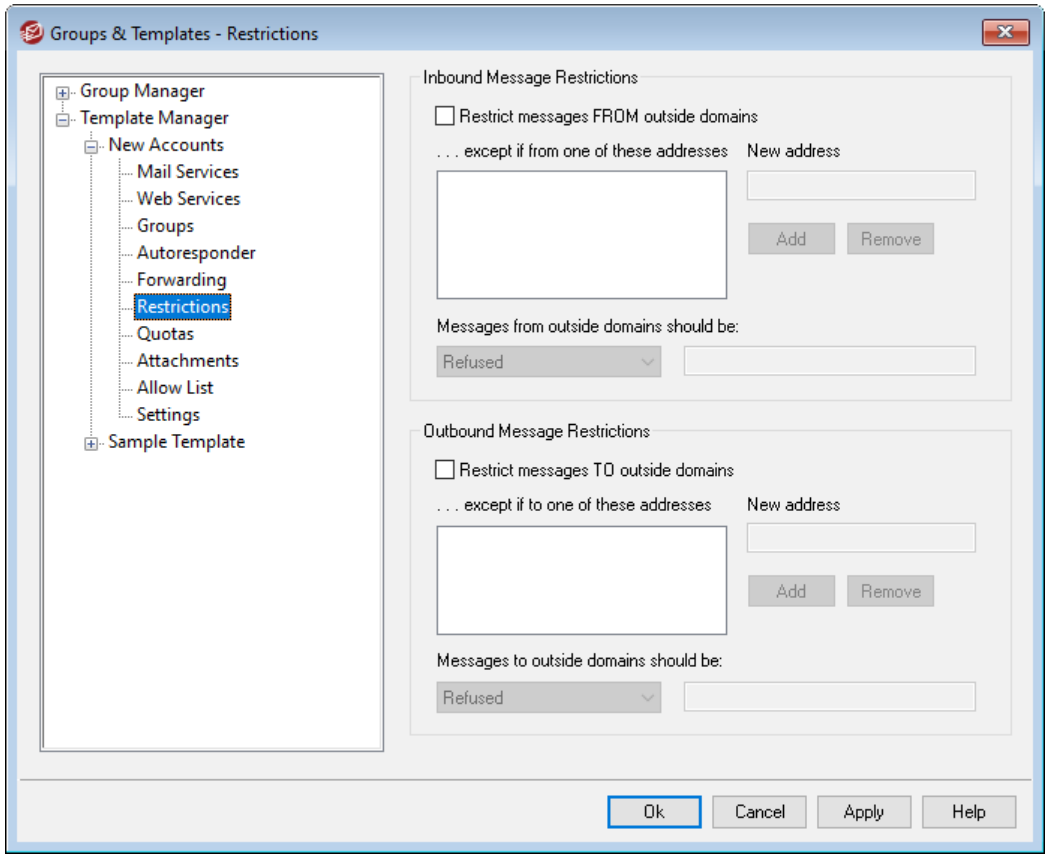
Schedule
Click this button to create a schedule for when the associated accounts' email will be forwarded. You can set a start date and time, an end date and time, and specify the days of the week on which mail will be forwarded.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Forwarding 711

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.6 Restrictions



The options on this template screen correspond to the options located on the Account Editor's Restrictions 713 screen. When a template is set to control this screen 776, it will control the Restrictions options for any account belonging to a Group 766 that utilizes the template.

Inbound Message Restrictions

Restrict messages FROM outside domains
Click this checkbox to prevent this account from receiving email messages from non-local domains.

...except if from one of these addresses
Addresses specified in this area are exceptions to the Inbound Message Restrictions. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then no inbound messages from any address at altn.com would be restricted.

New address
If you wish to add an address exception to the Inbound Message Restrictions list then type it here and click the *Add* button.

Add
After entering an address into the *New address* option, click this button to add it

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages from outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that are destined for this account but originate from a non-local domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

Returned to sender – Messages from restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of this account.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

Outbound Message Restrictions

Restrict messages TO outside domains
Click this checkbox to prevent this account from sending email messages to non-local domains.

...except if to one of these addresses
Addresses specified in this area are exceptions to the Outbound Message restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then outbound messages to any address at altn.com would not be restricted.

New address
If you wish to add an address exception to the Outbound Message Restrictions list then type it here and click the *Add* button.

Add
After entering an address into the *New address* option, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages to outside domains should be...
The options in this drop-down list box govern what MDaemon will do with messages that originate from this account but are destined for a non-local domain. You may choose any of the following options:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

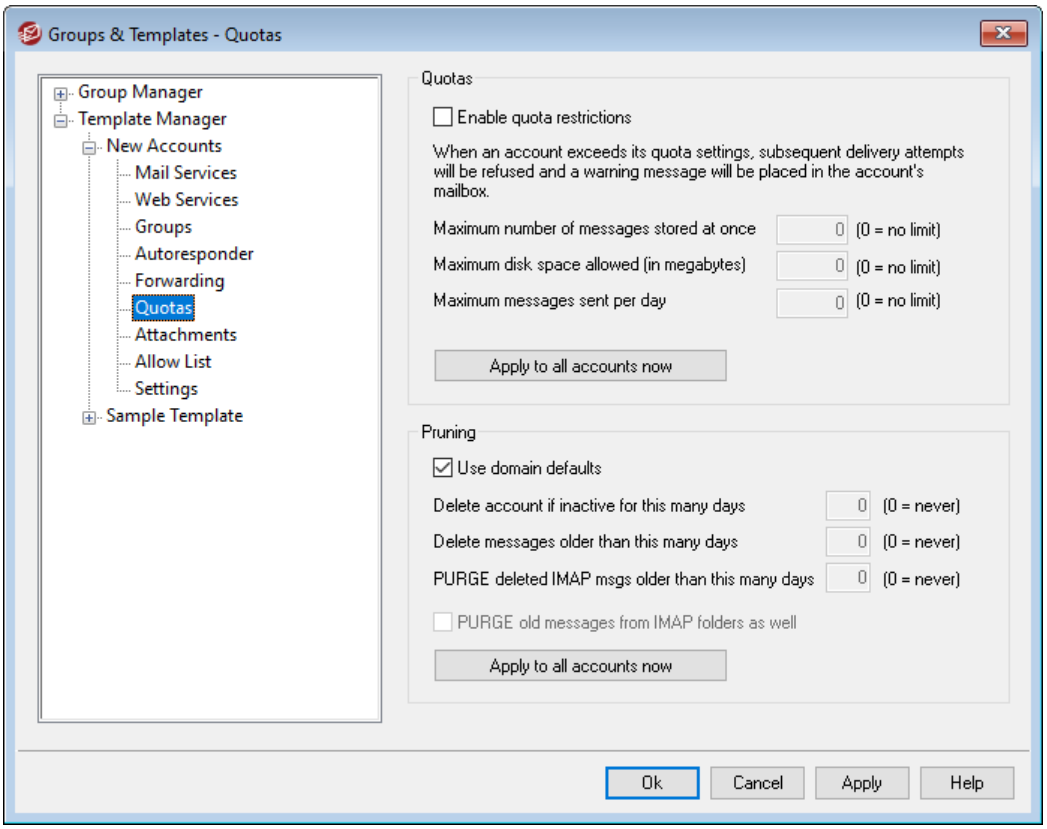
Refused – Restricted messages will be refused by MDaemon.

Returned to sender – Messages to restricted domains will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of the designated recipient.

Sent to... – Messages that are restricted will be accepted but delivered to the address that you specify in the text box on the right.

5.2.2.1.7 Quotas



The options on this template screen correspond to the options located on the Account Editor's Quotas 715 screen. When a template is set to control this screen 776, it will control the Quotas options for any account belonging to a Group 766 that utilizes the template.

Quotas

Enable quota restrictions
Check this box if you wish to specify a maximum number of messages that accounts controlled by this template can store, set a maximum amount of disk space that the accounts can use (including any file attachments in each account's Documents folder), or designate a maximum number of messages that the accounts can send

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

via SMTP per day. If a mail delivery is attempted that would exceed the maximum message or disk space limitations, the message will be refused and an appropriate warning message will be placed in the user's mailbox. If a MultiPOP[723] collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Use the *Email a warning to user if this percent of their quota is reached* option at "Accounts » Account Settings » Quotas[796]" to cause a warning message to be sent when an account nears its quota limits. When the account exceeds a designated percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* restriction, a warning message will be sent to the account at midnight. The message will list the account's number of stored messages, the size of its mailbox, and the percent used and remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message.

Maximum number of messages stored at once
Use this option to designate the maximum number of messages that can be stored for the accounts. Using "0" in the option means there will be no limit to the number of messages permitted.

Maximum disk space allowed (in megabytes)
Use this option to designate the maximum amount of disk space that the accounts can use, including any file attachments that may be stored in each account's Documents folder. Using "0" in the option means there will be no limit to the amount of disk space that the accounts can use.

Maximum messages sent per day
Use this option to designate the maximum number of messages that each account can send per day via SMTP. If the account reaches this limit then new mail from the account will be refused until the counter is reset at midnight. Use "0" in the option if you do not wish to limit the number of messages the account can send.

Apply to all accounts now

Click this button to apply the settings on this screen to all existing MDaemon accounts whose Quotas settings are not specifically controlled by an account template. This will reset the accounts to the default Quotas values. This option is only available on the New Accounts Template[775].

Pruning

The options in this section are used to designate when or if an account controlled by this template will be deleted if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain amount of time. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use domain defaults
The default Pruning settings are domain-specific and located on the Domain Manager's Settings 205 screen. If you wish to override the domain defaults for template-controlled accounts, clear this checkbox and set the desired values in the options below.

Delete account if inactive for this many days (0 = never)
Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account will never be deleted due to inactivity.

Delete messages older than this many days (0 = never)
This is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age. **Note:** This option's setting does not apply to messages contained in IMAP folders unless you also enable the "*PURGE old messages from IMAP folders as well*" option below.

PURGE deleted IMAP msgs older than this many days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in a user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

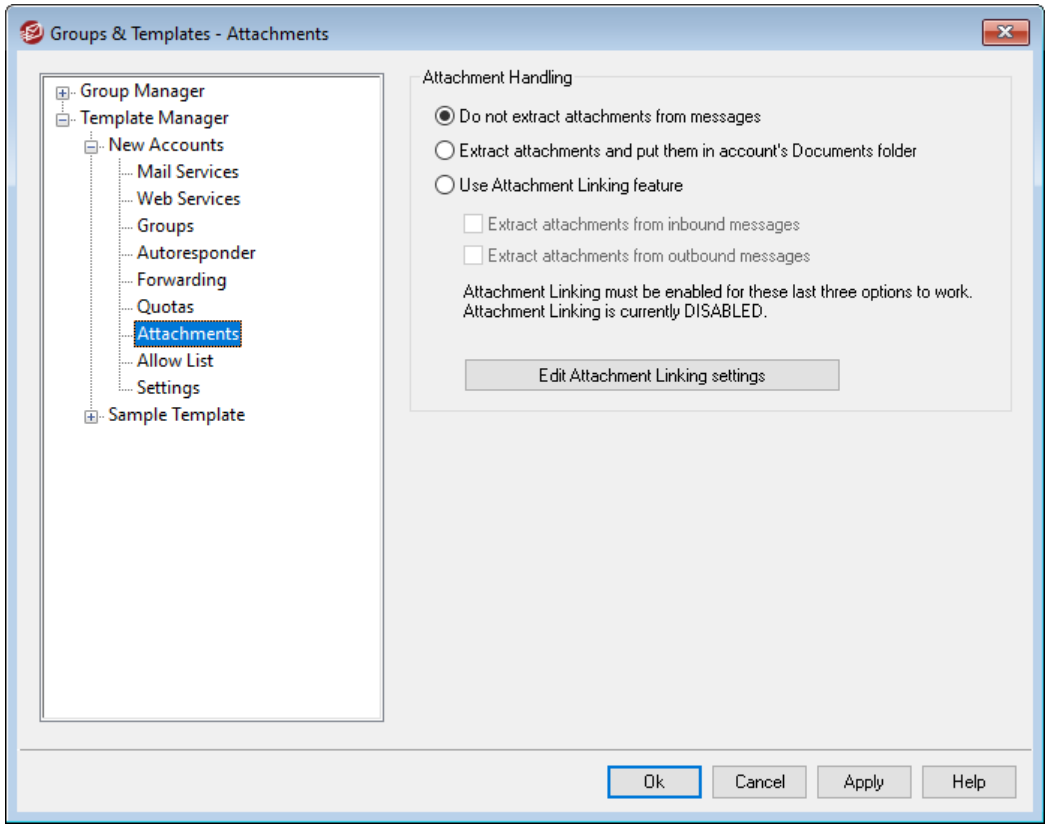
PURGE old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages older than this many days*" option above to apply to messages in IMAP folders as well. When this control is disabled, regular messages contained in IMAP folders will not be deleted due to their age.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Quotas 715
Account Settings » Quotas 844

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.8 Attachments



The options on this template screen correspond to the options located on the Account Editor's Attachments 718 screen. When a template is set to control this screen 776, it will control the Attachments options for any account belonging to a Group 766 that utilizes the template.

Attachment Handling

Do not extract attachments from messages
If this option is selected, attachments will not be extracted from a template-controlled account's messages. Messages with attachments will be handled normally, leaving the attachments intact.

Extract attachments and put them in account's Documents folder
If set, this option causes MDaemon to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages for the account. Extracted files are removed from the incoming message, decoded, and placed in the account's Documents folder. A note is then placed within the body of the message, stating the names of the files that were extracted. This option does not provide a link to the stored attachments, but users can use Webmail 308 to access their Documents folder.

Use Attachment Linking feature
Select this option if you wish to use the Attachment Linking feature for inbound or outbound messages with attachments.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If this option is selected but the Attachment Linking feature is disabled on the Attachment Linking 357 dialog, then attachments will not be extracted.

Extract attachments from inbound messages
When this option is enabled, attachments will be extracted from the account's incoming messages and stored in the location designated on the Attachment Linking 357 dialog. URL links are then placed within the body of the message, which the user can then click to download the files. For security these URL links do not contain direct file paths. Instead they contain a unique identifier (GUID) that the server uses to map the file to the actual path. This GUID map is stored in the `AttachmentLinking.dat` file..

Extract attachments from outbound messages
Check this box if you wish to use the Attachment Linking feature to extract attachments from the account's outbound messages. When the account sends an email, Attachment Linking will extract the file, store it, and replace it with a URL to download the file.

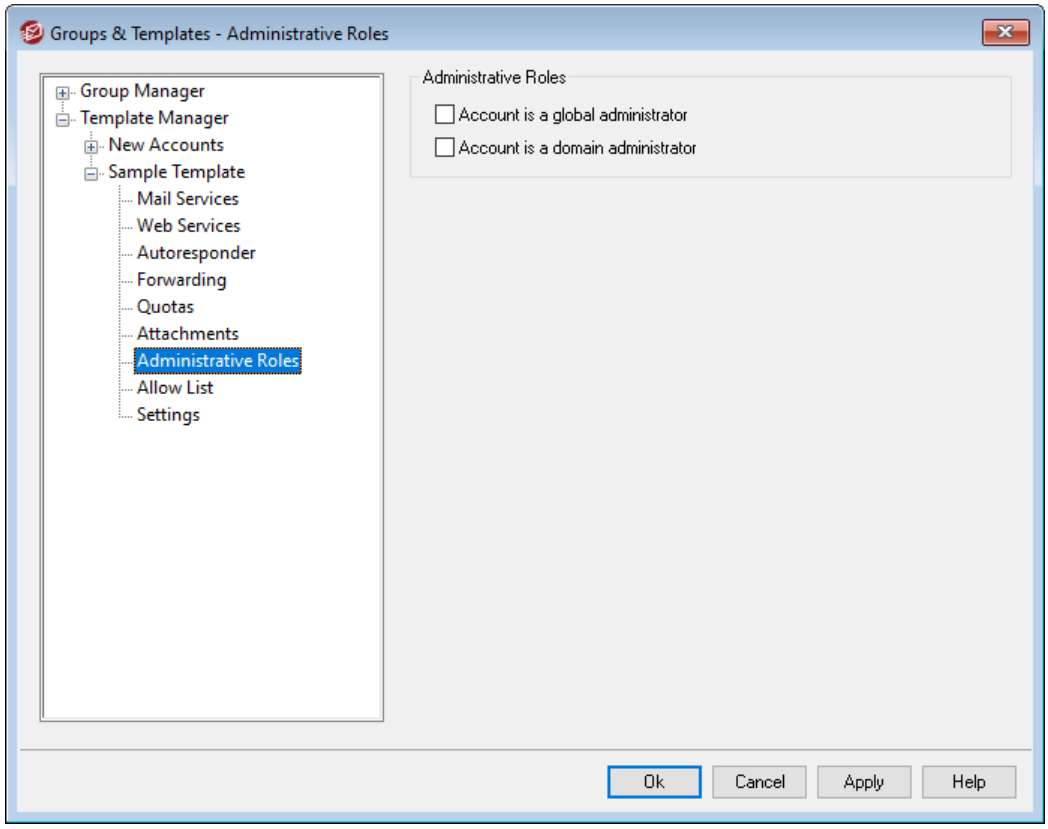
Edit Attachment Linking settings
Click this button to open the Attachment Linking 357 dialog.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Attachment Linking 700
Account Editor » Attachments 718

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.9 Administrative Roles



Administrative Roles

Account is a global administrator
Enable this checkbox to grant these users server-level administrative access. Global administrators have:

- Full access to server configuration, all users, and all domains via Remote Administration
- Access to all MDaemon users of all MDaemon domains as Instant Messaging buddies.
- The ability to post to all mailing lists even if flagged as "Read Only".
- The ability to post to all mailing lists even if not a member.

The user will have complete access to MDaemon's files and options. For more on the administrative options within the Remote Administration web-interface, see Remote Administration 341.

Account is a domain administrator
Click this checkbox to designate the users as Domain Administrators. Domain administrators are similar to global administrators except that their administrative access is limited to this domain and to the permissions granted on the Web Services 703 page.

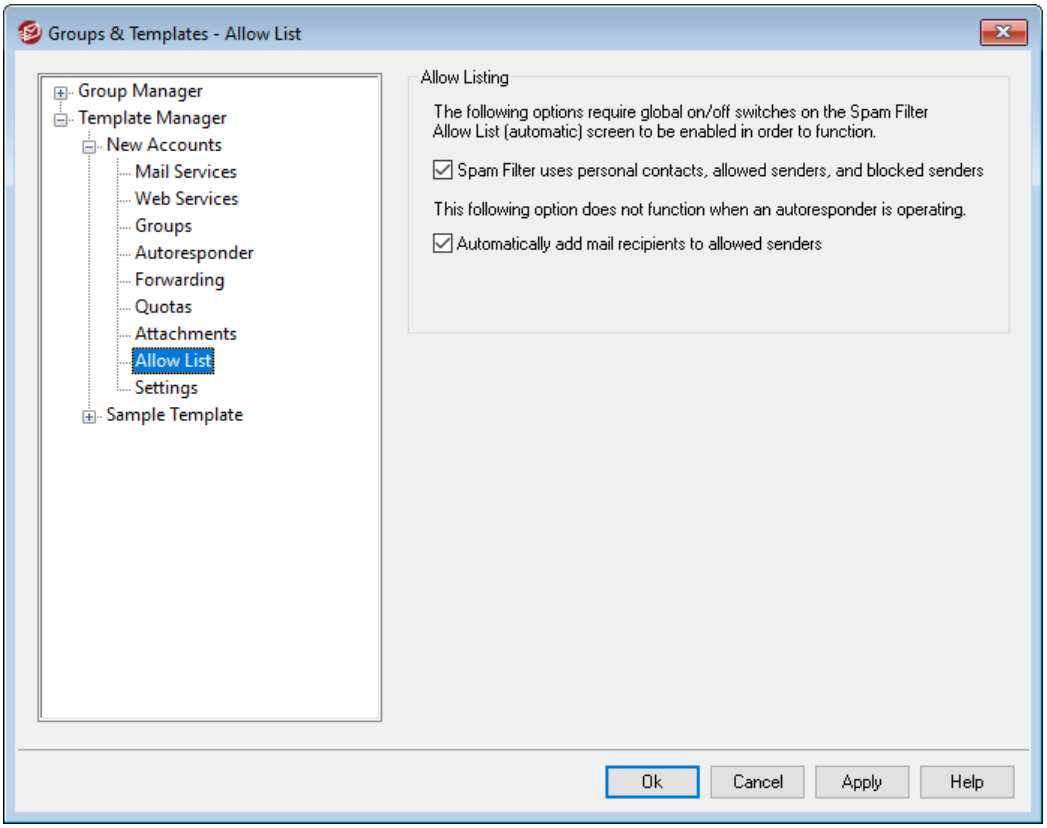
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

This screen is not available on the New Accounts template[775]. Administrative access cannot be automatically granted to new accounts. To grant administrative access to an account, associate the account with a customized template that uses this screen to grant that access, or manually designate the account as an administrator from the Account Editor's Administrative Roles[741] screen.

See:

Template Properties[776]
Group Properties[766]
New Accounts Template[775]
Account Editor » Administrative Roles[741]

5.2.2.1.10 Allow List



The options on this template screen correspond to the settings located on the Account Editor's Allow List[742] screen. When a template is set to control this screen[776], it will control the Allow List screen settings for any account belonging to a Group[766] that utilizes the template.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Allow Listing

Spam Filter uses personal contacts, allowed senders, and blocked senders
The Spam Filter's Allow List (automatic) 672 screen contains a global option that can be used to cause the Spam Filter allow a message automatically when the sender of the message is found in the local recipient's personal contacts or allowed senders folder. It will also automatically block a message when the sender is found in the user's blocked senders folder. If you have enabled the Spam Filter's global option but do not wish to apply it to these accounts, clear this check box to override the global setting. If the global option is disabled then this option will not be available.

Automatically add mail recipients to allowed senders
Click this option if you wish to update each account's allowed senders folder each time it sends an outgoing message to a non-local email addresses. When used in conjunction with the above option, *Spam Filter uses personal contacts, allowed senders, and blocked senders*, the number of Spam Filter false positives can be drastically reduced. The *Automatically add mail recipients to allowed senders* option located on the Allow List (automatic) 672 screen must be enabled before you can use this feature.

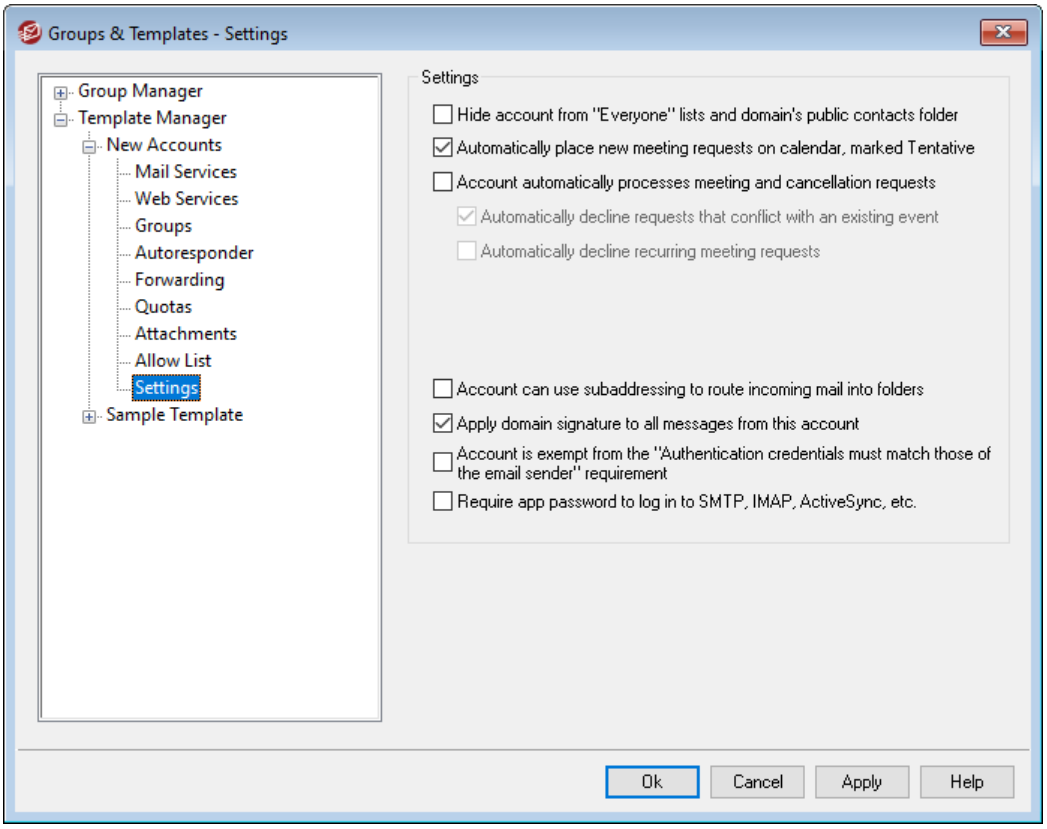
This option is disabled when the account is using an autoresponder.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Allow List 742

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.2.2.1.11 Settings



The options on this template screen correspond to the settings located on the Account Editor's Settings 744 screen. When a template is set to control this screen 776, it will control the Settings screen for any account belonging to a Group 766 that utilizes the template.

Settings

Account hidden from "Everyone" lists, shared calendars, and VRFY
MDaemon automatically creates and maintains an "everyone@" mailing list for each domain, which can be used to send a message to everyone at once. By default MDaemon will include all accounts when it constructs this list. Check this box if you wish to exclude accounts controlled by this template from that list. This will also hide the accounts from shared calendars and VRFY 86 results.

Automatically place new meeting requests on calendar, marked Tentative
By default when an account receives a new meeting request, the meeting is placed on the user's calendar and marked as *Tentative*. Clear this checkbox if you do not wish this to be the default setting for new accounts.

Account automatically processes meeting and cancellation requests
Click this checkbox if you wish to cause automatic processing of meeting requests, changes, and cancellations for each account. When an account receives a message that contains a meeting request, the account's calendar will be updated automatically. This option is disabled for all accounts by default.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Automatically decline requests that conflict with an existing event
If automatic processing of meeting requests and cancellations is enabled, those meeting requests will be automatically declined by default when they conflict with an existing event. Clear this checkbox if you wish to allow the conflicting event to be created.

Automatically decline recurring meeting requests
Click this box if automatic processing of meeting requests and cancellations is enabled but you wish to decline those requests when they are for recurring meetings.

Account can use subaddressing to route incoming mail into folders
Click this checkbox if you wish to permit subaddressing 746 for the accounts.

Apply domain signature to all messages from this account
When there is a Domain Signature 195 for the domain to which accounts governed by this template belong, this option causes it to be added to all emails sent by those accounts.

Account is exempt from the "Authentication credentials must match those of the email sender" requirement
Use this option if you wish to exempt accounts governed by this template from the "*Authentication credentials must match those of the email sender*" global option located on the SMTP Authentication 509 screen.

Require app password to log in to SMTP, IMAP, ActiveSync, etc.
Check this box if you wish to require that accounts using this template must use App Passwords 734 in mail clients, to log in to SMTP, IMAP, ActiveSync, or other mail service protocols. The account's regular password 840, however, must still be used to sign in to Webmail or Remote Admin.

Requiring App Passwords can help protect an account's password from dictionary and brute force attacks via SMTP, IMAP, etc. This is more secure because even if an attack of this sort were to guess an account's actual password, it wouldn't work and the attacker wouldn't know, because MDaemon would only accept a correct App Password. Additionally, if your accounts in MDaemon are using Active Director authentication and Active Directory locks an account after a number of failed attempts, this option can help prevent accounts from being locked out, because MDaemon will only check the App Passwords, not try to authenticate to Active Directory.

See:

Template Properties 776
Group Properties 766
New Accounts Template 775
Account Editor » Settings 744

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3 Account Settings

5.3.1 Active Directory

Using the Active Directory options located at Accounts » Account Settings » Active Directory, MDaemon can be configured to monitor Active Directory and automatically create, edit, delete and disable MDaemon accounts when their associated accounts are altered in Active Directory. Further, it can also be set to keep all public contact records updated with the most recent information stored in Active Directory. Common fields like an account's postal address, phone numbers, business contact information, and so on can be populated into the public contact records and updated any time they are changed in Active Directory.

Creating Accounts

When set to monitor Active Directory, MDaemon will query for changes at a designated interval and then create a new MDaemon user account whenever it finds that a new Active Directory account has been added. This new MDaemon user account will be created using the full name, logon, mailbox, description, and enabled/disabled state found within Active Directory.

By default, new MDaemon accounts created as a result of Active Directory monitoring will be added to MDaemon's Default Domain. Alternatively, you can choose to have those accounts added to the domain found within the account's "UserPrincipalName" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain 174 will be created automatically.

You can alternatively configure your *Search filter* 809 to monitor a group within Active Directory, so adding a user to the group or a group to the user will cause the user to be created in MDaemon, and removing a user from a group will cause the account to be disabled (not deleted) in MDaemon.

Deleting Accounts

MDaemon can be configured to take one of the following actions when an account is deleted from Active Directory: do nothing, delete the associated MDaemon account, disable the associated MDaemon account, or freeze the associated MDaemon account (i.e. the account can still receive mail but the user can't collect it or access it).

Updating Accounts

When MDaemon detects changes to Active Directory accounts, it will automatically update the associated properties in the matching MDaemon account.

Synchronizing MDaemon with Active Directory

A "*Perform full AD scan now*" option is available to cause MDaemon to query the Active Directory database and then create or modify MDaemon user accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it. Then, any future changes made to the Active Directory accounts will be propagated to the MDaemon accounts automatically.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Active Directory Authentication

Accounts created by MDaemon's Active Directory feature will be setup for Active Directory (AD) Authentication by default. With AD Authentication, MDaemon has no need to store the account's password within its own user database. Instead, the account holder will use his or her Windows login/password credentials and MDaemon will pass those to Windows for authentication of the associated account.

To use AD Authentication with Active Directory, a Windows domain name must be present in the space provided on the Monitoring 812. This is the Windows domain that MDaemon will use when attempting to authenticate accounts. In most cases, MDaemon will detect this Windows domain name automatically and fill it in for you. However, you can use an alternate domain in this option if you choose, or you can use "NT_ANY" if you wish to allow authentication across all of your Windows domains instead of limiting it to a specific one. If you leave this option blank then MDaemon will not use AD Authentication when new accounts are created. Instead it will generate a random password, which you will have to edit manually before users will be able to access their mail accounts.

Persistent Monitoring

Active Directory monitoring will continue to work even when MDaemon is shut down. All Active Directory changes will be tracked and then MDaemon will process them once it restarts.

Active Directory File Security

It is worth noting that MDaemon's Active Directory features do not alter the Active Directory schema files in any way — all monitoring is one-way from Active Directory to MDaemon. MDaemon will not alter your directory.

Active Directory Template

Whenever MDaemon adds or makes changes to accounts due to Active Directory monitoring and scanning, it will use an Active Directory template ("MDaemon/app/ActiveDS.dat") to link certain Active Directory attribute names to MDaemon's account fields. For example, MDaemon links the Active Directory attribute "cn" to MDaemon's "FullName" field by default. These links, however, are not hard-coded. You can easily edit this template with Notepad if desired and alter any of the default field mappings. For example, "FullName=%givenName% %sn%" could be used as a replacement for the default setting: "FullName=%cn%". See ActiveDS.dat for more information.

Updating the Public Address Books

Active Directory monitoring can be used to periodically query Active Directory and keep all public contact records in MDaemon updated with the most recent information. Common fields like an account's postal address, phone numbers, business contact information, and so on will be populated into their public contact record, and this data will be updated any time it is changed in Active Directory. To enable this feature, use the "*Monitor Active Directory and update public address book(s)*" option located at: Active Directory » Monitoring 812.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Numerous contact record fields can be monitored using this feature. For a complete list of which public contact record fields can be mapped to Active Directory attributes, see the `ActiveDS.dat` file. This file has several new mapping templates which allow you to specify one or more Active Directory attributes from which to populate a particular contact record field (for example, `%fullName%` for the fullname field, `%streetAddress%` for the street address field, and so on).

MDaemon must match an account's email address to some attribute within Active Directory in order to know which contact record to update. If it can't find such a match it does nothing. By default MDaemon will try to construct an email address using the data taken from the attribute mapped to the Mailbox template (see `ActiveDS.dat`) to which MDaemon will internally append the default domain 174 name, just as it would when actually creating and deleting accounts based on Active Directory data. However, you can uncomment the "abMappingEmail" template inside `ActiveDS.dat` and tie it to any Active Directory attribute you wish (like `%mail%`, for example). However, please note that the value of this attribute must contain an email address that will be recognized as a valid local user account.

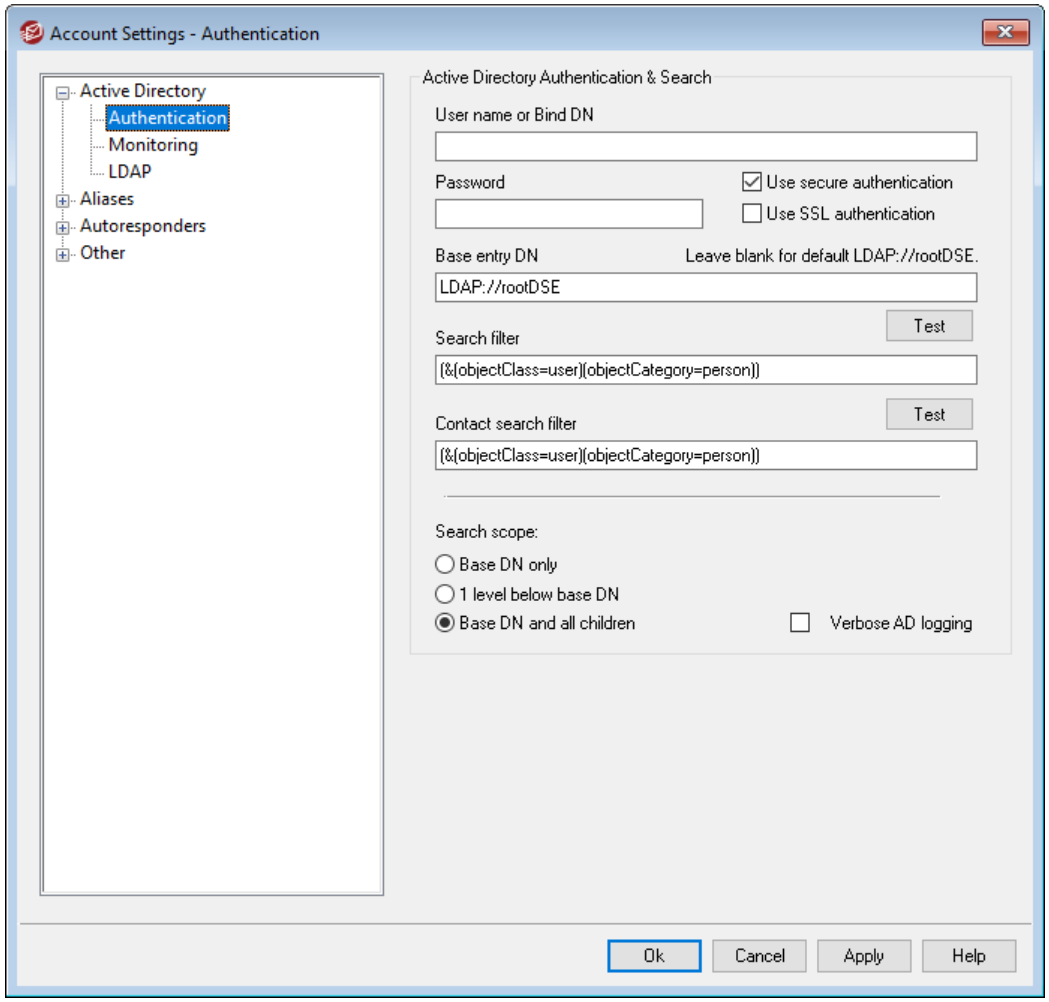
This feature will create the contact records on the fly if they don't already exist and it will update contact records that do exist. Further, please note that it will overwrite any changes you make outside of Active Directory. Contact record fields that are not mapped are left unaltered. Therefore any existing data that is not subject to this process will not be altered or lost. Finally, MDaemon accounts that are set to hidden 744 are not subject to having their contact records created or updated.

See:

Active Directory » Monitoring 812
Active Directory » Authentication 809

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.1.1 Authentication



Access to Active Directory may require special permissions to be set for all features to function.

Active Directory Authentication & Search

User name or Bind DN
This is the Windows account Logon or DN that MDaemon will use when binding to Active Directory using LDAP. Active Directory permits the use of a Windows account or UPN when binding.

When using a DN in this option rather than a Windows logon, you must disable/clear the "*Use secure authentication*" option below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Password
This is the password that corresponds to the DN or Windows logon used in the *Bind DN* option above.

Use secure authentication
Click this checkbox if you wish to use secure authentication when performing your Active Directory searches. You cannot use this option when you are using a DN rather than a Windows logon in the *Bind DN* option above.

Use SSL authentication
Click this checkbox if you wish to use SSL authentication when performing your Active Directory searches.

Use of this option requires an SSL server and infrastructure on your Windows network and Active Directory. Contact your IT department if you are unsure if your network is setup this way, and to find out if you should enable this option.

Active Directory Searching

Base entry DN
This is the Distinguished Name (DN) or starting point in the Directory Information Tree (DIT) at which MDaemon will search your Active Directory for accounts and changes. By default MDaemon will begin searching at Root DSE, which is the topmost entry in your Active Directory hierarchy. Designating a more precise starting point closer to the location of your user accounts in your particular Active Directory tree can reduce the amount of time required to search the DIT for accounts and account changes. Leaving this field blank will restore the default setting of `LDAP://rootDSE`

Search filter
This is the LDAP search filter that will be used when monitoring or searching your Active Directory for accounts and account changes. Use this filter to more precisely locate the desired user accounts that you wish to include in Active Directory monitoring.

You can also configure your search filter to monitor a group within Active Directory, so adding a user to the group or a group to the user will cause the user to be created in MDaemon, and removing a user from a group will cause the account to be disabled (not deleted) in MDaemon. For example, a proper search filter for a group called 'MyGroup' could look like this:

```
(|(&(ObjectClass=group)(cn=MyGroup))(&(objectClass=user)
(objectCategory=person)
(memberof=cn=MyGroup,ou=me,dc=domain,dc=com)))
```

Replace the 'ou=' and 'dc=' bits with something appropriate to your network.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Contact search filter
Use this option to specify a separate search filter for contact searches. If you use the same text in this field as in the *Search filter* option above, only one query is used to update all data. When the search filters are different, two separate queries are necessary.

Test
Use the *Test* buttons to test your search filter settings.

Search scope:

This is the scope or extent of your Active Directory searches.

Base DN only
Choose this option if you wish to limit your search to only the base DN specified above. The search will not proceed below that point in your tree (DIT).

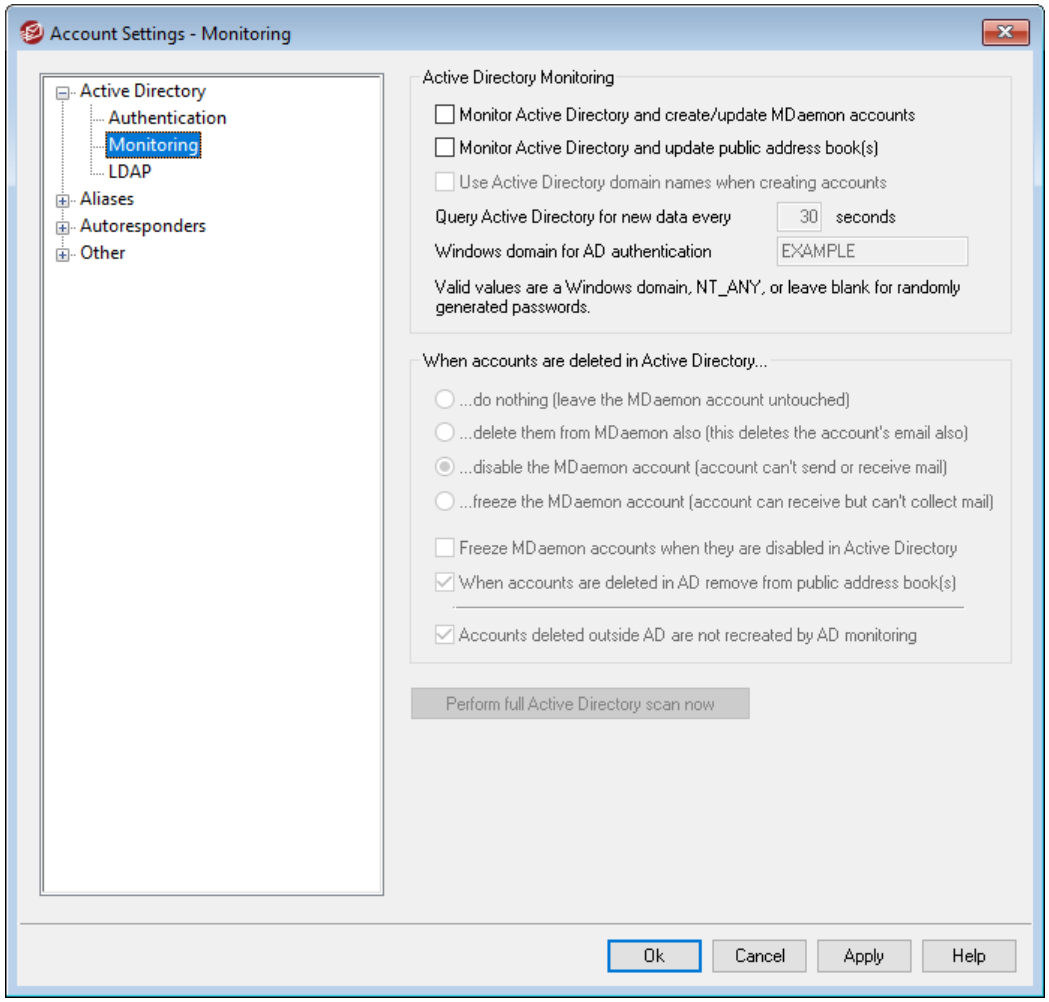
1 level below base DN
Use this option if you wish to extend your Active Directory search to one level below the supplied DN in your DIT.

Base DN and all children
This option will extend the scope of your search from the supplied DN to all of its children, down to the lowest child entry in your DIT. This is the default option selected, which when combined with the default Root DSE setting above means that the entire DIT below the Root DSE will be searched.

Verbose AD logging
By default MDaemon will use verbose logging for Active Directory. Clear this checkbox if you wish to use less extensive Active Directory logging.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.1.2 Monitoring



Active Directory Monitoring

Monitor Active Directory and create/update MDaemon accounts
Click this option to activate Active Directory monitoring, which will create and update MDaemon accounts as Active Directory is updated.

Monitor Active Directory and update public address book(s)
Enable this option if you wish to use Active Directory to keep all public contact records updated with the most recent information stored in Active Directory. Common fields like an account's postal address, phone numbers, business contact information, and so on will be populated into their public contact record and this data will be updated any time it is changed in Active Directory. Numerous contact record fields will be monitored in this way. For a complete list of which public contact record fields can be mapped to Active Directory attributes, see the `ActiveDS.dat` file. See: Updating the Public Address Books 807, for more information.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Use Active Directory domain names when creating accounts
Use this option if you would like new accounts created as a result of Active Directory monitoring to be added to the domain found within the account's "UserPrincipalName" Active Directory attribute. When using this option, if an account requires a domain that doesn't yet exist within MDaemon, a new domain 174 will be created automatically. Clear/disable this option if you would like all new accounts to be added to MDaemon's Default Domain 174.

Query Active Directory for new data every [XX] seconds
This is the interval at which MDaemon will monitor Active Directory for changes.

Windows domain for AD authentication
Specify a Windows domain name here if you wish to use Active Directory Authentication for accounts created by Active Directory monitoring. If you leave this field blank then new accounts will be assigned random passwords. You will then have to edit those passwords manually in order for the accounts to be accessed.

When accounts are deleted in Active Directory...
The option selected below determines the action MDaemon will take when an MDaemon account's associated Active Directory account is deleted.

...do nothing
Choose this option if you do not wish MDaemon to make any changes to an MDaemon account when its associated account is deleted from Active Directory.

...delete them from MDaemon also
Choosing this option will cause the MDaemon account to be deleted when its associated account is deleted from Active Directory.

This will cause the associated MDaemon account to be completely removed. All of the account's messages, message folders, address books, calendars, and so on will be deleted.

...disable the MDaemon account
When this option is selected and an Active Directory account is deleted, its corresponding MDaemon account will be disabled. This means that the MDaemon account will still exist on the server, but it cannot send or receive email or be accessed by anyone.

...freeze the MDaemon account
When this option is selected MDaemon will still accept the account's incoming mail but effectively "lock" it so that it cannot be accessed. In other words, incoming mail addressed to that account will not be rejected or deleted by MDaemon but the account holder will not be able to collect or access that mail as long is the account is frozen.

Freeze MDaemon accounts when they are disabled in Active Directory
By default, when you disable an account in Active Directory, MDaemon will also disable the associated account in MDaemon. This makes the account inaccessible

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

and MDaemon will neither accept nor deliver messages for it. However, if you prefer to have the associated MDaemon account frozen instead of disabled, enable this option. MDaemon will still accept messages for frozen accounts, but users will not be able to access those accounts to collect or send their email.

When accounts are deleted in AD remove from public address book(s)
By default, a public folder contact is deleted whenever its associated account is deleted from Active Directory. However, the contact is only deleted if it was originally created by the Active Directory integration feature 807. Disable this option if you do not wish to delete contacts when associated accounts are deleted in Active Directory.

Accounts deleted outside AD are not recreated by AD monitoring
When you delete an MDaemon account outside of Active Directory (for example, by manually deleting it using the MDaemon interface), by default the account will not be recreated by the Active Directory monitoring feature. Disable this option if you want these accounts to be recreated.

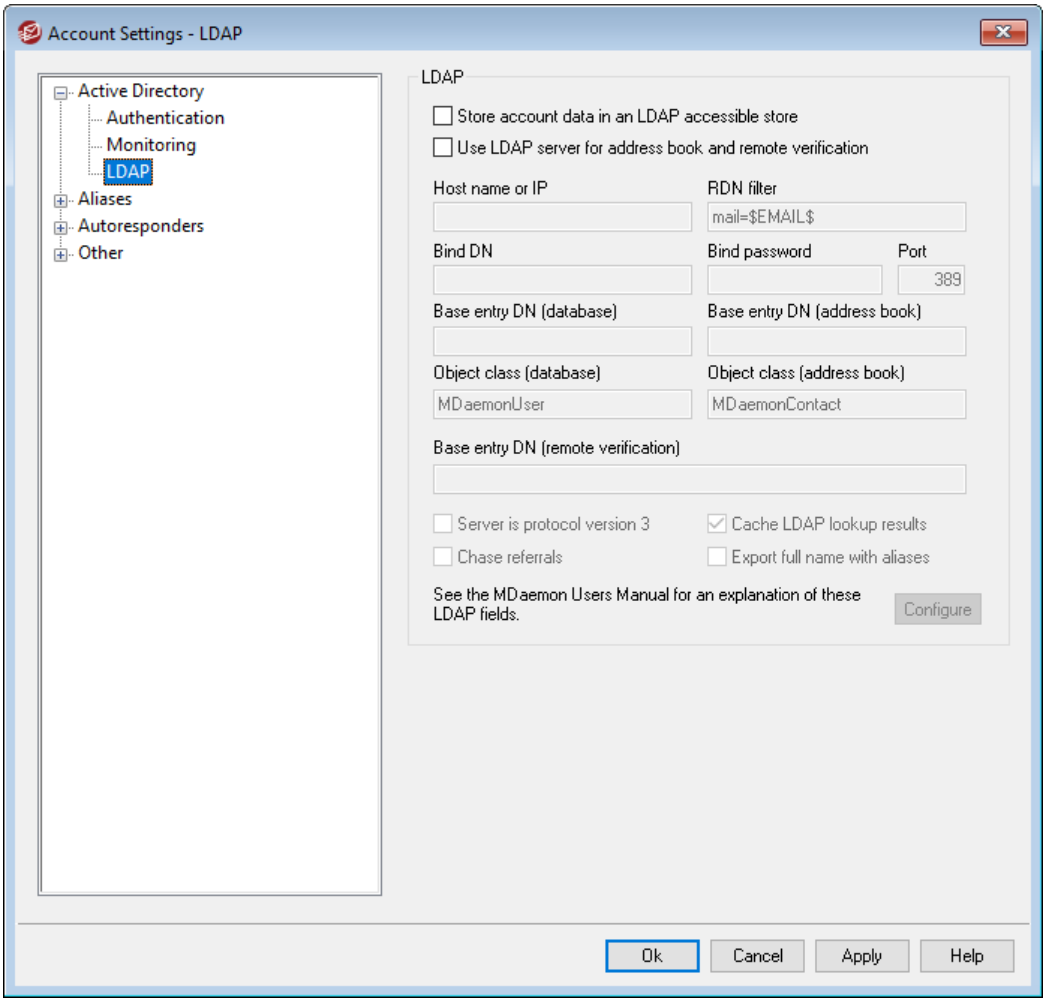
Perform full Active Directory scan now
Click this button to cause MDaemon to query the Active Directory database and then create, edit, or delete accounts as necessary. When an Active Directory account is found that matches an already existing MDaemon account, the MDaemon account will be linked to it.

See:

Active Directory 806
Active Directory » Authentication 809

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.1.3 LDAP



MDaemon supports Lightweight Directory Access Protocol (LDAP) functionality. Click "Accounts » Account Settings » LDAP" to reach the LDAP screen used for configuring MDaemon to keep your LDAP server up to date on all of its user accounts. MDaemon can maintain an accurate and continuously up to date LDAP database of users by communicating with your LDAP server each time an MDaemon account is added or removed. This makes it possible for users with mail clients that support LDAP to "share" a global address book that will contain entries for all of your MDaemon users as well as any other contacts that you include.

You can also use your LDAP server as the MDaemon user database 833 rather than its local `USERLIST.DAT` system or an ODBC compliant database. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

LDAP

Store account data in an LDAP accessible store
Click this check box if you want MDaemon to use your LDAP server as the MDaemon user database rather than ODBC or its local `USERLIST.DAT` system. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

Use LDAP server for address book and remote verification
If you are using ODBC or the default `USERLIST.DAT` method of maintaining your account database rather than the LDAP server method, you can still keep an LDAP server up to date with all of your users' names, email addresses, and aliases by enabling this checkbox. Thus, you can still keep an LDAP server up to date for use as a global address book system for users of email clients that contain support for LDAP address books.

This will maintain a database of your mailboxes, aliases, and mailing lists that your remote backup servers can query for remote verification of address information. See *Base entry DN (remote verification)* below for more information.

LDAP Server Properties

Host name or IP
Enter the host name or IP address of your LDAP server here.

RDN filter
This control is used to generate the RDN for each user's LDAP entry. The relative distinguished name (RDN) is the leftmost component in each entry's distinguished name (DN). For all peer entries (those sharing a common immediate parent) the RDN must be unique, therefore we suggest using each user's email address as their RDN to avoid possible conflicts. Using the $EMAIL$ macro as the value of the attribute in this control (i.e. `mail=$EMAIL$`) will cause it to be replaced by the user's email address when their LDAP entry is created. The user's DN will be comprised of the RDN plus the *Base entry DN* below.

Bind DN
Enter the DN of the entry to which you have granted administrative access to your LDAP server so that MDaemon can add and modify your MDaemon user entries. This is the DN used for authentication in the bind operation.

Bind Password
This password will be passed to your LDAP server along with the *Bind DN* value for authentication.

Port
Specify the port that your LDAP server is monitoring. MDaemon will use this port when posting account information to it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Base entry DN (database)
Enter the base entry (root DN) that will be used in all of your MDaemon user entries when you are using the LDAP server as your user database rather than the `USERLIST.DAT` file. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Base entry DN (address book)
When mirroring account information to an LDAP database address book, enter the base entry (root DN) that will be used in all of your MDaemon user address book entries. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Object class (database)
Specify the object class to which each MDaemon user's user database entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

Object class (address book)
Specify the object class to which each MDaemon user's LDAP address book entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

Base entry DN (remote verification)
One common problem with domain gateways and backup servers is that they don't usually have a method for determining whether or not the recipient of an incoming message is valid. For instance, if a message comes to example.com's backup server for `user1@example.com` then the backup server has no way of knowing whether or not there is actually a mailbox, alias, or mailing list at example.com for "`user1`". Thus the backup server has no choice but to accept all of the messages. MDaemon contains a method for verifying these addresses and solving this problem. By specifying a Base entry DN that will be used for all mailboxes, aliases, and mailing lists, your LDAP server can be kept up to date with all of this information. Then, your backup server can simply query your LDAP server each time a message arrives for your domain and verify whether or not the recipient's address is valid. If it isn't then the message will be rejected.

Server is protocol version 3
Click this checkbox if want MDaemon to use LDAP protocol version 3 with your server.

Chase referrals
Sometimes an LDAP server doesn't have a requested object but may have a cross-reference to its location, to which it can refer the client. If you want MDaemon to chase (i.e. follow) these referrals, enable this option. This is disabled by default.

Cache LDAP lookup results
By default MDaemon caches LDAP lookup results. Disable this option if you do not wish to cache them.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Export full name with aliases
Non-aliases exported to an LDAP address book put the account's full name in the CN field. Aliases, however, have the account's actual (non-alias) email address placed there. Check this box if you want to put the account's full name (if known) there instead. This option is disabled by default.

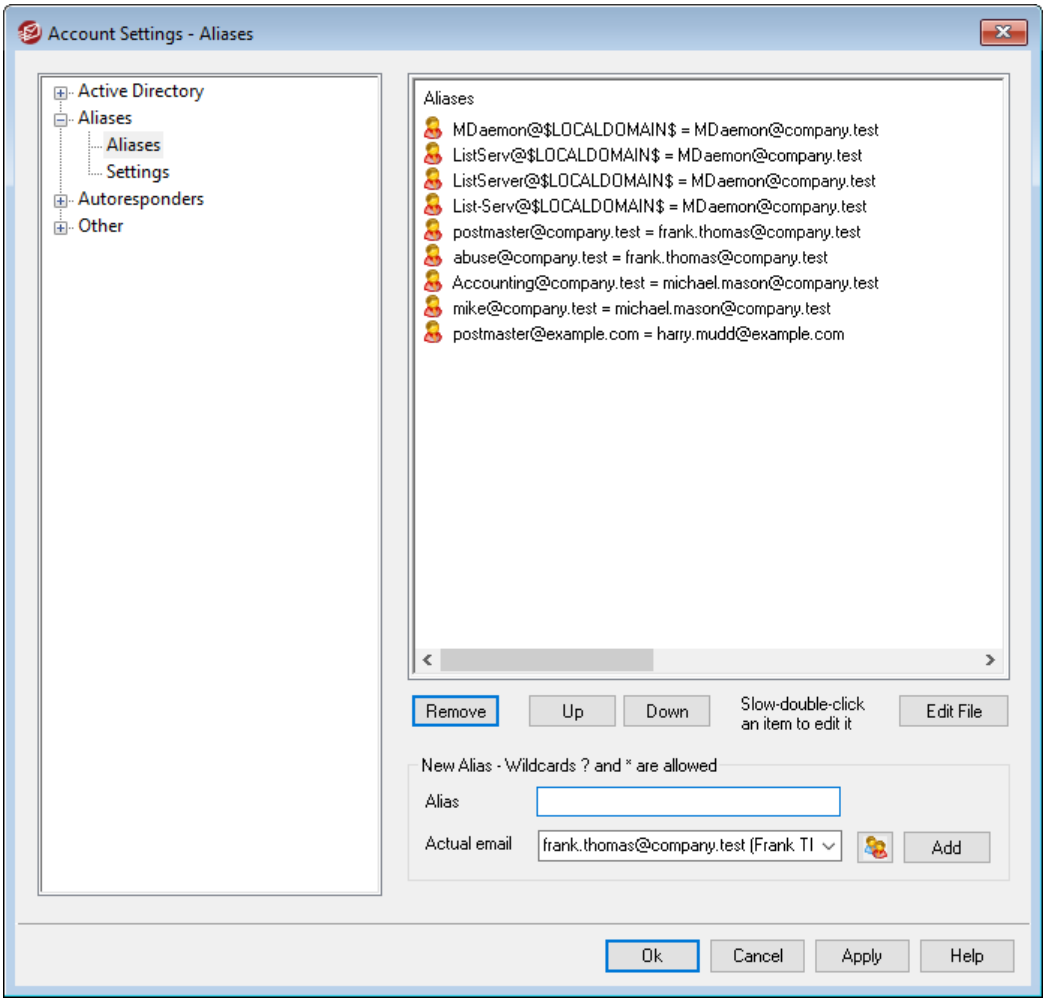
Configure
Click this button to open the `LDAP.dat` configuration file in a text editor. It is used for designating the LDAP attribute names that will correspond to each MDaemon account field.

See:

Account Database Options 833

5.3.2 Aliases

5.3.2.1 Aliases



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The Aliases features makes it possible for you to create alternate mailbox names for your accounts or mailing lists, which are useful when you want multiple mailbox names to resolve to a single user account or list. Without aliases you'd have to create separate user accounts for each address and then forward messages or use complicated filter rules to associate them with other accounts.

For example, if `user1@example.com` handled all billing inquiries to your domain, but you wanted to tell everyone to send them to `billing@example.com`, then you could create an Alias so that messages addressed to `billing@example.com` would actually go to `user1@example.com`. Or, if you were hosting multiple domains and wanted all messages addressed to the Postmaster (regardless of the domain) to go to `user1@example.com`, then you could use a wildcard to associate the alias, `Postmaster@*`, with his address.

Current Aliases

This window contains all current aliases that you have created.

Remove
Click this button to remove a selected entry from the *Current Aliases* list.

Up
Aliases are processed in the order in which they are listed. You can move an alias to a higher position in the list by selecting it and then clicking this button.

Down
Aliases are processed in the order in which they are listed. You can move an alias to a lower position in the list by selecting it and then clicking this button.

Edit File
Click this button if you wish to open the `Alias.dat` file in a text editor, to manually search or edit it. After making any desired changes, exit the text editor and then MDaemon will reload the file.

Alias
Enter the email address that you wish to be an alias of the "*Actual email*" listed below. Wildcards of "`?`" and "`*`" are acceptable, and you can use "`@$LOCALDOMAIN$`" in the alias as a wildcard that will match only your local domains. For example: "`user1@example.*`", "`*@$LOCALDOMAIN$`", and "`user1@$LOCALDOMAIN$`" are all valid for use in an alias.

Actual email
Select an account from the drop-down list, use the Account icon to browse for an account, or type a new email address or mailing list into this space. This is the actual email address that will receive the message when it is addressed to a corresponding alias.

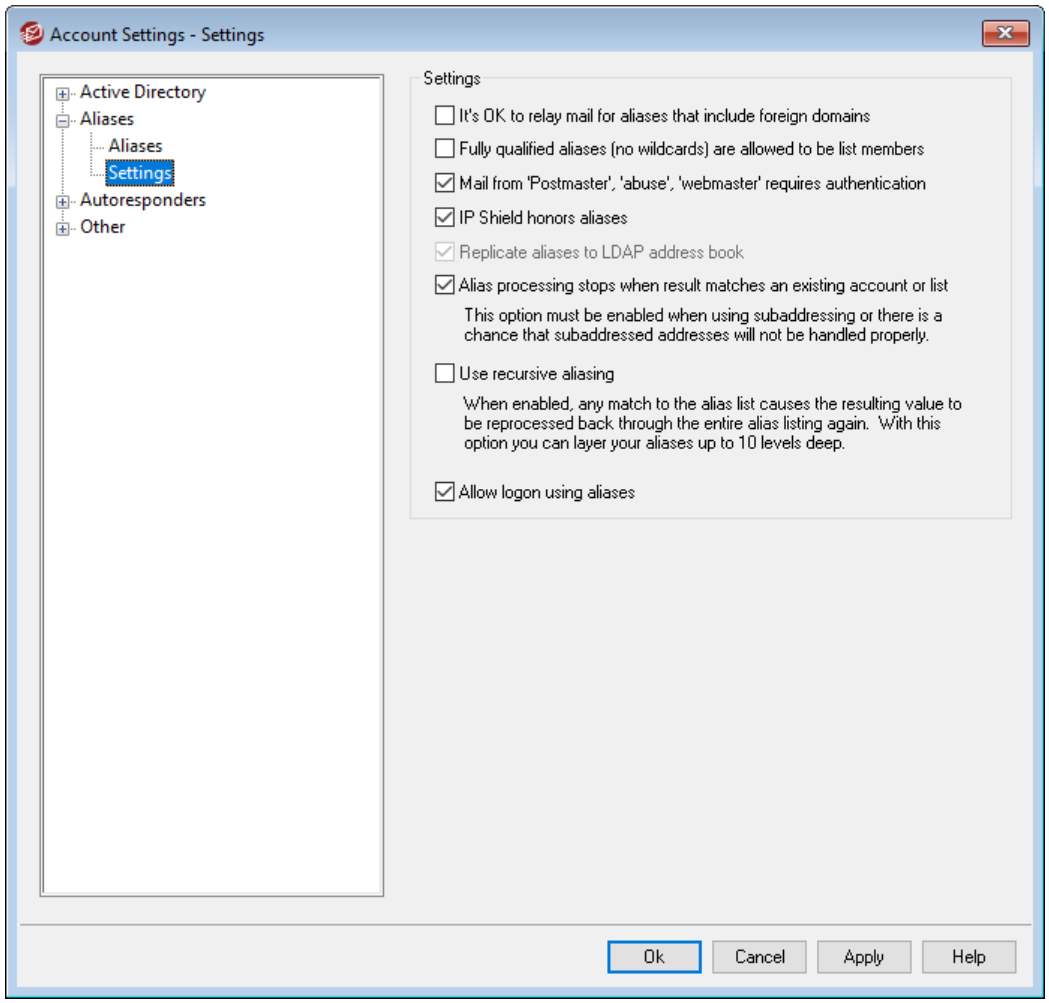
Add
Click the *Add* button to add the alias to the list. The *Alias* and *Actual email* values will be combined and placed in the *Current Aliases* window.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

Aliases » Settings 820
Account Editor » Aliases 725

5.3.2.2 Settings



Settings

It's OK to relay mail for aliases that include foreign domains
Check this box if you wish to allow MDaemon to relay mail for aliases that include non-local domains. This option overrides the *Do not allow message relaying* option in Relay Control 498 for those aliases.

Fully qualified aliases (no wildcards) are allowed to be list members
Click this checkbox if you want to allow aliases to be members of MDaemon mailing lists. Only actual accounts can be list members if this control is not enabled. **Note:**

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

aliases containing wildcards are not permitted to be list members even if this option is enabled.

Mail from 'Postmaster,' 'abuse,' 'webmaster' requires authentication
When this option is enabled, MDaemon will require messages claiming to be from any of your "postmaster@...", "abuse@..." or "webmaster@..." aliases or accounts to be authenticated before MDaemon will accept them. Spammers and hackers know that these addresses might exist, and may therefore attempt to use one of them to send mail through your system. This option will prevent them and other unauthorized users from being able to do so. For your convenience this option is also available on the SMTP Authentication 509 screen, located at: Security » Security Settings. Changing the setting here will change it there as well.

IP Shield honors aliases
By default the IP Shield 507 will honor aliases when checking incoming messages for valid domain/IP pairs. The IP Shield will translate an alias to the true account to which it points and thus honor it if it passes the shield. If you clear this checkbox then the IP Shield will treat each alias as if it is an address independent of the account that it represents. Thus, if an alias' IP address violates an IP Shield then the message will be refused. This option is mirrored on the IP Shield screen — changing the setting here will be change it there as well.

Replicate aliases to LDAP address book
Click this check box if you want aliases to be replicated to the LDAP address book. Alias replication is necessary for the LDAP remote verification feature to work reliably, but if you are not using that feature then replicating aliases to the LDAP address book is unnecessary. If you are not using remote verification then you can safely disable this feature to save processing time. For more information on remote LDAP verification, see: LDAP 815.

Aliases processing stops when result matches an existing account or list
When this option is enabled, alias processing will stop when the recipient of the incoming message matches an existing account or mailing list. This typically applies to aliases that include a wildcard. For example, if you have an alias set to, "`*@example.com=user1@example.com`," then this option will cause that alias to be applied only to addresses that do not actually exist on your server. So, if you also have the account, "`user2@example.com`," then messages addressed to user2 would still be delivered to him because the alias wouldn't be applied to those messages. But messages addressed to some non-existent account or list would be sent to "`user1@example.com`" because the wildcard alias would be applied to those messages. This option is enabled by default.

This option must be enabled when you are using Subaddressing 746, to avoid potential problems with handling those messages.

Use recursive aliasing
Click this check box if you want to process aliases recursively. Any alias match causes the resulting value to be reprocessed back through the entire alias list—it is

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

possible to nest aliases up to 10 levels deep. For example, you could set up something like this:

```
user2@example.com = user1@example.com
user1@example.com = user5@example.net
user5@example.net = user9@example.org
```

This is logically identical to the single alias:

```
user2@example.com = user9example.org
```

It also means that:

```
user1@example.com = user9example.org
```

Allow Logon using aliases
By default users are permitted to log in to their accounts using one of their account aliases 818 instead of their actual mailbox name. Clear this checkbox if you do not wish to allow this.

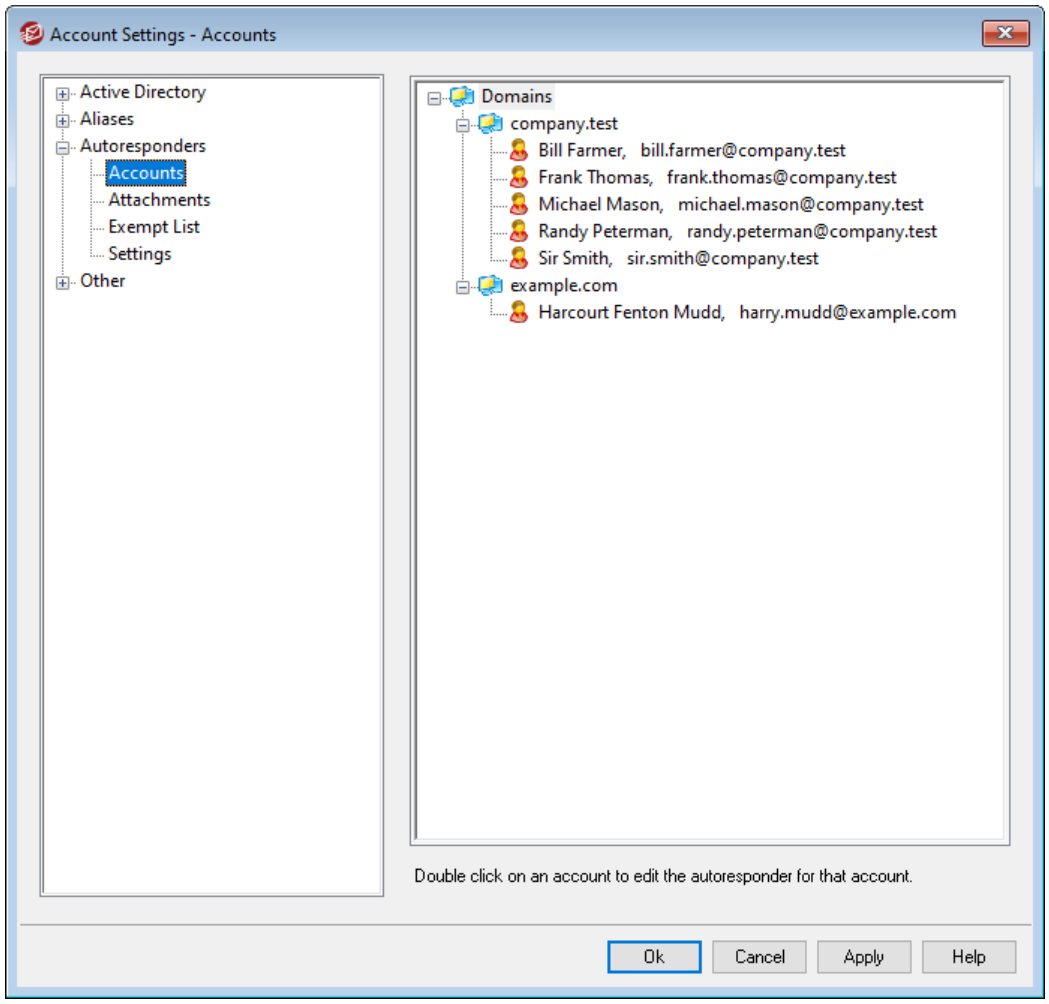
See:

Aliases 818

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.3 Autoresponders

5.3.3.1 Accounts



Autoresponders are useful tools for causing incoming email messages to trigger certain events automatically, such as running a program, adding the sender to a mailing list, responding with an automatically generated message, and more. The most common use of autoresponders is to reply to incoming messages automatically with a user-defined message stating that the recipient is on vacation, is unavailable, will reply as soon as possible, or the like. MDaemon users with Web Access 703 to Webmail 308 or Remote Administration 341 can use the options provided to compose auto response messages for themselves and schedule the dates they will be in use. Finally, automated response messages are based on the contents of the `OOF.mrk` file, found in each user's root `\data\` folder. This file supports a large number of macros, which can be used to cause much of the message's content to be generated dynamically, making autoresponders quite versatile.

Auto response events are always honored when the triggering message is from a remote source. However, for

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

messages originating from a user's same domain, autoresponders will only be triggered if you enable the *Autoresponders are triggered by intra-domain mail* option, located on the Autoresponders » Settings 827 screen. You can also use an option on that screen to limit auto response messages to one response per sender per day.

Account List

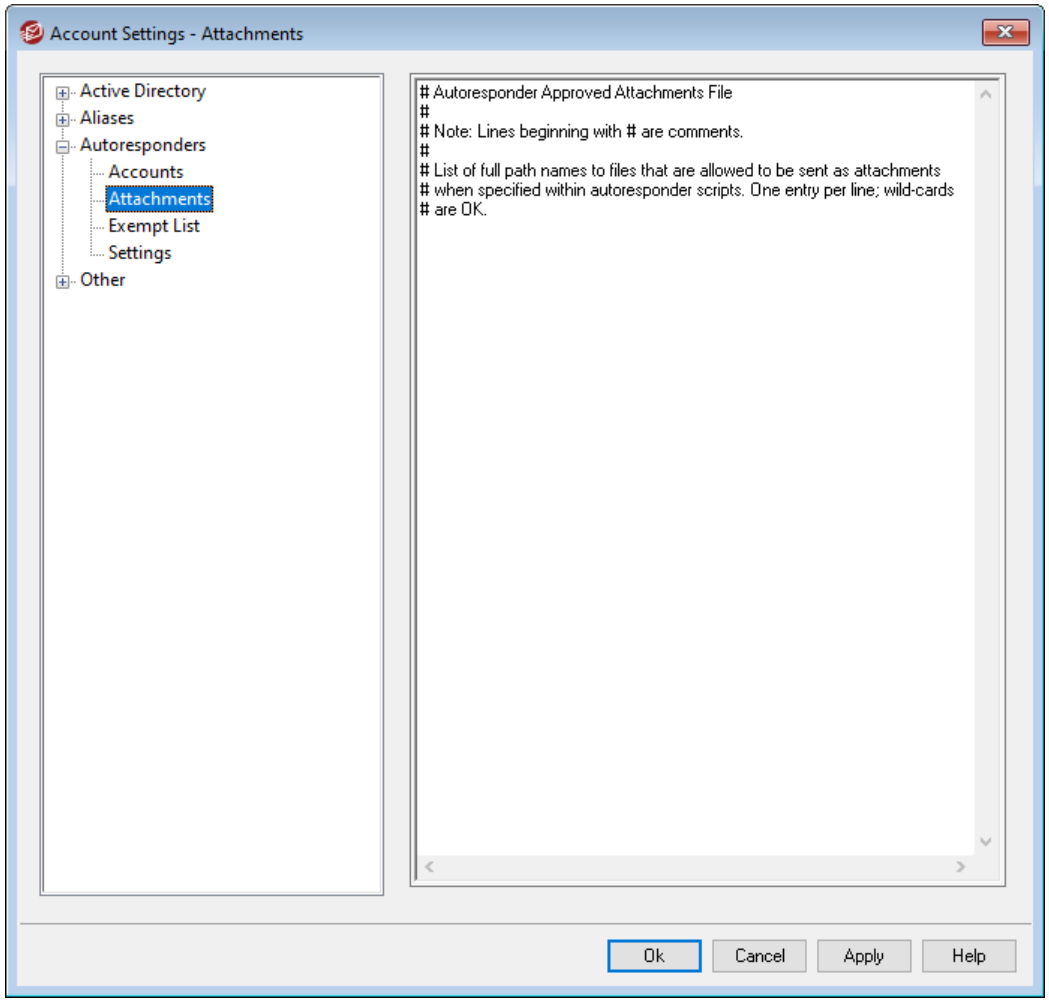
This area lists all available local mailboxes that can host an autoresponder. Double-click an account in this list to open its corresponding Autoresponder 708 screen, which is used to configure an autoresponder for that account.

See:

Autoresponders » Exempt List 826
Autoresponders » Settings 827
Creating Auto Response Messages 828
Account Editor » Autoresponders 708

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.3.2 Attachments



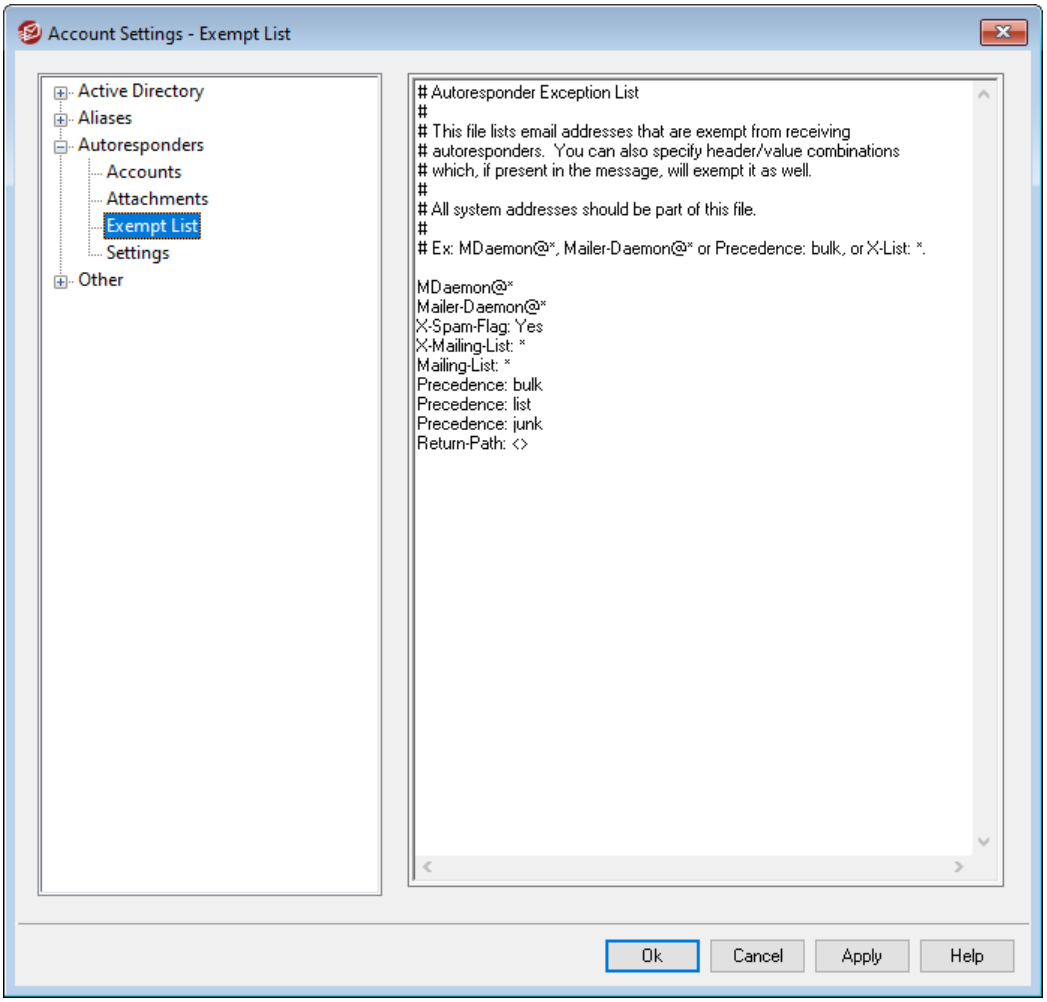
Provide the full file paths here to any files that you wish to allow to be used as attachments in autoresponder scripts[828]. In the autoresponse script, use the **%SetAttachment%** replacement macro to attach the file.

See:

Autoresponders » Accounts[823]
Autoresponders » Exempt List[826]
Autoresponders » Settings[827]
Creating Auto Response Scripts[828]
Account Editor » Autoresponders[708]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.3.3 Exempt List



Use Autoresponder » Exempt List to configure global exceptions to autoresponders. Messages from entries in this list will not receive any autoresponders. Both email addresses and header/value pairs can be included in the list. Enter one address or header/value pair per line. Wildcards are permitted.

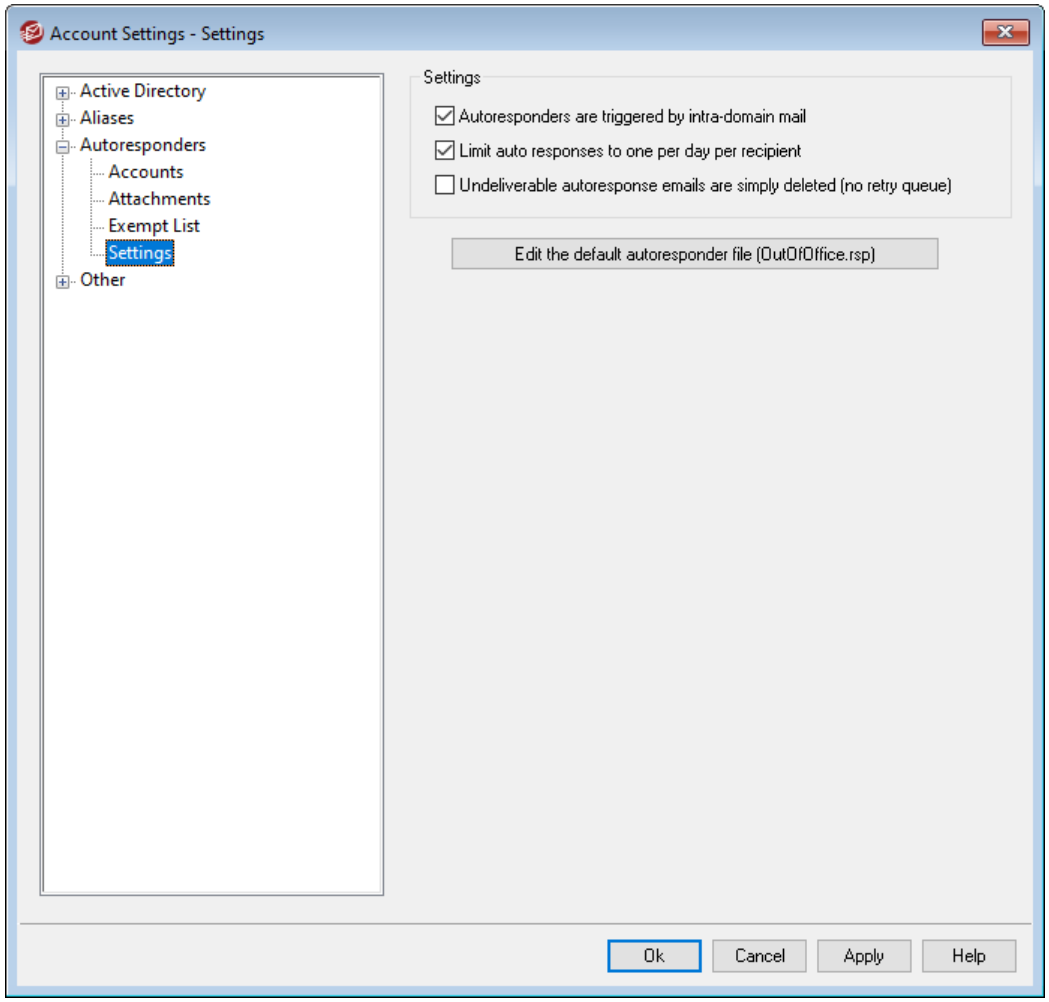
All system addresses (i.e. mdaemon@*, mailer-daemon@*, and so on) should be listed to help prevent mail loops and other problems.

See:

Autoresponders » Accounts 823
Autoresponders » Settings 827
Creating Auto Response Scripts 828
Account Editor » Autoresponders 708

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.3.4 Settings



Settings

Autoresponders are triggered by intra-domain mail
By default, both local and remote mail will trigger autoresponders. Clear this box if you do not wish to trigger autoresponders when the incoming message is from the same domain as the user.

Limit auto responses to one per day per recipient
By default, autoresponders will only generate one response message per day for any given address. This prevents people from receiving the same redundant auto response message from you over and over again on the same day, every time they send you an email. Clear this box if you wish to send auto response messages each time someone sends you a message, even if they have already received one that day.

This option also helps to prevent message loops, which can occur when your auto response message is returned to an

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

address that also has an autoresponder active. Instead of allowing both addresses to send auto response messages constantly back and forth to each other, this option would allow only one message to be sent to that address per day.

Undeliverable autoresponse emails are simply deleted (no retry queue)
Enable this option if you wish to delete undeliverable autoresponse messages when they expire from the remote queue, rather than move them into the retry queue 856 system.

Edit the default autoresponder file (OutOfOffice.rsp)
This is the default autoresponder message file. The contents of this file will be copied into an account's oof.mrk file 708 if its file is missing or empty.

See:

Autoresponders » Accounts 823
Autoresponders » Exempt List 826
Creating Auto Response Scripts 828
Account Editor » Autoresponders 708

5.3.3.5 Creating Auto Response Messages

OOF.mrk files are plain ASCII text files contained in each user's root `\data\` folder, which define the messages that are returned as the result of an autoresponder. When an auto response message is triggered by an autoresponder, the file is processed and scanned for macros, which will then be replaced by actual data from the incoming message that triggered the response. Lines beginning with the "#" character are ignored and are used for comments. There are two sample messages 831 listed below.

Auto Response Macros

`$HEADERS$`	This macro will be replaced by all of the incoming message's headers. Text immediately preceding this macro will be duplicated at the start of each expanded line.
`$HEADER:XX$`	This macro will cause the value of the header specified in place of "`xx`" to be expanded in the message. For example: If the incoming message has "`TO: joe@example.com`" then the `$HEADER:TO$` macro will expand to "`joe@example.com`". If the original message has "`SUBJECT: This is the subject`" then the `$HEADER:SUBJECT$` macro would be replaced with the text "`This is the subject`".

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$BODY$	This macro will be replaced by the entire message body. In an attempt to preserve character sets for different languages, MDaemon will read the message body as binary data rather than pure text, thus allowing a byte-for-byte copy of the message body.
$BODY-AS-TEXT$	Like the $BODY$ macro, this macro will be replaced by the entire message body, but as text rather than binary. Text immediately preceding this macro will be duplicated at the start of each expanded line. So, using ">>$BODY-AS-TEXT$" in a script would place each line of the original message into the generated message, but each line would begin with ">>". Text can also be added to the right of this macro.
$SENDER$	This macro resolves to the full address contained in the incoming message's "From:" header.
$SENDERMAILBOX$	This macro resolves to the mailbox of the sender. The mailbox is the portion of the email address to the left of the "@" symbol.
$SENDERDOMAIN$	This macro resolves to the domain of the sender. This is the portion of the email address to the right of the "@" symbol.
$RECIPIENT$	This macro resolves to the full address of the message recipient.
$RECIPIENTMAILBOX$	This macro resolves to the mailbox of the message recipient. The mailbox is the portion of the email address to the left of the "@" symbol.
$RECIPIENTDOMAIN$	This macro resolves to the domain of the message recipient. The domain is the portion of the email address to the right of the "@" symbol.
$SUBJECT$	This macro resolves to the value of the "Subject:" header.
$MESSAGEID$	This macro resolves to the value of the "Message-ID" header.
$CONTENTTYPE$	This macro resolves to the value of the "Content-Type" header.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

$PARTBOUNDARY$	This macro resolves to the value of the MIME "Part-Boundary" value found in the "Content-Type" header for multipart messages.
$DATESTAMP$	This macro expands to an RFC-2822 style date-time stamp line.
$ACTUALTO$	Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro expands to that value.
$ACTUALFROM$	Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro expands to that value.
$REPLYTO$	This macro resolves to the value found in the "ReplyTo" header.
$PRODUCTID$	This macro expands to the MDaemon version information string.
AR_START	Returns the auto-responder start date/time.
AR_END	Returns the auto-responder end date/time.

Header Replacement Macros

The macros listed below control the auto response message's headers.

%SetSender%
ex: %SetSender%=mailbox@example.com
Just for the purpose of the auto-response message, this macro resets the sender of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's TO header. For example, if the sender of the original message were "user2@example.org" and recipient's autoresponder used the %SetSender% macro to change it to "user1@example.com" then the auto-response message's TO header would be set to "user1@example.com."

%SetRecipient%
ex: %SetRecipient%=mailbox@example.com
Just for the purpose of the auto-response message, this macro resets the recipient of the original message before constructing the auto-response message headers. Thus, this macro controls the auto-response message's FROM header. For example, if the recipient of the original message were "michael@example.com" and Michael's account had an autoresponder using the %SetRecipient% macro to change it to

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

"michael.mason@example.com," then the auto-response message's FROM header would be set to "michael.mason@example.com."

%SetReplyTo%
ex: %SetReplyTo%=mailbox@example.com
Controls the value of the auto-response message's ReplyTo header.

%SetSubject%
ex: %SetSubject%=Subject Text
Replaces the value of the original message's subject.

%SetMessageId%
ex: %SetMessageId%=ID String
Changes the ID string of the message.

%SetPartBoundary%
ex: %SetPartBoundary%=Boundary String
Changes the part boundary.

%SetContentType%
ex: %SetContentType%=MIME type
Changes the content-type of the message to the declared value.

%SetAttachment%
ex: %SetAttachment%=filespec
Forces MDaemon to attach the specified file to the newly generated auto-response message. Only files specified on the Attachments 825 screen can be attached to autoresponders.

5.3.3.5.1 Auto Response Message Samples

A simple oof.mrk auto response message using several auto response macros:

```
Greetings $SENDER$

Your message regarding '$SUBJECT$' won't be read by me because I'm
on vacation. Hurray!!!
Yours truly,

$RECIPIENT$
```

You can also use some of the header replacement macros to expand this script and control the headers that will be generated when the auto response message is mailed back to $SENDER$:

```
Greetings $SENDER$

Your message regarding '$SUBJECT$' won't be read by me because I'm
on vacation. Hurray!!!
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
Yours truly,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\photos\me_on_vaction.jpg
```

Using that script the auto response message will have "RE: " added to the beginning of the subject and have the specified file attached.

The "%SetSubject%=RE: $SUBJECT$" line is handled like this:

1. The $SUBJECT$ portion is expanded and replaced by the original message's subject text. This makes the string equivalent to:

   ```
   %SetSubject%=RE: Original Subject Text
   ```

2. MDaemon replaces the original subject, which it has stored in its internal buffers, with this newly calculated one. From that point forward, any use of "$SUBJECT$" in the script will return the new result.

Note the placement of the new macros - they are listed at the bottom of the response script. This is needed to avoid side effects. For example, if the %SetSubject% macro were placed before the $SUBJECT$ macro, which appears in the second line of the response script, the subject text would have already been changed by the time the $SUBJECT$ macro was expanded. Therefore, instead of replacing $SUBJECT$ with the content of the original message's "Subject:" header, it would be replaced with whatever you have set the value of %SetSubject% to be.

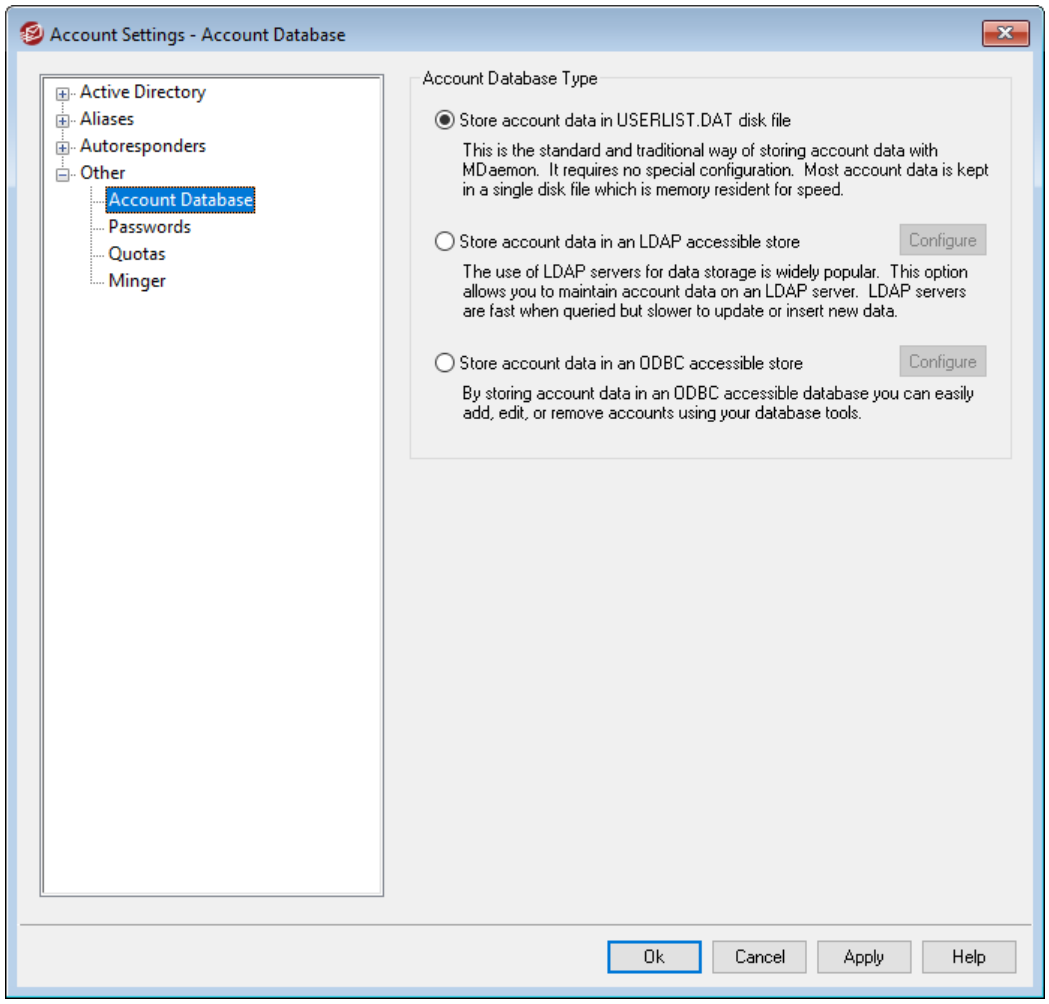
See:

Autoresponders » Accounts 823
Autoresponders » Exempt List 826
Autoresponders » Settings 827
Account Editor » Autoresponders 708

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.4 Other

5.3.4.1 Account Database



The Account Database dialog (located under Accounts » Account Settings) is used to designate the method that you want MDaemon to use to maintain your user accounts: ODBC, LDAP, or the local USERLIST.DAT system.

Account Database Type

Store account data in USERLIST.DAT disk file
Choose this option if you want MDaemon to use its internal USERLIST.DAT file as the account database. This is MDaemon's default setting and causes all of the MDaemon user account information to be stored locally. Most information is stored in a single file, which is memory resident to increase efficiency and speed.

Store account data in LDAP accessible store
Choose this option if you want MDaemon to use your LDAP server as the MDaemon user database rather than ODBC or its local USERLIST.DAT system. You might want to use this method of maintaining your user account data if you have multiple

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally. LDAP servers typically respond quickly and efficiently to queries but are slower to update or insert new data.

Configure
When the LDAP account data option is selected, click this button to open the LDAP screen[815] for configuring your LDAP server settings.

Store account data in an ODBC accessible store
Choose this option if you want to use an ODBC compliant database as your MDaemon account database.

Configure
When the ODBC account data option is selected, click this button to open the ODBC Selector Wizard[834] for selecting and configuring your ODBC compliant database.

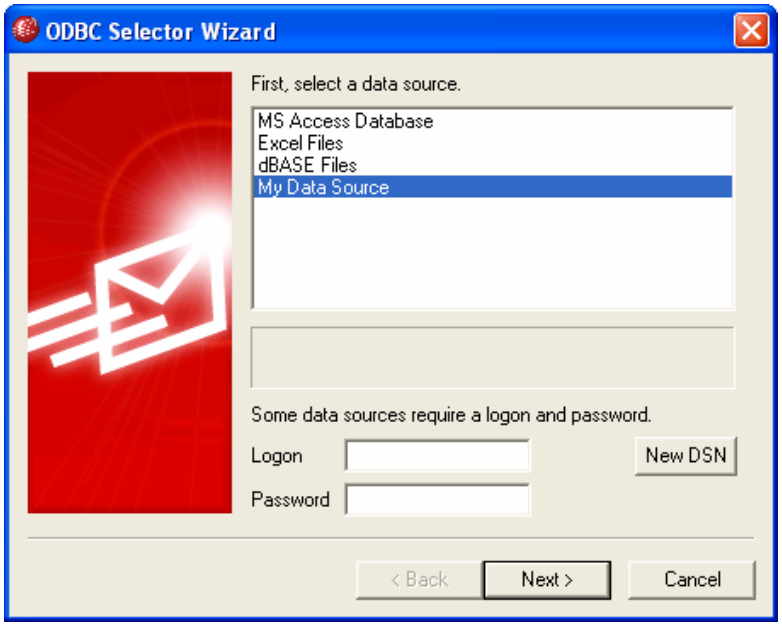
5.3.4.1.1 ODBC Selector Wizard

Use the ODBC Selector Wizard to select or configure an ODBC compliant data source to use as your MDaemon account database.

Migrating Your Account Database to an ODBC Accessible Store

1. On the Account Database dialog (Accounts » Account Settings » Account Database), click **Store account data in an ODBC accessible store**, and then click **Configure** to open the ODBC Selector Wizard.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

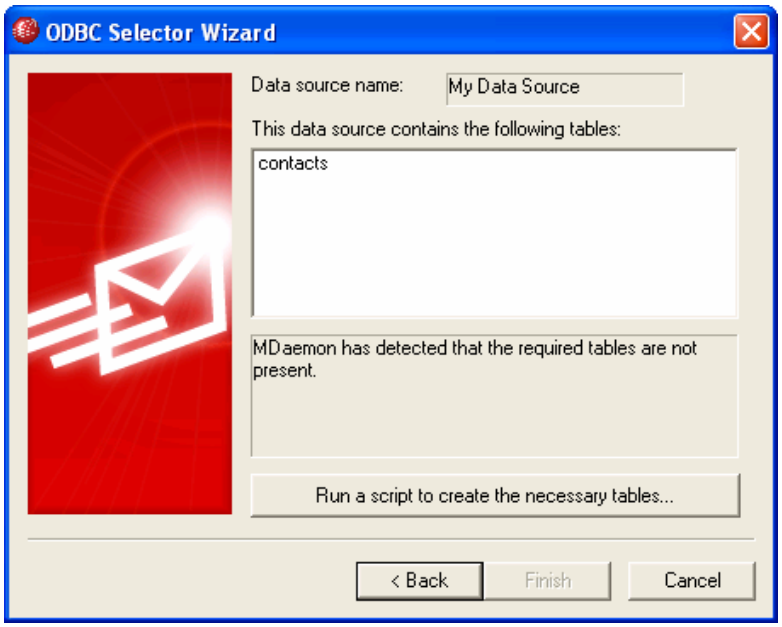


2. Select the **data source** that you wish to use for your account database. If there is not a compatible data source listed, click **New DSN** and then follow the instructions listed under, **Creating a New ODBC Data Source** 836.

3. If required, enter the data source's **Logon** and **Password**.

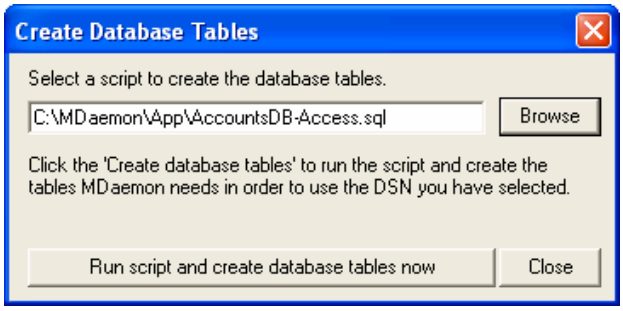
4. Click **Next**.

5. If the data source already contains the tables that are required by MDaemon, go to **Step 8**. Otherwise, click **Run a script to create the necessary tables...**



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6. Type the file path (or **Browse**) to the desired script file that you wish to use to create the tables for your database application. The \MDaemon\app\ folder contains scripts for several of the most popular database applications.



7. Click **Run script and create database tables now**, Click **OK**, and click **Close**.
8. Click **Finish**, and click **OK** to close the Account Database dialog.
9. A database migration tool will migrate all of your user accounts to the ODBC data source and then close MDaemon. Click **OK**, and then restart MDaemon and begin using the new ODBC account database.

See:

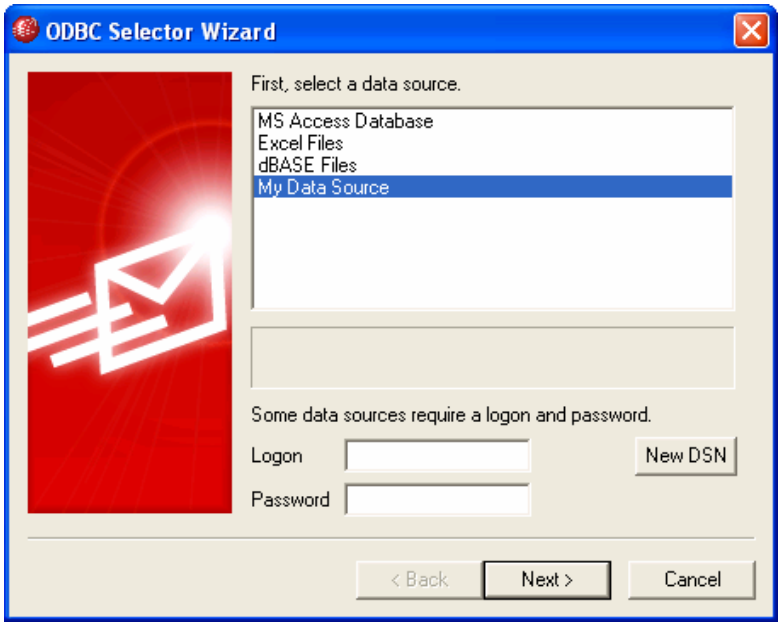
Account Database 833
Creating a New ODBC Data Source 836

5.3.4.1.1.1 Creating a New Data Source

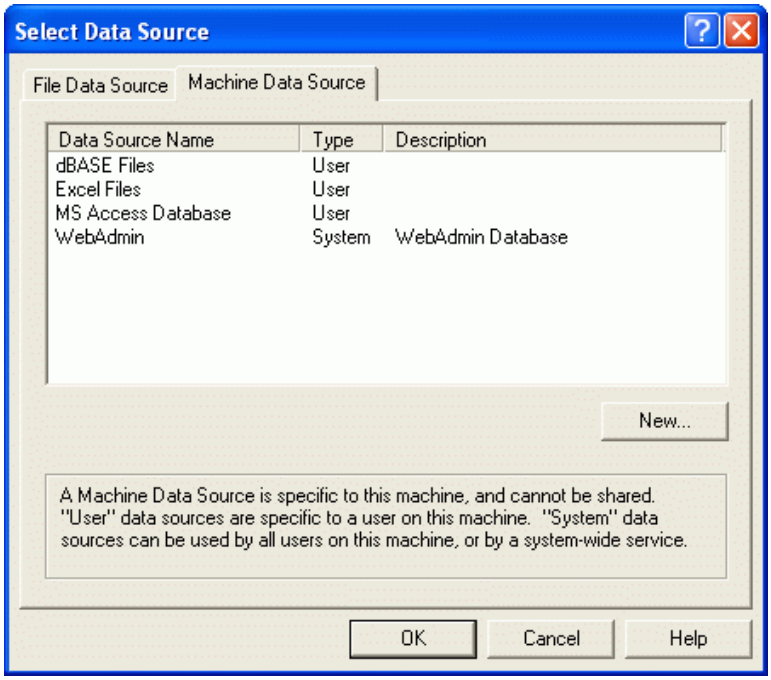
To create a new ODBC data source:

1. On the Account Database dialog (Accounts » Account Settings » Account Database), click **Store account data in an ODBC accessible store**, and then click **Configure** to open the ODBC Selector Wizard.
2. Click **New DSN** to open the Select Data Source dialog.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

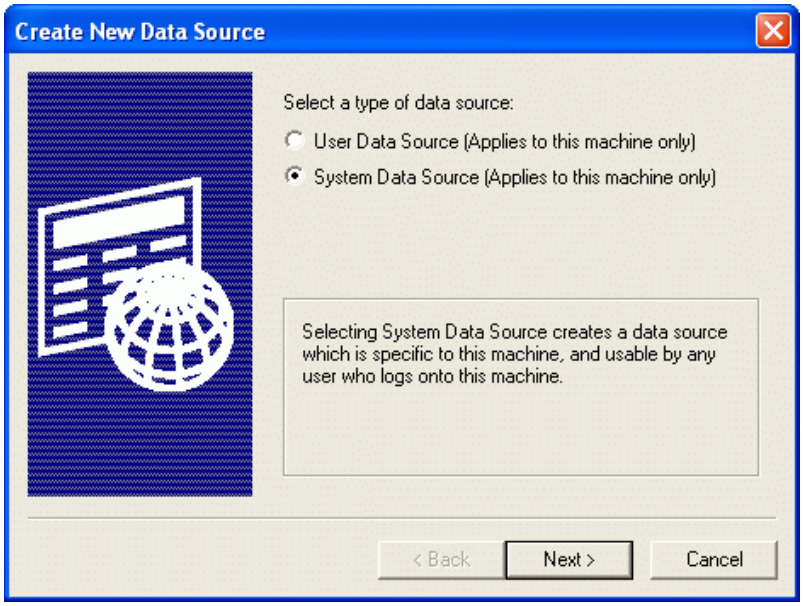


3. Switch to the **Machine Data Source** tab, and click **New...** to open the Create New Data Source dialog.

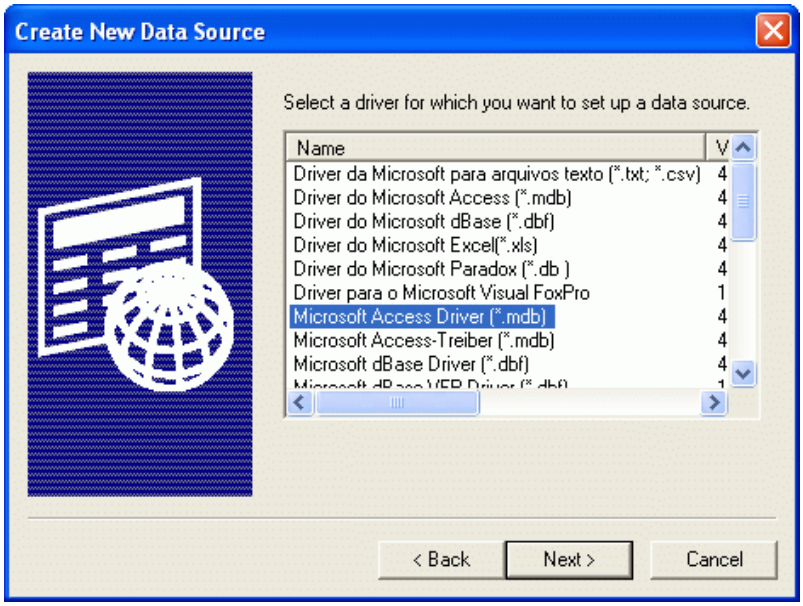


4. Select **System Data Source**, and click **Next**.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

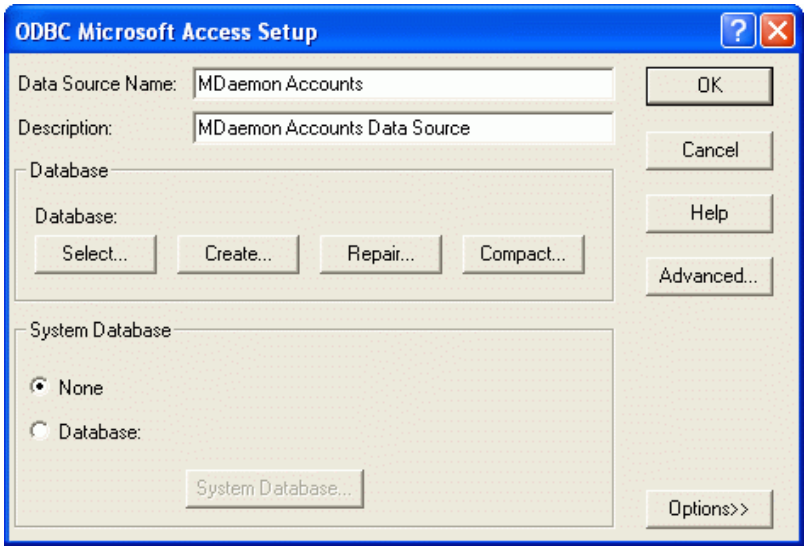


5. Select the **database driver** for which you wish to set up the data source, and click **Next**.



6. Click **Finish** to display the driver-specific setup dialog. The appearance of this dialog will vary based on which driver you have selected (Microsoft Access Setup dialog shown below).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies



7. Designate a **Data Source Name** for your new data source and provide any other information required by the driver-specific dialog (such as creating or specifying a database, choosing a directory or server, and so on).

8. Click **OK** to close the driver-specific dialog.

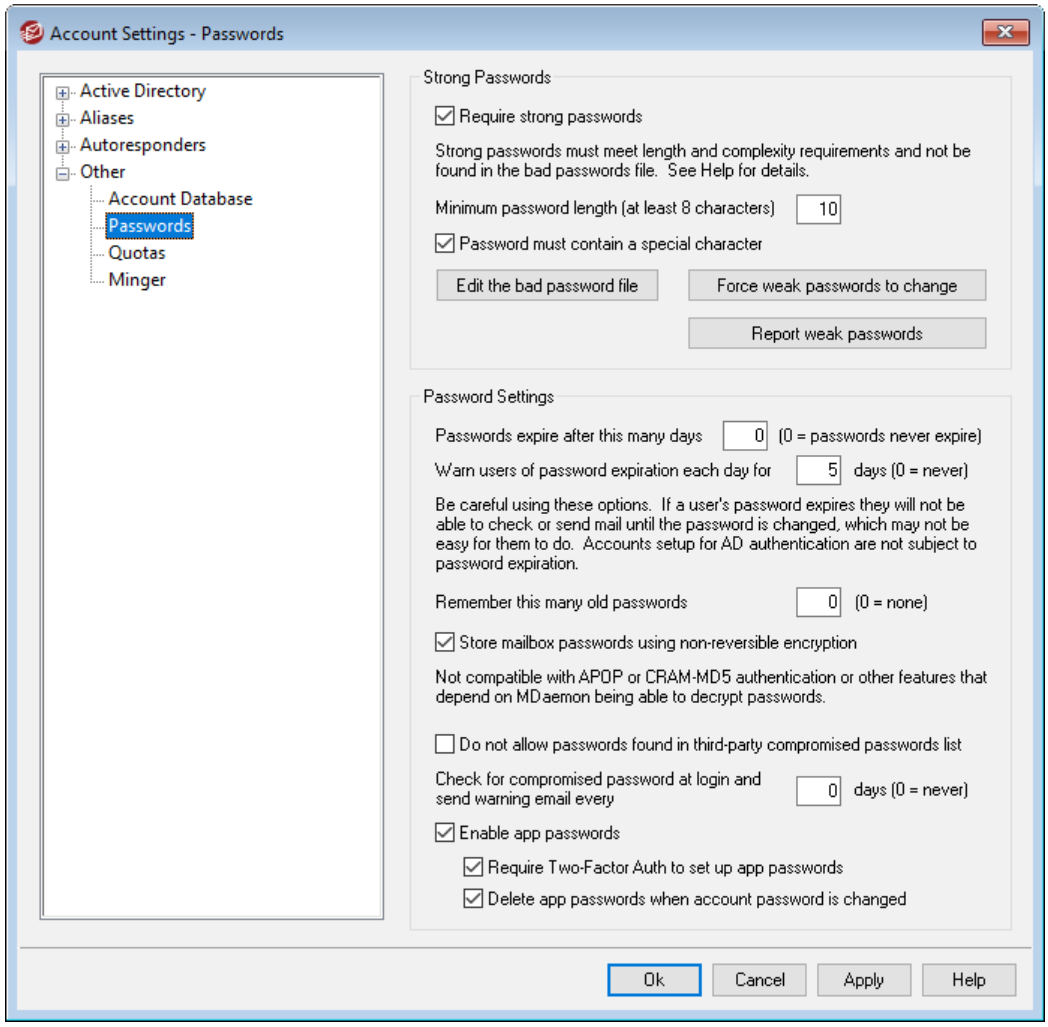
9. Click **OK** to close the Select Data Source dialog.

See:

Account Database 833
ODBC Selector Wizard - Account Database 834

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.3.4.2 Passwords



Strong Passwords

Require strong passwords
By default, MDaemon requires strong passwords when creating new accounts or changing existing passwords. Clear this check box if you wish to disable the strong password requirement.

Strong passwords must:

- Meet the minimum length requirement.
- Contain upper and lower case letters.
- Contain letters and numbers.
- Contain a special character (if the special character option is set below)
- Not contain the user's full name or mailbox name.
- Not be found in the bad passwords file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Minimum password length (at least 8 characters)
Use this option to set the minimum password length required for strong passwords. This must be set to at least 8 characters, but a higher value is recommended. The default value for new MDaemon installations is 10 characters. Changing this setting does not automatically trigger a required password change for accounts with passwords shorter than the new minimum, but when those users next change their password this setting will be enforced.

Regardless of the minimum setting, passwords can be longer than 72 characters when the "*Store mailbox passwords using non-reversible encryption*" option below is set. If that option is disabled, passwords can be no longer than 15 characters.

Passwords must contain a special character
By default for new MDaemon installations, strong passwords also require at least one of the following special characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~. Disable this option if you do not wish to require a special character in strong passwords.

Edit the bad password file
Click this button to edit the bad password file. Entries listed in this file are case insensitive and cannot be used as passwords. If you wish to create more complex or versatile entries, you can use Regular Expressions 638 to do so. Entries beginning with "!" are treated as Regular Expressions.

Force weak passwords to change
Click this button if you wish to force all accounts with a weak password to change their passwords. This will lock out every account with a weak password until the password is changed. The password can be changed by an administrator via the MDaemon interface, or a locked out user can change the password via Webmail or the remote administration interface. When the user attempts to log in using the old password, he or she will be required to create a new one before proceeding. **Note:** This option is not available when using the "*Store mailbox passwords using non-reversible encryption*" option below.

Report weak passwords
Click this button to generate a report of all MDaemon accounts with a weak password. The report will be emailed to whatever email address you specify after clicking OK. **Note:** This option is not available when using the "*Store mailbox passwords using non-reversible encryption*" option below.

Password Settings

Passwords expire after this many days (0=passwords never expire)
Use this option if you wish to set a maximum number of days that an account can be accessed before being required to change its password. The default value in this option is "0", which means that passwords never expire. But if you set it to, for example, 30 days then the user will have 30 days to change his or her password, **starting from the last time the account's password was changed**. Therefore when you initially set an expiration value, any account with a password that hasn't been changed within the specified number of days will immediately have an expired

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

password. When a user's password expires he or she will not be able to access POP, IMAP, SMTP, Webmail, or Remote Administration. The user can, however, still connect to Webmail or Remote Administration where he or she will then be required to change the password before proceeding. Email clients such as Outlook, Thunderbird, and the like cannot be used to change the password. Further, many clients will not even show a helpful error message to users, therefore they may need administrator assistance to figure out why their login is failing.

In order for users to be able to change their passwords via Webmail or Remote Administration they must first be granted the "...edit password" web access permission on the Web Services 782 screen. Further, because changing the password may not be easy or possible for some users, you should exercise caution before using this option.

Warn users of password expiration each day for [xx] days (0 = never)
Accounts with a password that is about to expire can receive a daily reminder email that the password needs to be changed. Use this option to designate the number of days before the password expires that you want MDaemon to start sending these daily emails.

Remember this many old passwords (0=none)
Use this option to specify the number of old passwords that you want MDaemon to remember for each user. When users change their passwords they will not be allowed to reuse old passwords. This option is set to "0" (disabled) by default.

Store mailbox passwords using non-reversible encryption
Check this box if you want MDaemon to store passwords using non-reversible encryption. This protects the passwords from being decrypted by MDaemon, the administrator, or a possible attacker. To do this, MDaemon uses the bcrypt password hashing function, which allows for longer passwords (up to 72 characters), and for passwords to be preserved yet not revealed when exporting and importing accounts. Some features, however, are not compatible with this option, such as weak password detection and APOP & CRAM-MD5 86 authentication, because they depend on MDaemon being able to decrypt passwords. Non-reversible passwords is enabled by default.

Compromised Passwords

MDaemon can check a user's password against a compromised password list from a third-party service. It is able to do this without transmitting the password to the service, and if a user's password is present on the list it does not mean the account has been hacked. It means that someone somewhere has used the same characters as their password and it has appeared in a data breach. Published passwords may be used by hackers in dictionary attacks, but unique passwords that have never been used anywhere else are more secure. See Pwned Passwords for more information.

Do not allow passwords found in third-party compromised passwords list
Check this box if you do not wish to allow an account's password to be set to one that is found in the compromised password list.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Check for compromised password at login and send warning email up to every [xx] days (0 = never)
With this option you can automatically check each user's password against the compromised passwords list once every specified number of days, when each user logs in. If they are found to be using a compromised password, a warning email is sent to the account and the postmaster. The warning emails can be customized by editing message template files in the `\MDaemon\App` folder. Since instructions for how a user should change their password may depend on whether the account is using a password stored in MDaemon or using Active Directory 806 authentication, there are two template files: `CompromisedPasswordMD.dat` and `CompromisedPasswordAD.dat`. Macros can be used to personalize the message, change the subject, change the recipients, and so on.

App Passwords

App Passwords 734 is an option that can be used to make accounts more secure by creating very strong, randomly generated passwords to be used only in email clients and email apps, since those apps can't be secured by Two-Factor Authentication 703 (2FA). See: App Passwords 734.

Enable app passwords
All users can create App Passwords for their accounts by default, when signed in to Webmail using Two-Factor Authentication. If you wish to disable App Password support for a specific user, you can do so with the *...edit app passwords* 703 option on the user's Web Services page.

Require Two-Factor Auth to set up app passwords
By default, users must be signed in to Webmail using Two-Factor Authentication 703 (2FA) in order to create a new App Password. Disabling this requirement is not recommended. Global Administrators 741 are exempt from this requirement in MDRA, but it is still recommended that they always use 2FA when signing it to MDRA or Webmail.

Delete app passwords when account password is changed
By default, when an account's password is changed, all app passwords will be deleted, requiring the user to create new ones if he wishes to use them or is required to use them by the "*Require app passwords...*" setting (see note below).

There is an account option on the Account Editor's Settings 744 page that you can use to "*Require app password to log in to SMTP, IMAP, ActiveSync, etc.*"

Requiring App Passwords can help protect an account's password from dictionary and brute force attacks via SMTP, IMAP, etc. This is more secure because even if an attack of this sort were to guess an account's actual password, it wouldn't work and the attacker wouldn't know, because MDaemon would only accept a correct App Password.

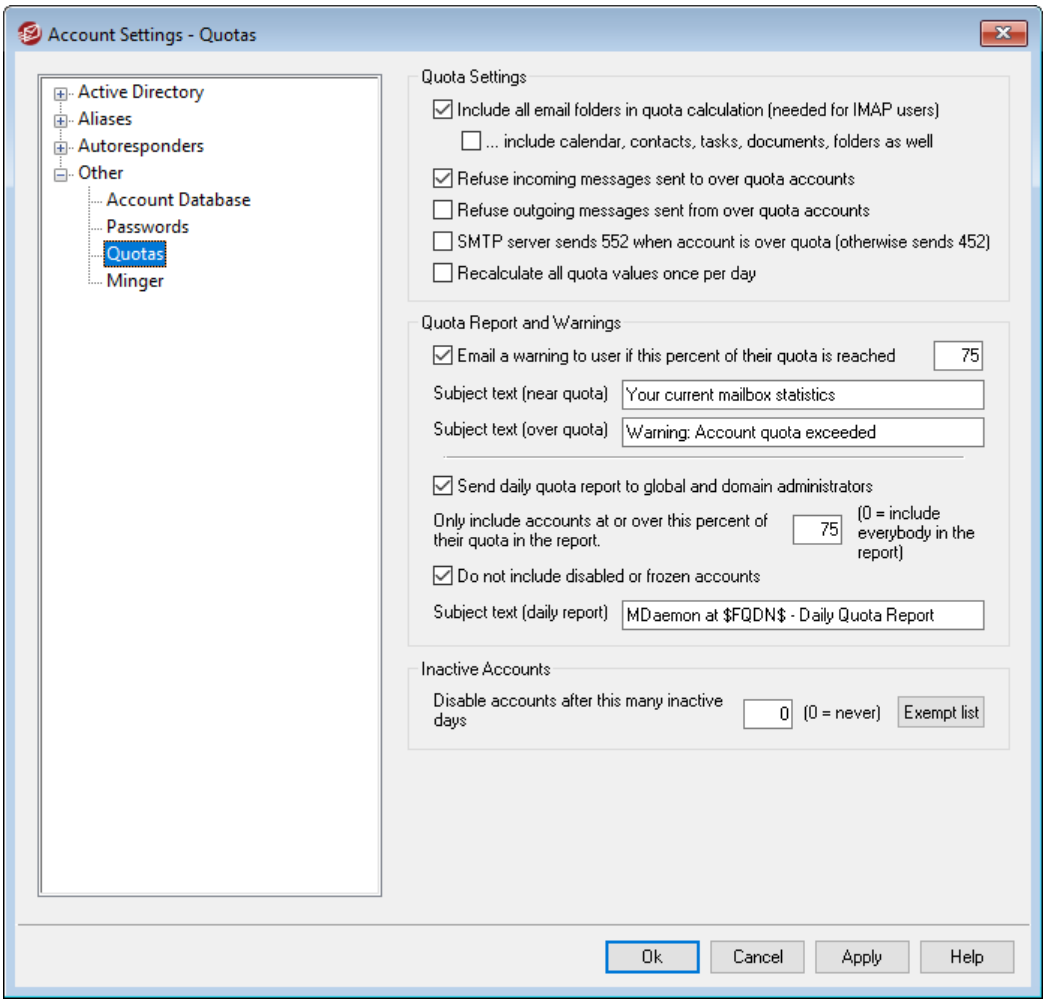
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Additionally, if your accounts in MDaemon are using Active Directory 806 authentication and Active Directory locks an account after a number of failed attempts, this option can help prevent accounts from being locked out, because MDaemon will only check the App Passwords, not try to authenticate to Active Directory.

See:

Account Editor » Account Details 697
Account Editor » Web Services 703
Account Editor » App Passwords 734
Regular Expressions 638

5.3.4.3 Quotas



Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Quotas Settings

Include all email folders in quota calculation (needed for IMAP users)
When this box is checked, all message files in all email folders under a user's account will apply toward any size or message number limitations placed on that account. Otherwise, only message files in the inbox will count toward those limitations. This is generally only needed for IMAP users.

...include Calendar, Contacts, Tasks, Documents, folders as well
Click this check box if you wish to include all calendar, contacts, tasks, and documents folders in the quota calculations.

Refuse incoming messages sent to over quota accounts
By default, when an account has a message quota restriction placed on it and the quota has been reached, MDaemon will no longer accept any incoming messages for the account until the account holder deletes some of his or her stored mail. Clear this checkbox if you do not wish to refuse incoming messages for over quota accounts.

Refuse outgoing messages sent from over quota accounts
Check this box if you wish to refuse outgoing messages sent from any account that has reached its quota. An over-quota account will no longer be able to send mail until some of its stored messages have been deleted. This option is disabled by default.

SMTP server sends 552 when account is over quota (otherwise sends 452)
By default, when an account is over quota 715 MDaemon sends the 452 error code (i.e "Requested action not taken: insufficient system storage") during the SMTP process. This code generally means that the server should try again later. Check this box if you wish to send the permanent failure 552 error code instead ("Requested mail action aborted: exceeded storage allocation").

Recalculate all quota values once per day
By default, cached quota values are only reset when the "*Send daily quota report...*" option below is enable and sent. Click this checkbox if you instead want the quota values to be recalculated as part of the daily maintenance routine.

Quota Report and Warnings

Email a warning to user if this percent of their quota is reached
If, during the daily maintenance and cleanup event 480, MDaemon determines that an account is exceeding this percentage value of either its *Maximum number of messages stored at once* or *Maximum disk space allowed* quota restriction designated on the Account Editor 715, a warning message will be sent to the account. Use the *Subject text (near quota)* option below to set the Subject for the message. The message will list the account's current number of stored messages, the size of its mailbox, and the percentage used and the percentage remaining. Further, if an existing warning is found in the account's mailbox it will be replaced with an updated message. Whenever a new warning message is placed in the user's Inbox, an entry is created in the system log to let you know it was done. No entry log is created when the message already exists and is just updated. If a log entry is

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

added over and over then that is an indication that the user is deleting the message from his Inbox. Disable this option if you do not wish to send the quota warning message to users.

The Near Quota Message Template (located at: MDaemon\app\NearQuota.dat) is used to create the near quota warning message. All macros related to user accounts (e.g. $EMAIL$, $MAILBOX$, $DOMAIN$, etc.) can be used in the template.

Subject text (near quota)
This is the Subject text of the warning messages sent to any users who exceed the quota percentage designated above. These messages are sent each day during the daily maintenance and cleanup event, which occurs at midnight by default.

Subject text (over quota)
Like the "near quota" warning message, another message will be sent when a user's account exceeds the quota. This is the Subject text of the "over quota" warning message.

Send daily quota report to global and domain administrators
Check this box and specify a value if you wish to send a daily quota report to all global and domain administrators. The report will contain quota statistics for all users at or over the designated percentage of their quota restriction. Use "0" as the value if you want the report to include quota statistics on everyone.

Do not include disabled or frozen accounts
By default, quota reports do not include disabled or frozen accounts. Uncheck this box if you wish to include them.

Subject text (daily report)
Use this option if you wish to customize the subject text of the daily quota report that MDaemon sends to the administrators. See `QuotaReport.dat` in the `MDaemon\APP` folder if you wish to customize the report itself.

Inactive Accounts

Disable accounts after this many inactive days XX (0=never)
Use this option if you wish to disable accounts automatically that have been inactive for more than a specified number of days. Once the maximum number of inactive days has been reached, the account is disabled and an email is sent to the postmaster. Replying to the email will re-enable the account. Processing is done as part of the midnight cleanup event each night. The default is 0 (disabled).

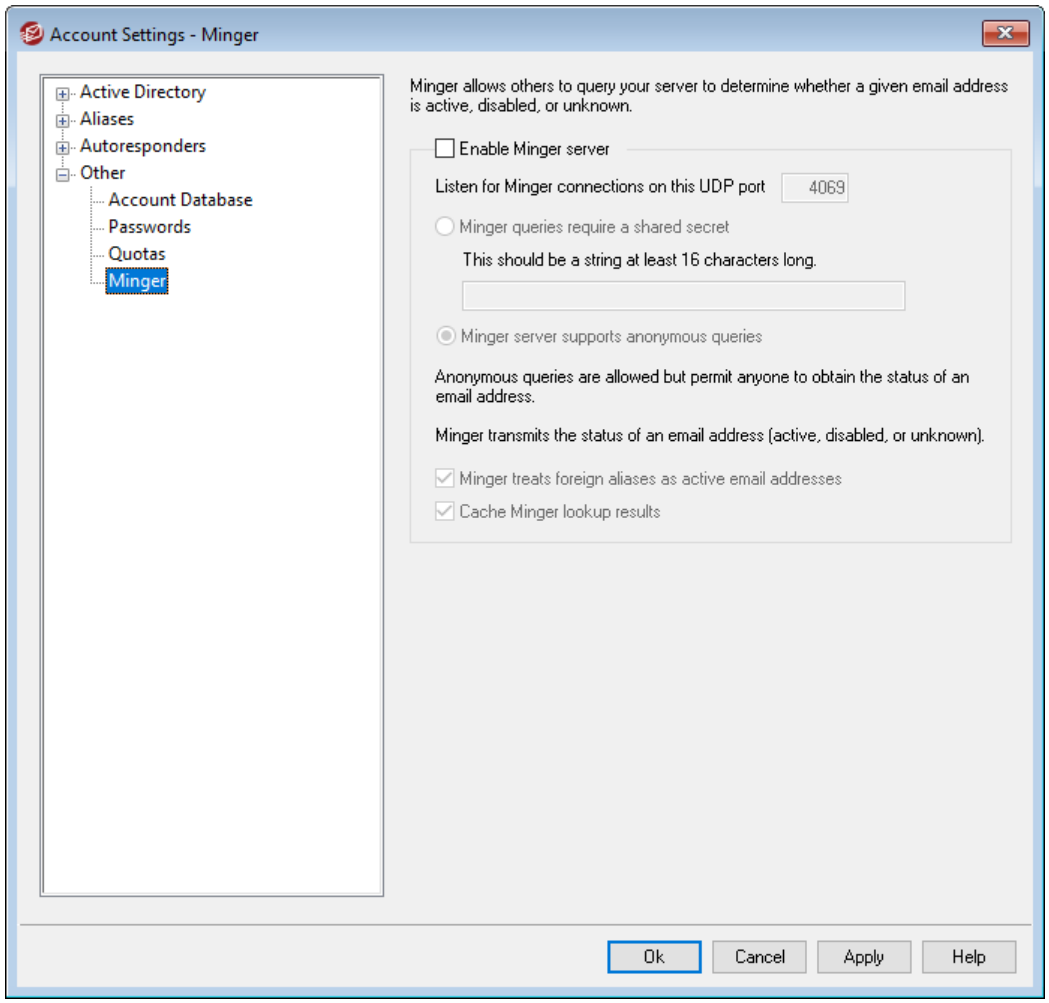
Exempt list
Accounts added to this list are exempt from the inactive account disabling feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

See:

[Account Editor » Quotas](#) 715
[Template Manager » Quotas](#) 796

5.3.4.4 Minger



Located under Accounts » Account Settings, Minger is an email address verification protocol created by MDaemon Technologies. Originally based loosely on the Finger protocol, Minger is primarily intended to provide a simple and efficient mechanism for allowing others to query your server in order to verify whether or not an email address is valid. For efficiency Minger uses UDP rather than TCP, and for security it can require authentication—though it supports anonymous queries as well. The Minger dialog is used to enable/disable MDaemon's Minger server, designate the port that it will use (the default is 4069), and choose whether to require authentication via a shared secret system or to allow anonymous queries.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon also has a Minger client, which is built in to the Domain Gateways system (see Verification 248). Each domain for which MDaemon is acting as a gateway or backup server can be configured to use Minger so that MDaemon will connect to the remote server and verify whether or not the recipients of incoming messages for that domain are valid. This prevents you from having to assume that all recipients are valid addresses.

You can find the latest draft of the Minger protocol at:

http://tools.ietf.org/html/draft-hathcock-minger-06

Minger Server

Enable Minger server
Click this checkbox to enable MDaemon's Minger server.

Listen for Minger connections on this UDP port
This is the port on which the Minger server will listen for connections. The Internet Assigned Numbers Authority (IANA) has reserved and assigned TCP and UDP port 4069 for use with Minger clients and servers. Changing this port is not recommended as it has been reserved exclusively for Minger use.

Minger queries require a shared secret
If you wish to require authentication via a shared secret system, choose this option and enter a text string of at least 16 characters. When this option is chosen the Minger server will refuse unauthenticated queries.

Minger server supports anonymous queries
Choose this option if you wish to support anonymous Minger queries—the connecting client isn't required to authenticate itself before making address verification queries. This is similar to what can be accomplished now by sources using the `SMTP VRFY` command or SMTP "call back" or "call forward", but it is much more efficient and doesn't result in lots of dropped SMTP sessions over TCP, SMTP logs cluttered with dropped sessions, and similar problems inherent in those methods.

Minger treats foreign aliases as active email addresses
When this box is checked, Minger will treat foreign aliases (aliases that point to external addresses) as if they were active known addresses. Also, this behavior is forced when a query comes from SecurityGateway to MDaemon regardless of the state of this option's setting.

Cache Minger lookup results
By default MDaemon will cache Minger lookup results. If you do not wish to cache them, disable this option.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

5.4 Importing Accounts

5.4.1 Importing Accounts from a Text File

Click the Accounts » Importing... » Import accounts from a comma delimited text file... menu selection to access this account generation feature. It can also be reached by clicking the *Import* button on the Account Manager. This is a simple method for importing and automatically generating mail accounts. MDaemon will read a text file and generate new mail accounts using as little as just the first and last names of the user. If you are careful to setup your account template strings properly (see New Accounts Template 775) you can generate unique accounts using only the first and last names, but you can also include many other options for specific user settings if you want to override the new account defaults. All fields must be separated by commas.

Each line of the comma delimited text file must contain only a single user's entry. The first line must be a base line giving the names and sequence of the fields in subsequent lines. A sample file would look something like this:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"michael", "Michael Mason", "C:\Mail\Michael\", N
```

The field names in the base line are used by MDaemon to determine the data sequence and can therefore appear in any order. Each of the field names must be in quotes.

All "String" values must be contained in quotes, and a "bool" field value is considered `FALSE` unless the first char is: `y`, `Y`, `1`, `t`, or `T`.

First, middle, and last names are acceptable in each full name. However, you may not use commas in them.

After running the import process, MDaemon will create `TXIMPORT.LOG`, detailing the import results and listing which accounts imported successfully and which failed. Typical reasons why an account might not be imported would include a conflict with an existing account's mailbox, name, or directory information, a conflict with an existing alias to an account, or a conflict with a mailing list name.

See the description of the `MD_ImportUserInfo()` and the `MD_ExportAllUsers()` within the `MD-API.HTML` file located in your `\API\` directory, for more information on the field mappings.

Use the following values in the base line to map to MDaemon account fields:

Field Name	Type
MailBox	string

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

UserDefined	string

See:

Windows Account Integration 851

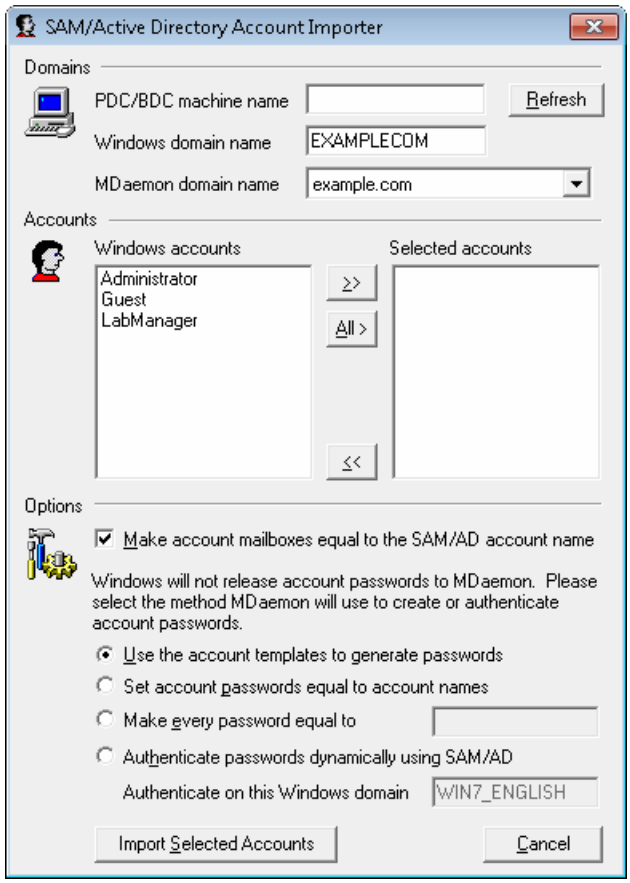
5.4.2 Windows Account Integration

MDaemon supports Windows Account integration. This support consists of a SAM/Active Directory import engine, which can be reached from MDaemon's Accounts menu (Accounts » Importing... » Import accounts from SAM/Active directory...). Additionally, support for Active Directory (AD) authentication of users is embedded into the MDaemon user management code. It is possible to specify a Windows domain in an account's password field and then MDaemon will dynamically authenticate such accounts in real-time, using the specified Windows domain's security system. Under such a scheme, changing the account's password in Windows user management will automatically update MDaemon. Therefore, your users will only have to remember one set of authentication credentials. This also makes for very easy account setup for new installations.

The security context of the account running MDaemon must have the **SE_TCB_NAME** privilege (i.e. "To act as part of the Operating System"). If the process is a service running in the *Local System* account, it will have this privilege by default. Otherwise, it must be set in the Windows user manager for the account under which MDaemon is running.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SAM/Active Directory Account Importer



Domains

PDC/BDC Machine name

This field allows you to specify the machine name from which MDaemon will read Windows account database information. You can specify \\<DEFAULT> and MDaemon will read data from the local machine.

Refresh

Click this button to refresh the Windows Accounts listing.

Windows domain name

Type the Windows domain name from which you wish to import accounts.

MDaemon domain name

Choose from the drop-down list box the MDaemon domain into which the accounts will be imported.

Accounts

Windows accounts

This window contains a list of all the account names collected from the Windows account database.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Selected accounts
This window contains all the account names that you have selected and wish to import.

>>
Click this button to move the highlighted account names from the "Windows Accounts" window into the "Selected Accounts" window.

<<
Click this button to remove the highlighted entries from the "Selected Accounts" window.

Options

Make account mailboxes equal to the SAM/AD account name
Click this switch to force each imported user's Windows account name to be used as their Mailbox value. With this method, you will not need to worry about setting up the correct New Account Template 780 macros.

Use the account template to generate passwords
This option causes MDaemon to generate passwords for imported accounts using the account template settings (see Account Defaults 780).

Set account passwords equal to account names
This switch causes MDaemon to use the account name as the account password.

Make every password equal to...
This switch allows you to specify a static password value that will be used by all imported accounts.

Authenticate passwords dynamically using SAM/AD
This switch enables AD authentication of imported accounts. Rather than specifying a password MDaemon will simply authenticate the mail client supplied USER and PASS values using the NT database in real-time.

Authenticate on this Windows domain
Enter the name of the Windows domain that MDaemon will use when authenticating connections dynamically. **This is not the machine name of the domain controller. It is the actual name of the Windows Domain.**

When accounts are configured for AD authentication, the name of the Windows domain preceded by two backslash characters is used in the account's `PASSWORD` field and is stored unencrypted within the `USERLIST.DAT` file. For example, if an account is configured for AD authentication on a Windows domain called `ALTN`, the account's password field will contain the value `\\ALTN`. The two backslash characters preceding the domain name signify to MDaemon that the password field actually contains the name of a Windows domain and that

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDaemon should attempt to authenticate the USER and PASS values provided by the mail client using that domain's account database. For that reason you must not start a password with two backslash characters unless the account is configured for AD authentication as described above. In other words, you can't just have regular passwords that start with two backslashes. Passwords beginning with two backslashes are always assumed to be providing a Windows domain name and not a password.

You may enter the two backslashes and Windows domain name combination into an account's password field on the Account Details 697 screen of the Account Editor. You need not restrict yourself to using the importer in order to setup accounts for AD authentication.

See:

Importing Accounts From a Text File 849
Account Editor » Account 697

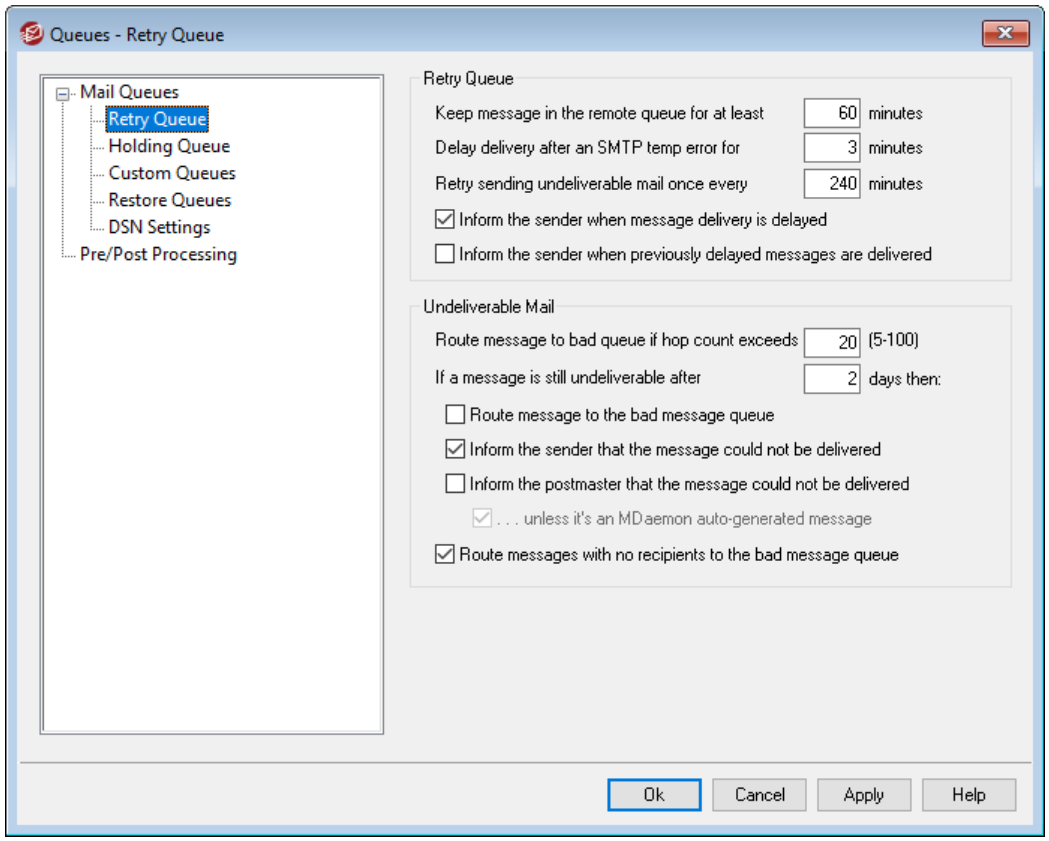
Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section VI

6 Queues Menu

6.1 Mail Queues

6.1.1 Retry Queue



The Retry Queue dialog, located under Queues » Mail Queues, is used to determine how MDaemon will handle messages that cannot be delivered due to some non-fatal error, such as when the receiving server is temporarily unavailable.

Retry Queue

Keep message in the remote queue for at least XX minutes
This setting governs the length of time a message will remain in the remote queue before being removed and placed in the retry queue. The remote queue will generally attempt to deliver the message more frequently than the retry queue.

Delay delivery after an SMTP temp error for xx minutes
When MDaemon encounters an SMTP temporary (4xx) error while attempting to deliver a message, it will delay each subsequent attempt to deliver that message by this many minutes. This helps to prevent MDaemon from trying to deliver the message over and over again too quickly. By default the delay is set to 3 minutes. If you wish to disable the delay, set the value to "0".

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Retry sending undeliverable mail once every xx minutes
This setting determines how frequently the messages in the retry queue are processed.

Inform the sender when message delivery is delayed
By default MDaemon will inform the sender when a message could not be delivered due to some temporary error, causing it to be placed in the retry queue. Uncheck this box if you do not wish to inform the sender of the delay.

Inform the sender when previously delayed messages are delivered
Check this box if you wish to inform the sender when a delayed message has finally been delivered. This is disabled by default.

Undeliverable Mail

Route message to bad queue if hop count exceeds (5-100)
RFC standards stipulate that a mail server must stamp each message each time that it is processed. These stamps can be counted and used as a stopgap measure against recursive mail loops that can sometimes be caused by errant configurations. If undetected, these looping message delivery cycles will consume your resources. By counting the number of times the message has been processed, such messages can be detected and placed in the bad message directory. The assumption is that if a message hasn't reached its recipient after being processed by a given number of mail servers then there is probably a mail loop in progress. Most likely, the default setting of this control should be sufficient to prevent mail loops and will not need to be changed.

If a message is still undeliverable after xx days then:
This setting determines the number of days that a message can remain in the retry queue before being removed. If you enter "0" days into this option then the message will be bounced back after the first retry attempt. The default setting is 2 days.

Route message to the bad message queue
When this option is enabled, a message will be moved to the bad message queue once it has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option.

Inform the sender that the message could not be delivered
Once a message has reached the time limit set in the "*If a message is still undeliverable after xx days then:*" option, this switch will cause MDaemon to send a Delivery Status Notification 864 message to the sender informing him that the message has been permanently removed from the server.

Inform the postmaster that the message could not be delivered
If this switch is enabled, the postmaster will be notified when a message has been permanently removed from the retry system.

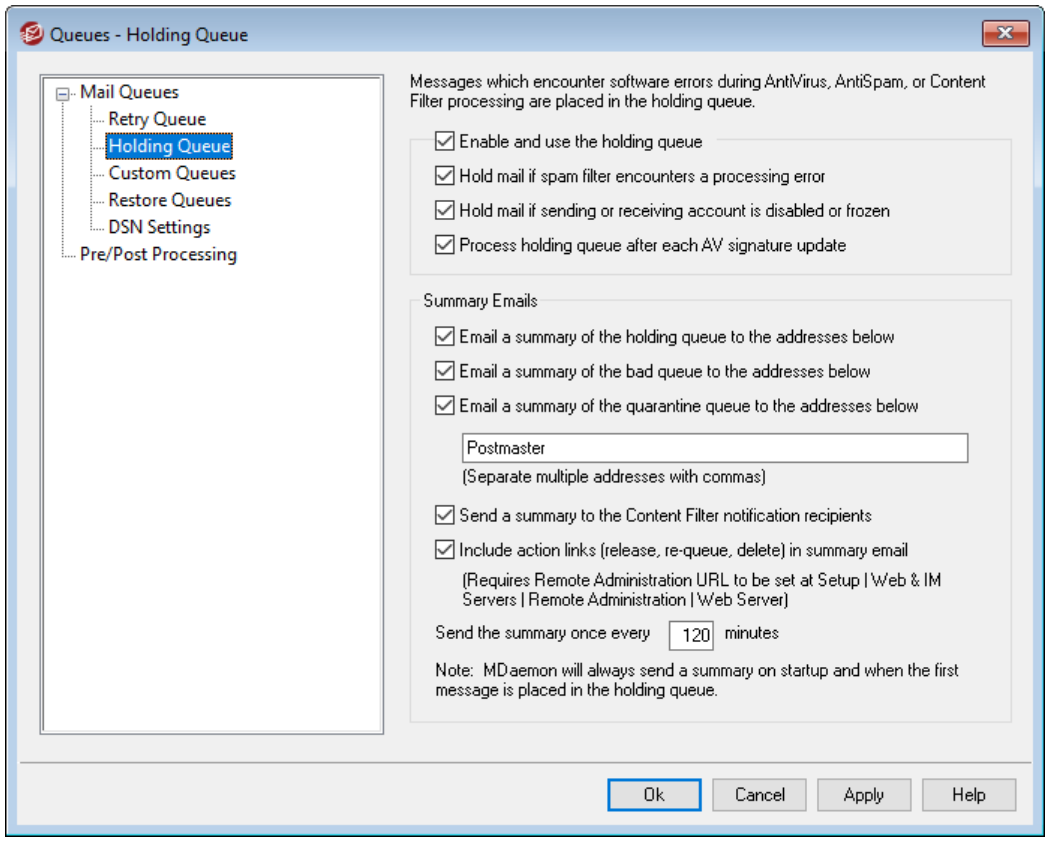
. . . unless it's an MDaemon auto-generated message
By default, the retry system will not inform the postmaster that a message could not be delivered when that message was auto-generated by MDaemon.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Clear this checkbox if you wish to inform the postmaster about the failure of those messages as well. Examples of auto-generated messages are return-receipt notifications, Autoresponder generated messages, results of account processing, and so on.

Route messages with no recipients to the bad message queue
When this option is enabled, messages with no recipient data will be moved to the bad message queue. When disabled, they will be deleted. This option is enabled by default.

6.1.2 Holding Queue



The Holding Queue, located under Queues » Mail Queues can be used to receive messages that cause software exceptions during AntiVirus, AntiSpam, or Content Filter processing. If a software error occurs when processing a message it will be moved into the holding queue and not delivered.

Messages placed into the holding queue will stay there until the administrator takes some action to remove them. There is a *Process Holding Queue* button on MDaemon's toolbar and an identical option on the Queues menu bar. You can also process the messages by right-clicking the holding queue on the main interface and then selecting "Re-Queue" from the right-click menu. Processing the holding queue will move all of its messages into either the remote or local queues for normal mail processing. If the error that caused a message to be placed into the holding queue still exists then that message will be placed back into the holding queue when the error reoccurs. If you

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

want to attempt to deliver the holding queue's messages regardless of any error which might occur, then you can do so by right-clicking the holding queue on the main interface and then selecting "Release" from the right-click menu. When releasing messages from the holding queue a confirmation box will open to remind you that the messages could contain viruses or otherwise not be able to filter properly through the Content Filter, AntiSpam and/or AntiVirus engines.

Holding Queue

Enable and use the holding queue
Click this check box to activate the holding queue. Messages that cause software exceptions during AntiVirus and Content Filter processing will be moved to this queue whenever an error occurs.

Hold mail if spam filter encounters a processing error
Click this option if you wish to move messages to the holding queue that cause errors during Spam Filter processing.

Hold mail if sending or receiving account is disabled or frozen
When this option is enabled, MDaemon will automatically hold messages when the sending or receiving account is disabled or frozen.

Process holding queue after each AV signature update
When this option is enabled, the holding queue will be processed automatically each time after the AntiVirus 630 virus signatures are updated.

Summary Emails

Email a summary of the holding queue to the addresses below
If you wish to send a summary of messages contained in the holding queue to one or more email addresses at regular intervals then click this option and list the addresses in the text space provided below.

Email a summary of the bad queue to the addresses below
If you wish to send a summary of messages contained in the bad queue to one or more email addresses at regular intervals then click this option and list the addresses in the text space provided below.

Email a summary of the quarantine queue to the addresses below
Enable this option if you wish to send a summary of the quarantine queue at the designated interval below.

Summary message recipients
Use the text box to specify the email addresses to which you wish to send the queue content summaries designated in the previous two options. When listing multiple addresses, separate them with commas.

Notification messages are sent at MDaemon startup, the first time a message is placed into the holding queue, and at the interval specified in the *Send the summary once every XX minutes* option below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

If a notification message causes a software error then it may not be delivered to remote recipients. It will, however, still be delivered to local recipients.

Send a summary to the Content Filter notification recipients
Click this option if you want an additional copy of each notification message to be sent to the Content Filter's designated notification Recipients 649.

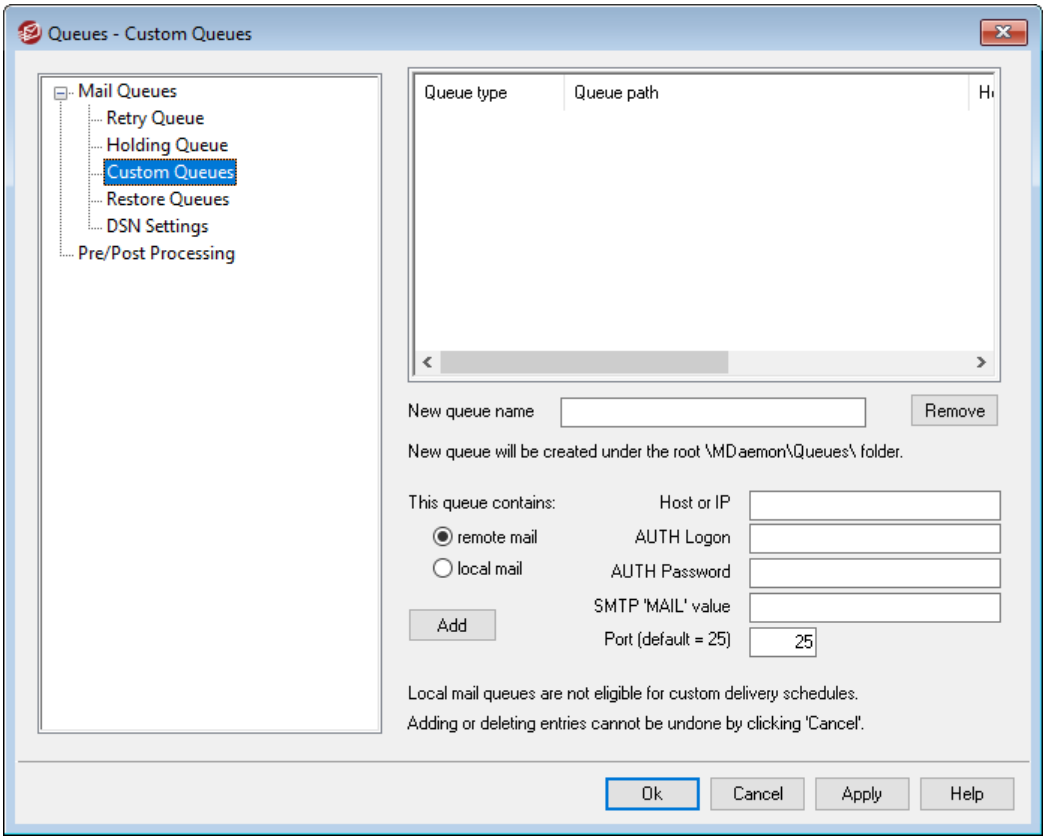
Include action link (release, re-queue, delete) in summary email
By default, the summary emails for the holding, quarantine, and bad queue have links to release, re-queue, or delete each message. Disable this option if you do not wish to include the links in the summary emails.

In order for the links to be generated, the Remote Administration URL 343 must be set.

Send the summary once every XX minutes
Use this option to designate the number of minutes that will pass before MDaemon will send a holding queue notification message to each specified address or Content Filter recipients.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.1.3 Custom Queues



Use the Custom Queues dialog under Queues » Mail Queues to create custom local and remote mail queues. Custom queue support makes it possible for you to have MDaemon monitor several locations from which to send mail. You can create new queues and designate them as local or remote, and you can then use Content Filter rules to cause messages to be automatically placed into your custom mail queues, and for remote queues you can use the Event Scheduler 372 to create custom schedules to control how often those queues will be processed.

Custom Queues

This area displays an entry for each custom queue, listing its file path and whether it is local or remote.

Remove

If you wish to remove a queue from the list, select its entry and then click the *Remove* button.

When you delete a custom queue, any custom schedules or content filter rules associated with that queue will also be deleted.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

New queue name
Enter a name for the new mail queue here. The queue will be created under MDaemon's `\MDaemon\Queues\` folder.

This queue contains...

...remote mail
Choose this option if you want the custom mail queue to be used for remote mail.

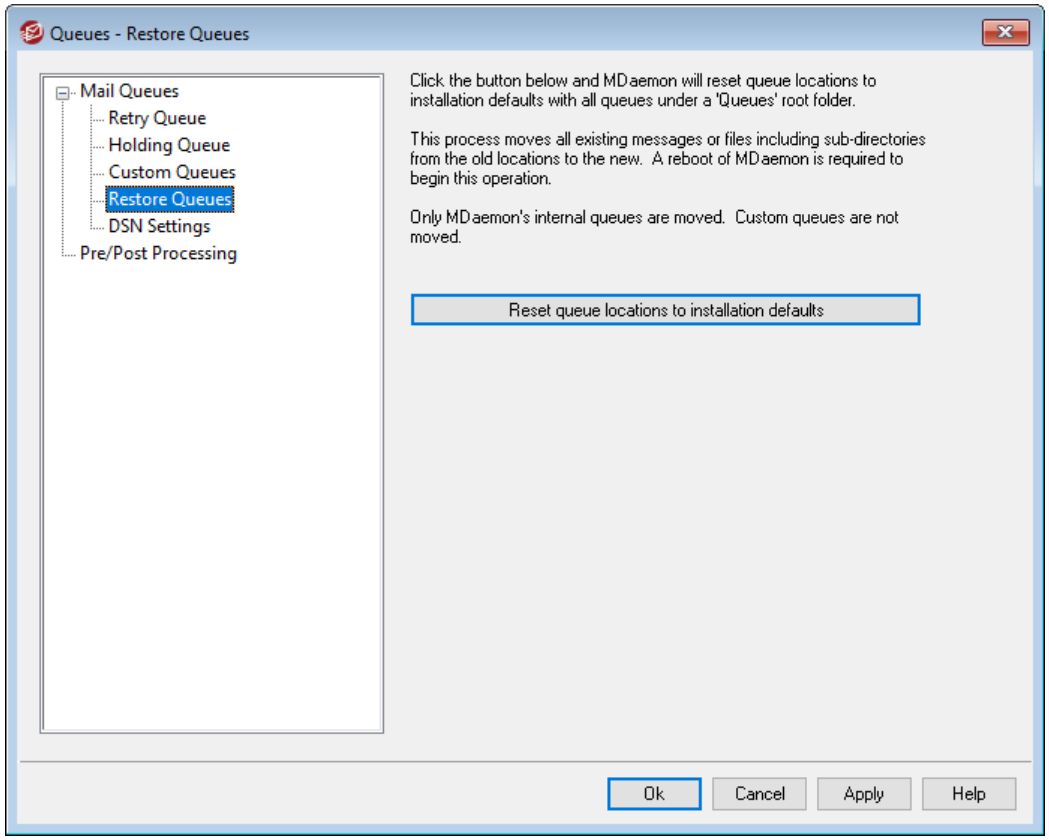
Queue Credentials
You can specify a *Host or IP*, *AUTH Logon/Password*, *SMTP 'MAIL' value*, and *Port* for any remote queue. If provided, all messages in the queue are delivered using those settings. However, it is still possible in some circumstances for individual messages within the queue to have their own unique delivery data, and, if so, that data will take priority over these settings.

...local mail
Choose this option if you want the custom mail queue to be used for local mail.
Note: Local mail queues are not eligible for custom delivery schedules.

Add
After you have chosen the name and type for your queue, click the *Add* button to add it to the list of custom queues.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.1.4 Restore Queues

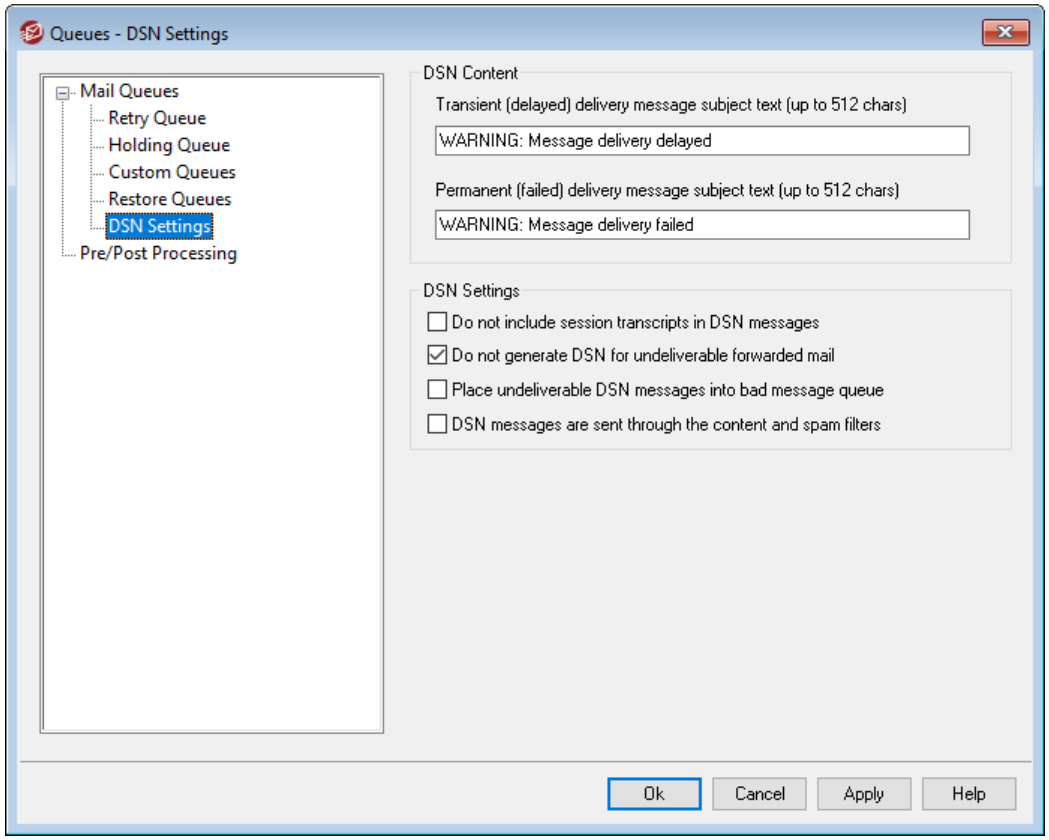


Reset queue locations to installation defaults
By default, a new installation of MDaemon stores message queues such as Remote, Local, Raw, and the like under the `\MDaemon\Queues\` subfolder. Previous versions of MDaemon stored queues elsewhere. If your installation of MDaemon is using the old folder locations and you would like to move your queues to this more organized structure then click this button and all queues and the files and messages they contain will be moved for you. After clicking this button you will need to restart MDaemon for the changes to be implemented.

Custom Queues 861 will not be moved by this feature.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.1.5 DSN Settings



When MDaemon has a problem delivering a message, whether it is a temporary or permanent delivery failure, a Delivery Status Notification (DSN) message is sent to the sender of the message. This screen contains various options related to those DSN messages. It is located at: Queues » Mail Queues/DSN... » DSN Settings.

DSN Content

Transient (delayed) delivery message subject text (up to 512 chars)
This is the subject heading of the DSN message that will be sent when there is a transient problem causing a delay in message delivery. For example, if the recipient's mail server isn't available when MDaemon tries to deliver a message, MDaemon will continue trying to send it at designated intervals, and it will send this DSN message informing the sender of the problem. See: Customizing DSN Messages 865.

Permanent (failed) delivery message subject text (up to 512 chars)
This is the subject heading of the DSN message that will be sent when there is a problem that makes it impossible for MDaemon to deliver a message. For example, if the receiving mail server rejects the message, stating that the recipient's email address doesn't exist, MDaemon will stop trying to deliver the message and will send a DSN message informing the sender that the message cannot be delivered. See: Customizing DSN Messages 865.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

DSN Settings

Do not include session transcripts in DSN messages
Click this option if you do not wish to include SMTP session transcripts in delivery error and warning messages. This option is disabled by default.

Do not generate DSN for undeliverable forwarded mail
When this option is enabled, forwarded messages that encounter permanent, fatal delivery errors or expire from the Retry queue 856 will be moved to the bad messages queue, with no DSN messages being sent to the original sender. This option is enabled by default.

Place undeliverable DSN messages into bad message queue
Click this checkbox if you wish to place undeliverable Delivery Status Notification messages into the bad message queue rather than retrying them.

This only applies to DSN messages generated by MDaemon.

DSN messages are sent through the content and spam filters
Enable this option if you wish to send DSN messages through the content and spam filters. This option is disabled by default.

Customizing DSN Messages

The "human-readable" portion of transient (delayed) and permanent (failed) DSN messages can be customized by creating a file called `DSNDelay.dat` or `DSNFail.dat` respectively, in the `\MDaemon\App\` folder. Edit them with a text file editor such as Notepad and enter the text you wish to use. The following macros can be used in your custom text:

$SESSIONID$ - expands to the delivery session's ID string

$QUEUEID$ - expands to the message's mail queue ID string

$MESSAGEID$ - expands to the message-id header value

$RETRYDAYS$ - length of time allowed in queue (in days)

$RETRYHOURS$ - length of time allowed in queue (in hours)

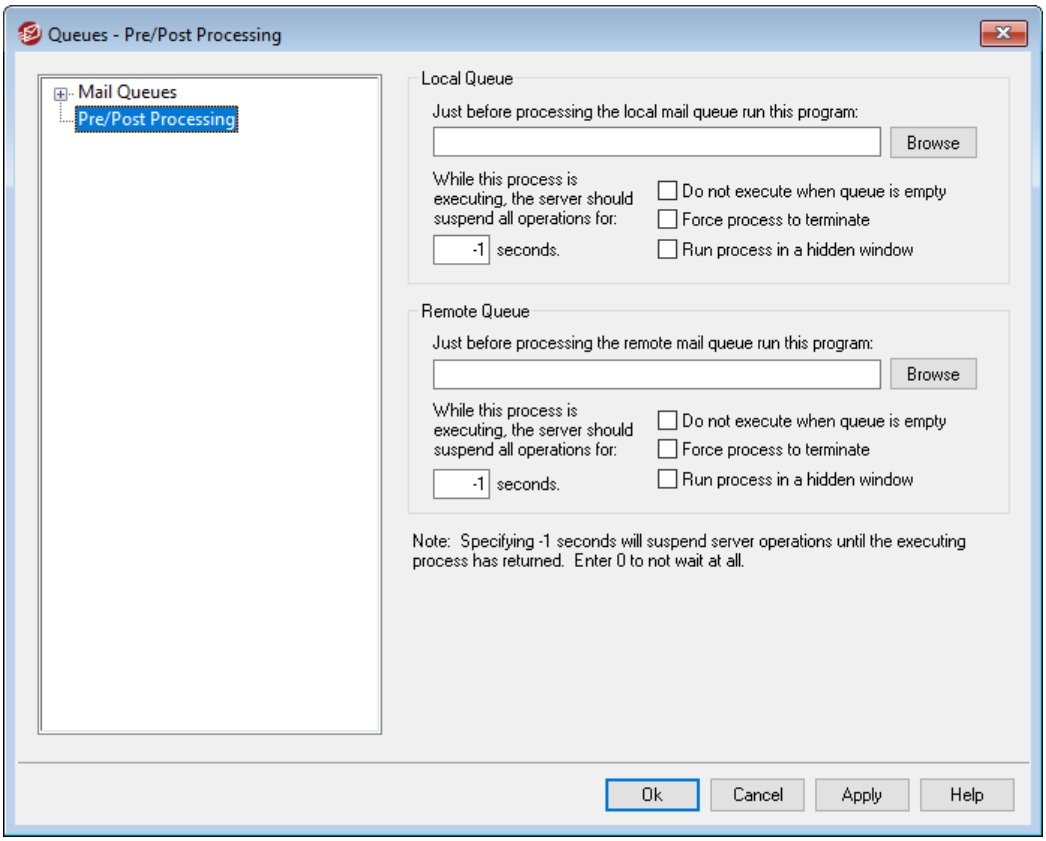
MDaemon must be restarted before changes to these files are loaded.

See:

Retry Queue 856

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.2 Pre/Post Processing



Local and Remote Queue Pre/Post Processing

Just before processing the (local/remote) mail queue run this program
This field specifies a program path and name that will be executed just prior to the processing and delivery of any RFC-2822 messages that might be in the local or remote message queues. If complete path information is not provided, MDaemon will first search for the executable in the MDaemon directory, then in the Windows System directory, next in the Windows directory, and finally the directories listed in the PATH environment variable.

...suspend all operations for xx seconds
The value entered here determines how MDaemon will behave while the specified program is in progress. MDaemon can be configured to pause its execution thread for the number of seconds specified while waiting for the process thread to return. If the process returns before the number of seconds has elapsed, MDaemon will resume its execution thread immediately. If you enter "0" in this option MDaemon will not suspend operations at all. Entering "-1" will cause MDaemon to wait until the process returns, no matter how long that might be.

Do not execute when queue is empty
Enable this switch if you do not want the specified program to run when the queue is empty.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Force process to terminate
Sometimes the process you need to run may not terminate on its own. This switch will cause MDaemon to force the session to terminate once the time specified in ...*Suspend all operations for XX seconds* has elapsed. This switch does not work if the elapsed time interval is set to "-1".

Run process in a hidden window
Click this checkbox if you want the process to run in a hidden window.

6.3 Queue and Statistics Manager

MDaemon's Queue and Statistics Manager is accessed from within MDaemon under the Queues » Queue and Statistics Manager menu selection. The Queue and Statistics Manager is made up of a four-page dialog. Each of these pages has been designed to serve a distinct and specific purpose while also maintaining a simple format that makes them very easy to use.

Queue Page 868

The default tab is the *Queue Page*. From this page you can easily manage all of MDaemon's standard mail queues, as well as the User Account mailbox folders. By simply clicking on the queue or user of your choice, a list of all message files contained within the specified queue will be displayed along with several key pieces of pertinent information about each message: the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location. In addition, controls are provided that make it easy to copy or move messages between folders, or delete them completely.

User Page 871

The *User Page* displays a list of all MDaemon users. This list includes their full name, mailbox name, the number of messages in their mailbox, the amount of disk space that their account is taking up, and the date that they last checked their mail. This list can also be saved to disk as a text file, or it can be saved in comma delimited format for use with databases.

Log Page 873

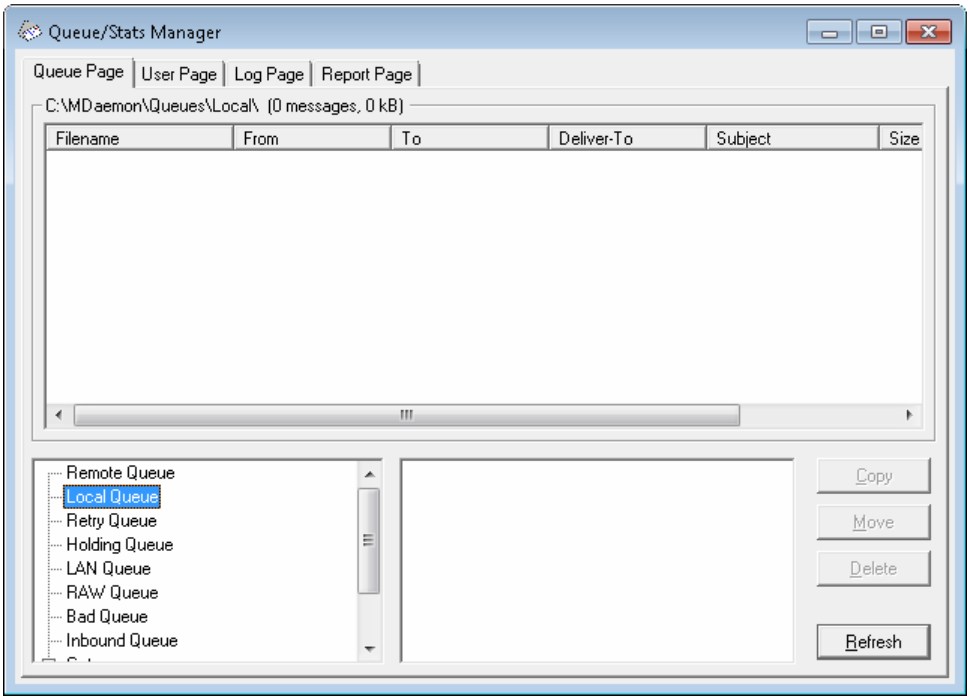
With this dialog you can display MDaemon's *Log Files* in a simple list format. This feature is very useful for quickly examining the history of MDaemon's mail transactions because it condenses the selected *Log File* into a columnar list which contains: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful. You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Logs displayed on the *Log Page* can be saved as a text file or in comma delimited format for use with databases.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Report Page

The last tab is the *Report Page*. With this feature you can produce a report containing all of MDaemon's configuration settings, written in a plain text readable format. Because of the large number of optional settings and configurations in MDaemon, this can greatly speed the process of administering configuration changes as well as aid in diagnosing possible configuration problems. Additionally, this report is displayed in a text editable format that makes it possible to Copy/Paste the information it contains (using the right-click shortcut menu), or add notations or other information to the file before saving it.

6.3.1 Queue Page



Queue page list box

When a queue or user is chosen from the *Message Queues* area or the user list box beside it, a list of all message files contained within the selected queue will be displayed in the main list box on this page. This list contains each message's file name, the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location (listed by date and time).

Above this box the complete file path to the currently displayed directory is given, as well as the number of messages displayed and the size of the directory.

You may copy, move, or delete one or more files by selecting them from the list and then clicking the appropriate button below it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

The content of these files may also be edited directly from the *Queue Page* list box. Simply double-click the file that you wish to edit (or choose "Edit" from the right-click shortcut menu) and the file will be opened in Notepad for editing.

If you want the Queue and Statistics Manager to open an editor other than Notepad by default, then you must edit the `mdstats.ini` file located in the `\MDaemon\app\` folder. Change the "`Editor=`" key located under the `[QueueOptions]` section heading to `Editor=MyEditor.exe`. If the file path of the `*.exe` file is not in your current path, then you will have to include the path here as part of the file name.

The list box can be navigated by using the vertical or horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *Queue Page* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z, 1-2), or click twice to sort it in descending order (Z-A, 2-1). Columns can also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

Selecting Files

To select files individually	Click the desired file.
To select contiguous files	Click the first file in the contiguous list of files that you wish to select, then while holding down the SHIFT key, click the last contiguous file in the desired list. Alternatively, you may use the ARROW, HOME, END, PAGE UP, and PAGE DOWN keys, while holding down the SHIFT key, to select files in contiguous order.
To select non-contiguous files	Click on the desired files in the **File Name** column while holding down the CTRL key.

Message queues
Click an in the lower left pane and a list of all files contained within the specified queue will be displayed in the *Queue Page* list box. If you click the *User Folders* option, a list of all MDaemon users will be displayed in the *User List Box* to the right of the *Message Queues* section.

Users list box
This box displays a list of all MDaemon users when the *User Folders* option is clicked in the *Message Queues* section (lower left pane). Click a user's name to display a list of all message files currently contained in the user's mailbox folder.

Refresh
Because mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them - you should regularly click this button to refresh any list of files that you may have displayed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

You can edit the `MDstats.ini` file to cause displayed lists to automatically refresh. To do this simply open the `MDstats.ini` file located in MDaemon's `\app\` directory and edit the AutoRefresh key under the `[QueueOptions]` heading to reflect the number of seconds that you wish to elapse between refreshes. Entering the value "`0`" means that you do not want the list to automatically refresh. Example: `AutoRefresh=15` (the list would refresh every 15 seconds).

Copy
When one or more files are selected, click this button to copy the selected files to another queue or user's mailbox folder. After clicking this button the *Copy Message(s)* dialog box will open, from which you can select the desired location to which you wish to copy the selected files.

Move
When one or more files are selected, click this button to move the selected files to another queue or user's mailbox folder. After clicking this button the *Move Message(s)* dialog box will open, from which you can select the desired location to which you wish to move the selected files.

Files copied or moved to other queues will rarely retain their original file names. To avoid overwriting files of the same name that may already be in the queue, MDaemon always calculates the next destination filename based on the `HIWATER.MRK` file located in the destination folder.

Delete
When one or more files are selected in the *Queue Status List Box*, click this button to delete the selected files. After clicking this button a confirmation box will open asking if you really do wish to delete the selected files.

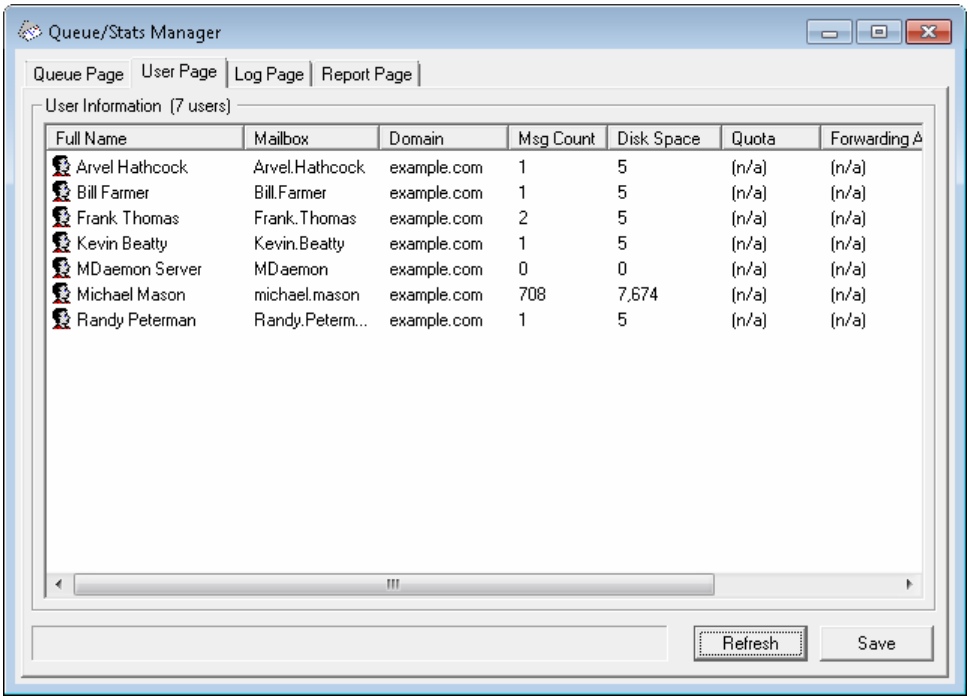
Mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them. For this reason you should be aware that when copying, moving, or deleting files you may at times encounter a message stating that the action that you are attempting cannot be completed. This will occur when the message file that you are attempting to work with has already been removed by MDaemon before the desired action has begun. By clicking the *Refresh* button, you can update the current list of files displayed in the list box.

You can prevent messages from being moved out of the queue while you are editing them by editing the `MDstats.ini` file. To do this simply open the `MDstats.ini` file located in MDaemon's

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

> \app\ directory and change the LockOnEdit=No key under the [QueueOptions] heading to LockOnEdit=Yes. This will cause a LCK file to be created whenever you are editing a message, which will prevent it from being moved out of the queue until you are finished with it.

6.3.2 User Page



User information
When the *User Page* is chosen, a list of all MDaemon accounts is loaded into the *User Information* list box. This list contains each user's full name, the name of their mailbox, the domain to which the account belongs, the number of messages it contains, its mail format, the amount of disk space (in kilobytes) that the account is taking up, their forwarding address, and finally, the date that their mail was last checked. Given that the information contained in this list is constantly changing, it can be easily updated by clicking the *Refresh* button.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *User Information* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z), or click twice to sort it in descending order (Z-A). Columns may also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width. Further, you can double-click any entry and MDStats will be shifted to the *Queue Page* with the contents of their mailbox folder displayed.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

By default, the list displays the Message Count not file count, and the Disk Space used *by messages* not the space used by all files in the directory. This is the *Quota* information reported by MDaemon. Alternatively, you can display the *file* count and disk space used by all *files* instead of by messages. To change this setting simply open the `MDstats.ini` file located in MDaemon's `\app\` directory and change the `ShowQuota=Yes` key under the `[UserOptions]` heading to `ShowQuota=No`.

User folders contain a file called "`hiwater.mrk`" which is used to determine some of this user information. You should avoid deleting this file unnecessarily as it will prevent the Queue and Statistics Manager from being able to obtain some of the information listed in the *User Information* list box.

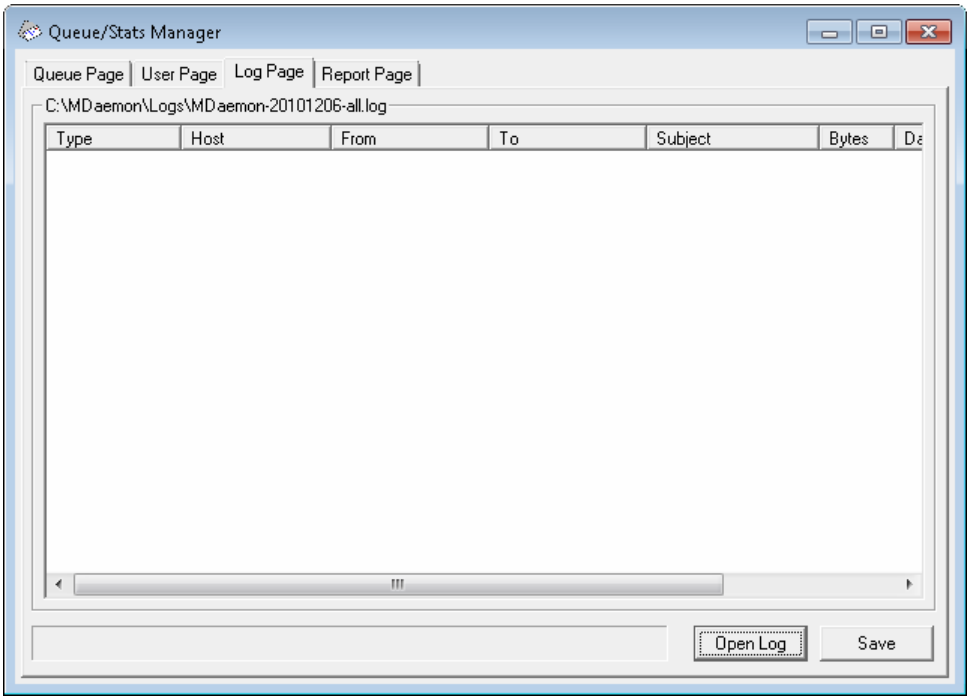
Refresh
User statistics such as the number of messages contained in their mailboxes, and the amount of disk space that their accounts are using, are constantly changing. You can easily update the information contained in the *User Information* list box by clicking the *Refresh* button. This will immediately make all displayed information current.

Progress indicator
Because *User Information* lists can at times be very large, below the *User Information* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded.

Save
The information contained in the *User Information* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.3.3 Log Page



Log report
The *Log Report* list box displays MDaemon's detailed log files that you select through the *Open Log* button and the Windows Open dialog that follows it. The *Log Report* display provides a quick and easy way to review the history of mail transactions that MDaemon has processed without having to sort through the large volume of information that MDaemon log files may sometimes contain. When a *Log Report* is displayed in this list box the Queue and Statistics Manager breaks it down into a simple format containing: the Type of the message (POP Inbound, DomainPOP, RFC2822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful.

You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Using the right-click shortcut menu you can copy/paste this detailed log portion to a text editor for saving or editing should you desire to do so.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can resize the list box's columns by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

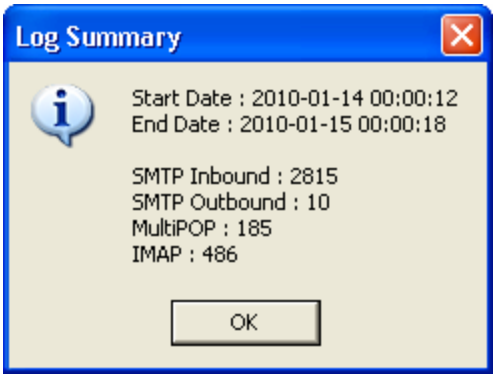
The *Log Page* will display log files that have been compiled using either the *Log detailed mail sessions* or the *Log summarized*

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

> *mail sessions* option located under Logging » Log Mode. However, we highly recommend that you use the *Log detailed mail sessions* option. When using the *Log summarized mail sessions* format you will find that there is very little information that will be displayed in your *Log Report*. Because the *Log Page* itself condenses the detailed log into a summary view of MDaemon's activity, while still providing the ability to look at the detailed view of every transaction when necessary (by double-clicking an entry), there is no need to have MDaemon summarize the log file while compiling it.

Open log
Click this button to open the Windows Open dialog for choosing which log file that you wish to view. If you click this button when there is a *Log File* already displayed in the *Log Report* list box, you will be given the option to append the new file to the one that is already displayed.

After a log is displayed, a message box will be opened which contains a summary of the selected log. When saving a Log Report as a text file, this log summary will be appended to it.

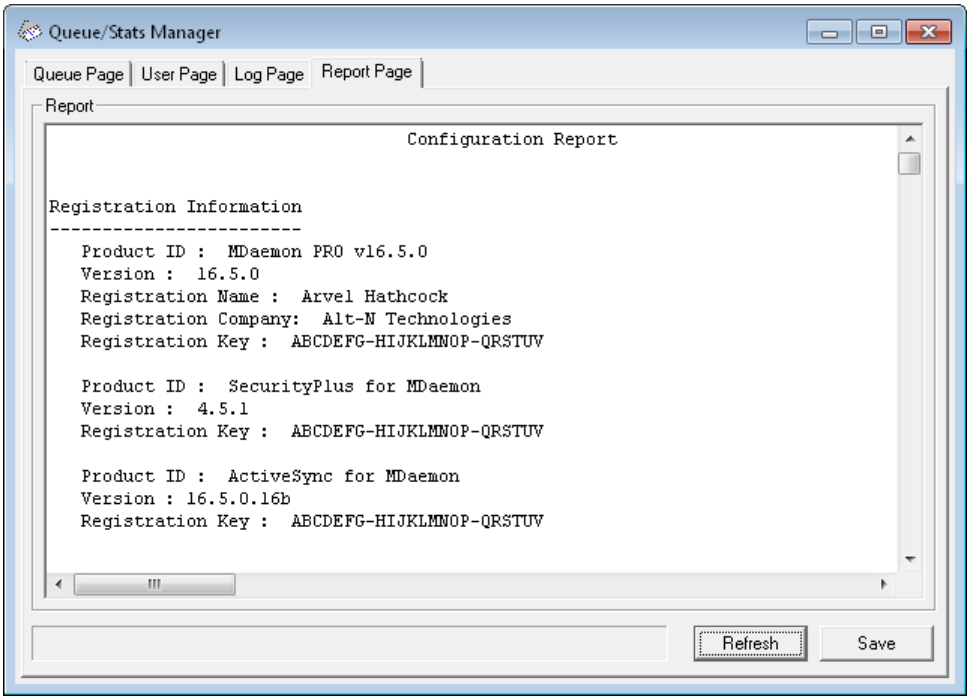


Progress indicator
Because *Log Files* can be very large, below the *Log Report* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded or saved.

Save
The information contained in the *Log Report* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, you will be asked whether you want to save the file in comma delimited format or as a plain text file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.3.4 Report Page



Report
When the *Report Page* is clicked, a comprehensive report will be produced that lists every setting within MDaemon in an easily readable text format. This feature greatly decreases the amount of time needed by an administrator to check MDaemon's many configuration settings, and it can aid in quickly solving possible configuration problems.

You can navigate through this report using either the scroll bars or the CURSOR keys, and the *Report* display is also a text editor - making it possible to insert notations or additional information that you may want on the report before saving it to a file. Additionally, you can use the shortcut menu to Cut, Copy, and Paste, to and from this display by right-clicking your mouse and making the desired selection from the menu that opens.

Refresh
Click this button to update the currently displayed *Report* of MDaemon settings.

Progress indicator
As with the other tabs in the Queue and Statistics Manager, the *Report Page* contains a progress indicator bar that serves as a visible indicator that the program is still operating while large files are being loaded or saved.

Save
Click this button to save the currently displayed *Report*. After clicking this button a standard Save As dialog will open so that you can designate a file name and location where you want to save it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

6.3.5 Customizing the Queue and Statistic Manager

6.3.5.1 MDstats.ini File

Customizing the Queue/Statistic Manager

The following is a list of settings that can be modified in the `MDstats.ini` file located in MDaemon's `\app\` directory:

[MDaemon]

AppDir=C:\mdaemon\app\	Location of MDaemon's \app\ directory.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor to use when a message is double-clicked, or when a message is right-clicked and then Edit is selected.
LockOnEdit=No	Whether or not to create a LCK file when editing a message. This will prevent a message from being moved out of the queue while it is being edited.
AutoRefresh=Yes	Time (in seconds) between auto refreshes of the message listing. 0 means no auto refresh.
ShowDirectories=Yes	Show subdirectories of the queues in the list box in addition to the messages. Directories will appear as <DirectoryName>.

[UserOptions]

ShowQuota=Yes	Determines whether the user listing displays quota information (message count and disk space just like MDaemon calculates it) or file information (number of files and total disk space).

[LogOptions]

ShowUnknown=Yes	Show sessions that MDStats couldn't determine if they were inbound or outbound, SMTP or POP.
ShowSmtpInbound=Yes	Show SMTP inbound sessions.
ShowPopInbound=Yes	Show POP inbound sessions (mail checks).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ShowSmtpOutbound=Yes	Show SMTP outbound sessions.
ShowPopOutbound=Yes	Show POP outbound sessions (MultiPOP, DomainPOP).
ShowRFC822=Yes	Show RFC822 local mail deliveries.
ShowSmtpHelo=Yes	For SMTP inbound sessions, show HELO domain in the Host column.
IgnoreEmptyPop=Yes	Ignore mail checks when no mail was deliverd.
ShowImap=Yes	Shows IMAP Sessions.
[Remap]	Drive letter remapping; for running MDStats from a different machine than the one MDaemon is on.
C:=\\server\c	When reading from MDaemon.ini, replace "C:" with "\\server\c".
[Special]	
OnlyOneInstance=No	Allow only one instance of MDStats to run. Attempting to open it again will activate the instance that is already running.

See:

MDStats Command Line Parameters 877

6.3.5.2 MDStats Command Line Parameters

Note: All command line parameters are not case sensitive.

Number 1 through 8	Display a specified queue in the Queue Page.
	= Remote Queue
	= Local Queue
	= Retry Queue
	= LAN Queue
	= RAW Queue
	= Bad Queue

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

= SmtpIn Queue

= Save Queue

/L[N] [InputFile] [OutputFile]	Produce a log file report. Specifying an "N" after the "L" means do not save as a comma delimited file.
/A	If producing a log file report, append new information to the output file rather than overwriting it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section

7 Additional MDaemon Features

7.1 MDaemon and Text Files

MDaemon uses a number of plain text files to store some of its data, system generated message templates, and configuration settings, which provides a great deal of flexibility. You can create new text files from within MDaemon by using the File » New menu selection. This can be useful for quickly creating data files for use with Autoresponders and various other MDaemon features, such as RAW files.

Editing MDaemon Files

MDaemon's various data files are plain text and can be edited in Notepad. You can easily open any of these files from within MDaemon by using the File » Open » Empty Text File menu selection. By default this looks in MDaemon's `\app\` folder for `*.txt` files. Switch the *Files of type:* drop down list to "All files" to see the rest of the files contained in that folder.

7.2 Remote Server Control via Email

Many functions of MDaemon can be accessed remotely using the email transport system itself, by sending a specially formatted email to the MDaemon system account, "`MDaemon@<MDaemon's Domain>`". Messages sent to the server are stored in the server's message directory just like any other user.

Some of these control messages require a valid account on the server. For those commands which require a valid account, the message must be authenticated during the SMTP process using SMTP AUTH.

There are two, broad categories of commands that can be used in email messages: Mailing List 880, and General Email 883.

See:

Mailing List Control 880
General Email Controls 883

7.2.1 Mailing List and Catalog Control

None of these commands require an account on the server. Parameters contained in [brackets] are optional. For example: "name [address]" could be entered as "Michael" alone or with the optional parameter added: "Michael user1@example.com". Messages should be sent to "mdaemon@[MDaemon domain]" with the each command and associated parameters contained on a single line in the body of the message.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

COMMANDS	PARMS	DESCRIPTIONS

SUBSCRIBE	listname [address] [{real name}] [(pass)]	The originator is added to the membership of the specified list provided that list exists and allows remote subscriptions. If an optional address is specified after the list name then that address is added to the list's membership rather than the address found in the FROM: field of the subscription message. A real name can be added for the subscriber by including it in braces (e.g. {Bill F}. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's subscribe function is switched off.
		Examples:
		`SUBSCRIBE list@example.com`
		`SUBSCRIBE list@example.com me@example.com {Bill F}`
		`SUBSCRIBE list@example.com you@example.org (PASS)`

UNSUBSCRIBE
Or
SIGNOFF
	listname [address] [(pass)]	The originator is removed from the membership of the specified list provided that list exists and contains the originator as a current member. If an optional address is specified after the list's name then that address is removed from the list's membership rather than the address found in the FROM: field of the unsubscribe message. If the list's password follows this command (parentheses around it are required) then the command will be honored even if this list's unsubscribe function is switched off.
		Examples:
		`UNSUBSCRIBE list@example.com (listPASS)`
		`SIGNOFF list@example.com me@example.com`

DIGEST	listname [address]	The sender is set to receive mail from the list in digest format. If an optional address is specified after the list name then that address is set to digest mode.
		Examples:
		`DIGEST list@example.com`
		`DIGEST list@example.com user1@example.com`

NORMAL	listname [address]	The sender is set to receive mail from "list" in normal (non-digest) format. If an

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

		optional address is specified after the list name then that address is set to receive in normal format instead of the sender.
		Examples:
		`NORMAL list@example.com`
		`NORMAL list@example.com user1@altn.com`

NOMAIL	listname [address]	This command sets 'address' to nomail mode. The account will enter a suspended state and will no longer receive list traffic. If no address is specified then the originator of the message will be used. Example: `NOMAIL list@example.com me@example.com`

MAIL	listname [address]	This command returns 'address' to normal mode from nomail mode. If no address is specified then the originator of the message will be used.
		Examples:
		`MAIL list@example.com`
		`MAIL list@example.com me@example.com`

REALNAME	listname [address] {real name}	This command sets the real name value for "address" who is a member of list "listname" to the given value. The real name must be enclosed in { and } characters. Example: `REALNAME list@example.com {Bill Farmer}`
LIST	[listname] [list password]	Provide information about a mailing list. If the list's name is not provided, then a summary of all lists is returned. If the lists password is provided then a greater level of information about the list is returned. Example: `LIST list@example.com Lz$12`

See:

Remote Server Control Via Email 880
General Email Controls 883

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

7.2.2 General Email Controls

These are general email commands that can be sent to the system account via email messages. Messages should be sent to "mdaemon@[MDaemon domain]" with the each command and associated parameters contained on a single line in the body of the message.

COMMANDS	PARMS	DESCRIPTIONS
HELP	none	A copy of the NEWUSERHELP.DAT is processed and mailed back to the message originator.
STATUS	none	A status report on server operations and current conditions will be mailed back to the message originator. Since the information contained in this status report is considered private, the user requesting the report must be authenticated as an administrator. Example: STATUS

See:

Remote Server Control Via Email 880
Mailing List Control 880

7.3 The RAW Message Specification

7.3.1 The RAW Message Specification

MDaemon has inherent support for a simple and powerful mail message format known as RAW mail. The purpose of the RAW mail system is to provide a simple and standard format that software systems such as MDaemon can use to create much more complex RFC-2822 compliant message. Use of mail transport agents such as RAW allow client software to offload to the server all the complicated work of maintaining adherence to Internet mail standards.

RAW mail consists of a series of required and optional text headers followed by a message body. Most headers consist of a token followed by a value enclosed in <> symbols. Each header line ends with a <CRLF> combination of characters. Headers are separated from the message body by a blank line and are case insensitive, and the *from* and *to* headers are the only ones that are required. All text, headers and body, are plain ASCII text and must be contained in a file that ends with the extension, ".raw" (for example "my-message.raw"). Then, to queue the message for delivery, place the *.raw file in MDaemon's RAW queue (typically located at, "C:\MDaemon\Queues\Raw").

Bypassing the Content Filter

By default, RAW messages are passed through the Content Filter like normal messages. If you want a given RAW message to bypass the filter then start the name of the file

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

with "p" or "P". For example, "P_my-message.raw" would bypass the Content Filter but "my-message.raw" would be processed through it normally.

Bypassing the Content Filter will prevent messages from being DKIM signed. If you have configured MDaemon to sign all messages then this could potentially cause some delivery problems. If you want MDaemon to sign RAW messages configured to bypass the Content Filter then you can do so by using the x-flag=sign option outlined below.

RAW Headers

From <mailbox@example.com>	This field contains the email address of the sender.
To <mailbox@example.com [, mailbox@example.com]>	This field contains the email address(es) of the recipient(s). Multiple recipients can be specified by separating each one with a comma character.
ReplyTo <mailbox@example.com>	An optional email address where replies to this message will be directed.
CC <maibox@example.com[, mailbox@example.com]>	An optional list of carbon copy recipients of this message. Multiple carbon recipients can be specified by separating each one with a comma character.
Subject <text>	An optional subject for the message.
Header <Header: Value>	Allows you to explicitly place Header/Value combinations into the message. This makes it possible for you to place custom or other non-standard headers into your *.raw messages.

Special Fields Supported by RAW

File attachment and encoding

```
x-flag=attach <filepath, method> [-x]
```

Example: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

This X-FLAG specifies the value "ATTACH" along with two parameters within the <> characters. The first parameter is a complete path to the file which should be attached to the message. The second parameter which is separated from the first by a comma character and specifies the method of encoding that is to be used when attaching the message. MDaemon supports two values for this parameter. The method of MIME instructs the server to use the Internet

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

standard Base64 method of message encoding. The method of ASCII instructs the server to simply import the file into the message. An optional -X parameter at the end of the string instructs the server to remove the file from disk once it has been attached.

Delivery Status Notification

```
x-flag=confirm_delivery
```

When converting a RAW message which contains this flag into RFC-2822 mail, the string is transformed to the "Return-Receipt-To: <sender@example.com>" construct.

Placing Specific Header/Value Combinations into the RFC-2822 Message

```
header <header: value>
```

If you wish to place a specific header/value combination into the RFC-2822 message that will be generated from a RAW file, you will need to use the HEADER macro listed in the RAW Headers section above. For example, if you want the header "Delivered-By: mail-machine@example.com" to be placed into the RFC-2822 message you would place this: "header <Delivered-By: mail-machine@example.com>" in the RAW message. Note that the "header" macro requires both the field and value. You can place as many "header" macros as you need into a RAW message.

DKIM Signing RAW Messages

```
x-flag=sign
```

Including this special command in a `*.raw` file will cause the RAW message to be DKIM signed. This should only be used in RAW messages that you have configured to bypass the Content Filter (by starting their filenames with "`p`" or "`P`"). You should not use this command in normal RAW Messages that are processed through the filter. Those messages will be signed normally.

All RAW messages that are generated by the Content Filter will use the `x-flag=sign` command automatically.

Sample RAW mail messages

Sample 1:

```
from <mdaemon@altn.com>
to <user01@example.com>

Hello John!
```

Sample 2:

```
from <user01@example.com>
to <user09@example.net>
subject <Requested Files>
```

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

```
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\docs\files\data01.zip, MIME> -X

Here are all those files you asked for.
```

7.4 Semaphore Files

MDaemon is equipped with support for Semaphore Files, which can be used for a variety of purposes, including causing MDaemon to perform specific actions. Periodically MDaemon will scan the \APP\ subfolder for the existence of these files. If it finds one, the associated behavior is triggered and the semaphore file is removed. This provides for a simple mechanism that enables administrators and developers to manipulate MDaemon without actually handling the interface. The following is a list of the semaphores and what they do:

FILENAME	ACTION
ACLFIX.SEM	Runs the ACL file cleanup routine.
ADDUSER.SEM	This semaphore creates new accounts. It is used to force MDaemon to append new records to the end of the USERLIST.DAT file without causing a potentially time consuming complete rebuild of the user database. Each line in this file must be a complete account record of the form specified in the Account Management Functions section of the MDaemon API (see MD-API.html in MDaemon's \docs\API\ subfolder). Multiple new accounts can be specified – one account record per line. MDaemon will process the file one line at a time and add each new account. You can create ADDUSER.LCK to lock the file while you are updating it and MDaemon will not touch ADDUSER.SEM until ADDUSER.LCK is deleted. To see a sample ADDUSER.SEM file open ADDUSER.SMP in your APP directory with a text editor.
ALERT.SEM	Displays in a pop-up window the contents of the semaphore file to all Webmail users who are logged in when the file is created. It is not, however, displayed to all users immediately—it is displayed to each user individually the next time his or her browser makes a request to the Webmail server. **Note:** Unlike other semaphore files, this file is Webmail specific. Instead of placing it in the \app\ directory it

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

must be placed in the \MDaemon\WorldClient\ directory.

ALIAS.SEM — Reloads aliases data file(s).

AUTORESPEXCEPT.SEM — Reloads the Autoresponder exception file(s).

BATV.SEM — Reloads Backscatter Protection (BATV) data file(s).

BAYESLEARN.SEM — This SEM manually starts the Bayesian learning process. This is like clicking the Learn button on the Bayesian tab of the Spam Filter. Note: this will start the Bayesian learning procedure even if you have Bayesian learning disabled.

BLACKLIST.SEM — Reloads the blacklist data files.

CFILTER.SEM — Reloads Content Filter rules, clears Content Filter cached data, reloads the Spam Filter's Allow List (no filtering) 675 file.

CLEARQUOTACOUNTS.SEM — The results of user quota checks are maintained in the quotacounts.dat file. If you wish to clear the cached quota value for a user, add the user's email address to this SEM file and then place it in the \app\ folder. If an asterisk (*) is on a line by itself, the entire file will be deleted thereby invalidating all cached quota counts.

DELUSER.SEM — You can use this semaphore file to delete one or more user accounts. Create a text file containing the addresses of each account that you want to be deleted (one address per line), name the file DELUSER.SEM and then move it to MDaemon's \app\ directory. MDaemon will delete the accounts and then delete the DELUSER.SEM file. If you wish to delete an account but not delete its mail folder, append "^" to the address (e.g. frank@example.com^).

DNS.SEM — Reloads the Windows DNS servers 99 and the Spam Filter's DNS settings.

DOMAINSHARING.SEM — Reloads domain sharing data file.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

EDITUSER.SEM	This semaphore is used to update specific user records within the USERLIST.DAT file without a potentially time consuming complete rebuild. To update any specific user records within USERLIST.DAT, create a file named EDITUSER.SEM that includes a complete replacement record, one record per line, for any user records you wish to edit. Each record must be constructed according to the USERLIST.DAT format outlined in the Userlist File Format knowledge base article, but it must begin with the original record's email address followed by a comma. MDaemon will process the EDITUSER.SEM file one line at a time. You can create EDITUSER.LCK to lock the file while you are updating it and MDaemon will not touch EDITUSER.SEM until EDITUSER.LCK is deleted. To see a sample EDITUSER.SEM file, open EDITUSER.SMP in your \APP\ directory with a text editor.
EXITNOW.SEM	Shuts down MDaemon.
GATEWAYS.SEM	For optimal performance, MDaemon keeps its list of gateways in memory. Create a GATEWAYS.SEM in MDaemon's APP directory for it to reload the gateways.dat file.
GREYLIST.SEM	Reloads Greylisting data file(s).
GROUPS.SEM	Reloads account grouping data file(s).
GRPLIST.SEM	Reloads the internal cache of Mailing List names.
HANGUPG.SEM	Forces a conditional hang-up of RAS device. MDaemon will wait for any pending mail sessions to close and will then hang-up the RAS session.
HANGUPR.SEM	Forces unconditional hang-up of RAS device. This is an immediate and unconditional hang-up without regard to mail sessions which may be in progress across the connection.
HOSTSCREEN.SEM	Reloads Host Screen data file(s).
IPSCREEN.SEM	Reloads IP Screen data file(s).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

IPSHIELD.SEM	The IPShield.dat file is cached in memory to increase access speed. Use IPSHIELD.SEM to reload the file into memory
LDAPCACHE.SEM	Reloads LDAP and gateway user data file(s).
LOCKSEMS.SEM	Prevents all semaphore file processing until user removes it.
LOGSETTINGS.SEM	Reloads log file settings.
MDSPAMD.SEM	Reloads the Spam Filter allow list and MDSPAMD, which forces it to reinitialize all its configuration data.
MINGER.SEM	Stops and then restarts the Minger 847 server.
MXCACHE.SEM	Reloads MX Cache data file(s).
NODNSBL.SEM	Reloads DNSBL allow list file.
NOPRIORITY.SEM	Forces MDaemon to reload the NoPriority.dat file.
ONLINE.SEM	MDaemon will create this semaphore file once it makes a successful connection using RAS to the ISP. MD will remove the semaphore once the connection has been terminated. This is useful if you want to know when MD is using the RAS sub-system.
POSTDIAL.SEM	MDaemon will create this file immediately after a connection made by MDaemon is taken down.
PREDIAL.SEM	MDaemon will create this file just before trying to use RAS/DUN. This will allow other software to detect when it should free the dialup port so that MDaemon can use it.
PRIORITY.SEM	Reloads Priority mail data file(s).
PROCBAD.SEM	Initiates delivery of Bad Queue content.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

PROCDIG.SEM	Initiates construction and delivery of mailing list digests.
PROCHOLDING.SEM	Initiates delivery of Holding Queue content.
PROCNOW.SEM	Initiates a check for remote mail and delivery of queued remote mail.
PROCREM.SEM	MDaemon will immediately go into mail processing mode and transact all remote mail.
PROCRETR.SEM	Initiates delivery of Retry Queue content.
PRUNE.SEM	Reloads auto-pruning settings.
PUBLICSUFFIX.SEM	Reloads the Public Suffix 537 file.
QUEUE.SEM	This semaphore file is used to enable/disable the mail queues. The file can contain any number of lines but each one has to contain one of the following strings (one per line): ENABLE INBOUND, ENABLE REMOTE, ENABLE LOCAL, or DISABLE INBOUND, DISABLE REMOTE, DISABLE LOCAL.
RESTART.SEM	Stops and then starts MDaemon.
RESTARTCF.SEM	Stops and restarts `CFEngine.exe` (the Content Filter executable).
RESTARTWC.SEM	Stops and restarts MDaemon Webmail. This only works when Webmail is running using its own built-in web server 313.
RELOADCACHE.SEM	Reloads all cached data settings and files except for Content Filter settings and files.
REVERSEEXCEPT.SEM	Reloads reverse lookups exception file.
SCHEDULE.SEM	Reloads schedule data file(s).
SPAMHONEYPOTS.SEM	Reloads spam honeypots data files(s)

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

SPF.SEM	Reloads SPF, DKIM, and VBR data files(s).
SUPPRESS.SEM	Reloads block list settings and clears cached domain settings.
TARPIT.SEM	Reloads tarpit and dynamic screening data file(s).
TRANSLAT.SEM	Reloads the header translation data files.
TRAY.SEM	Redraws MDaemon's icon in the system tray.
TRUST.SEM	Trusted domains and IP addresses are kept memory resident for optimal performance. If you need to reload these settings manually you can create TRUST.SEM to do it.
UPDATEAV.SEM	Initiates antivirus definition update.
UPDATESA.SEM	Initiates a Spam Filter update.
USERLIST.SEM	Reload the USERLIST.DAT file. Use this when you make modifications to the USERLIST.DAT and need MDaemon to reload it.
WATCHDOG.SEM	MDaemon will check for and remove this semaphore from the APP directory at approximately 10-20 second intervals. This file can be used by external apps to check if MDaemon is running. If this file remains in the APP directory for more than 20 seconds, that is a good indication that MDaemon is no longer running.

7.5 Route Slips

A message file waiting in a queue typically contains within its headers all the information that is needed to get the message delivered to the proper location. There are headers stored within the file (such as the X-MDaemon-Deliver-To header) which provide MDaemon with instructions as to where and to whom the message should be delivered. Sometimes however it is necessary or useful to override this information and

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

provide specific alternatives to where and to whom a message must be sent. Route Slips provide just such a mechanism. A route slip is a file that provides MDaemon with very specific instructions as to where and to whom a message should be sent. If a route slip is present for a particular message file then the settings within the route slip, and not those within the .MSG file itself, control where and to whom the message is sent.

Route slips end with the extension `.RTE`. For example, if a message file waiting to be sent is called "`MD0000.MSG`," then the corresponding route slip file for this message will be called `MD0000.RTE` and must be located in the same folder (mail queue) as the message file.

The format of a route slip is as follows:

```
[RemoteHost]
DeliverTo=example.net
```

This section of a route slip provides MDaemon with the server to which the corresponding `.MSG` file is to be sent. MDaemon will always attempt a direct connection to this host attempting to route the message in as short a time as possible. Only one host may be specified.

```
[Port]
Port=xxx
```

This switch specifies the port that the TCP/IP connection and delivery attempt should be made on. Port 25 is the default for SMTP email.

```
[LocalRcpts]
Rcpt0=address@example.com
Rcpt1=other-address@example.com
Rcpt2=yet-another-address@example.com

[RemoteRcpts]
Rcpt0=address@example.net
Rcpt1=other-address@example.net
Rcpt2=yet-another-address@example.net
```

These sections of the route slip allow you to specify any number of local and remote recipients who should receive a copy of the associated `.MSG` file. Local and remote recipient addresses must be kept separate and placed in their corresponding `[LocalRcpts]` and `[RemoteRcpts]` sections.

Route slips provide a good mechanism for delivering or redirecting email but they are not generally necessary. One use that MDaemon makes of route slips is in the case of "routed" mailing list mail. When you have a mailing list that is set to route a single copy of the list message to some remote host, a route slip is employed to accomplish this. It is a very efficient method of mail delivery when you have bulk addresses to deliver mail to since only a single copy of the message is required while any number of recipients of the message can be specified. Not all remote hosts allow this sort of routing to occur however. Since it is ultimately they who will have to deliver a copy of the message file to each address, some hosts place an upper limit on the number of recipients they will allow you to specify.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section VII

8 Creating and Using SSL Certificates

When using the SSL & TLS dialog to create certificates, MDaemon generates certificates that are self-signed. In other words, the issuer of the certificate, or Certificate Authority (CA), is the same as the owner of the certificate. This is perfectly valid and allowed, but because the CA won't already be listed in yours users' lists of trusted CAs, whenever they connect to Webmail or Remote Administration's HTTPS URL, they will be asked whether or not they wish to proceed to the site and/or install the certificate. Once they agree to install the certificate and trust your Webmail's domain as a valid CA they will no longer have to see the security alert message when connecting to Webmail or Remote Administration.

When connecting to MDaemon via a mail client such as Microsoft Outlook, however, they will not be given the option to install the certificate. They will be allowed to choose whether or not they wish to continue using the certificate temporarily, even though it isn't validated. Each time they start their mail client and connect to the server, they will have to choose to continue using the non-validated certificate. To avoid this you can either obtain a certificate from a Certificate Authority, such as Let's Encrypt 580, or you can export your self-signed certificate and distribute it to your users via email or some other means. Then, they can manually install and trust your certificate to avoid future warning messages.

Creating a Certificate

To create a certificate from within MDaemon:

1. Move to the SSL & TLS dialog within MDaemon (click **Security » Security Settings » SSL & TLS » MDaemon**).
2. Check the box labeled, **Enable SSL, STARTTLS, and STLS**.
3. Click **Create Certificate**.
4. In the text box labeled, **Host name**, enter the domain to which the certificate belongs (for example, "*mail.example.com*").
5. Type the name of the organization or company that owns the certificate into the text box labeled, "*Organization/company name*".
6. In "*Alternative host names...*," type all other domain names that your users will be using to access your server (for example, "`*.example.com`", "`example.com`", "`mail.altn.com`", and so on).
7. Choose a length for the encryption key from the drop-down list box.
8. Choose the Country/region where your server resides.
9. Click **OK**.

Using Certificates Issued by a Third-party CA

If you have purchased or otherwise generated a certificate from some source other than MDaemon, you can still use that certificate by using the Microsoft Management Console to import it into the certificate store that MDaemon uses. To do so in Windows XP:

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

1. On your Windows toolbar, click **Start » Run...** and then type "**mmc /a**" into the text box.
2. Click **OK**.
3. In the Microsoft Management Console, click **File » Add/Remove Snap-in...** on the menu bar (or press **Ctrl+M** on your keyboard).
4. On the Standalone tab, click **Add...**
5. On the *Add Standalone Snap-in* dialog, click **Certificates**, and then click **Add**.
6. On the *Certificates snap-in* dialog, choose **Computer account**, and then click **Next**.
7. On the *Select Computer* dialog, choose **Local computer**, and then click **Finish**.
8. Click **Close**, and click **OK**.
9. Under *Certificates (Local Computer)* in the left pane, if the certificate that you are importing is self-signed, click **Trusted Root Certification Authorities** and then **Certificates**. If it is not self-signed then click **Personal**.
10. On the menu bar, click **Action » All Tasks » Import...**, and click **Next**.
11. Enter the file path to the certificate that you wish to import (using the Browse button if necessary), and click **Next**.
12. Click **Next**, and click **Finish**.

MDaemon will only display certificates that have private keys using the Personal Information Exchange format (PKCS #12). If your imported certificate does not appear in the list then you may need to import a `*.PEM` file, which contains both a certificate key and private key. Importing this file using the same process outlined above will convert it to the PKCS #12 format.

Using Let's Encrypt to Manage Your Certificate

Let's Encrypt is a Certificate Authority (CA) that provides free certificates via an automated process designed to eliminate the currently complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites.

To support using Let's Encrypt's automated process to manage a certificate, the Let's Encrypt 580 screen is provided to help you easily configure and run the PowerShell script included in the "`MDaemon\LetsEncrypt`" folder. Running the script will set up everything

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

for Let's Encrypt, including putting the necessary files in the Webmail HTTP folder to complete the http-01 challenge. It uses the SMTP host name[177] of the default domain[174] as the domain for the certificate, includes any *Alternate host names* you have specified, retrieves the certificate, imports it into Windows, and configures MDaemon to use the certificate for MDaemon, Webmail, and Remote Administration. Further, the script creates a log file in the "`MDaemon\Logs\`" folder, called `LetsEncrypt.log`. This log file is removed and recreated each time the script runs, and it includes the starting date and time of the script. Also, notification emails will be sent when errors occur if you specify an *Admin email for notifications*. See the Let's Encrypt[580] topic for more information.

See:

SSL & TLS[561]

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Section

9 Glossary

ACL—Stands for **A**ccess **C**ontrol **L**ists. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access to your folders to other users whom also have accounts on your mail server. Further, you can set permissions governing the extent to which each user has control over those folders. For example, you can designate whether or not a user is allowed to delete messages, flag them as read or unread, copy messages to folders, create new subfolders, and so on. Only email clients that support ACL can be used to share this access and set permissions. However, if your email client doesn't support ACL you can still set these permissions from the MDaemon interface.

ACL is fully discussed in RFC 2086, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII—Pronounced as-key, ASCII is an acronym for "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". It is the worldwide standard code for representing all upper and lower-case Latin letters, numbers, and punctuation as a 7 digit binary number, with each character assigned a number from 0 to 127 (i.e. 0000000 to 1111111). For example, the ASCII code for uppercase M is 77. The majority of computers use ASCII codes to represent text, which makes it possible for them to transfer data to other computers. Most text editors and word processors are capable of storing files in ASCII format (sometimes called ASCII files). However, most data files—particularly those containing numeric data—are not stored in ASCII format.

Several larger character sets have 128 additional characters because they use 8 bits instead of 7. These extra characters are used to represent symbols and non-English characters. The DOS operating system uses a superset of ASCII called extended ASCII or high ASCII. A standard that is closer to universal, however, is ISO Latin 1, which is used by many operating systems and Web browsers.

ATRN—See ETRN and ODMR below.

Attachment—A file attached to an email message. Most email systems only support sending text files as email, therefore if the attachment is a binary file or formatted text file (e.g. a word processor document), it must first be encoded as text before it is sent and then decoded once it is received. There are a number of encoding schemes—two of the most prevalent being Multipurpose Internet Mail Extensions (MIME) and Unix-to-Unix encode (Uuencode). For incoming messages, MDaemon can be configured to either leave the decoding process to the recipient's email client or automatically decode attachments and store them in a specific location before delivering the message to the local user.

Backbone—A line or series of connections that form the major pathway within a network. This term is relative since the non-backbone lines in a large network might be larger than the backbone in a smaller network.

Bandwidth—The amount of data that can be transmitted in a fixed amount of time through a network or modem connection, usually measured in bits-per-second (bps).

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

A full page of English text is about 16,000 bits, which a fast modem could transfer in about 1 to 2 seconds. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

A good illustration of bandwidth is a highway. The highway represents the connection while the cars traveling on it represent the computer data. The wider the highway (the greater the bandwidth) the more cars that will be able to travel on it.

Baud—Baud rate is a measure of how frequently carrier signals change value on a phone line. It is a reference to the speed at which a modem transmits data. Usually, slower modems are described in terms of Baud rate while higher speed modems are described in bits per second. "Baud rate" and "bits per second" are not necessarily synonymous terms since each signal can encode more than one bit in high-speed connections.

Bit—A single **B**inary dig**it**. It is the smallest unit of computer data; a single digit number in base-2 (i.e. 0 or 1). It is usually abbreviated with a lower case "b" as in "bps" (bits per second). A full page of text is approximately 16,000 bits.

Bitmap—Most pictures you see on your computer, including all the ones found on the Internet, are bitmaps. A bitmap is a really just a map of dots (or bits) that looks like a picture as long as you're not to close to the screen, or have the bitmap magnified too much, to see the shape they make. Common Bitmap file types include BMP, JPEG, GIF, PICT, PCX, and TIFF. Because bitmap images are made up of a bunch of dots, if you zoom in on a bitmap it looks blocky rather than smooth. Vector graphics (usually created in CorelDraw, PostScript, or CAD formats) scale up much better because they are geometric shapes generated mathematically rather than simply being made of seemingly "random" dots.

Bps—"**B**its **P**er **S**econd" is a measurement of how fast computer data can be moved from one place to another. For example, a 33.6 kbps modem can transfer 33,600 bits per second. Kilobits (1000 bits) per second and megabits (1.000,000 bits) per second are abbreviated "Kbps" and "Mbps" respectively.

Browser—Short for "Web browser", it is an application used to display web pages. It interprets HTML code, text, hypertext links, images, JavaScript, and so on. The most widely distributed browsers are Internet Explorer and Netscape Communicator.

Byte—A set of bits (usually eight) that represent a single character. There are 8 bits in a byte, sometimes more, depending on how the measurement is being made. "Byte" is abbreviated with an uppercase "B".

Cache—Pronounced like "cash". There are various types of caches, but all are used to store recently used information so that it can be accessed quickly later. For example, a web browser uses a cache to store the pages, images, URLs, and other elements of web sites that you have recently visited. When you return to a "cached" page the browser will not have to download these elements again. Because accessing the cache on your hard disk is much faster than accessing the Internet, this significantly speeds up browsing.

MDaemon's IP Cache stores the IP addresses of domains to which you have recently delivered messages. This prevents MDaemon from having to lookup these addresses

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

again when delivering additional messages to the same domains. This can greatly speed up the delivery process.

CGI—Common **G**ateway **I**nterface is a set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. However, a CGI program is usually a small program that takes data from a web server and does something with it, like putting the content of a form into an email message, or doing something else with that data. CGI programs are often stored in a web site's "cgi-bin" directory and therefore appear in a URL that accesses them, but not always.

cgi-bin—The most common name of the directory on a web server in which CGI programs are stored. The "bin" part of "cgi-bin" is short for "binary" because most programs used to be referred to as "binaries". In reality, most cgi-bin programs are text files; scripts executed by programs located elsewhere.

CIDR—"**C**lassless **I**nter-**D**omain **R**outing" is a new IP addressing system that replaces the older system, which was based on classes A, B, and C. CIDR IP addresses look like normal IP addresses followed by a slash and number, called the IP prefix. For example:

123.123.0.0/12

The IP prefix defines how many addresses are covered by the CIDR address, with lower numbers covering more addresses. In the above example, the IP prefix of "/12" can be used to address 4,096 former Class C addresses.

CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

CIDR is addressed in RFCs 1517-1519, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Client—A software program that is used to contact and obtain data from or send data to a *server* software program. The server is usually located on another computer, either on your local network or at some other location. Each *client* program is designed to work with one or more specific kinds of *server* programs, and each server requires a specific kind of client. A web *browser* is a specific kind of client that communicates with web *servers*.

Common Gateway Interface—See CGI above.

Cookie—In computer terminology, a *cookie* is data sent by a web server to your web browser, which is saved and later used for various purposes when you return to the same site or go to another location on the site. When a web server receives a request from a web browser that includes a cookie, it is able to use the information the cookie contains for whatever purpose it was designed, such as customizing what

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

is sent back to the user, or for keeping a log of the user's requests. Typically, cookies are used for storing passwords, usernames, preferences, shopping cart information, and similar things related to the site to which they correspond so that the site can appear to "remember" who you are and what you've done there.

Depending on your browser's settings, you may accept or not accept the cookies, and save them for various amounts of time. Usually cookies are set to expire after a predetermined amount of time and are saved in memory until the web browser software is closed down, at which time they may be saved to disk.

Cookies **cannot** read your hard drive. They can, however, be used to gather information about you related to your usage of their particular web sites, which would be impossible without them.

Dial-up Networking—A component in Windows that enables you to connect your computer to a network via a modem. Unless your computer is connected to a Local Area Network (LAN) with access to the Internet, you will need to configure Dial-Up Networking (DUN) to dial a Point of Presence (POP) and log on to your Internet Service Provider (ISP) before you will have Internet access. Your ISP may need to provide certain information, such as the gateway address and your computer's IP address.

DUN is accessed through the My Computer icon. A different dialup profile can be configured for each online service that you use. Once configured, you can copy a profile shortcut to your desktop so that all you need to do to make a connection is double-click the connection icon.

Default—This term is used to refer to the preset value for options in computer programs. Default settings are those settings which are used when no specific setting has been designated by the user. For example, the default font setting in Netscape Communicator is "Times". This setting will remain "Times" unless you change it to something else. Default settings are usually the value that most people will choose.

Frequently the term *default* is also used as a verb. If a custom setting won't work or the program lacks some needed bit of data for completing a task, it will usually "default" to a specific setting or action.

DHCP—An acronym for "**D**ynamic **H**ost **C**ontrol **P**rotocol". Network servers use this protocol to dynamically assign IP addresses to networked computers. A DHCP server waits for a computer to connect to it and then assigns it an IP address from a stored list.

DHCP is addressed in RFC-2131, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2131.txt

Domain Gateway—See Gateway below.

Domain Name—This is the unique name that identifies an Internet web site. For example, "mdaemon.com" is the domain name of MDaemon Technologies. Each domain name contains two or more parts separated by dots; the leftmost part is the most specific while the rightmost part is the most general. Each domain name also points to the IP address of a single server, but a single server may have more than

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

one domain name. For example, "mail.mdaemon.com", "smtp.mdaemon.com", and "example.com" could all point to the same server as "mdaemon.com", but "mdaemon.com" could not point to two different servers. There are, however, methods for designating alternate servers to which clients will be directed if the main server goes down or is otherwise unavailable.

It is also common for a domain name to be registered but not be connected to an actual machine. The usual reason for this is the domain name's owner hasn't created a web site yet, or so that they can have email addresses at a certain domain without having to maintain a web site. In the latter case, there must be a real Internet machine to handle the mail of the listed domain name.

Finally, it is common to see the term "domain name" shortened and referred to as simply "domain". The word "domain" has other meanings and can refer to other things, such as a Windows NT domain or a class of values, so you should be aware of the distinction in order to avoid confusion.

Domain Names are addressed in RFCs 1034-1035, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP—Developed by MDaemon Technologies to be a part of the MDaemon server, DomainPOP makes it possible to provide email services for an entire LAN or workgroup from a single ISP POP mailbox. In the past, unless a company's email server had on constant "live" connection to the Internet, the only way to provide Internet email services to a workgroup was for each person to have their own mailbox on the company's ISP from which they could collect their mail. With DomainPOP only a single mailbox is required. The ISP pools all mail for the company's domain name into the mailbox from which it is periodically collected by DomainPOP. Then, DomainPOP parses the messages to determine the intended recipients of each and distributes them to the appropriate local user mailboxes. Thus email is provided for an entire network from a single dialup ISP account.

Download—The process by which your computer retrieves or obtains data from another computer. For example, information is obtained from the Internet by *downloading* it from other computers. The reverse of this is *uploading*. If you wish to send information to another computer then you will *upload* it to them.

Driver—A small program that communicates with a certain hardware device. Drivers contain information needed by the computer and other programs to control and recognize the device. Windows-based computers often have drivers packaged as a dynamic link library (DLL) file. Most hardware devices used with Macs do not need drivers, but when a driver is necessary it will usually come in the form of a System Extension.

DUN—See Dial-up Networking above.

Email—Stands for "Electronic mail". This term also appears in the forms: "E-mail", "e-mail", and "email"; all have the same meaning. Email is the transmission of text messages over communications networks. Most computer networks have some form of email system. Some email systems are confined to a single computer network, but

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

others have gateways to other networks (which enables them to communicate with multiple locations), or to the Internet (which enables them to send email anywhere in the world).

Most email systems include some form of *email client* (also referred to as a *mail client* or just *client*) which contains a text editor and other tools for composing messages, and one or more *servers* which receive the email from the clients and route it to its appropriate destination. Typically, a message is composed using the client, passed to a server for delivery to the *email address* (or addresses) specified in the message, and then routed by the server to another server that is responsible for storing messages destined for that address. If the message's destination is a local address for which the original server is responsible then it may be stored on the original server rather than routed to another. Last, the recipient of the message will connect to their server and retrieve the message by using their email client. This entire process of transferring an email message from your client to its destination server usually only takes a few seconds or minutes.

Besides containing simple text, email messages may also include file *attachments*. These attachments can be any type of file that you desire: pictures, text files, program files, other email messages, and so on. However, since most email systems only support sending text files, attachments must first be encoded (converted to a text format) before they can be sent, and then decoded when they arrive at their final destination. This process is usually done automatically by the sending and receiving mail clients.

All Internet Service Providers (ISPs) offer email. Most also support gateways so that you can exchange email with users of other email systems. Although there are many different protocols used for processing email by many different email systems, several common standards make it possible for users on virtually all systems to exchange messages.

Email Address—A name or string of characters that identifies a specific electronic mailbox on a network to which email can be sent. Email addresses are the locations to and from which email messages are sent. Email servers need email addresses so that they can route messages to their proper destinations. Different types of networks have different formats for email addresses, but on the Internet all email addresses have the form: "mailbox@example.com".

For example,

```
Michael.Mason@altn.com
```

Email Client—Also called a *mail client* (or just *client*), an *email client* is a software application that enables you to send, receive, and organize email. It is called a client because email systems are based on client-server architecture; a client is used to compose the email and then send it to a server, which then routes it to the recipient's server from which it will be retrieved by the recipient's client. Usually, email clients are separate software applications installed on the user's machine, but products such as MDaemon contain a built in Webmail client that is "served" to the user's web browser. Thus, their browser is used as the client rather than needing to install one on their machine. This greatly enhances the portability and convenience of email.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Encryption—A security measure, *encryption* is the coding or scrambling of information in a file so that it will only be intelligible when it has been decoded or decrypted. Encryption is frequently used in email so that if a third party intercepted the email they would not be able to read it. The message is encrypted when it is sent and then decrypted at its final destination.

Ethernet—The most common type of connection used in a Local Area Network (LAN). Two of the most widely used forms of Ethernet are 10BaseT and 100BaseT. A 10BaseT Ethernet can transfer data at speeds up to 10 mbps (megabits per second) through a cable or wireless connection. A 100BaseT Ethernet transfers data at speeds up to 100 mbps. A Gigabit Ethernet can transfer data at rates up to 1000 mbps and is employed by some Apple computers.

ETRN—An acronym meaning **E**xtended **TURN**. It is an extension to SMTP that enables an SMTP server to send a request to another SMTP server to send, or "dequeue", mail that is being held for it. Because SMTP by itself cannot request mail (email is usually requested via the POP or IMAP protocols), this makes it possible for the SMTP server making the ETRN request to cause the remote server to start an SMTP session and begin sending the stored email to the host specified in the request.

The `TURN` command used for this purpose posed a security risk because it caused the SMTP session to reverse direction and begin sending the stored mail immediately without any verification or authentication that the requesting server was actually who it claimed to be. `ETRN` starts a new SMTP session rather than reversing direction. Thus if the server making the request is a "spoofed" host, the sending server will still attempt to deliver the mail to the real host instead. There is now a proposed standard that introduces Authenticated TURN (`ATRN`), which, like `TURN`, reverses the direction of the SMTP session but requires authentication before doing so. This new standard is On-Demand Mail Relay (ODMR). MDaemon supports both ETRN and ODMR's ATRN.

ETRN is addressed in RFC 1985, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1985.txt

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ—Pronounced together as "fack" or as separate letters "F-A-Q", FAQ stands for "**F**requently **A**sked **Q**uestions". FAQs are documents that provide answers to the most commonly asked questions on a given subject. They usually appear in some form of list format with each question listed first followed by its answer. In larger FAQs, oftentimes all of the questions will be listed at the beginning of the document with references (or hyperlinks, in online FAQs) to the location of the question and answer in the document. FAQs are frequently used as a starting point for technical support and instructions—a great deal of time and effort can be saved if you have access to a FAQ that answers your question instead of being forced to contact technical support.

File Transfer Protocol—See FTP below.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Firewall—In computer terminology, a *firewall* exists when you undertake security measures, through either software or hardware means, to separate a computer network into two or more parts, or otherwise limit access to it to certain users. For example, you might want to let everyone view the home page of a web site hosted on your network but allow only your employees to get to an "employee only" area. Regardless of the method that you use to accomplish this—requiring a password, allowing connections from only certain IP addresses, or the like—the employee area is said to be behind a firewall.

FTP—Acronym for "**F**ile **T**ransfer **P**rotocol." It is a common and efficient method of transferring files via the Internet from one computer to another. There are specific client/server applications designed for this purpose called "FTP servers" and "FTP clients"—FileZilla, for example, is one of the most common clients. Usually FTP clients can perform quite a few other functions besides simply transferring files and are thus highly useful products. Some web browsers also contain support for File Transfer Protocol, though sometimes for downloading only. Additionally, most FTP servers are "anonymous FTP", which means that anyone can log in to them in order to download files—usually by specifying "anonymous" as the user name and then your email address as the password. Oftentimes you can download files from anonymous FTP sites without having to log in at all—they can be retrieved by simply clicking on a link. For browsers that support FTP, usually all that needs to be done is to connect to the FTP site using "ftp://..." in its URL rather than "http://..."

FTP is addressed in RFC-959, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc959.txt

Gateway—Computer hardware or software that translates data between two applications or networks with protocols that are dissimilar. "Gateway" is also used to describe any means by which access is provided from one system to another. For example, your ISP is a gateway to the Internet.

MDaemon Messaging Server can function as an email gateway for other domains through the use of its Domain Gateways feature. It acts as an intermediary, or Gateway, by collecting the domain's email and then holding it until the domain collects it. This is useful both for domains that do not maintain a continuous connection to the Internet and for domains that require a backup server in case theirs goes down.

GIF—"**G**raphics **I**nterchange **F**ormat" is a popular format for image files and is the most common format of images found on the Internet. GIF uses indexed colors or a palette of a certain number of colors, which greatly reduces file size—especially when the image contains large areas of the same color. The reduced size enables them to be quickly transferred between systems and accounts for their popularity on the Internet. The GIF compression formula was originally developed by CompuServe and thus you will often see GIF referred to as CompuServe GIF.

Graphical User Interface—See GUI below.

GUI—Pronounced "gooey", this acronym stands for "**G**raphical **U**ser **I**nterface". A GUI makes it possible to interact with your computer or application by using a pointing device to click graphical elements on the screen rather than typing in text at a command line. The Microsoft Windows and Apple Mac operating systems are both

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

GUI-based, but—although first introduced by Apple—the idea of a graphical user interface actually originated from Xerox.

Host—Any computer on a network that acts as a server for other computers on the same network. The host machine may be running a web server, email server, or other services, and it is common for it to provide several services at once. Host is also often used in the verb form "to host". For example, a machine running an email server would be "hosting" the email.

On peer-to-peer networks it is common for machines to be both hosts and clients at the same time. For example, your machine may host your network's printer but also be used by you as a client to collect email and download files from another host.

HTML—An acronym for "**H**ypertext **M**arkup **L**anguage. It is the coding language used to create Hypertext documents used on the World Wide Web. Simply put, an HTML document is a plain text document that contains formatting codes and tags that the user's web browser interprets and presents as a web page complete with formatted text and colors. For example, a browser receiving an HTML document containing the text "<B>Text</B>" would present the word "Text" in Bold. Because plain text files are very small, this makes it possible for them to be quickly transferred over the Internet.

HTTP—Hyper**t**ext **T**ransfer **P**rotocol (HTTP) is the protocol used for transferring *hypertext* files between computers over the Internet. HTTP requires a client program on one end (usually a web browser) and an HTTP server on the other end.

HTTP is addressed in RFC-2616, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2616.txt

Hypertext—Any text that contains a hyperlink or jump to another document or place within the same document is called hypertext. Sometimes the text is also called a hypertext link or simply link. Hypertext can be either a word or phrase and has the link embedded in it so that clicking it will move you to the "book marked" location or cause the linked document to be displayed. Usually hypertext links are apparent because the text is underlined and a different color, but that is not required. Sometimes hypertext will look no different than normal text, but will almost always be indicated by some sort of graphical change to your pointer when the mouse pointer is paused over it.

Hypertext Markup Language—See HTML above.

IMAP—Developed by Stanford University, **I**nternet **M**essage **A**ccess **P**rotocol (IMAP) is a protocol used for managing and retrieving email messages. The latest version is IMAP4 and is similar to POP3 but with a number of additional features. IMAP4 is best known as a protocol used for managing email messages on the server rather than on the user's local machine—messages can be searched for keywords, organized in folders, specifically selected for downloading, and other features, all while they are still on the server. Thus IMAP places less demand on the user's machine and centralizes email so that it can be accessed from multiple locations.

IMAP is addressed in RFC-2060, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2060.txt

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

IMAP4 ACL extension—See ACL above.

Internet—The Internet was created in 1969 by the United States military, originally to be a communications network that couldn't be destroyed during a nuclear war. It now consists of millions of computers and networks all over the world. By design, the Internet is decentralized—it is not controlled by any company, organization, or country. Each host (or machine) on the Internet is independent of the others and can provide whatever information or services its operators wishes to make available. Nevertheless, most information transferred over the Internet at some point passes through "backbones", which are extremely high-bandwidth high-speed connections controlled by the largest Internet Service Providers and organizations. Most people access the Internet through an online service such as AOL or through an Internet Service Provider (ISP) that maintains or is connected to one of these backbones.

Many people believe that the *World Wide Web* (WWW) and the Internet are the same thing, but this is not the case. The WWW is only one part of the Internet not the Internet itself. It is the most visible and popular part, largely driven by commerce, but still only a part.

Intranet—Simply put, an intranet is a small or private Internet used strictly within a company or organization's network. Although intranets vary widely from organization to organization, they may contain any of the features available on the Internet. They may have their own email systems, file directories, web pages to be browsed, articles to be read, and so on. The primary difference between an intranet and the Internet is that an intranet is relatively small and confined to an organization or group.

IP—An acronym for "**I**nternet **P**rotocol" (e.g. as in TCP/IP). Internet protocols make it possible for data to be transferred between systems over the Internet. Regardless of each machine's platform or operating system, if the same Internet Protocol is used by each machine then they will be able to transfer data to each other. The term "IP" is also commonly used as a further abbreviation of the term "IP Address". The current standard Internet Protocol is IP version 4 (IPv4).

Internet Protocol is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

IP Address—Occasionally called an IP Number, IP Address stands for **I**nternet **P**rotocol Address and is used to identify a particular TCP/IP network and the hosts or machines on that network. It is a 32-bit numeric address containing four numbers between 0 and 255 separated by dots (e.g. "127.0.0.1"). Within an isolated network, each computer must have a unique IP address, which can be assigned at random. But, every computer on the Internet must have a registered IP address to avoid duplication. Each Internet IP address can be either static or dynamic. Static addresses do not change and always represent the same location or machine on the Internet. Dynamic IP addresses change and are usually assigned by an ISP to computers that are only on the Internet temporarily—such as when a user with a dial-up account accesses the Internet. However, it is still possible for a dial-up account to have a static IP address assigned to it.

ISPs and large organizations usually attempt to acquire a range or set of IP addresses from the InterNIC Registration Service so that all clients on their network

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

or using their service may have similar addresses. These sets are broken up into three classes: Class A, B, and C. Class A and B sets are used by very large organizations and support 16 million and 65,000 hosts respectively. Class C sets are for smaller networks and support 255 hosts. Class A and B sets are now very difficult to get due to the shortage of available addresses; consequently most companies have to settle for multiple class C sets instead. Because of this IP address shortage, there is a new IP address protocol called Classless Inter-domain Routing (CIDR) that is gradually replacing the older system.

The current Internet Protocol standard, IPv4, is addressed in RFC-791, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc791.txt

IP version 6 (IPv6) is addressed in RFC-2460 at:

http://www.rfc-editor.org/rfc/rfc2460.txt

CIDR is addressed in RFCs 1517-1519 at:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

IP Number—See *IP Address* above.

ISP—An **I**nternet **S**ervice **P**rovider (ISP) is a company that provides Internet access and services to the end user. Most ISPs provide multiple Internet services to their customers, such as: WWW access, email, access to newsgroups and news servers, and so on. Typically, users will connect to their ISP via dial-up, or some other form of connection, and then the ISP will connect them to a router, which will in turn route them to the Internet backbone.

Java—Developed by Sun Microsystems, Java is a network-oriented computer programming language with syntax much like C/C++ but is structured around classes instead of functions. In Internet applications it is commonly used for programming applets, which are small programs embedded in web pages. These programs can be automatically downloaded and executed by a user's browser in order to provide a large number of functions that wouldn't ordinarily be possible with just HTML or other scripting languages, and without fear of viruses or harm to your computer. Because Java is both efficient and easy to use, it is becoming popular among many software and hardware developers.

JavaScript—Not to be confused with Java, JavaScript was developed by Netscape as a scripting language designed to extend the capabilities of HTML and create interactive web pages. It is a highly pared down and easy to use programming language, which makes it much easier to use than Java and other languages but also limits it to some degree. It spite of its limitations it is very useful for adding a number if interactive elements to web sites. For example, JavaScript is useful when you want data to be preprocessed before it is submitted to the server, or when you want your pages to respond to user interaction with links or form elements. It can also be used to control plug-ins and applets based on user choices, and to

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

accomplish a large number of other functions. JavaScript is included within the text of HTML documents and is interpreted by web browsers in order to perform the functions.

JPEG—A graphics file format that is very efficient at compressing high-color and photographic images—much more so than the GIF format. While GIF is the best choice for images containing regular shapes and large areas of repeating color patterns, JPEG is much more suited to images with irregular patterns and large numbers of colors. JPEG is the most commonly used format for high-color and photographic images on the Internet. The acronym JPEG stands for "**J**oint **P**hotographic **E**xperts **G**roup"—the group that developed the format.

Kbps—Commonly used when referring to modem speeds (e.g. 56 Kbps), this acronym stands for "**K**ilo**b**its **P**er **S**econd". It is the number of kilobits (1000 bits) of data being moved or processed every second. Note that this is kilo*bits* not kilo*bytes*—a kilobyte would be eight times more data than a kilobit.

Kilobyte—A kilobyte (K or KB) is a thousand bytes of computer data. Technically it is 1024 bytes (2^10 = 1024) but in normal usage it is usually rounded off to 1000 for simplicity.

LAN—A **L**ocal **A**rea **N**etwork (LAN) is a computer network limited to a single building or area, usually having all nodes (computers or workstations) connected together with some configuration of wires or cables or some other form of media. Most large companies have a LAN, which greatly simplifies the management and sharing of information amongst employees and offices. Most LANs utilize some form of email or chat system, and share devices such as printers in order to avoid having to have a separate device for each station. When the network's nodes are connected together via phone lines, radio waves, or satellite links it is called a Wide Area Network (WAN) instead of LAN.

Latency—The time it takes a data packet to move across a network connection. While a data packet is being sent, there is "latent" time during which the sending computer waits for a confirmation that the packet has been received. In addition to bandwidth, latency is one of the factors that determine the speed of your connection.

LDAP—Lightweight **D**irectory **A**ccess **P**rotocol (LDAP) is an online directory service protocol that is a simplification of Directory Access Protocol (DAP). The directory system is in a hierarchical structure consisting of the following levels: The "root" or starting directory, country, organization, organizational unit, and individual within that unit. Each LDAP entry is a collection of attributes with a unique identifier, called a distinguished name (DN). Because it is an open protocol, is efficient, and has the ability to be distributed across many servers, LDAP may eventually make it possible for virtually any application on any platform to access directory information for locating email addresses, organizations, files, and so on worldwide.

LDAP is addressed in RFC-2251, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2251.txt

Link—See *Hyperlink* above.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

List server—A server application that is used to distribute email messages to multiple recipients by simply addressing the message to a single address. Simply put, when an email message is addressed to a *mailing list* maintained by the list server it will be automatically broadcast to the members of the list. Mailing lists typically have a single normal email address (for example, listname@example.com) but that address refers to a whole list of recipients rather than to a specific person or mailbox. When someone *subscribes* to a mailing list, the list server will automatically add the address to the list and distribute future emails directed to the list to that address, or member, and all other members. When someone unsubscribes, the list server simply removes the address so that it will receive no further list messages.

Frequently the term listserv is used generically to refer to any mailing list server. However, Listserv® is a registered trademark of L-Soft international, Inc. and is a specific program developed by Eric Thomas for BITNET in 1986. Besides other list servers, MDaemon is equipped with an entire suite of list server, or mailing list, functions and features.

Logon—a unique code or series of characters used to gain access or otherwise identify yourself to a server or machine. In most cases a password must accompany the logon in order to gain access.

There are many terms used synonymously with "logon", such as *login*, *username*, *user name*, *user ID*, *sign-in*, and others. Frequently, "logon" is also used as a verb. For example, "I am going to *logon* to the mail server". In that context, however, the more common usage (and perhaps more proper) is "I am going to *log on* to the mail server".

Mailbox—An area in memory or on a storage device that is assigned to a specific email address and where email messages are stored. In any email system, each user has a private mailbox in which messages are stored when that user's mail server receives them. It is also common for the term "mailbox" to be used when referring to the leftmost portion of an email address. For example, "user01" in "user01@example.com" is the mailbox while "example.com" is the domain name.

Mailing List—Also called email groups, a mailing list is a list or group of email addresses identified by a single email address. For example, "listname@example.com". Typically when a list server receives an email message addressed to one of its mailing lists that message will be automatically distributed to all of the list's members (i.e. the addresses included in the list). MDaemon is equipped with an extensive suite of mailing list features that enable lists to be public or private (anyone can post or join, or only members can post or join), moderated (each message must be approved by someone before it will go to the list), sent in digest format or as individual messages, and used in a variety of other ways.

Megabyte—Though technically 1,048,576 bytes (or 1024 kilobytes), a megabyte is more commonly rounded off and used to refer to a million bytes. Megabyte is abbreviated: "MB", as in "20 MB".

MIME—Defined in 1992 by the Internet Engineering Task Force (IETF), **M**ultipurpose **I**nternet **M**ail **E**xtensions (MIME) is the standard encoding method used for attaching non-text files to standard Internet email messages. Because typically only plain text files can be transferred via email, non-text files must first be encoding into a plain text format and then decoded after reaching their destination. Thus, an email program is said to be MIME Compliant if it can both send and receive files using the

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MIME standard. When a MIME-encoded message attachment is sent, generally both the type of file being sent and the method that should be used to turn it back into its original form are specified as part of the message. There are many predefined MIME content types, such as "image/jpeg" and "text/plain". However, it is also possible to define your own MIME types.

The MIME standard is also used by web servers to identify the files they are sending to web browsers. Because web browsers support various MIME types, this enables the browser to display or output files that are not in HTML format. Further, by updating the browser's lists of MIME-Types and the software used for handling each type, new file formats can be readily supported.

MIME is addressed in RFCs 2045-2049, which can be viewed at:

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—A server (usually an FTP server) that has a copy of the same files that are on another server. Its purpose is generally to provide an alternate location from which the mirrored files can be downloaded should the original server go down or be overloaded. The term "mirror" can also refer to a configuration whereby information is written to more than one hard disk simultaneously. This is used as a redundancy measure so that if one disk fails the computer can continue to operate without losing any vital data.

Modem—An acronym derived from **mo**dulator-**dem**odulator. A modem is a device connected to a computer that enables the transfer of data to other computers over telephone lines. The modem converts the computer's digital data to an analog format (modulates) and then transmits it to another modem where the process is reversed (demodulates). Put simply, a modem is an analog-to-digital and digital-to-analog converter. The speed at which the data is transferred is expressed in either baud-rate (e.g. 9600 baud) or kilobits per second (e.g. 28.8 kbps).

MultiPOP—A component of MDaemon that can be configured to collect email, via the POP3 protocol, simultaneously from various email servers on behalf of MDaemon's users. This makes it possible for MDaemon account holders who have email accounts elsewhere on other email servers to have that email collected and pooled with their MDaemon account email. Thus storing all of their email in a single mailbox.

NAT—See Network Address Translation below.

Network—Two or more computers connected together in some fashion. The purpose of a network is to enable the sharing of resources and information between multiple systems. Some common examples are: multiple computers sharing printers, DVD-ROM drives, hard disks, individual files, and so on.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

There are many types of networks, but the most broadly defined types are Local Area Networks (LANs) and Wide Area Networks (WANs). In a LAN, the individual computers (or nodes) are geographically close together—usually in the same building. They are also usually connected together directly with wires, although wireless connections are becoming common as well. The nodes in a WAN are usually farther apart (in another building or city) and connected via telephone lines, satellite hook-up, or some other form of connection.

The Internet itself is a network. It is often described as a network of networks.

Network Address Translation—Network address translation (NAT) is a system whereby two sets of Internet Protocol addresses (IP addresses) are used by a single network —one for external traffic and the other for internal traffic. This is mainly used as a firewall measure to help ensure network security. Your computer will appear to have a certain IP address to computers outside your LAN while your actual IP address is altogether different. Hardware or software placed "between" your network and the Internet performs the translations between the two addresses. Using this method, it is common for multiple computers in a LAN to "share" one company IP address. Thus there is no way for someone outside your network to know your actual address and directly connect to your computer without it first being qualified or authenticated during the translation.

Network Interface Card—A network interface card (NIC) is a computer circuit board that enables a computer to be connected to a network. NICs provide a full-time network connection whereas a modem (used by most home computers to dial-in to a network via telephone lines) usually provides only a temporary connection. Most NICs are designed for specific types of networks and protocols, such as Ethernet or token ring and TCP/IP.

Network News Transfer Protocol—See NNTP below.

NIC—See Network Interface Card above.

NNTP—Network **N**ews **T**ransfer **P**rotocol (NNTP) is the protocol used to transfer and distribute messages on USENET newsgroups. The most common and popular browsers and email clients now have NNTP clients built-in.

NNTP is addressed in RFC-977, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc977.txt

Node—Any single computer connected to a network.

ODMR—On-**D**emand **M**ail **R**elay is a new protocol designed to enable mail servers with only an intermittent connection to a service provider, and which do not have a static IP address, to receive mail similarly to those servers that do have one and use the `ETRN` command. If the system has a static IP address, the ESMTP ETRN command can be used. However, systems with dynamic IP addresses have no widely deployed solution. ODMR solves this problem. Among other things, ODMR introduces the Authenticated TURN command (`ATRN`) which causes the flow of an SMTP session to be reversed (like the older TURN command) but with the added security of requiring that the requesting server be authenticated. This makes it possible for an SMTP server with a dynamic IP address to connect to its ISP and have one or more

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

host's email delivered to it via SMTP rather than collect it via POP or IMAP. This helps meet the widespread demand for a low-cost solution for those companies that need to their own mail server but cannot afford a static IP address or dedicated online presence.

ODMR is addressed in RFC 2645, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM—Original **E**quipment **M**anufacturer (OEM) is an often confusing and misunderstood term. An OEM is a company that uses another company's equipment or products in its own product that is packaged and sold under a different brand or company name. For example, HyperMegaGlobalCom, Inc. is an OEM because it purchases computer components from one or more different companies, puts them all together into a single customized product, and then sells it with "HyperMegaGlobalCom" stamped on it. The company that sold HyperMegaGlobalCom the components might also be an OEM if they in turn got their components from someone else as well. "OEM" is an unfortunate misnomer because OEMs are not actually the original manufacturers; they are the "packagers" or "customizers". In spite of this, many people still often use the term "OEM" when referring to the actual hardware manufacturers instead of those who repackage it—and understandably so.

On the fly—The term "on the fly" is commonly used it two different ways. First, it is often used to denote something that can be done "in a hurry" or easily while "in the middle" of performing some other task. For example, a bookkeeping product might support creating accounts "on the fly" while in the middle of entering sales figures —"Simply stop entering figures, click button X, enter a name, and then continue entering more figures." The other way that "on the fly" is used is in referring to something that can be generated dynamically or automatically instead of manually or statically. For example, by using the information stored in a "cookie" a customized web page might be generated "on the fly" when a user returns to a web site. Rather than requiring someone to manually create a page customized to the user's tastes, it would be generated dynamically based upon that person's actions while browsing.

Original Equipment Manufacturer—See OEM above.

Packet—A unit of computer data sent over a network. Any time you receive data from another computer on your LAN or over the Internet it comes to your computer in the form of "packets". The original file or message is divided into these packets, transmitted, and then recombined at the destination. Each packet contains a header containing its source and destination, a block of data content, and an error-checking code. It is also "numbered" so that it can be connected to related packets being sent. The process of sending and receiving packets is known as "packet-switching". Packets are also commonly called "datagrams".

Packet Switching—The process of sending and receiving packets over a network or the Internet. In contrast to circuit switching (such as in an analog telephone), which sends the data in a continuous stream over a single path or circuit, packet switching transmits the data broken up into "packets", which may not necessarily take the same route to get to their destination. Further, because the data is in separate units, multiple users can send different files simultaneously over the same path.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Parameter—A parameter is a characteristic or value. In computing, it is any value passed to a program by a user or another program. Your name and password, a preference setting, font size, and so on are all parameters. In programming, a parameter is a value that is passed to a subroutine or function for processing.

PDF—Portable **D**ocument **F**ormat (PDF) is a highly compressed multi-platform file format developed by Adobe Systems Incorporated that captures document formatting, text, and images from a variety of applications. This makes it possible for the document to appear the same and print accurately on multiple computers and platforms (unlike many word processors). Viewing a PDF file requires the Adobe Acrobat Reader, a free application distributed by Adobe Systems. There is also a plug-in for viewing PDF files with your web browser. This makes it possible to view PDF files posted on a web site directly instead of having to download them first and then view them with a separate program.

Parse—In linguistics, to parse is to divide language into its grammatical components that can be analyzed. For example, dividing a sentence into verbs, adjectives, nouns, and so on.

In computers, to parse is to divide a computer language statement into parts that can be made useful for the computer. A parser in a compiler is takes each program statement that a developer has written and divides it into parts that can then be used for developing further actions or for creating the instructions that form an executable program.

MDaemon and other products often parse email messages to determine their destination or to process them through filters and other tools.

Ping—An acronym for **P**acket **In**ternet **G**roper. It is a basic Internet program used to determine whether a specific IP address is reachable and accepting requests. It does this by sending an Internet Control Message Protocol (ICMP) Echo request and waiting for a response. "Ping" is commonly used as a verb when referring to this process. For example, "I am going to ping that server to see if it is online." "Pinging" an IP address is usually as simple as typing "ping" followed by the IP address or domain at the DOS prompt. For example "Ping 192.0.2.0."

ICMP is addressed in RFC-792 and the Echo protocol is addressed in RFC-862. These can be viewed at:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP—Stands for **P**ost **O**ffice **P**rotocol. POP (also commonly appears as POP3) is the most commonly used email protocol for retrieving email from a mail server. Most email clients use the POP protocol although some also support the newer IMAP protocol as well. POP2 became a standard in the mid 1980s and required SMTP to send messages. It was replaced by the newer version, POP3, which can be used with or without SMTP. POP is sometimes used as a verb when referring to collecting your email from a server. For example, "I'm going to POP my mailbox to get my mail."

POP3 is addressed in RFC-1939, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1939.txt

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Port—In TCP/IP and UDP networks and the Internet, a port is the endpoint of a logical connection and is identified by a number from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged protocols and services. For example, web servers typically are listed on port 80, SMTP servers typically communicate on port 25, and POP servers send and receive mail on 25. Generally, only one program at a time can use, or "bind", to any given port on each machine. When browsing the Internet, oftentimes certain servers will be running on non-default ports, which require you to specify the port in the URL after a colon. For example, "www.example.com:3000."

Port can also be used to refer to the sockets on a computer used for connecting peripheral devices and hardware to it. For example, serial ports, parallel ports, USB ports, and so on.

Finally, port is often used to describe the process of making a program designed for a specific platform or machine function on another platform. For example, "to port a Windows application to UNIX" or "to create a UNIX port for an application."

Post—In Internet messaging, such as email or newsgroups, it is a single message entered into a network communications system for others to see. For example, a message displayed on a newsgroup, mailing list, or discussion board is a post. It can also be used as a verb, as in "post a message to the mailing list or on the newsgroup."

PPP—Stands for "Point to Point Protocol." It is the Internet standard for dial-up connections. PPP is a set of rules that defines how your modem connection exchanges packets of data with other systems on the Internet.

PPP is addressed in RFC-1661, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocol—In computing, a protocol is a set of guidelines or standards by which servers and applications communicate. There are many different protocols used for many different purposes, for example, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, and so on.

Registry—A database used by Microsoft Windows to store configuration information about software installed on the computer. This includes things like user settings, file extension associations, desktop background, color schemes, and many others. It has the following six parts:

HKEY_User—Stores user information for each user of the system.

HKEY_Current_User—Preferences for the current user.

HKEY_Current_Configuration—Stores settings for the display and printers.

HKEY_Classes_Root—File associations and OLE information.

HKEY_Local_Machine—Hardware, operating system, and installed application settings.

HKEY_Dyn_Data—Performance data.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

When programs are installed on your computer the installer usually writes some information to the registry automatically. You can manually edit the registry, however, by using the regedit.exe program that is built in to Windows. But, you should exercise extreme caution when doing this because altering the wrong setting in the registry could cause your computer to function improperly, or not at all.

RFC—Request **F**or **C**omments is the name of the result and the process for creating a standard on the Internet. Each new standard and protocol is proposed and published on the Internet as a "Request For Comments." The Internet Engineering Task Force (IETF) facilitates discussions on the new standard and eventually it is established. In spite of the fact that the standard is established and no further "comments" are "requested," the standard still retains the "Request for Comment" acronym along with its identifying number. For example RFC-822 (now superseded by RFC-2822) is the official standard, or "RFC," for email. However, those protocols that are officially adopted as "standards" do have an official standard number associated with them that is listed in the Internet Official Protocol Standards document (which itself is STD-1 and currently RFC-3700). You can find RFCs on the Internet at many locations but the authoritative source is The RFC Editor, located at http://www.rfc-editor.org/.

The Internet Official Protocol Standards document is located at:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF—Rich **T**ext **F**ormat is a universal file format developed by Microsoft that is supported by nearly all word processors. In contrast to plain text format, RTF enables you to retain formatting, font information, text color, and so on. The file size of RTF files can be very large when compared to other file formats such as Microsoft Word's format (*.doc and *.docx) and Adobe PDF.

Server—A computer, or program, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as an SMTP server, or a machine on which the software is running. A single server *machine* could have many different server *programs* running on it concurrently. For example, your network's server might be running a web server, email server, FTP server, fax server, and others all at once.

SMTP—An acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is the primary protocol used to send email on the Internet from one server to another or from a client to a server. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Once a server has received email via SMTP it is usually stored there and can then be retrieved by a client via the POP, IMAP, or other protocol.

The SMTP protocol is addressed in RFC-2821, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam—Junk mail on the Internet. "Spam" is most commonly used to refer to unsolicited bulk email, although it is often used to refer to any unwanted email in general. A "spammer" will obtain hundreds, thousands, or even millions of email addresses from various sources and then "spam" the list with a message or solicitation. "Spam" can, however, be used to refer to a newsgroup or discussion

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

board posting as well, when the posting is some unwanted or unrelated advertisement for a product or web site.

Spam is quickly becoming a serious problem on the Internet, tying up a great deal of time and server resources. And because spammers oftentimes use various techniques to attempt to mask the origin of the message—such as "spoofing" their addresses to appear to be someone else or attempting to relay the spam covertly through multiple mail servers—preventing it can be a challenge. MDaemon Technologies' MDaemon server is equipped with a number of features designed specifically to aid in fighting spam, such as: DNS Block Lists (DNS-BL), IP Shielding, IP Screening, Relay Control, and others.

The origin of using the term "Spam" to refer to junk email is debated, but it is generally accepted that it comes from a popular Monty Python sketch in which the word "spam" is repeated over and over and periodically accompanied by Vikings singing, "Spam spam spam spam, spam spam spam spam…" However, it may simply be a disparaging comparison to the trademarked Hormel meat product of the same name—everybody gets it at one time or another, but does anyone ever really ask for it?

TCP/IP—Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) has been described as the foundation of the Internet. It is the basic suite of communication protocols used on the Internet to connect hosts. It is the most commonly used protocol on Local Area Networks as well. It is a two-layer system, the topmost layer being TCP, which manages the disassembling and assembling of files into packets for transmitting over the network. IP, which is the lower layer, handles the addressing of the packets so that they get to the proper destinations. TCP is addressed in the following RFC-793. IP is addressed in RFC-791. These RFCs can be found at:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet—A command and program used to log on to Internet sites that support Telnet access. The Telnet command gets you to the logon prompt of the Telnet server. If you have an account on that server, you can access your permitted resources such as your files, email, and so on. The downside of Telnet is that it is a command line program that uses Unix commands.

The TELNET protocol is addressed in RFCs 854-855, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminal—A device that allows you to send commands to a remote computer. A terminal is a keyboard, display screen, and some simple circuitry. Oftentimes, however, personal computers are used to "emulate" terminals.

Tiff—An acronym for **T**agged **I**mage **F**ile **F**ormat. It is a graphics file format created to be a universal graphics translator across multiple computer platforms. TIFF can handle color depths ranging from 1-bit to 24-bit.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

UDP—User **D**atagram **P**rotocol (UDP) is one of the protocols that make up the TCP/IP suite of protocols used for data transfers. UDP is a known as a stateless protocol because it doesn't acknowledge that packets being sent have been received.

UDP is addressed in RFC-768, which can be viewed at:

http://www.rfc-editor.org/rfc/rfc768.txt

Unix—Unix, or UNIX, is an operating system created by Bell Labs in the 1960s. Designed to be used by many users at the same time, it is the most popular operating system for servers on the Internet. There are now many different operating systems based on UNIX such as Linux, GNU, Ultrix, XENIX, and others.

URL—Every file or server on the Internet has a **U**niform **R**esource **L**ocator (URL). It is the address that you enter into your web browser to get to that server or file. URLs cannot have spaces and always use forward slashes. They have two parts separated by "://". The first part is the protocol being used or resource being addressed (for example, http, telnet, ftp, and so on) and the second part is the Internet address of the file or server (for example, www.altn.com or 127.0.0.1).

Uuencode—A set of algorithms for converting files into a series of 7-bit ASCII characters for transmission over the Internet. Although it stands for Unix-to-Unix encode, it is no longer exclusive to UNIX. It has become a universal protocol used to transfer files between different platforms. It is an encoding method commonly used in email.

WAN—A WAN, or **W**ide **A**rea **N**etwork, is similar to a Local Area Network (LAN) but is usually spread across multiple buildings, or even cities. WANs are sometimes composed of smaller LANs that are interconnected. The Internet could be described as the biggest WAN in the world.

Zip—Refers to a compressed or "zipped" file, usually with the "`.zip`" file extension. "Zipping" is compressing one or more files into a single archive file in order to save space for storage or to facilitate faster transfer to another computer. To use a zip file, however, you'll need to unzip it first with the appropriate program such as PKZIP or WinZip. There are multiple compression/decompression utilities available—both shareware and freeware—from many sites on the Internet. Hopefully you won't have to unzip the utility before you can install it.

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Index

- 2 -

2FA 703
2-Factor Authentication 703

- A -

Access Control List 300, 302, 728
Access Rights 302, 728
Account
  Database Options 833
  Quotas 844
Account Aliases 818
Account Autoresponders 708
Account Database Options 833, 834
Account Details 697
Account Editor
  Account Details 697
  ActiveSync Client Settings 748
  ActiveSync Clients 755
  ActiveSync Enabling/Disabling 747
  ActiveSync Policy 754
  Aliases 725
  Allow List 742
  App Passwords 734
  Attachments 718
  Autoresponder 708
  Filters 720
  Folder 700
  Forwarding 711
  Groups 700
  Mail Folder 700
  Mail Services 701
  Mobile Devices 755
  MultiPOP 723
  Quotas 715
  Restrictions 713
  Settings 744
  Shared Folders 726
  Web Services 703
Account Groups 764, 766
Account Hijack Detection 554
Account Integration 851
Account Manager 694
Account Options
  Passwords 840
Account permissions 703
Account Pruning 715
Account Restrictions 713
Account Restrictions Template 794
Account Signature 737
Accounts 849, 851
  ActiveSync 442
  ActiveSync Domain Accounts 223
  Autoresponders 823
  Domain Manager 181
  DomainPOP 144
  Groups 764, 766
  MDaemon Connector 381
  ODBC Selector Wizard - Account Database 834
ACL 302, 728
Activating MDaemon Connector 380
Active Directory 806, 809
  Authentication 809
  Creating Accounts 806
  Deleting Accounts 806
  Dynamic Authentication 806
  File Security 806
  Monitoring 812
  Persistent Monitoring 806
  Port (Gateway) 248
  Server (Gateway) 248
  Synchronization 812
  Synchronizing with MDaemon 806
  Template 806
  Updating Accounts 806
  Using with Mailing Lists 290
  Verification (Gateway) 248
Active Directory Authentication 851
ActiveSync
  Account Clients 755
  Account Policy 754
  Accounts 442
  Account-specific Client Settings 748
  Account-specific Options 747
  Advanced Options 410, 422
  Advanced policy settings 408
  Assigned Policy 222
  assigning client settings to client types 466
  assigning client settings to Groups 460

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ActiveSync
Assigning Policies 426
Auto Discover Service 408
Blacklist 420
Client Settings (Global) 413
Client Settings for Domains 208, 214
Client-level settings 451
Clients 451
Clients (Domain) 232
Client-specific settings 755
Client-Types 466
Data Wipe 451
Debugging 422
Default Policies 426
Deleting Devices 451
Devices 451
Devices (Domain) 232
Diagnostics 422
Disabling 408
Domain (Clients) 232
Domain Accounts 223
Domain Enable/Disable 207
Domain Settings 208, 214
Domains 426
Dumps 422
Enabling 408
Full Wipe 451
Global Client Settings 410
Global Settings 413
Groups 460
Logging 422
Managing Clients 413
Policies 434
Policies for Domains 222
Process Dumps 422
Quick access menu items 408
Remotely Wiping a Device 451
Removing Devices 451
Restricting protocols 424
Restrictions 424
Security 420
Soft Wipe 451
Tuning 410
Whitelist 420
Wiping Devices 451
ActiveSync Policy Editor 434
AD 290
AD Authentication 809, 812, 851
adding list members 267
Adding MDaemon Connector accounts 381
Address
Block List 545, 547
Suppression 545, 547
Address Books
CardDAV 360
Address Aliases 725, 818
Address Aliases Settings 820
Address Verification 847
Address Verification (Gateway) 248
Administrative Roles 741
Template 801
Administrator
Domain 741
Global 741
Administrators 801
Admins/Attachments 643
ADSP 516
Advanced Options
ActiveSync 410, 422
Debugging 422
Diagnostics 422
Dumps 422
Logging ActiveSync 410, 422
Process Dumps 422
Tuning 410
AI Message Features
Account Template Setting 782
Default Setting 333
Enabling for Accounts 703
Enabling for Domains 187
Alias display name in Webmail 333
Alias Editor 818
Aliases 725, 818
Aliases Settings 820
ALL_USERS list macro 265
ALL_USERS:<domain> list macro 265
Allow List
Automatic 742
DNS-BL 686
Spam Filter 675
Template 802
Allow List auto 672
Allow List from 677
Allow List to 676
AntiSpam 624
AntiVirus 369, 370, 624, 630, 653, 657, 659

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

AntiVirus 369, 370, 624, 630, 653, 657, 659
Configuring updater 657, 659
EICAR test message 657, 659
Malware 657, 659
Quarantine 653
Scheduler 369, 370, 657, 659
Testing 369, 370, 657, 659
Updater 369, 370, 657, 659
Urgent Updates 369, 370, 657, 659
Viewing update report 657, 659
virus scanning 653
AntiVirus support 630
AntiVirus Updates 369, 370
APOP 86
App Passwords 734
Approved List 544
Archival 123
Archiving Logs 166
Archiving mail in a pre 154
ATRN 101, 193, 253
Attachment extension 480
Attachment Linking 357, 718
Attachment restricting 643
Attachments
Autoresponders 825
deleting restricted 126
Template 799
AUTH 193, 509
Authentication 509
Active Directory 812
Authentication-Results header 516
Authorizing MDaemon Connector accounts 381
Auto Discover ActiveSync 408
Auto Response Messages 828
Auto Response Script Samples 828, 831
Auto-discovering MC Client Settings 382
AutoDiscovery Service 73
Auto-generated a Spam Folder and Filter 687
Automatic
Gateways 245
IP Screening 588
Log Archiving 166
Automatic Learning 668
Automatic Updates 487
automatically extracting attachments 357
automatically linking attachments 357
Autoresponder
Template 788
Autoresponder Exception List 826
Autoresponder Exempt List 826
Autoresponder Options 827
Autoresponders 708, 823, 828, 831
Account list 823
Attachments 825
Overview 823
AV
AntiVirus 653
AntiVirus Updater 657, 659
MDaemon AntiVirus 657
Available Disk Space 482

- B -

Backing up logs 166
Backscatter Protection 583
Backscatter Protection - Overview 582
Backup Server 248
Bad Address file 159, 268
Bad Messages 856
BadAddress.txt 159, 268
Bandwidth 585
Bandwidth Throttling 585, 586
Banners 341
Base Entry DN 290, 809
BATV 582, 583
Bayesian
Auto-learning 668
Classification 664
Learning 668
Bayesian Classification 660
Bayesian Learning 660, 664
Binding 105, 177
Black List 660
ActiveSync 420
Black Lists 683
Block List 678
Address 545, 547
Block Lists 683
Blocked recipients 547
Blocked users 545
Blocking IP addresses 600
BOSH server 365

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- C -

Cache 106
Caching IPs 106
CalDAV 360
Calendar 185, 322
Calendar & Scheduling 308
Calendar Sync 360
Calendars
  CalDAV 360
Canonicalization 521
CardDAV 360
Categories
  Creating 332
  Custom 332
  Domain 332
  Editing 332
  Personal 332
  Translating 332
Certificate 580
Certificates 316, 348, 561, 563, 566, 570
  SSL 896
  Using third-party 896
  Webmail 896
Certification 538, 541
Certification Service Providers 538, 541
Changes in MDaemon 15
Changing WorldClient's Port Setting 312
Choosing your account database 833
ClamAV 630
Clear message counts at startup 477
Client Settings
  ActiveSync 413
  ActiveSync Domains 208, 214
  Global 413
Client Signatures 200, 766, 769
  Default 132
  for Outlook 132
  for Webmail 132
  Macros 132
Client Types
  ActiveSync 466
Clients
  ActiveSync (Domain) 232
  Domain (ActiveSync) 232
Closing the RAS session 155
Cluster Nodes 399, 402, 404, 406
Cluster Service 399, 402, 404, 406
Collecting stored SMTP mail 193
Composite Log 161
Configuring
  DomainPOP Settings 142
  IP Cache 106
  IP Screen 548
  IP Shield 507
  MDaemon remotely 341
  ODBC Data Source for a List 293
  RAS Settings 155
Connection
  attempts 155
  Profile 157
Connection Window 82
Contact Sync 360
Contacts
  CardDAV 360
Content Filter 630
  Actions 633
  Administrators 643, 649
  Conditions 633
  Editor 631
  Recipients 649
  rules 638
Content Filter Editor 631
Content-ID header 485
Converting Headers 121
Cookies 313
Copying an autoresponder to other accounts 708
Copying an IMAP filter rule to all of a domain's accounts 720
Copying mail before parsing 154
CRAM-MD5 86
Create Rule Dialog 638
Creating
  Auto Response Messages 828
  New Content Filter Rule 633
  New ODBC Data Source 836
  New System Data Source 296
  ODBC data source 836
  Site Policy 595
Creating Account Templates 774
Creating and Using SSL Certificates 896
Cryptographic
  Signing 514, 518
  Verification 514, 516
CSP 538, 541

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Customizing DSN messages 864
Customizing the Queue/Statistic Manager 876
Customizing Webmail's Banner Images 341

- D -

Daemon 670
Data Source 834, 836
Database Options 833, 834
Date header 485
Debugging
  ActiveSync 422
Decryption 614
Deduping Mail 146
Default Domain
  Archival 123
Default headers 146
Default Security Settings Values 496
Deferred Delivery 115
Defining Content Filter administrators 643
Deleting Account Templates 774
Deleting mail 149
Deleting POP mail after collection 144
Delivery 89
Delivery based on non-address info 152
Delivery Options 89
Delivery Status Notification message 864
Delivery Times 372
Dequeue 193
Dequeue AUTH 193
Dequeuing 253
Dequeuing Gateway Messages 253
Dequeuing Mail 193, 194, 253
Devices
  ActiveSync (Domain) 232
  Domain (ActiveSync) 232
Diagnostics
  ActiveSync 422
Dialup Profile 157
Dialup Settings 155
Digest 279
Disk 482
Disk Space
  Low 482
  Monitoring 482
  Settings 482
disk space limits 256
Display 68, 75
display font 477
DK & DKIM signing 518
DKIM 514, 538, 541
  ADSP 516
  Canonicalization 521
  DNS 518
  including in DMARC reports 537
  Options 521
  Overview 514
  Private Keys 518
  Public Keys 518
  Selectors 518
  Signature tags 521
  Signatures 516
  Signing 518
  tags 521
  Verification 516
DKIM verifying 516
DMARC
  aggregate reports 533
  and Mailing Lists 523
  Creating a DNS record 523
  DNS record 523
  Effect on Mailing Lists 268, 271
  failure reports 533, 537
  filtering messages to Junk E-mail 530
  including DKIM in reports 537
  logging records 537
  Overview 523
  Public suffix file 537
  records 533, 537
  refusing failed messages 530
  Reporting 533, 537
  restrictive policies 530
  tags 533
  Verificaiton 530
DNS
  Block List Exceptions 686
  Block Lists 683
  DMARC Record 523
  Server 99
  Server IP Address 99
DNS Block Lists 684
DNS Security Extensions 579
DNS-BL 683
  Allow List 686
  Hosts 684
  Options 687

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

DNSSEC 579
Do Not Disturb 766
Documents 328
Documents Folders
  Allowing or blocking file types 110
  Enabling 110
  Limiting document size 110
Domain Administrators 741
Domain Gateways 239, 582, 583
Domain Manager 174
  Accounts 181
  ActiveSync 207
  AI Message Features 187
  Calendar 185
  Client Signatures 200
  Domain Signatures 195
  Host Name & IP 177
  MDaemon Connector Signatures 200
  MDaemon Instant Messenger 183
  Settings 205
  Signatures 195
  Smart Host 179
  Webmail Settings 187
  Webmail Signatures 200
Domain Name Replacement 148
Domain NAT Exemptions 613
Domain Settings 247
Domain Sharing 108
Domain Signatures 195
DomainKeys Identified Mail 514, 516, 518
DomainPOP 142
  Foreign Mail 151
  Host & Settings 144
  Mail Collection 142
  Name Matching 152
  Parsing 146
  Processing 148
  Routing Rules 149
  Security 154
DomainPOP Mail Collection 142
Domains 593
  Administrators 741
  Creating 174
  Deleting 174
  FQDN 174
  Renaming 174
  Sharing 108
  Trusted 505
Download
  Limits 144, 715
  Size Limits 144, 715
Dropbox
  Integration with Webmail 325
Dropbox Integration 308
DSN message 864
DSN Settings 864
Duplicate mail 146
Dynamic Screening
  Advanced logging options 596
  Advanced Options 607
  Allow List 609
  Auth Failure Tracking 600
  Block List 611
  Blocking IP addresses 600
  Customizing 596
  Diagnostics 607
  Domain NAT Exemptions 613
  Dynamic Allow List 609
  Dynamic Block List 611
  Freezing accounts 600
  Location Screening 609
  Logging 607
  Notifications 604
  Options 596
  Process Dumps 607
  Protocols 603
  Reports 604
  Router Exemptions for Domains 613
  SMTP Screen 552, 609, 611
  Tarpitting 609

- E -

Edit Rule 638
Editing
  Gateways 239
  Headers 121
EICAR virus test messages 657, 659
Email Recall 115
Email SSL 561, 563
Enabling
  DomainPOP Mail Collection 144
  Public Folders 113
  Webmail Server 313
Encryption 614
Encryption in Webmail 308

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

ESMTP 86, 193, 253
ESMTP SIZE command 86
ESMTP VRFY commands 86
ETRN 193, 253
ETRN Dequeue 253
Event Log 165
Event Scheduler 370, 372, 377
Event Tracking Window 68, 75
Exception List 675
  Autoresponders 826
Excluding addresses from filtering 675
Exempt List
  Autoresponders 826
  DNS-BL 686
  STARTTLS 574
EXPN 86
expressions 638
Extracting Attachments 357, 718

- F -

Faxing 324
File Attachments 718
File Compression 650
Filtering Messages 630, 631
Filtering Spam 660, 661, 681
Filters 720
Fingering an ISP 193
Fixes 484
Flagging Spam 661, 681, 684
Flags 300
fo tag 533
Folder
  Mail 700
Folder access rights 302, 728
Folders 110, 300
Footer 287
Foreign Mail 151
Forwarding 258, 711
  Gateway 243
  Template 792
  to a Domain Gateway 252
Forwarding Mail 149, 711
Forwarding messages automatically 720
Free Busy Services 322
Free/Busy Server Options 322
Freezing Accounts 600
From header modification 554
From Header Screening 560

- G -

Gateway 239, 583
  Address Verification 847
  Automatic creation 245
  Domain Settings 247
  Global Gateway Settings 243
  Options 258
  Quotas 256
  Verification 847
Gateway Domain Editor
  Active Directory 248
  Domain Settings 247
  ESMTP ETRN 253
  Forwarding 252
  LDAP 248
  Mail Forwarding 258
  Minger 248
  Quotas 256
  Verification 248
Gateway Manager 239
  Domains 239
  Editor 239
Gateways 582
GatewayUsers.dat file 248
General Email Controls 883
Getting Help 64
Global
  Administrators 741
  Auth 509
  Block List 545, 547
Global ActiveSync Client Settings 410
Global Gateway Settings 243
Glossary 900
Google Drive 328
Greylisting 590
Group Manager 764
Group Properties 766
  Client Signatures 766, 769
GROUP:<groupname> list macro 265
Groups 700
  ActiveSync 460
  Adding an account 764
  assigning ActiveSync Client Settings 460
  Assigning an account template 766
  Creating 764

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Groups 700
Deleting 764
Do Not Disturb 766
Instant Messaging 766
MDaemon Instant Messenger 766
Priority 766
Removing an account 764
Template 787
GUI 68, 75

- H -

Header 287
Header Screening 560
Header Translation 121
Exceptions 122
Headers 121, 146, 485
DMARC and Mailing Lists 271
List From 271
List Reply-To 271
List To 271
List-Archive 283
List-Help 283
List-ID 268, 283
List-Owner 283
List-Post 283
List-Subscribe 283, 489
List-Unsubscribe 283, 489
Mailing List 271, 283
Health Check 496
Help 64, 68, 75
Help with WorldClient 312
Heuristics 661
Hijack Detection 554
From header modification 554
Holding Queue 858
Contents 858
Summary Email 858
Host Authentication 118
Host Name & IP 177
Host Screening 550
Hosts 684
HTTPS 316, 348, 566, 570

- I -

IIS 313
Running WebAdmin under 352
Images in signatures 127, 132, 195, 200, 766, 769
IMAP 95, 101, 697, 701
Filters 720
Folder access rights 302, 728
Folders 300
Mail Rules 720
IMAP message flags 300
IMAP Spam Folder 687
Importing
Accounts 849, 851
Accounts From a Text File 849
Inbound Session Threads 92
Indexing
daily message indexing 473
indexing messages for searches 473
indexing public folders 473
real-time message indexing 473
Instant Messaging 183, 308, 320, 365
Integration 851
Interface 68, 75
Introduction 12
IP addresses
Trusted 506
IP Cache 106
IP Screening 548
Automatic 588
IP Shield 507
IP Shielding 507
IPv6 104, 105, 177
ISP LAST command 144
ISP Logon Settings 157
ISP POP Accounts 144

- J -

Jabber 365

- K -

Keys
Encryption 614
Private 614
Public 614

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

- L -

LAN Domains 593
LAN IPs 594
Latency 95
LDAP 290, 815
  Base Entry DN 290, 809
  Gateway verification 243
  Port (Gateway) 248
  Root DN 809
  Root DSE 809
  Root Entry DN 290
  Server (Gateway) 248
  Verification (Gateway) 248
LDAP Database Option 833
LDAP Options 815
LDAP/Address Book Options 815
Learning
  Bayesian 668
Leaving mail at ISP 144
Let's Encrypt 316, 566, 580, 896
Limiting bandwidth 585
Limits 144, 715
Linking Attachments 357, 718
List Moderation 283
List of Security Settings 496
List Routing 285
List Security 283
List-Archive header 283
List-Help header 283
List-ID header 283
List-Owner header 283
List-Post header 283
List-Subscribe header 283, 489
List-Unsubscribe header 283, 489
literals 638
Load Balancing 399, 402, 404, 406
Local Queue prepost processing 866
Location Screening 558
  Dynamic Allow List 609
Locking the MDaemon interface 80
Log
  Archiving 166
  Backups 166
  Maintenance 166
Log Mode 159
Log Page 873
Log Settings 168, 171
Logging
  ActiveSync 410
  Composite Log 161
  DMARC records 537
  Event Log 165
  Log Mode 159
  Maintenance 166
  Reporting 163
  Settings 168, 171
  Statistics Log 163
  Windows Event Log 165
Logging in to WorldClient 312
Logon Name 157
Logon Settings 157
Loop Detection 95
Low Disk Space 482

- M -

Macros
  Client Signature 132
  for groups 265
  for lists 265
  for MC Client Settings 384
  mailing list 265
  Message 645, 646
  Signature 127
Macros in mailing list messages 285
Mail
  Custom Queues 861
  Filters 720
  Forwarding 258, 711
  Pruning 715
  Queues 110
  Rules 720
Mail Folder 700
Mail quotas 844
Mail Release 193, 194
Mail Schedule 372, 377
Mail Sending & Collecting 372
Mail Services 701
  Template 780
Mailing List Control 880
Mailing List message macros 285
Mailing Lists
  Active Directory 290
  adding members 267

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Mailing Lists
ALL_USERS list macro 265
ALL_USERS:<domain> list macro 265
Creating 259
Digest 279
Digest toggle 265
DMARC 268, 523
DMARC and Mailing Lists 271
GROUP:<groupname> list macro 265
Headers 271, 283
List-ID header 268
List-Subscribe header 489
List-Unsubscribe header 489
Members 265
Membership Type 265
Moderating lists 283
Modifying 259
Name 268
Notifications 281
ODBC 292
Post Only toggle 265
Public Folder 289
Read Only toggle 265
Refusing restrictive DMARC messages 268
Routing 285
Security 283
Settings 268
Subscription reminder messages 278
Subscriptions 274
Support Files 287
URLs 283
Using Active Directory with 290
Main Window 68, 75, 477
Maintenance 166
Manager 694
Managing Domains 174
Marking Messages as Spam 684
Max
domains listed 477
messages 256
number of accounts shown 477
number of log lines displayed 477
Maximum Message Hop 95
MC Client Settings
Add-ins 398
Advanced 388
Auto-discovering client settings 382
Database 395
Folders 390
General 384
Macros 384
Miscellaneous 393
Send/Receive 391
Signature 397
MDaemon 563
Upgrading 59
MDaemon and Text Files 880
MDaemon AntiVirus 624, 630, 653
Configuring updater 657, 659
EICAR test message 657, 659
Malware 657, 659
Scheduler 369, 370, 657, 659
Testing 369, 370, 657, 659
Updater 369, 370, 657, 659
Urgent Updates 369, 370, 657, 659
Viewing update report 657, 659
MDaemon CA 896
MDaemon Connector 379, 701
Accounts 381
Activating 380
Adding Users 381
Authorizing Users 381
Client Settings 382
Contact Folders 380
Generating Shared Folders 380
Options 380
Removing Users 381
Restricting Users 380
MDaemon Connector Client 382
Add-ins 398
Advanced 388
Database 395
Folders 390
General 384
Macros 384
Miscellaneous 393
Send/Receive 391
Signature 397
MDaemon Features 12
MDaemon GUI 68, 75
MDaemon Instant Messenger 308
Domains 183
MDaemon Messaging Server 12
MDaemon Technical Support 64
MDaemon's SMTP Work Flow 83
MDIM 320

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

MDIM 320
Domains 183
MDPGP 614
MDSpamD 670
MDStats Command Line Parameters 877
MDStats.ini File 876
Meetings 322
Members 265
Menu 68, 75
Message Certification 538, 541
Message Filters 720
Message Flags 300
Message Indexing
Advanced Options 475
Customizing 473
daily message indexing 473
Diagnostics 475
indexing messages for searches 473
indexing public folders 473
Logging 475
Options 473
Process Dumps 475
real-time message indexing 473
Message Macros 645, 646
Message Recall 115
Message Routing 89
Message size limit 205
Message-ID header 485
metacharacters 638
Migrating Account DBase to ODBC 834
Minger 108, 248, 847
Gateway verification 243
Miscellaneous 489
Moderating lists 283
Modify Rule 638
Modifying an Existing Content Filter Rule 638
Monitoring Active Directory 812
Multiple Domains 108
MultiPOP 137, 375, 701, 723
Deleting messages from server after collecting 137
MultiPOP and Gmail 137
MultiPOP and Office365 137
OAuth 2.0 137

- N -

Name Matching 152
Network Resource Access 491
Network Shares 491
New Accounts template 774
New Features 15
Nodes 399, 402, 404, 406
Notepad 880
Notifications 281, 645
Delivery Status Notification 864
DSN 864

- O -

OAuth 2.0 328
ODBC
Account Database 834
Data Source 834, 836
Database Option 833
Mailing Lists 292
Selector Wizard - Account Database 834
System Data Source 293
ODMR 101, 193, 253
Old Mail Pruning 715
On-Demand Mail Relay 193, 253
On-Demand Mail Relay (ODMR) 193, 194
oof.mrk files 823, 828
OpenPGP 614
Options
Autoresponders 827
Free/Busy Services 322
Order of processing 83
Outbound Session Threads 92
Outbreak Protection 624
Outlook Connector for MDaemon 379
OutOfOffice.rsp 827
Overview 12

- P -

Parsing
Deduping Mail 146
List of parsed headers 146
Names preceeding email address 152
parsing 146
Skipping over 146
Password 157
ISP POP accounts 144
POP mail account 144

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Passwords 840
App Passwords 734
Expiration 840
Non-reversible 840
Strong 840
Performance Enhancements 15
Per-user flags 300
PGP 614
Phishing protection 560
Policies
ActiveSync 426, 434
Assigning to a Domain 222
POP Before SMTP 504
POP DELE command 86
POP mail collection 142
POP Server 144
POP3 701
Ports 101
MultiPOP 723
Post Connection 158
Postmaster
informed when dialup fails 155
receiving summary of non 151
Precedence bulk header 485
Preferences
Automatic Updates 487
Disk 482
Fixes 484
Headers 485
Miscellaneous 489
MultiPOP 375
Quotas 844
Servers 86
System 480
UI 477
Updates 487
pre-process list mail 480
Pre-processing 866
Preventing duplicate messages 146
Priority Mail 119
Private keys 614
Process 158
Processing 148
Profile 157
Programs 158
Protection
Against backscatter 582, 583
Pruning 126, 715
Public Folder
Pruning 126
Public Folder Manager 300
Public Folders 110, 113, 726
Mailing Lists 289
Public IMAP Folders 110
Public keys 614
Public suffix file 537
Publishing an autoresponder to other accounts 708
Publishing IMAP filters to all of a domain's accounts 720

- Q -

QSND 193
Quarantined files
deleting 126
Quarantined messages
deleting 126
Queue and Statistics Manager 867
Queue Page 868
Queue pre-processing 866
Queued Mail 68, 75
Queues 110, 856, 863
Custom 861
Holding 858
Restoring default locations 863
Quotas 256, 715, 844
Template 796

- R -

RAS Dialup 155
Dialup Settings 155
Engine 155
Settings 155
RAS Dialup Settings
ISP Logon Settings 157
Post Connection 158
RAW
Bypassing the Content Filter 883
Message Specification 883
Sample messages 883
Special fields supported by 883
RBL 683
RBL Hosts 684
Real-time Block Lists 683

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Recalling a message 115
Received header 146
Recipients 649
Redirecting messages automatically 720
Refusing non 151
Regular Expressions 638
Rejecting Spam 661, 681
Relay Control 498
Relay Settings 498
RelayFax
  Integration with Webmail 324
Release Notes 15
Reminders 322
  Mailing List 278
Remote Access and Control 880, 883
Remote Address Verification 847
Remote Administration 703
  Certificates 348, 570
  HTTPS 348, 570
  SSL 348, 570
Remote Configuration 341, 343
Remote LDAP server 248
Remote Mail Scheduling 372
Remote verification of addresses 248
Renaming Account Templates 774
Report
  Quota 844
Report Page 875
Reporting 163, 680
Require a Terms of Use acknowledgment 356
Requirements 12
Resources 68, 75
Restart Spam Filter 661
Restore 863
Restricting ActiveSync Protocols 424
Restricting attachments 643
Restricting IP addresses 105, 177
Restrictions
  Account 713
  Template 794
Retrieving stored SMTP mail 193
Retry 856
Retry Queue Settings 856
Return-Receipt-To header 485
Reverse Lookup 500
rf tag 533
ri tag 533
Roles 741
Root DN 290, 809
Root DSE 809
Route Slips 891
Router Exemptions for Domains 613
Routing 285
Routing mail to various users 149
Routing Rules 149
rua tag 533
ruf tag 533
Rules 149, 720
Running WebAdmin under IIS 352

- S -

Saving Mail 154
Scanning for viruses 653
Scheduler 372, 679
  AntiVirus updating 369, 370
  Custom queue scheduling 372
  Event Scheduling 372
  Remote Mail Scheduling 372
  Spam Filter updates 679
Scheduling AntiVirus Updates 370
Screening 494, 548
  Countries 558
  From Header Screening 560
  Location 558
  SMTP 552
  Spambot Detection 556
Screening Hosts 550
Secure Sockets Layer protocol 316, 561, 563, 566, 574, 896
Securing DNS 579
Security 154, 851
  Backscatter Protection 583
  Backscatter Protection - Overview 582
  BATV 582, 583
  Features 494
  Hijack Detection 554
  Location Screening 558
  Mailing List 283
  Settings 494
  SMTP Screen 552
Security Settings
  Default Values 496
  Health Check 496
Semaphore Files 886
Send & Collect Mail 372

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Sender Policy Framework 512
Sender-ID 538, 541
Sending mail to various users 149
Server
  Webmail 308
Server level administrators 741
Server Settings
  Delivery 89
  Dequeue 193
  DNS 99
  Ports 101
  Pruning 126
  Servers 86
  Threads 92
  Timers 95
  Unknown Mail 97
Servers 86
Service 491
Session Threads 92
Session Window 82
Setting Download Size Limits 144
Setting IMAP Folder Flags 113
Setting parameters for mail delivery 149
Setting the number if dialup attempts 155
Setting up
  Auto Response Messages 828
  DomainPOP Mail Collection 142
  Global Block List 545, 547
  IP Screen 548
  IP Shielding 507
  RAS 155
  Remote configuration 341
Setting up an MDaemon Cluster 399, 402, 404, 406
Settings
  Aliases 820
  Domain Manager 205
  Template 804
Shared Folders 110, 113, 726
Shared IMAP Folders 113, 300
Shared user folders 302, 728
Sharing Calendars 360
Sharing Domains 108
Sharing mail folders 110
Shortcut Menu 80
Signaling ISP to dequeue mail 193
Signature
  Account 737
  Pushing the client signature to Outlook 397
Signatures
  Client 200
  Default 127
  Default Client 132
  Domain 195
  for MDaemon Connector 200
  for Outlook 132
  for Webmail 132, 200
  Group Client 766, 769
  HTML 127, 195, 200
  Inserting images 127, 195, 200
  Macros 127
  Macros for client signatures 132
  Plain text 195, 200
  push to Outlook 132
  push to Webmail 132
  Text 127
Signing 518
Signing Messages 514
Simple Message Recall 115
Simple Reporting 680
Site Policy 595
Site Security Policy 595
Size limit
  Message 205
Skipping 146
Smart Host 179
  Default 89
SMTP Authentication 89, 509
SMTP call-back 847
SMTP call-forward 847
SMTP Connection Window 82
SMTP RCPT threshold 588
SMTP Screen 552, 609, 611
SMTP Work Flow 83
Socket binding 105, 177
Space 482
Spam
  Addresses 690
  Allow List 676, 677
  Automatic allow listing 672
  Bayesian Learning 664
  Black List 681
  Block List 678
  Classification 664
  Deleting 661, 681
  Directory 664
  False negative classification 664

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Spam
  False positive classification 664
  Filtering 661, 672, 676, 677, 678, 681
  Inserting tag into subject 661
  Non-spam directory 664
  Rejecting 661, 681
  Reporting 680
  Required score 661
  Scoring 661
  Simple Reporting 680
  Threshold 661
  Traps 690
  White List 681
Spam Assassin 670
Spam Filter 660, 687
  Allow List 675
  Bayesian Auto-learning 668
  Exception List 675
  MDSpamD 670
  Reports 680
  Spam Daemon 670
  Spam Filtering 681
  Updates 679
  using and external spam daemon 670
Spam Folder 687
Spam protection 560
Spam Traps 690
Spambot Detection 556
SpamD 670
SPF 512, 538, 541
SRV Record 73
SSL 316, 348
SSL & Certificates 316, 561, 563, 566, 896
SSL & TLS
  CA 580
  Certificate 580
  DNSSEC 579
  Let's Encrypt 580
  MDaemon 563
  No STARTTLS List 574
  Remote Administration 570
  STARTTLS 574
  STARTTLS List 575, 576
  TLS 574
  Webmail 566
SSL Certificates 896
SSL Ports 101
Starting WorldClient 312
STARTTLS 561, 563, 574
STARTTLS List 575, 576
STARTTLS Required List 575, 576
startup 477
Statistics 68, 75
Statistics Log 163
STLS 561, 563
Stopping a message 115
Subscribe 274, 276
Subscribe header 283, 489
Subscribing To Mailing Lists 276
Subscription reminders 278
Subscriptions 274
Support 64
Support Files 287
Suppressed users 545
Suppression 287
Synchronization 308
System 480
System account email address 480
System Data Source 836
System Requirements 12
System Service 491
system tray 477

- T -

tagged expressions 638
Tags
  DKIM 521
  DMARC 533
  fo 533
  fr 533
  ri 533
  rua 533
  ruf 533
Tarpit Settings 588
Tarpit Threshold 588
Tarpitting 609
task bar 477
Task reminders 322
Tasks
  CalDAV 360
TCP 101
Technical Support 64
Template
  Account Restrictions 794
Template Control 776

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Template Manager 774
Template Control 776
Template Properties 776
Template Properties 776
Administrative Roles 801
Allow List 802
Attachments 799
Autoresponder 788
Forwarding 792
Groups 787
Mail Services 780
Quotas 796
Settings 804
Web Services 782
Templates
Creating 774
Deleting 774
New Accounts 774
Renaming 774
Terms of Use 356
Text Files 880
Third-party Certificates 896
Threading 92
Threads 92
Threshold
Spam rejection 661
Throttling 586
Timeout 95
Timers 95, 372
TLS 561, 563, 574
Toolbar 68, 75
Tray Icon 80
Trusted
Domains 505
Hosts 505
IP addresses 506
Trusted Domains 498
Tuning 410
Two-Factor Authentication 703

- U -

UDP 101
UI 477
Undeliverable Mail 856
Unknown Mail 97
Unlocking the MDaemon interface 80
Unsubscribe 274
Unsubscribe header 283, 489
Updates 487, 679
Updating virus definitions 369, 370
Upgrading MDaemon 59
Urgent Updates 369, 370
User Folders 110
User Page 871
Userlist.dat Database Option 833
Using Regular Expressions 638

- V -

VBR 538, 541
Verification
Gateways 248
Remote Address 248
via Active Directory 248
via GatewayUsers.dat file 248
via LDAP 248
via Minger 248
Verifying DKIM 516
Verifying Signatures 514
Virus
Protection 630
Updater 369, 370
Viruses 624
Vouch-By-Reference 538, 541
VRFY 86, 847

- W -

Web Access Permissions 703
Web configuration 341
Web Server 313
Web Services
Template 782
WebAdmin 341, 343
Reports 163
Running under IIS 352
WebDAV 360
Webmail 308, 703
Address Book 333
Branding 341
Calendar 322
Categories 332, 333
Custom Settings 333
Customizing Banners 341

Copyright © 1996-2023. All rights reserved. MDaemon Technologies

Webmail 308, 703
Date Format 333
Default Language 333
Default Theme 333
Domain Options 320
Domain Settings 333
Dropbox 325
Edit alias display name 333
HTTPS 316, 566
HTTPS Port 316, 566
Instant Messaging 320, 365
Jabber 365
MDIM 320
Meetings 322
RelayFax integration 324
Reminders 322
Settings 333
SSL 316, 566
SSL & Certificates 896
Task reminders 322
Web Server 313
Webmail IM 365
XMPP 365
Webmail Settings 187
Welcome File 287
Welcome message subject header 485
What's New? 15
White List 660, 681
ActiveSync 420
Windows Account Integration 851
Windows Service 491
winmail.dat 650
WorldClient
CalDAV 360
CardDAV 360
Free/Busy Options 322
Getting Help 312
Logging in 312
Signing in 312
SSL 561
Starting WorldClient 312
WorldClient SSL 561
WorldClient Documents Folders 110
WorldClient Help 312

- X -

XMPP 365
X-RBL-Warning headers 485
X-type headers 485

Copyright © 1996-2023. All rights reserved. MDaemon Technologies