MDaemon Features that Stand Out over Exchange

MDaemon users can still have all of the features they need in a mail server without the hassle and overhead of running Microsoft Exchange Server. Here are a few MDaemon features that set MDaemon apart from Exchange.

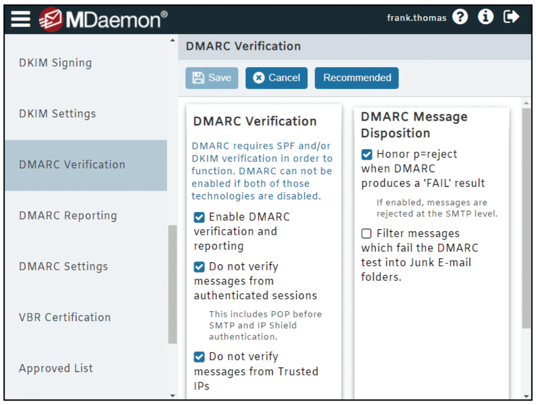
DMARC - Anti-spoofing & Email Validation

DMARC is an anti-spoofing process that defines a scalable mechanism by which a mail server administrator can express, using DNS records, domain level policies and preferences for message validation, disposition, and reporting. A mail receiving organization can also use those policies and preferences to improve mail handling.

DMARC takes out the guesswork on determining what to do with messages that did not originate from the domain specified in the message's From field. When a message fails DKIM and SPF lookups, DMARC allows domain administrators to tell receiving mail server administrators or mailbox providers what to do with the message, such as accept, quarantine, or reject the message. Forensic and aggregate reports allow domain administrators to see how, when and where their domain is being abused.

For a more technical, more thorough explanation of DMARC, visit www.dmarc.org.

[Figure 1-1]



DMARC Verification

DMARC Verification

DMARC requires SPF and/or DKIM verification in order to function. DMARC can not be enabled if both of those technologies are disabled.

☑ Enable DMARC verification and reporting

☑ Do not verify messages from authenticated sessions

This includes POP before SMTP and IP Shield authentication.

☑ Do not verify messages from Trusted IPs

DMARC Message Disposition

☑ Honor p=reject when DMARC produces a 'FAIL' result

If enabled, messages are rejected at the SMTP level.

☐ Filter messages which fail the DMARC test into Junk E-mail folders.

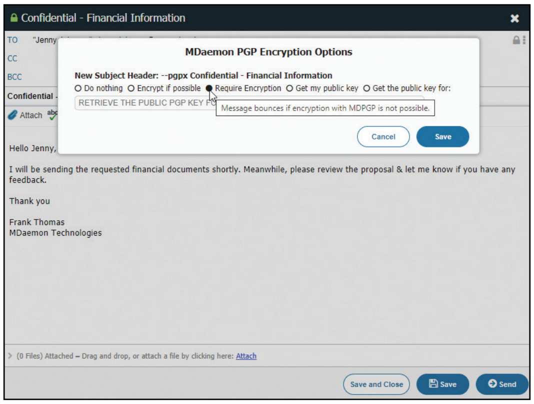
Figure 1-1

Server-Side Encryption with OpenPGP - Including Simplified Email Encryption for Webmail

MDaemon supports server-side email encryption with OpenPGP. Administrators can configure policies and content filtering rules to automate the encryption and key exchange processes.

When composing a message, MDaemon Webmail users can use the Advanced Options screen to instruct MDaemon to encrypt the message, retrieve their public key, or retrieve the public key of another user (if available). This greatly simplifies the process of sending secure, encrypted email using OpenPGP.

[Figure 1-2]



TO "Jenny

Confidential -

MDaemon PGP Encryption Options

New Subject Header: --pgpx Confidential - Financial Information

○ Do nothing ○ Encrypt if possible ● Require Encryption ○ Get my public key ○ Get the public key for:

RETRIEVE THE PUBLIC PGP KEY FO

Message bounces if encryption with MDPGP is not possible.

Hello Jenny,

I will be sending the requested financial documents shortly. Meanwhile, please review the proposal & let me know if you have any feedback.

Thank you

Frank Thomas
MDaemon Technologies

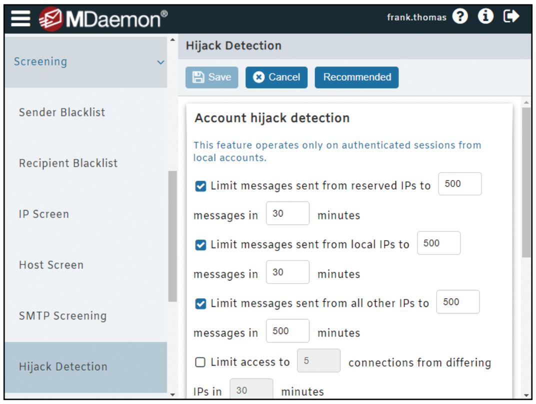
(0 Files) Attached – Drag and drop, or attach a file by clicking here: Attach

Figure 1-2

Account Hijack Detection

When a spammer has managed to obtain the login credentials for a user's account, a common goal is to send out as many spam messages as possible in a short period of time. MDaemon's account hijack detection feature allows you to disable or freeze accounts that send out a designated number of messages in a given period of time over an authenticated session.

[Figure 1-3]



Hijack Detection

Account hijack detection

This feature operates only on authenticated sessions from local accounts.

☑ Limit messages sent from reserved IPs to 500 messages in 30 minutes

☑ Limit messages sent from local IPs to 500 messages in 30 minutes

☑ Limit messages sent from all other IPs to 500 messages in 500 minutes

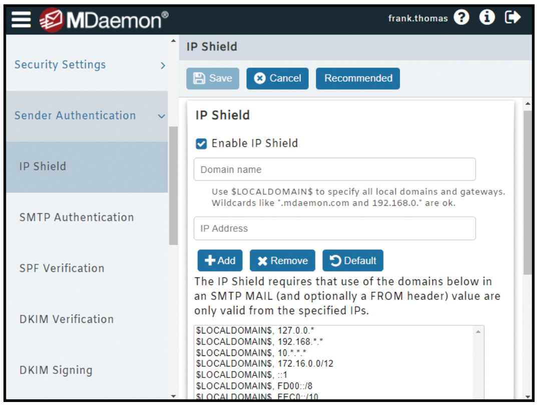
☐ Limit access to 5 connections from differing IPs in 30 minutes

Figure 1-3

IP Shielding - For Added Protection Against Spoofing

IP Shielding allows you to block mail from specific domains when it is sent to the MDaemon server from unauthorized IP addresses. Any email server that is accepting email via SMTP is susceptible to being used by unknown users claiming to be a user at the local domain name to 'spoof' email out through the server. MDaemon's IP Shielding can stop this by specifying that when a user sends an email claiming to come from a specified domain name, the IP address the email is sent from must be within a certain defined range. If you are running multiple domain names on your server, you can create one or more separate IP Shielding entries for each domain. For users who are sending email from outside of the local network, exceptions can be made for accounts using SMTP authentication or for connections from trusted IPs.

[Figure 2-1]



IP Shield

☑ Enable IP Shield

Use $LOCALDOMAIN$ to specify all local domains and gateways. Wildcards like *.mdaemon.com and 192.168.0.* are ok.

The IP Shield requires that use of the domains below in an SMTP MAIL (and optionally a FROM header) value are only valid from the specified IPs.

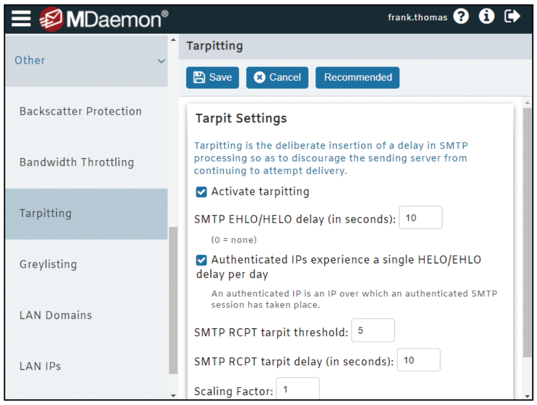
```
$LOCALDOMAIN$, 127.0.0.*
$LOCALDOMAIN$, 192.168.*.*
$LOCALDOMAIN$, 10.*.*.*
$LOCALDOMAIN$, 172.16.0.0/12
$LOCALDOMAIN$, ::1
$LOCALDOMAIN$, FD00::/8
$LOCALDOMAIN$, FEC0::/10
```

Figure 2-1

Tarpitting - To Protect Against Spam & Server Abuse

A common goal for spammers is to send spam to as many recipients as possible, thus, spam messages may contain many RCPT commands (message recipients). Tarpitting makes it possible to deliberately slow down a connection once a specified number of RCPT commands have been received from the sending server. This is to discourage spammers from trying to use your server to send unsolicited bulk email. 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 RCPT command is received from that host during the connection. The assumption behind this technique is that if it takes spammers a longer period of time to send each message then this will discourage them from trying to use your server to do so again in the future.

[Figure 2-2]



Tarpit Settings

Tarpitting is the deliberate insertion of a delay in SMTP processing so as to discourage the sending server from continuing to attempt delivery.

☑ Activate tarpitting

SMTP EHLO/HELO delay (in seconds): 10

(0 = none)

☑ Authenticated IPs experience a single HELO/EHLO delay per day

An authenticated IP is an IP over which an authenticated SMTP session has taken place.

SMTP RCPT tarpit threshold: 5

SMTP RCPT tarpit delay (in seconds): 10

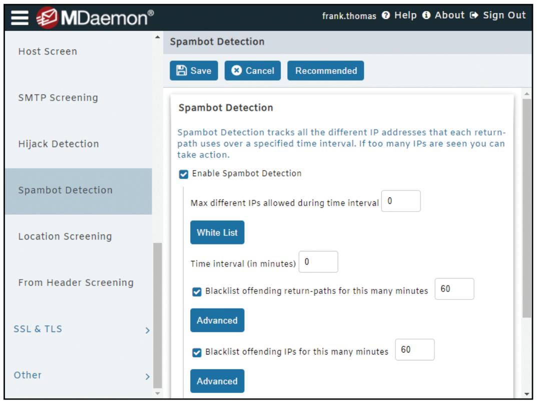
Scaling Factor: 1

Figure 2-2

Spambot Detection

MDaemon's Spambot Detection feature tracks the originating IP address from which every return-path value (sender) uses over a period of time. If the same return-path is used by multiple IP addresses (more than can normally be expected) within a given period of time, then this typically indicates a possible spambot network is being used. When a spambot is detected, the connection is dropped and the sending address can optionally be blacklisted for a designated period of time.

[Figure 2-3]



Spambot Detection

Spambot Detection tracks all the different IP addresses that each return-path uses over a specified time interval. If too many IPs are seen you can take action.

☑ Enable Spambot Detection

Max different IPs allowed during time interval 0

Time interval (in minutes) 0

☑ Blacklist offending return-paths for this many minutes 60

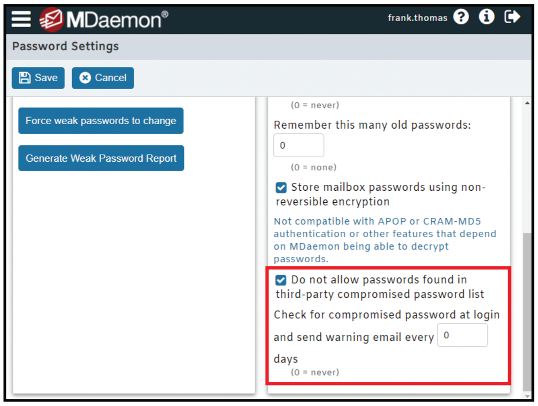
☑ Blacklist offending IPs for this many minutes 60

Figure 2-3

Compromised Password Check

MDaemon can check a user's password against a compromised password list from a third-party service, and then prevent users from using passwords found on the list. If a user's password is present on the list it does not mean the account has been hacked. It means that the password has appeared in a data breach at some point. Published passwords may be used by hackers in dictionary attacks.

[Figure 3-1]



Password Settings

(0 = never)

Remember this many old passwords: 0

(0 = none)

☑ Store mailbox passwords using non-reversible encryption

Not compatible with APOP or CRAM-MD5 authentication or other features that depend on MDaemon being able to decrypt passwords.

☑ Do not allow passwords found in third-party compromised password list

Check for compromised password at login and send warning email every 0 days

(0 = never)

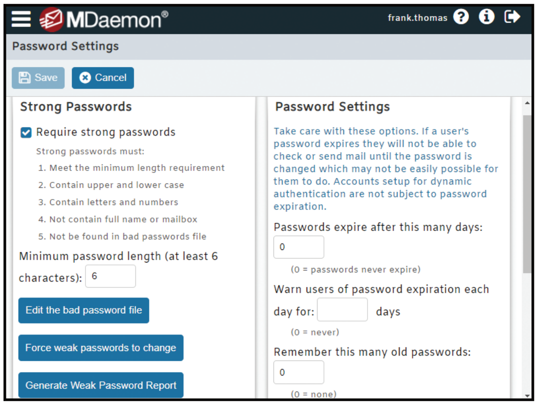
Figure 3-1

Password Controls

MDaemon and Exchange (using Active Directory) both allow you to configure minimum password length and maximum password age. Both also have settings to require complex passwords and to prevent users from reusing passwords or simple variations of passwords. MDaemon has the following three features, which are not present in Active Directory:

- "Weak Passwords" Report
- Ability to Force Weak Passwords to Change
- "Bad Password" file, which designates passwords or variations of passwords that are forbidden, such as "password1."

[Figure 3-2]


MDaemon®
frank.thomas
Save
Cancel
Edit the bad password file
Force weak passwords to change
Generate Weak Password Report

Password Settings

Strong Passwords

☑ Require strong passwords

Strong passwords must:

1. Meet the minimum length requirement
2. Contain upper and lower case
3. Contain letters and numbers
4. Not contain full name or mailbox
5. Not be found in bad passwords file

Minimum password length (at least 6 characters): 6

Password Settings

Take care with these options. If a user's password expires they will not be able to check or send mail until the password is changed which may not be easily possible for them to do. Accounts setup for dynamic authentication are not subject to password expiration.

Passwords expire after this many days: 0

(0 = passwords never expire)

Warn users of password expiration each day for: days

(0 = never)

Remember this many old passwords: 0

(0 = none)

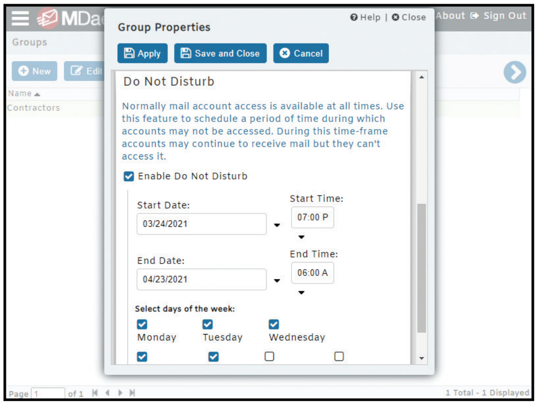
Figure 3-2

Managing Employee Workload with Email Do Not Disturb

Companies in many countries are being challenged by the need to manage email access "after hours" to prevent overtime pay and promote a stronger work/life balance. To date, most companies can only implement Human Resource policies to address the issue. To help IT Administrators deliver another layer of compliance to the organization, MDaemon includes an "Email Do Not Disturb" feature.

Located within the Accounts | Groups & Templates settings, Do Not Disturb allows the MDaemon administrator to set a time frame during which email may not be accessed by its users. Accounts in this state will receive incoming mail but users may not be able to login to their MDaemon account or send/reply to messages until the Do Not Disturb period has lapsed.

[Figure 3-3]



Group Properties

Do Not Disturb

Normally mail account access is available at all times. Use this feature to schedule a period of time during which accounts may not be accessed. During this time-frame accounts may continue to receive mail but they can't access it.

☑ Enable Do Not Disturb

Start Date: 03/24/2021

Start Time: 07:00 P

End Date: 04/23/2021

End Time: 06:00 A

Select days of the week:

☑ Monday ☑ Tuesday ☑ Wednesday

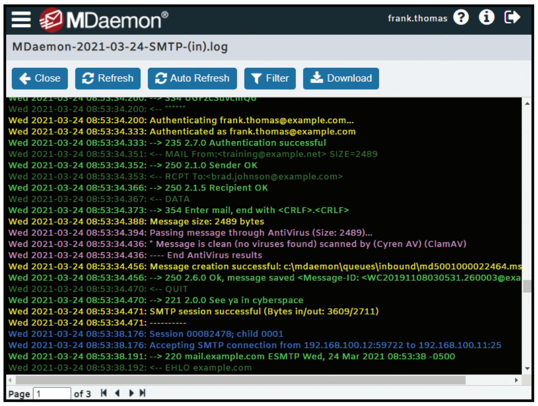
☑ ☑ □ □

Figure 3-3

Colorized Session Logs

Mail routing information in MDaemon's on-screen session logs is color coded for easy identification of protocol commands and errors. This makes it easier for administrators to review inbound and outbound activity and to troubleshoot email issues.

[Figure 3-4]



MDaemon-2021-03-24-SMTP-(in).log

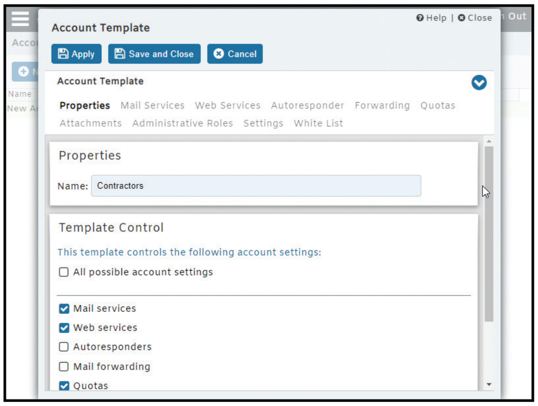
```
Wed 2021-03-24 08:53:34.200: --> 334 UGFzc3dvcmQ6
Wed 2021-03-24 08:53:34.200: <-- ******
Wed 2021-03-24 08:53:34.200: Authenticating frank.thomas@example.com...
Wed 2021-03-24 08:53:34.333: Authenticated as frank.thomas@example.com
Wed 2021-03-24 08:53:34.333: --> 235 2.7.0 Authentication successful
Wed 2021-03-24 08:53:34.351: <-- MAIL From:<training@example.net> SIZE=2489
Wed 2021-03-24 08:53:34.352: --> 250 2.1.0 Sender OK
Wed 2021-03-24 08:53:34.353: <-- RCPT To:<brad.johnson@example.com>
Wed 2021-03-24 08:53:34.366: --> 250 2.1.5 Recipient OK
Wed 2021-03-24 08:53:34.367: <-- DATA
Wed 2021-03-24 08:53:34.373: --> 354 Enter mail, end with <CRLF>.<CRLF>
Wed 2021-03-24 08:53:34.388: Message size: 2489 bytes
Wed 2021-03-24 08:53:34.394: Passing message through AntiVirus (Size: 2489)...
Wed 2021-03-24 08:53:34.436: * Message is clean (no viruses found) scanned by (Cyren AV) (ClamAV)
Wed 2021-03-24 08:53:34.436: ---- End AntiVirus results
Wed 2021-03-24 08:53:34.456: Message creation successful: c:\mdaemon\queues\inbound\md5001000022464.ms
Wed 2021-03-24 08:53:34.456: --> 250 2.6.0 Ok, message saved <Message-ID: <WC20191108030531.260003@exa
Wed 2021-03-24 08:53:34.470: <-- QUIT
Wed 2021-03-24 08:53:34.470: --> 221 2.0.0 See ya in cyberspace
Wed 2021-03-24 08:53:34.471: SMTP session successful (Bytes in/out: 3609/2711)
Wed 2021-03-24 08:53:34.471: ----------
Wed 2021-03-24 08:53:38.176: Session 00082478; child 0001
Wed 2021-03-24 08:53:38.176: Accepting SMTP connection from 192.168.100.12:59722 to 192.168.100.11:25
Wed 2021-03-24 08:53:38.191: --> 220 mail.example.com ESMTP Wed, 24 Mar 2021 08:53:38 -0500
Wed 2021-03-24 08:53:38.192: <-- EHLO example.com
```

Figure 3-4

Account Grouping & Templates

The Accounts menu includes a Groups and Templates menu. Templates are used to configure the services and features that are available to accounts belonging to groups that are assigned the selected template. Thus, groups can be used to assign most of an account's settings automatically. For example, if you want to assign an auto-responder to a certain set of accounts, you can create and name an account template which defines the auto-responder, then assign that account template to a group, and then finally assign one or more of your accounts to the group. From that point, the template will determine the account's auto-responder settings. Templates can control almost all or just select portions of an account's settings. You can decide what portions of an account's settings are to be part of a template.

[Figure 4-1]



Properties

Name: Contractors

Template Control

This template controls the following account settings:

□ All possible account settings

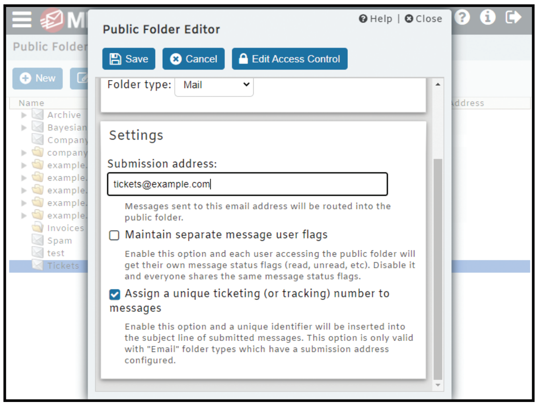
☑ Mail services
☑ Web services
□ Autoresponders
□ Mail forwarding
☑ Quotas

Figure 4-1

Public Folder Ticketing System

MDaemon includes a public folder ticketing system. MDaemon allows public folders to be configured for message ticketing using any client with access to public folders. When this feature is enabled for a public folder, MDaemon will add the public folder name and a unique identifier to the subject of messages sent to the submission address of the public folder. 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.

[Figure 4-2]



Folder type: Mail

Settings

Submission address: tickets@example.com

Messages sent to this email address will be routed into the public folder.

□ Maintain separate message user flags

Enable this option and each user accessing the public folder will get their own message status flags (read, unread, etc). Disable it and everyone shares the same message status flags.

☑ Assign a unique ticketing (or tracking) number to messages

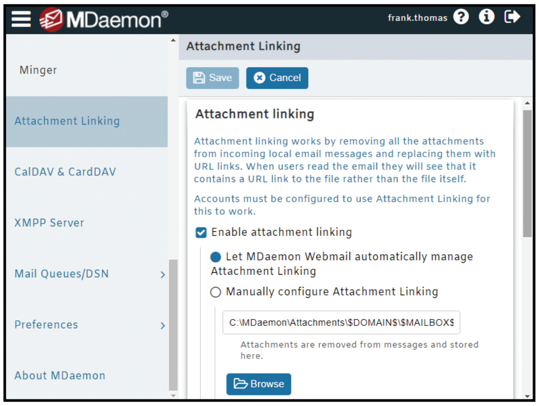
Enable this option and a unique identifier will be inserted into the subject line of submitted messages. This option is only valid with "Email" folder types which have a submission address configured.

Figure 4-2

Attachment Linking

MDaemon's Attachment Linking feature removes attachments from inbound (and optionally outbound) messages and places them inside a directory on the MDaemon server. A link that the recipient can click on to download the attachment is then placed in the email message. Because attachments are stored on the server and not sent with every message that they were originally attached to, bandwidth usage can be greatly reduced.

[Figure 4-3]



Attachment linking

Attachment linking works by removing all the attachments from incoming local email messages and replacing them with URL links. When users read the email they will see that it contains a URL link to the file rather than the file itself.

Accounts must be configured to use Attachment Linking for this to work.

☑ Enable attachment linking

● Let MDaemon Webmail automatically manage Attachment Linking

○ Manually configure Attachment Linking

C:\MDaemon\Attachments\$DOMAIN$\$MAILBOX$

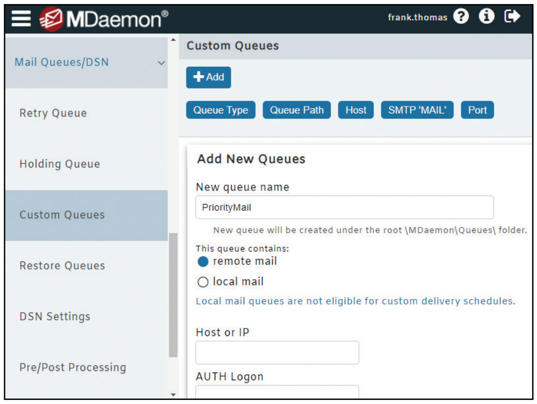
Attachments are removed from messages and stored here.

Figure 4-3

Custom Mail Queues

Administrators can create custom queues in MDaemon, and then use the content filter to send messages over a certain size, or messages that contain the X-MDMailing-List header (for all mailing list messages) to your custom queues, and delivery schedules can be assigned to these custom queues. Custom queues can be used for dealing with large attachments, or for sending out newsletters after-hours without clogging general mail traffic.

[Figure 5-1]



Add New Queues

New queue name: PriorityMail

New queue will be created under the root \MDaemon\Queues\ folder.

This queue contains:
● remote mail
○ local mail

Local mail queues are not eligible for custom delivery schedules.

Host or IP

AUTH Logon

Figure 5-1

Easy Backup & Restore via Flat File Structure

MDaemon's flat file structure makes it easy to backup and restore your data. Configuration files can be backed up by simply making a backup copy of the MDaemon/App directory, MDaemon/WorldClient directory and MDaemon/WebAdmin directory. Email messages can be backed up by copying the MDaemon/Users directory.

All settings are stored in various configurations files, which can be edited with a simple text editor.

[Figure 5-2]

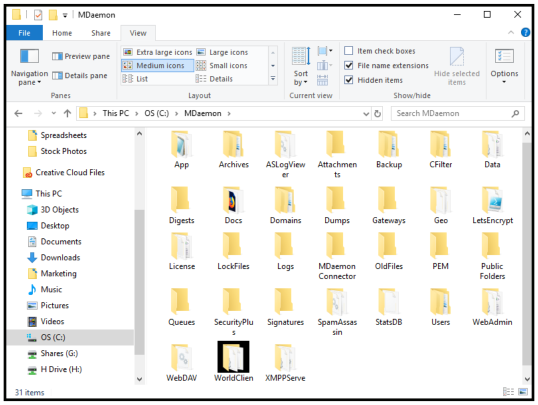


Figure 5-2

Traffic & Mailbox Charts

Administrators can select "Traffic Charts" or "Mailbox Charts" in MDaemon Remote Administration to gain a graphical view of basic email patterns, top users and other key stats.

[Figure 5-3]

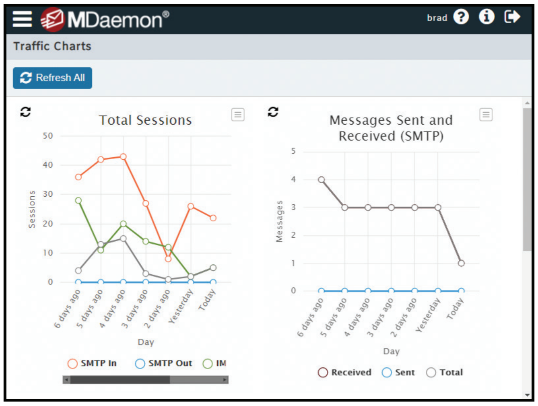


Figure 5-3

MDaemon® technologies

3.29.2021