Email Server Settings - Best Practices Guide

The following are best practice recommendations specific to the MDaemon Email Server that can also be applied to other mail servers as well. By following these recommendations, you greatly improve the overall performance of your server and reduce the chances of abuse of your domain by spammers.

Prevent Your Server from Sending Spam

Account hijack detection allows administrators to specify the maximum number of messages that an account can send in a given timeframe. Often, when a spammer manages to guess an account's login credentials, his goal is to send out as many spam messages as possible before being blocked. Account hijack detection can prevent this kind of behavior.

In MDaemon, Account Hijack Detection is configured from within the Screening section of the Security Settings configuration screen. Simply specify the maximum number of messages that can be sent, and enter a timeframe. You can optionally freeze the account when the message count limit is reached. A frozen account cannot send mail or check its mail, but MDaemon will still accept mail for the account. When an account is frozen, an email notification is sent to the administrator about the account's status. This allows administrators to be notified of problems before they are reported by end users and before the queues back up. The administrator can easily re-enable the account by replying to the email notification message.

> Instructions for enabling account hijack detection can be found in the following knowledge base article:
> https://knowledge.mdaemon.com/how-to-enable-hijack-detection

Know Who is Accessing Your System

When someone tries unsuccessfully to authenticate against an account, the administrator can be notified. These notification messages include the date, time, IP address, and protocol used during the authentication attempt. This information is also written to MDaemon's logs. With this information, the administrator can contact the user to verify the activity, change the account's password, or disable the account.

> For more information, please see the Dynamic Screening section in the following knowledge base article:
> https://knowledge.mdaemon.com/recommended-security-dynamic-screening-spam-filter-anti-virus-and-outbreak-protection-settings

Avoid Being Blacklisted

PTR records are used to map a network interface (IP) address to a host name. They allow receiving mail servers to perform a reverse DNS lookup on connections coming from your server. Many major Internet Service Providers (ISPs) require a PTR record. Having a PTR record will reduce your chances of ending up on a blacklist. Also, make sure your mail server is not an open relay. A server that acts as an open relay allows mail to pass through it that is neither "To" nor "From" a local domain. It is also recommended that you require users to use SMTP authentication when sending mail through your server.

> Instructions for configuring the IP Shield feature to prevent relaying can be found in this knowledge base article:
> https://knowledge.mdaemon.com/using-mdaemon-ip-shield

> Instructions for configuring SMTP authentication requirements can be found in the following knowledge base article:
> https://knowledge.mdaemon.com/configuring-smtp-authentication-on-the-mdaemon-server-and-outlook-mail-client

Improve Message Delivery Size and Bandwidth Management Using Outbound Attachment Linking

Outbound attachment linking can be used to reduce the size of outbound email messages. This feature places attachments in a designated directory on the mail server, and a secure link is placed in the email that points to the file. The message recipient then clicks on the link to download the file. This can greatly reduce the size of email messages and the amount of bandwidth transmitted. This feature also minimizes the chance a message is rejected by a recipient's server because it is too large. In MDaemon, Attachment Linking is enabled on a per-user basis.

> For information on enabling Attachment Linking, please see the following knowledge base article:
> https://knowledge.mdaemon.com/configure-attachment-linking

Prevent Forged Messages and Abuse

MDaemon uses multiple methods to prevent spoofing, the attempt to mislead the recipient about the origin of a message.

Sender Policy Framework (SPF) - Sender Policy Framework (SPF) is an email validation method that uses a DNS record (the SPF record) to specify what hosts are allowed to send email for a given domain. MDaemon will query the SPF record of the domain taken from the MAIL FROM header, and compare the connecting IP address with the IP addresses listed in the SPF record. If no match is found, then it is likely that the FROM header was spoofed. The spam score is then adjusted upward for messages that fail SPF lookups.

> For more information, please see the SPF Verification section in the following knowledge base article:
> https://knowledge.mdaemon.com/recommended-security-dynamic-screening-spam-filter-anti-virus-and-outbreak-protection-settings

DomainKeys Identified Mail (DKIM) - DomainKeys Identified Mail (DKIM) is another email validation method that can be used to verify that an incoming message has not been altered in any way. It does this by providing positive identification of the sender's identity along with an encrypted "hash" of the message content. The primary advantage of DKIM is that it allows domain-based whitelists and blacklists to be more effective.

> Instructions for configuring DKIM signing in MDaemon can be found in the following knowledge base article:
> https://knowledge.mdaemon.com/configure-dkim-signing

Domain-Based Message Authentication, Reporting and Conformance (DMARC) - DMARC expands on SPF and DKIM by removing the guesswork from the receiver's message handling process. Messages that don't properly pass SPF and DKIM processing are quarantined or rejected based on the sending domain's policies.

More information on DMARC can be found here:
https://knowledge.mdaemon.com/how-to-enable-dmarc-and-configure-records

TLS and SSL

TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are methods for encrypting communications between clients and servers.

> Instructions for configuring TLS for SMTP, POP and IMAP in MDaemon can be found in the following knowledge base article:
> https://knowledge.mdaemon.com/how-to-enable-configure-ssl-tls-for-smtp-pop3-imap-in-mdaemon

MDaemon® technologies