Recommended Security Settings - Best Practices Guide

This guide provides a list of recommended MDaemon security settings to protect against spam, malware, hacking & abuse.

Use Email Authentication

❑ Require SMTP Authentication

SMTP authentication is a security feature that requires a user to authenticate with a valid username and password when an email claims to come from a local user. MDaemon can be configured to require SMTP authentication for all mail sent from local users.

Knowledge Base Article:
https://knowledge.mdaemon.com/configuring-smtp-authentication-on-the-mdaemon-server-and-outlook-mail-client

❑ Use the IP Shield

The IP Shield is used to associate a domain with IP addresses that are authorized to send mail on behalf of that domain. Enabling the IP Shield and checking the "Check FROM header address against IP Shield" box can help prevent what one could call "semi-spoofing" (the "MAIL FROM" command contains a non-local email address but the "From" header contains a local address).

Knowledge Base Article:
https://knowledge.mdaemon.com/using-mdaemon-ip-shield

Protect Sensitive Data from Unauthorized Access

❑ Enable SSL & TLS

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are used to encrypt the connection between email clients and servers, and between sending and receiving email servers during delivery.

Knowledge Base Article:
https://knowledge.mdaemon.com/how-to-enable-configure-ssl-tls-for-smtp-pop3-imap-in-mdaemon

❑ Enable RequireTLS & MTA-STS

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.

MTA-STS, or Mail Transfer Agent Strict Transport Security, is an email security standard that enforces secure connections between email servers. It ensures emails are delivered using encrypted connections (TLS), preventing potential man-in-the-middle attacks.

These settings are located in MDaemon Remote Administration under **Security | SSL & TLS | SMTP Extensions**.

Knowledge Base Article:
https://knowledge.mdaemon.com/setup-mta-sts-in-mdaemon

❑ Use PGP Encryption

PGP Encryption (OpenPGP) allows MDaemon users to send and receive encrypted emails. It provides server-to-server and optionally end-to-end email encryption.

Knowledge Base Article:

https://knowledge.mdaemon.com/enable-and-configure-mdaemon-pgp

Protect Against Hacking & Abuse

❑ Prevent MDaemon from Being an Open Relay

A mail server is considered to be an open relay when email that is neither to nor from a local domain is allowed to pass through it. Open relays are often exploited by spammers. Having an open relay on your mail server can cause your IP address to be added to blocklists.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--relay_settings.html

❑ Enable MDaemon AntiVirus

MDaemon AntiVirus scans all inbound and outbound email messages for malware using the Ikarus and ClamAV antivirus engines. It also includes a mailbox scanning feature, allowing administrators to perform on-demand virus scanning.

From the MDaemon Manual:
https://help.mdaemon.com/mdaemon/en/antivirus.html

- MDaemon AntiVirus is a licensed feature that can be purchased here: https://mdaemon.com/products/mdaemon-email-antivirus-antispam

❑ Enable SMTP Screening to Protect Against Hackers

SMTP screening is used to block connections based on their activity - for example, when a given IP address connects too many times in a given timeframe, when too many reset (RSET) commands are detected in an attempt to keep a connection open, or when too many invalid recipients are detected in a session.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--smtp_screen.html

❑ Enable Dynamic (Authentication Failure) Screening

Dynamic Screening is used to block connections from sending servers that fail authentication too many times in a given timeframe. This behavior is often indicative of a bad actor trying to guess passwords in an attempt to take over an account. When too many authentication failures are detected, the connecting IP address is blocked, and if the email account used in these attempts is a valid local account, the account can optionally be frozen for a given period of time. Frozen accounts can collect mail, but the user cannot check for new email or send outbound mail until the account is un-frozen.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/dynamic-screening_auth-failure-tracking.html

❑ Enable Account Hijack Detection

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.

Knowledge Base Article:
https://knowledge.mdaemon.com/how-to-enable-hijack-detection

❑ Use Location Screening

Use Location Screening to disable SMTP/IMAP/POP connections from unauthorized regions of the world. Because spam is sent from many countries all over the world, enabling Location Screening can potentially block large amounts of spam.

Knowledge Base Article:
https://knowledge.mdaemon.com/how-to-block-incoming-connections-based-on-geographical-location-location-screening

❑ Use IP & Host Screening to Block Connections from Untrusted Servers

IP Screening and Host Screening (located in MDaemon Remote Administration under **Security | Screening**) can be used to block connections from designated servers. This is useful when a particular server has been used to send spam or phishing emails to the MDaemon server.

Knowledge Base Article:
https://knowledge.mdaemon.com/what-are-the-recommended-host-screen-settings-for-mdaemon

❑ Use Trusted Hosts & Trusted IPs Only for Trusted Connections

Many security features include a setting to exempt emails from trusted hosts and trusted IPs (located under **Security | Security Settings**) from being filtered by that particular feature. When adding IP addresses and host names to these lists, ensure that they are only used to send legitimate mail and that they are not used to send spam. Adding a spammer's IP or host name to these lists by mistake can result in unwanted spam.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--trusted_hosts.html

❑ Use Blocklists to Block Email Based on the Sender or Recipient Address

MDaemon includes sender blocklists (located under **Security | Screening**) to block incoming email from untrusted senders, and recipient blocklists to block messaages sent to certain addresses. Messages from blocked senders can either be deleted or placed in the Bad queue.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--sender-blacklist.html

❑ Require Users to use HTTPS Connections for MDaemon Webmail

HTTPS ensures an encrypted connection between the Webmail client and the MDaemon mail server. MDaemon administrators can configure MDaemon Webmail to only accept HTTPS connections, or to redirect HTTP connections to a more secure HTTPS connection. In MDaemon Remote Administration, these settings are located under **Main | Webmail Settings | SSL & HTTPS**.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/wc--https.html

❑ Enable Two-factor Authentication for MDaemon Webmail

Two-factor authentication is a security mechanism that requires users to use two forms of authentication (such as a password and a one-time code) when logging into MDaemon Webmail. MDaemon administrators can enable two-factor authentication requirements for MDaemon Webmail users via account templates **(Main | Account Templates | (Template Name) | Web Services)**.

Knowledge Base Article:
https://knowledge.mdaemon.com/enable-two-factor-authentication-webmail-remote-administration

Protect Against Spoofing

❑ Enable Reverse Lookups

When performing reverse lookups, MDaemon will attempt to acquire all of the MX and A record IP addresses for a 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.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--reverse_lookup.html

❑ Enable SPF Verification Lookups

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.

Knowledge Base Article:
https://knowledge.mdaemon.com/spf-verification-record-creation

❑ Enable DKIM Lookups

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 allow lists and blocklists to be more effective.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--dkim_verify.html

❑ Enable DMARC Lookups

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an anti-spoofing feature that helps protect against incoming spam and phishing messages that forge (spoof) the sending domain in the messages's From header. It uses a combination of SPF and DKIM lookups to validate the sender, along with policies outlined by domain owners to determine whether to quarantine or reject messages that fail DKIM & SPF lookups.

Knowledge Base Article:
https://knowledge.mdaemon.com/how-to-enable-dmarc-and-configure-records

❑ Enable From Header Screening to Help Users Identify Suspicious Senders

Spam and phishing emails often change the display name (the name-only portion) of the sender to make it appear as if the message came from somoene else. Because some smaller screens only show the display name and not the full sender email address, users can sometimes get tricked into responding to a phishing email. From Header Screening helps users identify spoofed emails by placing the actual email address found in the From header in the visible portion of the email header.

Knowledge Base Article:
https://knowledge.mdaemon.com/from-header-screening-configuration

Protect Against Spam

❑ Enbable the Spam Filter & Spam Scoring Settings

MDaenon's spam filter is based on industry-standard SpamAssassin. In MDaemon Remote Administration, you can enable the spam filter via **Spam Filter | Filter Settings | Heuristic Engine**. Inbound email messages are analyzed & compared against a list of SpamAssassin rules, and based on these rules, a spam score is assigned to the message. There are two scoring values:

- **A message is spam if it scores greater or equal to....** 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 (Fate of Spam).
- **SMTP rejects messages with scores greater or equal to...** By default, MDaemon scans messages during the SMTP session to determine whether or not they should be rejected for having a spam score above this 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. 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 it scores greater or equal to..." 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.
- The default scoring values of these settings should be sufficient for most business environments, however, these values can be adjusted up or down to make the spam filter more strict or more lenient as needed.
    - If you need to view a message's spam score, you can open it in Notepad or another text editor and review the following header: *X-Spam-Status: No, score=4.10 required=4.4*

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/sf_spam_filtering.html

❑ Train the Spam Filter via Bayesian Learning - Artificial Intelligence

Enable Bayesian Classification to train the spam filter by feeding it samples of spam and non-spam messages. You can designate a folder for spam messages and non-spam message that can be scanned manually or automatically at regular intervals. All of the messages in these 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.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/sf_bayesian.html

❑ Use DNS Blocklists to Block Mail from Known Spammers

DNS blocklists are lists of servers that are known to relay spam. When this feature is enabled, 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 can flag the message or refuse to accept it. There are several DNS blocklist services available. Zen.spamhaus.org is included by default.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/dns_black_lists_dns-bl.html

❑ Enable Automatic Spam Filter Updates

When heuristic engine updates are available, they can be applied automatically by enabling automatic spam filter updates (located under **Spam Filter | Filter Settings | Updates**)

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/sf_antispam_updates.html

❑ Enable Spambot Detection

MDaemon's Spambot Detection feature (located in Remote Administration under **Security | Screening**) can detect possible spambot activity. When MDaemon receives multiple inbound messages with the same return-path (sender) from multiple IP addresses (indicative of a spambot), the offending return-path and IP can be blocked for a designated period of time.

From the MDaemon Manual:
https://help.mdaemon.com/MDaemon/en/security--spambot_detection.html

❑ Enable the Spamhaus Data Query Service (DQS)

The Data Query Service is a set of DNS blocklists that are updated in real-time. When enabled, this feature can block up to 99% of email-borne threats.

- This is a subscription service offered by Spamhaus. More information can be found here: https://www.spamhaus.com/product/protect-email-with-spamhaus-and-mdaemon-technologies/

From the MDaemon Manual:
https://help.mdaemon.com/mdaemon/en/data_query_service.html

❑ Enable Outbreak Protection

Outbreak Protection (located in MDaemon Remote Administration under **Security | Outbreak Protection**) uses recurrent pattern detection and zero-hour technologies to identify spam and malware outbreaks often within minutes (or even seconds) after an initial outbreak. By analyzing distribution and structural mail delivery patterns in real-time, Outbreak Protection can identify malware-infected messages often before traditional antivirus software has been updated with new virus definitions.

- Outbreak Protection is a feature of MDaemon AntiVirus, a licensed feature that can be purchased here: https://mdaemon.com/products/mdaemon-email-antivirus-antispam

From the MDaemon Manual:
https://help.mdaemon.com/mdaemon/en/sp_outbreak_protection.html

---

When used together, these MDaemon security features can help protect businesses against spam, phishing, spoofing, hacking, malware, data breaches, and other email-borne threats.

MDaemon® technologies