Administration Guide

FortiMail 7.6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 09, 2026
FortiMail 7.6.4 Administration Guide
06-764-1208562-20260409

TABLE OF CONTENTS

Change log

The following is a list of documentation changes. For a list of software changes, see the FortiMail Cloud Release Notes.

Date	Change Description
2025-04-22	Initial release.
2025-04-24	Updates to FortiMail Cloud version.
2026-04-09	Add tip for using GeoIP groups with authentication servers in Configuring GeoIP groups on page 273.

Email concepts and process workflow

This section describes some basic email concepts, how FortiMail works in general, and the tools that you can use to configure your FortiMail unit.

Email protocols

There are multiple prevalent standard email protocols:

- SMTP
- POP3
- IMAP
- HTTP and HTTPS

See also Appendix: Port Numbers on page 375.

SMTP

Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending email between:

- two mail transfer agents (MTA)
- a mail user agent (MUA) and an MTA

For definitions of MTA and MUA, see Client-server connections in SMTP on page 12.

When an email user sends an email, their MUA uses SMTP to send the email to an MTA, which is often their email server. The MTA then uses SMTP to directly or indirectly deliver the email to the destination email server that hosts email for the recipient email user.

When an MTA connects to the destination email server, it determines whether the recipient exists on the destination email server. If the recipient email address is legitimate, then the MTA delivers the email to the email server, from which email users can then use a protocol such as POP3 or IMAP to retrieve the email. If the recipient email address does not exist, the MTA typically sends a separate email message to the sender, notifying them of delivery failure.

While the basic protocol of SMTP is simple, many SMTP servers support a number of protocol extensions for features such as authentication, encryption, multi-part messages and attachments, and may be referred to as extended SMTP (ESMTP) servers.

FortiMail units can scan SMTP traffic for spam and viruses, and support several SMTP extensions.

POP3

Post Office Protocol version 3 (POP3) is a standard protocol used by email clients to retrieve email that has been delivered to and stored on an email server.

Unlike IMAP, after a POP3 client downloads an email to the email user's computer, a copy of the email usually does **not** remain on the email server's hard disk. The advantage of this is that it frees hard disk space on the server. The disadvantage of this is that downloaded email usually resides on only one personal computer. Unless all of their POP3 clients are always configured to leave copies of email on the server, email users who use multiple computers to view email, such as both a desktop and laptop, will not be able to view from one computer any of the email previously downloaded to another computer.

FortiMail units do not scan POP3 traffic for spam and viruses.

IMAP

Internet Message Access Protocol (IMAP) is a standard protocol used by email clients to retrieve email that has been delivered to and stored on an email server.

Unless configured for offline availability, IMAP clients typically initially download only the message header. They download the message body and attachments only when the email user selects to read the email.

Unlike POP3, when an IMAP client downloads an email to the email user's computer, a copy of the email remains on the email server's hard disk. The advantage of this is that it enables email users to view email from more than one computer. This is especially useful in situations where more than one person may need to view an inbox, such where all members of a department monitor a collective inbox. The disadvantage of this is that, unless email users delete email, IMAP may more rapidly consume the server's hard disk space.

FortiMail units do not scan IMAP traffic for spam and viruses, but may use IMAP when operating in server mode, when an email user retrieves their email.

HTTP and HTTPS

Secured and non-secured HyperText Transfer Protocols (HTTP/HTTPS), while not only for the transport of email, are often used by webmail applications to view email that is stored remotely.

FortiMail units do not scan HTTP or HTTPS traffic for spam or viruses, but use them to display quarantines and, if the FortiMail unit is operating in server mode, FortiMail webmail.

Client-server connections in SMTP

Client-server connections and connection directionality in SMTP differ from how you may be familiar with them in other protocols.

For example, in the SMTP protocol, an SMTP client connects to an SMTP server. This seems consistent with the traditional client-server model of communications. However, due to the notion of relay in SMTP, the SMTP client may be either:

- an email application on a user's personal computer
- another SMTP server that acts as a delivery agent for the email user, relaying the email to its destination email server

The placement of clients and servers within your network topology may affect the operation mode you choose when installing a FortiMail unit. If your FortiMail unit will be operating in gateway mode or server mode, SMTP clients — including SMTP servers connecting as clients — must be configured to connect to the FortiMail unit.

Terms such as MTA and MUA describe server and client relationships specific to email protocols.

MTA

A Mail Transfer Agent (MTA) is an SMTP server that relays email messages to another SMTP server.

Not all MTAs are full email servers: some MTAs exist solely to relay email, and do not host email user accounts.

FortiMail units operating in gateway mode function as an MTA. FortiMail units operating in server mode function as an MTA and full (SMTP, IMAP, POP3, webmail) email server.

To deliver email, unless the email is incoming and the email server has no domain name and is accessed by IP address only, an MTA must query a DNS server for the MX record and the corresponding A record. For more information, see DNS role in email delivery on page 15.

MUA

A Mail User Agent (MUA), or email client, is software such as Microsoft Outlook that enables users to send and receive email.

FortiMail units support SMTP connections for sending of email by a MUA.

FortiMail units operating in server mode support POP3 and IMAP connections for retrieval of email by a MUA. For email users that prefer to use their web browsers to send and retrieve email instead of a traditional MUA, FortiMail units operating in server mode also provide FortiMail webmail.

Connection directionality versus email directionality

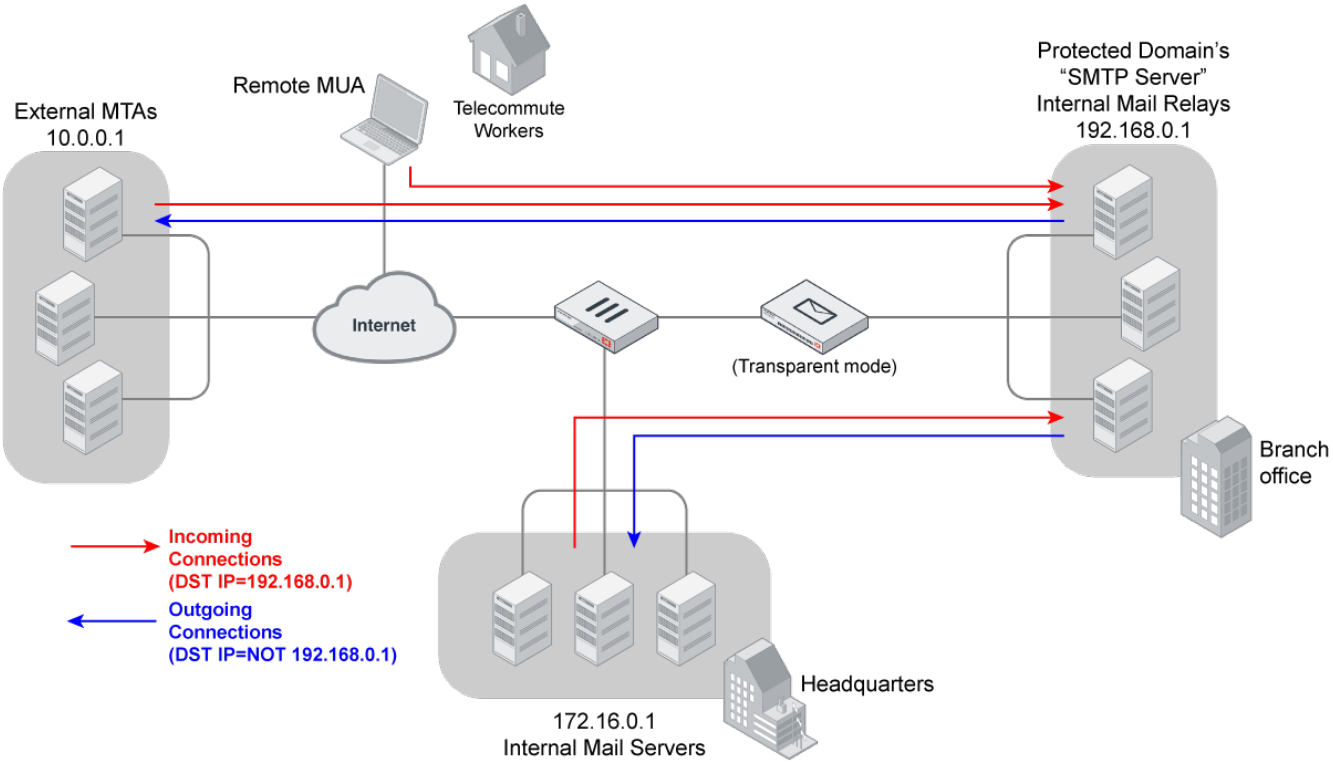
Many FortiMail features such as proxies and policies act upon the directionality of an SMTP connection or email message.

Incoming SMTP connections consist of those destined for the SMTP servers that are protected domains of the FortiMail unit. For example, if the FortiMail unit is configured to protect the SMTP server whose IP address is 192.168.0.1, the FortiMail unit treats all SMTP connections destined for 192.168.0.1 as incoming.

Outgoing connections consist of those destined for SMTP servers that the FortiMail unit has not been configured to protect. For example, if the FortiMail unit is **not** configured to protect the SMTP server whose IP

address is 10.0.0.1, all SMTP connections destined for 10.0.0.1 will be treated as outgoing, regardless of their origin.

Incoming versus outgoing SMTP connections



Incoming versus outgoing email

Incoming email messages consist of messages sent to the protected domain recipients (`RCPT TO:`). For example, if the FortiMail unit is configured to protect the SMTP server whose domain name is example.com, the FortiMail unit treats all email messages sent to example.com as incoming email.

Outgoing email messages consist of messages sent to recipients (`RCPT TO:`) on domains that the FortiMail unit is **not** configured to protect. For example, if the FortiMail unit is **not** configured to protect the domain example.com, all email messages sent to recipients at example.com will be treated as outgoing email, regardless of their origin.

Directionality at the connection level may be different than directionality at the level of email messages contained by the connection. It is possible that an incoming connection could contain an outgoing email message, and vice versa.

For example, in the above figure, connections from the internal mail relays to the internal mail servers are outgoing connections, but they contain incoming email messages. Conversely, connections from remote MUAs to the internal mail relays are incoming connections, but may contain outgoing email messages if the recipients' email addresses (`RCPT TO:`) are external.

Because directionality is considered separately at the network layer and the application layer, the directionality of an SMTP connection can be the opposite of the directionality of an email message: the connection may be destined for an SMTP server that is not associated with a protected domain, while the recipient email address is associated with a protected domain, or vice versa.

DNS role in email delivery

SMTP can be configured to operate without DNS, using IP addresses instead of domain names for SMTP clients, SMTP servers, and recipient email addresses. However, this configuration is rare.

SMTP as it is typically used relies upon DNS to determine the mail gateway server (MX) for a domain name, and to resolve domain names into IP addresses. As such, you usually must configure email servers and FortiMail units to be able to query a DNS server.

In addition, you may also be required to configure the DNS server with an MX record, an A record, and a reverse DNS record for protected domain names and for the domain name of the FortiMail unit itself.

MX record

Mail exchanger (MX) records are configured on a DNS server. MX records for a domain name indicate designated email servers or email gateways that deliver email to that domain, and their order of preference. In their most simple form, MX records use the following format:

```
example.com IN MX 10 mail.example.com
```

where:

- `example.com` is the name of the domain
- `IN` indicates the Internet protocol class
- `MX` indicates that the DNS resource record is of the MX type
- `10` indicates the order of preference (greater values indicate lower preference)
- `mail.example.com` is the host name of an email server or gateway

When an email client sends an email, the sender's MTA queries a DNS server for the MX record of the domain name in the recipient's email address. To resolve the host name of the MTA referenced by the MX record, it then queries for the A record of the destination MTA. That A record provides the IP address of the email server or gateway. The sender's MTA then attempts to deliver the email to that IP address.

For example, if the recipient email address is user1@example.com, in order to deliver the email, the sender's MTA would query the MX and A records to determine the IP address of the email gateway of example.com.

Often, the domain name and/or IP address of the email domain is different from that of its email server or gateway. The fully qualified domain name (FQDN) of an email server or gateway may be a subdomain or another domain name entirely, such as that of the MTA of an Internet service provider (ISP). For example, the email gateways for the email domain example.com could be mail1.example.com and mail2.example.com, or mail.isp.example.net.

If your FortiMail unit will operate in transparent mode, and you will configure it be fully transparent at both the IP layer and in the SMTP envelope and message headers by enabling Hide this box from the mail server in the session profile, Configuring protected domains in the protected domain, and Use client-specified SMTP server to send email for the proxies, no MX record changes are required.

If your FortiMail unit will operate in gateway mode or server mode, or in transparent mode while not configured to be fully transparent, you must configure the public DNS server for your domain name with an MX record that refers to the FortiMail unit which will operate as the email gateway, such as:

```
example.com IN MX 10 fortimail.example.com
```

If your FortiMail unit will operate in gateway mode or server mode, or in transparent mode while not fully transparent, configure the MX record to refer to the FortiMail unit, and remove other MX records. If you do not configure the MX record to refer to the FortiMail unit, or if other MX records exist that do not refer to the FortiMail unit, external MTAs may not be able to deliver email to or through the FortiMail unit, or may be able to bypass the FortiMail unit. If you have configured secondary MX records for failover reasons, consider configuring FortiMailhigh availability (HA) instead. For details, see FortiMail high availability modes.

Exceptions include if you are configuring a private DNS server for use with the Use MX Record option. In that case, rather than referencing the FortiMail unit as the mail gateway and being used by external SMTP servers to route mail, the MX record references the protected SMTP server and is used by the FortiMail unit to define the SMTP servers for the protected domain.

A record

Address records (A records) are configured on a DNS server. A records indicate the IP address to which a host name resolves. In their most simple form, A records use the following format:

```
mail IN A 192.168.1.10
```

where:

- `mail` is the name of the host
- `IN` indicates the Internet protocol class
- `A` indicates that the DNS resource record is of the IPv4 address type
- `192.168.1.10` indicates the IP address that hosts the domain name

When an email client sends an email, the sender's MTA queries a DNS server for the MX record of the domain name in the recipient's email address. To resolve the host name of the MTA referenced by the MX record, it then queries for the A record of the destination MTA. That A record provides the IP address of the email server or gateway. The sender's MTA then attempts to deliver the email to that IP address.

You must configure the public DNS server for your host names with an A record to resolve the host names referenced in MX records, and the host name of the FortiMail unit, if any. For example, if an MX record is:

```
example.com IN MX 10 fortimail.example.com
```

the required A record in the example.com zone file might be:

```
fortimail IN A 192.168.1.15
```

Reverse DNS record

Because the SMTP protocol does not strictly require SMTP clients to use their own domain name during the SMTP greeting, it is possible to spoof the origin domain. In an attempt to bypass antispam measures against domain names known to be associated with spam, spammers often exploit that aspect of SMTP by pretending to send email from legitimate domains.

For example, the spammer spam.example.com might initiate an SMTP session with the command:

```
EHLO nonspam.example.edu
```

To prevent this form of attack, many SMTP servers query reverse DNS records to verify that the domain name provided in the SMTP greeting genuinely matches the IP address of the connecting SMTP client.

You should configure the public DNS server for your protected domain names with a reverse DNS record to resolve the IP addresses of your protected SMTP servers and/or FortiMail unit into domain names.

For example, if the outgoing MTA for example.com is the FortiMail unit, fortimail.example.com, and the public network IP address of the FortiMail unit is 10.10.10.1, a public DNS server's reverse DNS zone file for the 10.10.10.0/24 subnet might contain:

```
1 IN PTR fortimail.example.com.
```

where `fortimail.example.com` is the FQDN of the FortiMail unit.

Reverse DNS records are required for FortiMail units operating in gateway mode or server mode. However, they are also required for FortiMail units operating in transparent mode, unless they have been configured to be completely transparent.

How FortiMail processes email

FortiMail units receive email for defined email domains and control relay of email to other domains. Email passing through the FortiMail unit can be scanned for viruses and spam. Policies and profiles govern how the FortiMail unit scans email and what it does with email messages containing viruses or spam. For information about policies, see Configuring policies on page 144. For information about profiles, see Configuring profiles on page 171.

In addition to policies and profiles, other configured items, such as email domains, may affect how your FortiMail unit processes email.

See also:

- Email domains
- Access control rules
- Recipient address verification
- Disclaimer messages and customized appearance
- Advanced delivery features
- Antispam techniques
- Order of execution for antispam scans

Email domains

An email domain is a set of email accounts that reside on a particular email server. The email domain name is the portion of the user's email address following the @ symbol.

FortiMail units can be configured to protect email domains (referred to as "**protected domains**" in this Administration Guide) by defining policies and profiles to scan and relay incoming and outgoing email.

If the FortiMail unit is operating in gateway mode or transparent mode, there is one local email domain that represents the FortiMail unit itself. If the FortiMail unit is operating in server mode, protected domains reside locally on the FortiMail unit's built-in email server.

For information about creating protected domains, see Configuring protected domains on page 92.

In transparent mode, each network interface includes a proxy and/or implicit MTA that receives and relays email. By default, the proxy/implicit MTA responds to SMTP greetings (HELO/EHLO) using the host name of the SMTP server of the protected domain. This "masquerade" hides the existence of the FortiMail unit. For information on configuring the SMTP greeting, see Configuring protected domains on page 92.

Access control rules

The access control rules allow you to control how email messages move to, from, and through the FortiMail unit. Using access control rules the FortiMail unit can analyze email messages and take action based on the result. Messages can be examined according to the sender email address, recipient email address, and the IP address or host name of the system delivering the email message.

Each access control rule specifies an action to be taken for matching email.

For information about configuring access control rules, see Configuring access control receiving policies on page 148.

Recipient address verification

Recipient address verification ensures that the FortiMail unit rejects email with invalid recipients and does not scan or send them to the protected email server. This verification can reduce the load on the FortiMail unit when a spammer tries to send messages to every possible recipient name on the email server.

If you want to use recipient address verification, you need to verify email recipient addresses by using either the email server or an LDAP server.

Usually you can use the email server to perform address verification. This works with most email servers that provide a `User unknown` response to invalid addresses.

For instructions on configuring recipient address verification, see Configuring protected domains on page 92.

Disclaimer messages and customized appearance

You can customize both the disclaimer and replacement messages, as well as the appearance of the FortiMail unit interface.

The disclaimer message is attached to all email, generally warning the recipient the contents may be confidential.

Replacement messages are messages recipients receive instead of their email. These can include warnings about messages sent and incoming messages that are spam or infected with a virus. See Configuring custom messages on page 71.

You can customize the appearance of the FortiMail unit web pages visible to mail administrators to better match a company look and feel. See Customizing custom messages, and email templates on page 71.

Advanced delivery features

Processing email takes time. Processing delays can cause clients and servers to time out. To reduce this problem, you can:

- defer delivery to process oversized email at a time when traffic is expected to be light
- send delivery status notifications (DSN)

For full configuration and procedural details regarding oversized emails, see Downloading oversized email attachments.

Antispam techniques

Spam detection is a key feature of the FortiMail unit. The feature is based on two tiers of spam defense:

- FortiMail antispam techniques
- FortiGuard Antispam service

Each tier plays an important role in separating spam from legitimate email. FortiGuard Antispam delivers a highly-tuned managed service for the classification of spam while the FortiMail unit offers superior antispam detection and control technologies.

In addition to scanning incoming email messages, FortiMail units can also inspect the content of outgoing email messages. This can help eliminate the possibility that an employee or a compromised computer could send spam, resulting in the blocklisting of your organization's email servers.

For more information on FortiMail antispam techniques, see Configuring profiles on page 171 and Configuring security settings on page 276.

FortiMail antispam techniques

The following table highlights some of the FortiMail antispam techniques. For information about how these techniques are executed, see Order of execution for antispam scans on page 22.

FortiMail antispam technique highlights

Greylist scanning	See Configuring greylisting on page 300.
DNSBL scanning	In addition to supporting Fortinet's FortiGuard Antispam DNSBL service, the FortiMail unit supports third-party DNS Blocklist servers. See DNSBL section on page 196.
SURBL scanning	In addition to supporting Fortinet's FortiGuard Antispam SURBL service, the FortiMail unit supports third-party Spam URL Realtime Block Lists servers. See SURBL section on page 195.

Bayesian scanning	See Training the Bayesian databases on page 316.
Heuristic scanning	See Heuristic section on page 195.
Image spam scanning	See Image spam section on page 199.
PDF scanning	See Scan PDF attachment on page 188.
Block/safe lists	• For information on global block/safe lists, see Managing the global block and safe list on page 296. • For information on domain-wide block/safe lists, see Managing the per-domain block lists and safe lists on page 297. • For information on personal block/safe lists, see Managing the personal block lists and safe lists on page 298. • For information on session block/safe lists, see Configuring sender reputation options on page 173.
Banned word scanning	See Banned word section on page 197.
Safe list word scanning	See Safelist word section on page 198.
Sender reputation	See Viewing sender reputation statuses on page 60.

FortiGuard Antispam service

The FortiGuard Antispam service is a Fortinet-managed service that provides a three-element approach to screening email messages.

The first element is a DNS Block List (DNSBL) which is a “living” list of known spam origins.

The second element is in-depth email screening based on a Uniform Resource Identifier (URL) contained in the message body – commonly known as Spam URL Real-time Block Lists (SURBLs).

The third element is the FortiGuard Antispam Spam Checksum Blocklist (SHASH) feature. Using SHASH, the FortiMail unit sends a hash of an email to the FortiGuard Antispam server which compares the hash to hashes of known spam messages stored in the FortiGuard Antispam database. If the hash results match, the email is flagged as spam.

FortiGuard query results can be cached in memory to save network bandwidth.

FortiGuard Antispam DNSBL

To achieve up-to-date real-time identification, the FortiGuard Antispam service uses globally distributed spam probes that receive over one million spam messages per day. The FortiGuard Antispam service uses multiple layers of identification processes to produce an up-to-date list of spam origins. To further enhance the service

and streamline performance, the FortiGuard Antispam service continuously retests each of the “known” identities in the list to determine the state of the origin (active or inactive). If a known spam origin has been decommissioned, the FortiGuard Antispam service removes the origin from the list, thus providing customers with both accuracy and performance.

The FortiMail FortiGuard Antispam DNSBL scanning process works this way:

1. Incoming email (SMTP) connections are directed to the FortiMail unit.
2. Upon receiving the inbound SMTP connection request, the FortiMail unit extracts the source information (sending server’s domain name and IP address).
3. The FortiMail unit transmits the extracted source information to Fortinet’s FortiGuard Antispam service using a secure communication method.
4. The FortiGuard Antispam service checks the sender’s source information against its DNSBL database of known spam sources and sends the results back to the FortiMail unit.
5. The results are cached on the FortiMail unit.
    - If the results identify the source as a known spam source, the FortiMail unit acts according to its configured policy.
    - The cache on the FortiMail unit is checked for additional connection attempts from the same source. The FortiMail unit does not need to contact the FortiGuard Antispam service if the results of a previous connection attempt are cached.
        - Additional connection requests from the same source do not need to be submitted to the FortiGuard Antispam service again because the classification is stored in the system cache.

Once the incoming connection has passed the first pass scan (DNSBL), and has not been classified as spam, it will then go through a second pass scan (SURBL) if the administrator has configured the service.

FortiGuard Antispam SURBL

To detect spam based on the message body URLs (usually web sites), Fortinet uses FortiGuard Antispam SURBL technology. Complementing the DNSBL component, which blocks messages based on spam origin, SURBL technology blocks messages that have spam hosts mentioned in message bodies. By scanning the message body, SURBL is able to determine if the message is a known spam message regardless of origin. This augments the DNSBL technology by detecting spam messages from a spam source that may be dynamic, or a spam source that is yet unknown to the DNSBL service. The combination of both technologies provides a superior managed service with higher detection rates than traditional DNSBLs or SURBLs alone.

The FortiMail FortiGuard Antispam SURBL scanning process works this way:

1. After accepting an incoming SMTP connection (passed first-pass scan), the email message is received.
2. After an incoming SMTP connection has passed the DNSBL scan, the FortiMail unit accepts delivery of email messages.
3. The FortiMail unit generates a signature (URL) based on the contents of the received email message.
4. The FortiMail unit transmits the signature to the FortiGuard Antispam service.
5. The FortiGuard Antispam service checks the email signature against its SURBL database of known signatures and sends the results back to the FortiMail unit.
6. The results are cached on the FortiMail unit.
    - If the results identify the signature as known spam email content, the FortiMail unit acts according to its configured policy.
    - Additional connection requests with the same email signature do not need to be re-classified by the FortiGuard Antispam service, and can be checked against the classification in the system cache.

- Additional messages with the same signature do not need to be submitted to the FortiGuard Antispam service again because the signature classification is stored in the system cache.

Once the message has passed both elements (DNSBL and SURBL), it goes to the next layer of defense; the FortiMail unit that includes additional spam classification technologies.

Order of execution for antispam scans

The following table shows the sequential order of FortiMail antispam scans during an SMTP connection. You can use the table to design a configuration to achieve intended results, and to optimize performance.

Only antispam techniques are shown. Other features may occur in parallel. Disabled scans are skipped. Some features also cause later antispam scans to be skipped. **Sort order of rows is by when scans end** and action occurs, not by when scans start (which could be earlier for complex scans).

Order of execution is configurable for safe lists and block lists. See the FortiMail CLI Reference. In this table, default order is shown.

By default, safe lists cause sender authentication (DKIM, SPF, DMARC) to be skipped, even though sender email addresses could be fake. This is configurable. See the FortiMail CLI Reference.

Actions are usually configurable, either in the profile's general Default action, or in each scan. Actions can be complex and determined by many factors, not only by antispam.

Categories include:

- **Final actions**: Reject, discard, rewrite, personal quarantine, and system quarantine. **If a final action occurs, skip remaining scans.**
- **Non-final actions**: Tag, add header, replace, archive, notify, BCC, and encrypt. If a non-final action occurs, more scans and actions can still occur.
- **Delivery actions**: After scans occur, delivery can be to the original host, alternate host, and BCC.

Factors include:

- If an antivirus and antispam scan ends with non-final actions, attachment scans still occur but skip content monitoring.
- If a FortiSandbox scan occurs, content monitoring still occurs.
- If FortiGuard Antispam and IP Reputation detects spam, skip remaining antispam scans, even though the actions are not final.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
Client initiates SMTP session with the FortiMail unit			
Sender reputation	• Client IP address (a.k.a. last hop address)	If the score is bad, perform the action. Else continue.	Add the IP address to the sender reputation database. Keep a reputation score based on the email. Continue.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
FortiGuard block IP	• Client IP address	Reject the email.	Continue.
Endpoint reputation	• Client endpoint ID	If the score is bad, perform the action. Else continue.	Add the IP address to the endpoint reputation database. Keep a reputation score based on the email. Continue.
Sender rate control per connection	• Client IP address	Apply limitations in the session profile.	Continue.
HELO/EHLO command received from SMTP client			
HELO/EHLO	• Domain name in the `HELO/EHLO`	If invalid characters are in the domain name, reject the `HELO/EHLO` command. Do not continue until a proper `HELO/EHLO` command is received.	Continue.
MAIL FROM: and RCPT TO: commands received from SMTP client			
Sender rate control per message	• Client IP address	Apply limitations in the session profile.	Continue.
Sender domain check	• Sender in the SMTP envelope (`MAIL FROM:`)	Return an error to the SMTP client. The error depends on which check failed.	Continue.
Recipient verification (for unknown recipients)	• Recipient in the SMTP envelope (`RCPT TO:`)	Reject the email.	Continue.
System safe list (Phase I)	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`)	Skip remaining antispam checks (but not antivirus and content checks).	Continue.
Greylist	• Sender in the SMTP envelope (`MAIL FROM:`) • Recipient in the SMTP envelope (`RCPT TO:`) • Client IP address subnet	Continue. **Note:** Skip this scan if the access control rule's action is *Relay*.	Return a temporary failure code to the SMTP client.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
Session sender safe list (Phase I)	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`)	Skip remaining antispam checks (but not the antivirus and content checks).	Continue.
Session sender block list (Phase I)	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`)	Perform the action.	Continue
Authentication difference	• Sender in the SMTP envelope (`MAIL FROM:`) • Authenticated username	Reject the email.	Continue.
Bounce verification	• Recipient in the SMTP envelope (`RCPT TO:`)	Perform the action.	Continue.
Access control rules	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Recipient in the SMTP envelope (`RCPT TO:`)	Perform the action.	• If recipient is in a protected domain, the default action is *Relay*. • Otherwise, the default action is *Reject*.
Check recipient domain	• Recipient in the SMTP envelope (`RCPT TO:`)	Return an error to the SMTP client. The error depends on which check failed.	Continue.
DATA command received from SMTP client			
System safe list (Phase II)	• Sender in message headers (`From:` and `Reply-to:`)	Skip remaining antispam checks (but not the antivirus and content checks).	Continue.
System block list	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:`	Perform the action.	Continue.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
	and `Reply-to:`)		
Session sender safe list (Phase II)	Sender in message headers (`From:` and `Reply-to:`)	Skip remaining antispam checks (but not the antivirus and content checks).	Continue.
Session sender block list (Phase II)	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:` and `Reply-to:`)	Perform the action.	Continue.
Session recipient safe list	• Recipient in the SMTP envelope (`RCPT TO:`) • Recipient in message headers (`To:`)	Skip remaining antispam checks (but not the antivirus and content checks). **Note:** If there are multiple recipients, the action only applies to safelisted recipients	Continue.
Session recipient block list	• Recipient in the SMTP envelope (`RCPT TO:`) • Recipient in message headers (`To:`)	Reject the email.	Continue.
Domain safe list	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:` and `Reply-to:`)	Skip remaining antispam checks (but not the antivirus and content checks).	Continue.
Domain block list	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:` and `Reply-to:`)	Perform the action.	Continue.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
Personal safe list	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:` and `Reply-to:`)	Skip remaining antispam checks (but not the antivirus and content checks).	Continue.
Personal block list	• Client IP address • Sender in the SMTP envelope (`MAIL FROM:`) • Sender in message headers (`From:` and `Reply-to:`)	Discard the email.	Continue.
End of message (EOM) command received from SMTP client			
Antivirus	• Body • Attachments	If the antispam profile is configured to treat viruses as spam, perform the action in Default action.	Continue.
Safe list word	• Subject line • Body	Skip remaining antispam checks.	Continue.
FortiGuard Antispam	• Message headers • Body	Perform the action. Skip remaining antispam checks.	Continue.
DMARC (SPF and DKIM)	• Client IP address	Perform the action. **Note:** If *ARC override* is enabled for DMARC, then the ARC result determines the action instead.	Continue.
SPF	• Client IP address	Perform the action. **Note:** If *ARC override* is enabled for SPF, then the ARC result determines the action instead.	Continue.
DKIM	• Message headers • Body	Perform the action. **Note:** If *ARC override* is enabled for DKIM, then the ARC result determines the action instead.	Continue.
ARC	• Message headers	Perform the action.	Continue.

Check	Check Involves	Action If Positive (Match Found)	Action If Negative
Spam outbreak protection	• Message headers • Body	Perform the action.	Continue.
Behavior analysis	• Message body	Perform the action.	Continue.
Impersonation	• Message headers	Perform the action.	Continue.
Banned word	• Subject line • Body	Perform the action.	Continue.
Dictionary	• Body	Perform the action.	Continue.
DNSBL	• Client IP address	Perform the action.	Continue.
SURBL	• Body	Perform the action.	Continue.
Heuristic	• Body	Perform the action.	Continue.
Image spam	• Body (embedded images) • Attachments (if *Aggressive* is enabled in the antispam profile)	Perform the action.	Continue.
Header analysis	• Message headers	Perform the action.	Continue.
Bayesian	• Body	Perform the action.	Continue.
Suspicious newsletter	• Message headers • Body	Perform the action.	Continue.
Content	• Message headers • Body • Attachments	Perform the action.	Continue.
DLP	• Message headers • Body • Attachments	Perform the action.	Continue.

See also

Order of execution of policies

Configuring antispam profiles

Configuring antivirus profiles

Using the dashboard

Dashboard displays system statuses, most of which pertain to the entire system, such as CPU usage and mail statistics.

This section includes:

- Viewing the dashboard

Viewing the dashboard

Dashboard > *Status* displays first after you log in to the GUI. It contains a dashboard with widgets that each indicate performance level or other statistics.

By default, widgets display the FortiMail serial number and current system status, including alert messages, system time, and email throughput.

Hiding, showing, and moving widgets

The dashboard is customizable. You can select which widgets to display, where they are located on the tab, and whether they are minimized or maximized.

To move a widget, position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To show or hide a widget select *Manage Widget* and then select the widgets you want displayed on the Dashboard. If the widget is grayed out, the widget will not display. Select *Apply* when you have made your selections.

Options vary slightly from widget to widget, but always include options to close, refresh, or minimize/maximize the widget.

FortiMail Cloud low resource user add-on feature (license based)

This license-based add-on feature behaves as a user accounting tool in deployments with a large number of users where most of them use few resources. Many users normally could make a deployment cost-prohibitive, so this license aligns the cost with their reduced system resource usage.

For example, large educational organizations have a large student-to-staff ratio, yet student email accounts have a fraction of the email volume of teachers. This license reduces the costs of email accounts for the students.

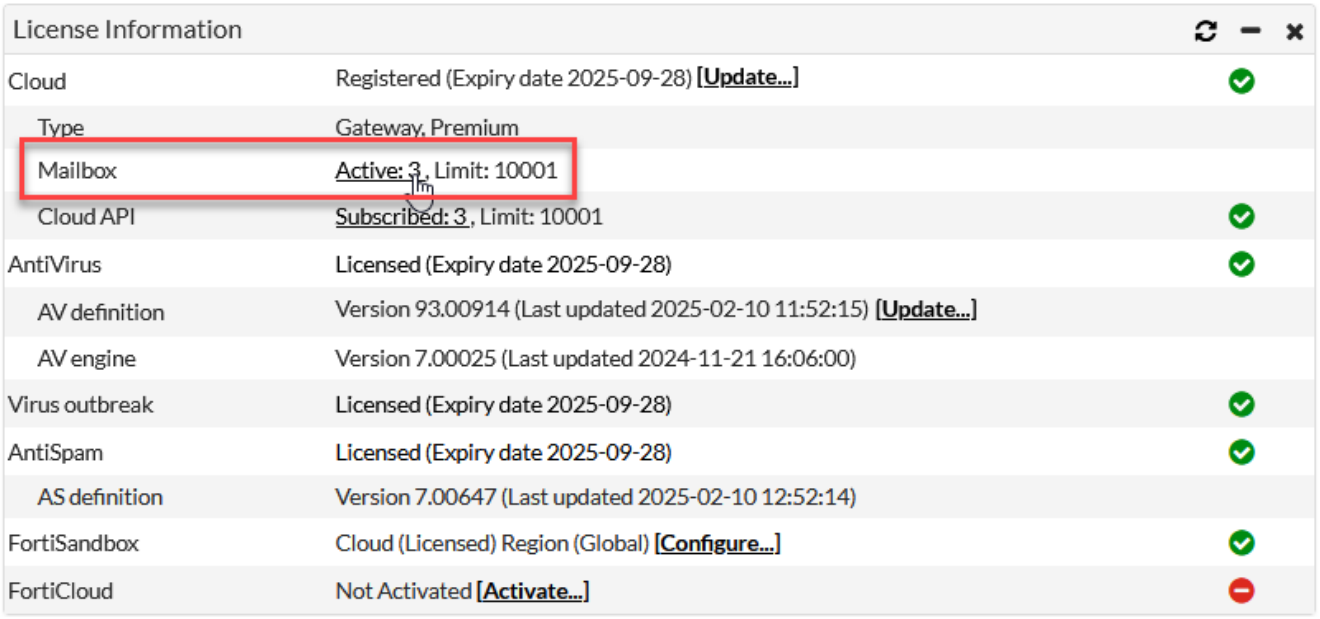
This FortiMail Cloud feature requires the purchase of SKU FC-10-FECLD-599-02-12. For more information, contact https://support.fortinet.com/.

You can view the status of low-resource additional users by going to Dashboard > Status in the License Information widget, where the number of Active accounts, the total Limit, and your Regular and Additional maximum values are displayed.

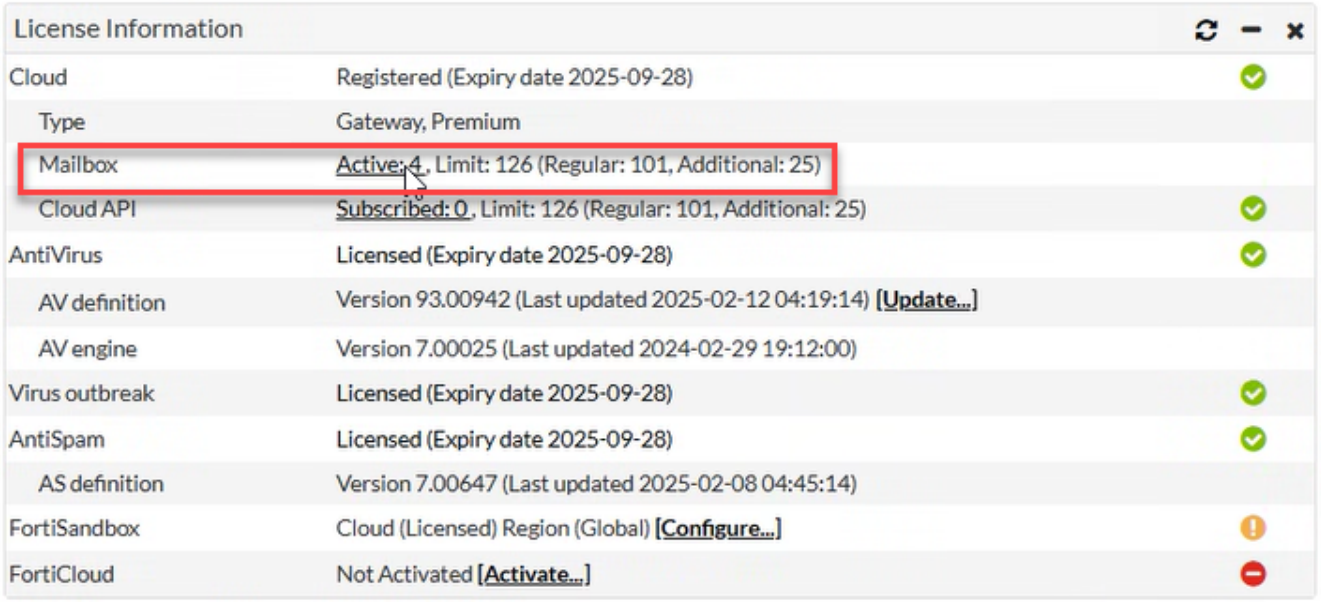
Active mailbox user list

On *Dashboard* > *Status*, in the *License Information* widget, there may be a row named *Mailbox*. Depending on the feature license, it may display numbers for recipient usernames on protected domains ("mailboxes").

License Information widget showing the active username count in FortiMail Cloud



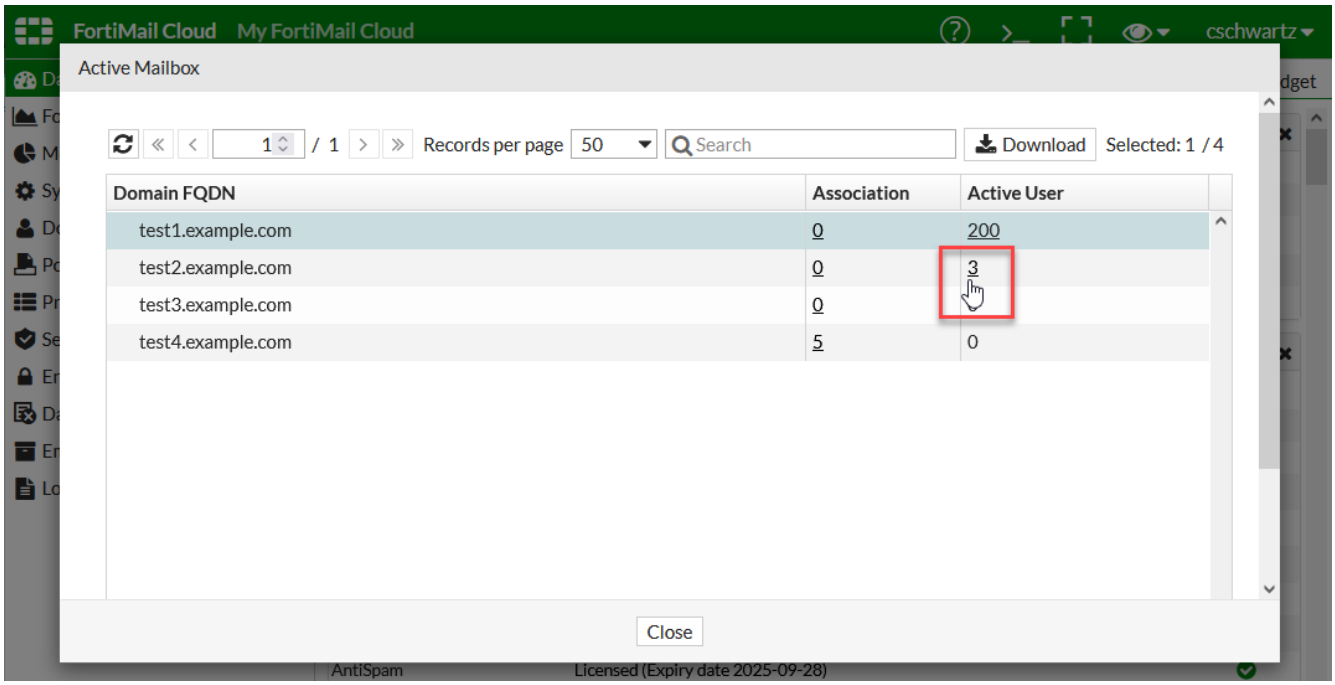
License Information widget showing the active username count in FortiMail Cloud with Low Resource User Add-on feature license

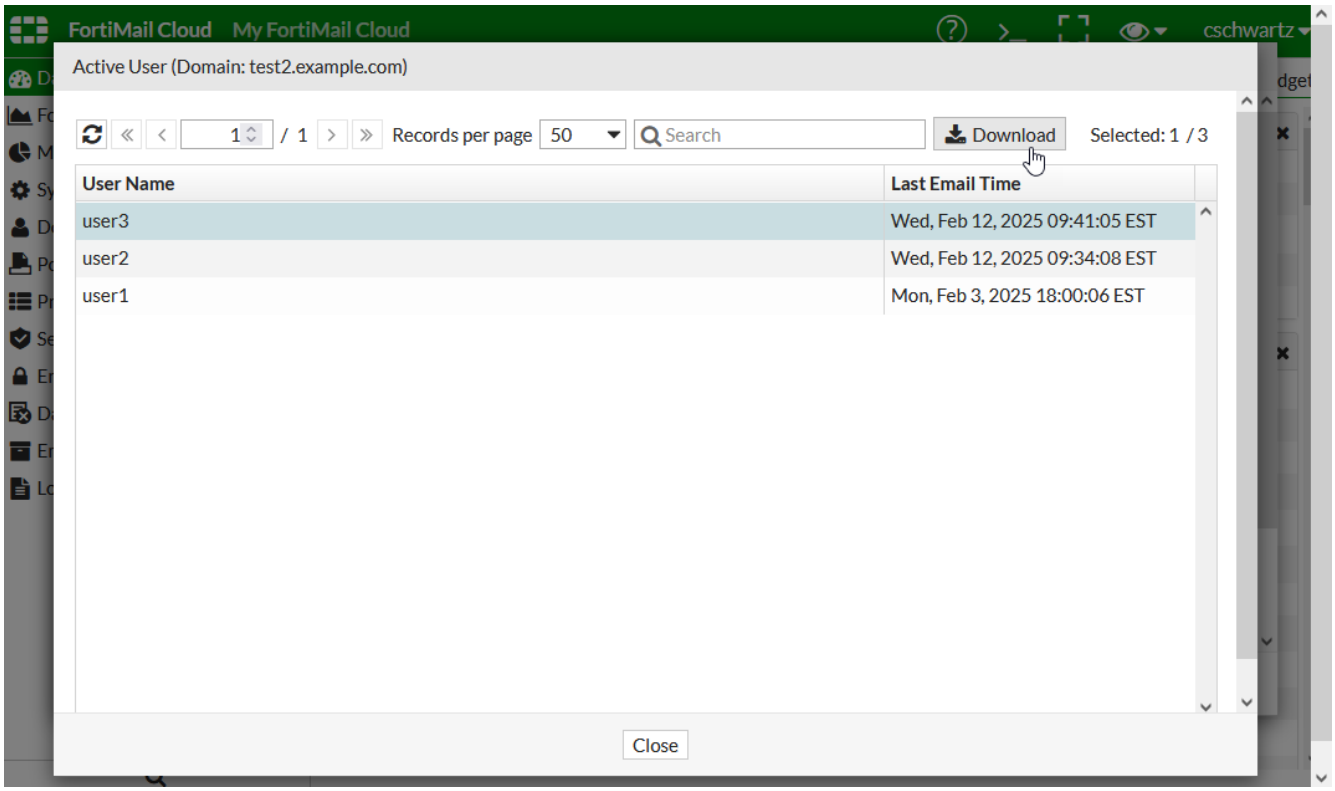


GUI item	Description
Active	Number of usernames where email was delivered in the past 30 days. This does not include sent email. Alternatively, to get statistics about recently used mailboxes, you can use reports or FortiView (see Configuring mailbox statistics reports on page 350 and Viewing mail statistics on page 33).
Limit	Maximum total number of usernames allowed by the service license.
Regular	Number of usernames that are allowed standard system resource usage. *Regular* only appears if you have the FortiMail Cloud Low Resource User Add-on feature license.
Additional	Number of usernames that are allowed less system resource usage. *Additional* only appears if you have the FortiMail Cloud Low Resource User Add-on feature license.

If you click *Active*, a dialog appears with a list of protected domains, and how many of the active usernames belong to each domain. Click the links in the columns to display either:

- *Association*
  Number of active usernames in each associated domain.
- *Active User*
  Active usernames, and when email was recently delivered to each username.





Alternatively, to get the same information as the *Active User* dialog, you can either:

- click *Download* to download the list in a comma-separated values (CSV) file format that you can open in spreadsheet software such as Microsoft Excel
- go to *Domain & User* > *Domain* > *Domain* and then click the number in the *Active User* column

Using FortiView

FortiView provides detailed summary of the mail, threat, and IP session statistics.

This section includes:

- Viewing mail statistics
- Viewing threat statistics

Viewing mail statistics

Your FortiMail unit can show data about the number of email in each time period that the FortiMail unit detected with viruses, spam, or neither. It can also track the file sizes of email, scan speed, and transfer speed.

For email messages classified as spam, mail statistics include which FortiMail feature classified the email as spam, such as access control rules, the system-wide block list, or per-user block lists.

For email that is not classified as spam by any antispam scan, mail statistics label it as *Not Spam*.

In addition to viewing overall trends via the graph, you can also view details at each point in time. To view these details, hover your mouse over a bar in the graph. A tool tip appears next to that point on the graph, including the name of the antispam category, message count, and percentage relative to the overall mail volume at that time.

To view mail statistics

1. If you want to view statistics about mailboxes or domain-level mail statistics, purchase the feature license and enable the feature. See Mailbox accounting service on page 1 and Domain mail statistics on page 1.

   By default, their corresponding areas of the GUI are hidden and disabled.
2. Configure your FortiMail unit to detect spam and/or viruses. See Configuring profiles on page 171 and Configuring policies on page 144.
3. Go to:
   - *FortiView > Mail Statistics > By Count*
   - *FortiView > Mail Statistics > By Size*
   - *FortiView > Mail Statistics > By Scan Speed*
   - *FortiView > Mail Statistics > By Transfer Speed*
   - *FortiView > Mail Statistics > Active Mailbox*

   Alternatively, instead of using the graph in FortiView, you can generate reports on the total number of active mailboxes during a particular time period, or use the dashboard to get the current number of active mailboxes and a list of their usernames. For details, see Configuring mailbox statistics reports on page 350 and Active mailbox user list on page 30.

Microsoft 365 and Google Workspace notification statistics

For FortiMail units that are subscribed to a Microsoft 365 or Google Workspace account, mail statistics may also be viewed by notification delay and by notifications received by FortiMail, to aid in troubleshooting and other purposes. These tabs are only available from the *Microsoft 365 & Google Workspace* view, under *FortiView > Mail Statistics > Notification Delay* and *FortiView > Mail Statistics > Received Notification*.

The *Notification Delay* tab contains summaries of the amount of time notifications were delayed. This is determined by the time when the email arrives in the Microsoft 365 or Google Workspace mailbox and the time when the FortiMail unit receives the notification. Notification delay can be viewed by varying time periods, including by minute, hour, day, month, and year.

The *Received Notification* tab contains summaries of the number of notifications received by FortiMail. Received notifications can be viewed by varying time periods, including by minute, hour, day, month, and year.

For more information on Microsoft 365 and Google Workspace specific mail statistics and other protection features, see Microsoft 365, Exchange and Google Workspace threat remediation on page 352.

Viewing threat statistics

Go to *FortiView > Threat Statistics* to view:

- *Threat Statistics*: Summary of spam and virus mail and a breakdown of detailed threats.
- *FortiSandbox Statistics*: Summary of FortiSandbox scan results.
- *Click Protection Statistics*: Summary of URL click protection, such as top URLs, top users, and top client IP addresses.

Monitoring the system

The *Monitor* menu displays system usage, mail queues, log messages, reports, and other status-indicating items.

It also allows you to manage the contents of the mail queue and quarantines, and the sender reputation and endpoint reputation scores.

Viewing log messages

The *Log* submenu displays locally stored log files. If you configured the FortiMail unit to store log messages locally (that is, to the hard disk), you can view the log messages currently stored in each log file.

Logs stored remotely cannot be viewed from the GUI of the FortiMail unit. If you need to view logs from the GUI, also enable local storage. For details, see Configuring logging on page 343.

The *Log* submenu includes the following tabs, one for each log type:

- *History*: Where you can view the log of sent and undelivered SMTP email messages.
- *System Event*: Where you can view the log of administrator activities and system events.
- *Mail Event*: Where you can view the log of normal email delivery activities.
- *AntiVirus*: Where you can view the log of email detected as infected by a virus.
- *AntiSpam*: Where you can view the log of email detected as spam.
- *Encryption*: Where you can view the log of IBE encryption. For more information about using IBE, see Configuring IBE encryption on page 324.
- *Log Search Task*: Where you can configure and view the log results of advanced searches. For more information, see To make an advanced log search on page 40.

For more information, see FortiMail log types on page 338.

Each tab contains a similar display.

The lists are sorted by the time range of the log messages contained in the log file, with the most recent log files appearing near the top of the list.

For example, the current log file would appear at the top of the list, above a previous ("rolled") log file whose time might range from `2008-05-08 11:59:36 Thu` to `2008-05-29 10:44:02 Thu`.

To view the list of log files and their contents

1. If you have domain-level administrators, and want them to be able to use the history logs, purchase the feature license and enable the feature. See History log access for domain level administrator on page 1.
2. Go to *Monitor* > *Log*.

3. Click the tab corresponding to the type of log file that you want to view (*History*, *System Event*, *Mail Event*, *AntiVirus*, *AntiSpam*, or *Encryption*).

GUI item	Description
Download (button)	Click to download the report in one of several formats: • *Normal Format*:A log file that can be viewed with a plain text editor such as Microsoft Notepad. • *CSV Format*: A comma-separated value (.csv) file that can be viewed in a spreadsheet application such as Microsoft Excel or OpenOffice Calc. • *Compressed Format* for a plain text log file like *Normal Format*, except that it is compressed and stored within a .gz archive.
Search (button)	Click to search all log files of this type during a specified time range, match conditions, and keywords. Alternatively, click *Advanced Search* from the dropdown menu for the ability to apply *And/Or* search filter criterion. Unlike the search when viewing the contents of an individual log file, this search displays results regardless of which log file contains them. For more information, see Searching log messages on page 39.
Start Time	Lists the beginning of the log file's time range.
End Time	Lists the end of the log file's time range.
Size	Lists the size of the log file in bytes.

4. To view messages contained in logs:
   - Double-click a log file to display the file's log messages

To view the current page's worth of the log messages as an HTML table, right-click and select *Export to Table*. The table appears in a new tab. To download the table, click and drag to select the whole table, then copy and paste it into a rich text editor such as Microsoft Word or OpenOffice Writer.

   - Click a row to select its log file, click *Download*, then select a format option

     Alternatively, to display a set of log messages that may reside in multiple, separate log files:
   - If the log files are of the **same type** (for example, all antispam logs), click *Search*. For details, see Searching log messages on page 39.
   - If the log messages are of **different types** but all caused by the **same email** session ID, you can do a cross-search to find and display all correlating log messages. For details, see Cross-searching log messages on page 41.

   Log messages can appear in either raw or formatted views.
   - Raw view displays log messages exactly as they appear in the plain text log file.
   - Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in formatted view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

   By default, log messages always appear in columnar format, with one log field per column. However, when viewing this columnar display, you can also view the log message in raw format by hovering your mouse over the index number of the log message, in the # column.

When hovering your mouse cursor over a log message, that row is temporarily highlighted; however, this temporary highlight automatically follows the cursor, and will move to a different row if you move your mouse. To create a row highlight that does not move when you move your mouse, click anywhere in the row of the log message.

Displaying and arranging log columns

When viewing logs in *Formatted* view, you can display, hide, sort and re-order columns.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see Searching log messages on page 39.

By default, each page's worth of log messages is listed with the log message with the lowest index number towards the top.

To sort the page's entries in ascending or descending order

1. Click the column heading by which you want to sort.
   The log messages are sorted in ascending order.
2. To sort in descending order, click the column heading again.
   Depending on your currently selected theme:
   - the column heading may darken in color to indicate which column is being used to sort the page
   - a small upwards-or downwards-pointing arrow may appear in the column heading next to its name to indicate the current sort order.

To display or hide columns

1. Go to *Monitor* > *Log*.
2. Click one of the log type tabs: *History*, *System Event*, *Mail Event*, *AntiVirus*, *AntiSpam*, or *Encryption*.
3. Click *Configure View* > *Show/Hide Column*.
4. Enable or disable the columns.
5. Click *OK*.

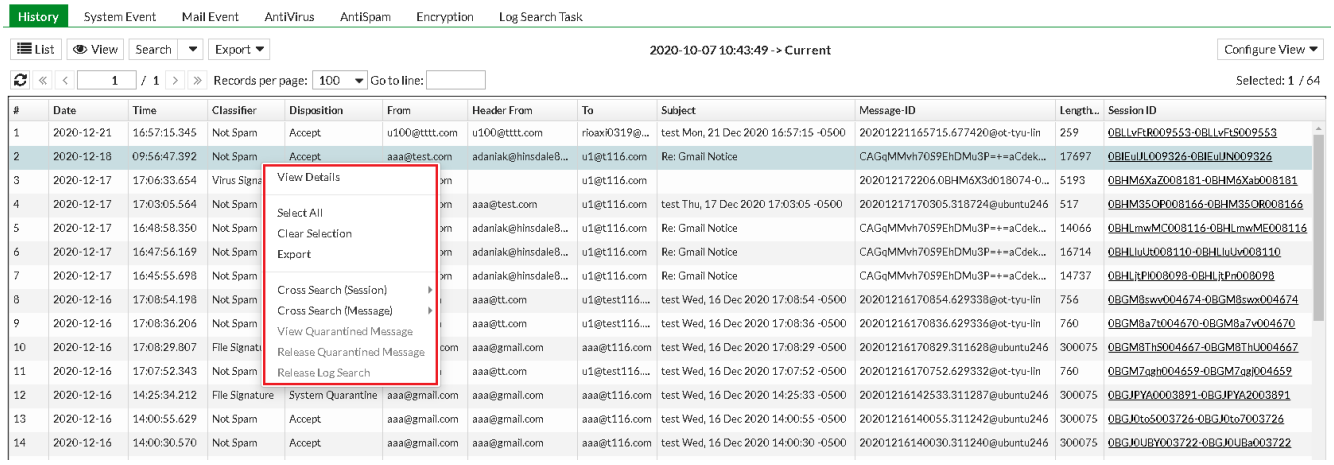
To change the order of the columns

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as *History*.
3. Double-click the row corresponding to time period whose log messages you want to view.
4. For each column whose order you want to change, click and drag its column heading to the left or right.
   While dragging the column heading within the heading row, two arrows follow the column, jumping to the nearest border between columns, indicating where the column will be inserted if you release the mouse button at that time.
5. Click *Configure View* > *Save View*.

Using the right-click pop-up menus

When you right-click a log message, a context menu appears.

Using the right-click menus on log reports



Log report right-click menu options

GUI item	Description
View Details	Select to view the log message in a pop-up window.
Select All	Select to select all log messages in the current page, so that you can export all messages to a table.
Clear Selection	Select to deselect one or multiple log messages.
Export	Select to export the selected log messages to .CSV format, allowing you to review the information elsewhere.
Cross Search (Session)	Select to search for the log messages triggered by the same SMTP session. This may result in multiple email messages if multiple messages were sent in the same SMTP session.search log messages by session ID and message ID. For details, see Cross-searching log messages on page 41.
Cross Search (Message)	Select to search for the log messages triggered by the same email message. For details, see Cross-searching log messages on page 41.
View Quarantined Message	When viewing quarantine logs on the *History* tab, select to view the quarantined email message. For details about quarantined email, see Managing the quarantines on page 42.
Release Quarantined Message	When viewing quarantine logs on the *History* tab, select one or multiple log entries of the “System Quarantine” messages, then from the right-click menu, select the Release Quarantined Message option to release the selected message/messages. For details about quarantined email, see Managing the quarantines on page 42.
Release Log Search	When viewing quarantine logs on the *History* tab, select one or multiple log entries of the “System Quarantine” messages, then from the right-click menu, select the Release Log Search option to release the selected message/messages. A message will show that the qurantined message was released, along with all logs related to the email being quarantined.

Searching log messages

You can search logs to quickly find specific log messages in a log file, rather than browsing the entire contents of the log file.

Search appearance varies by the log type.

Some email processing such as mail routing and subject-line tagging modifies the recipient email address, the sender email address, and/or the subject line of an email message. If you search for log messages by these attributes, enter your search criteria using text exactly as it appears in the log messages, not in the email message. For example, you might send an email message from `sender@example.com`; however, if you have configured mail routing on the FortiMail unit or other network devices, this address, at the time it was logged by the FortiMail unit, may have been `sender-1@example.com`. In that case, you would search for `sender-1@example.com` instead of `sender@example.com`.

To search log messages

1. Go to *Monitor* > *Log*.
2. Click one of the log type tabs: *History*, *System Event*, *Mail Event*, *AntiVirus*, *AntiSpam*, or *Encryption*.
3. To search **all** log files of that type, click *Search*.

   To search **one** of the log files, first double-click the name of a log file to display the contents of the log file, then click *Search*.
4. Configure the following settings:

GUI item	Description
Time Range	Select a time range of log messages to include in the search results. Either search the last hour, 4 hours, 8 hours, 12 hours, or a custom date or time span. For example, you might want to search only log messages that were recorded during the last 10 days and 8 hours previous to the current date. In that case, you would select *Custom*, select *Date*, and specify the required dates and time of day to conduct the search.
Match condition	Select from one of the following options: • *Contains*: searches for the exact match. • *Does not contain*: searches exclude keyword instances. • *Matches (wildcard)*: supports wildcards in the entered search criteria. • *Does not match (wildcard)*: searches exclude wildcard instances.
Keyword	Enter any word or words to search for within the log messages. For example, you might enter `starting daemon` to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the message log field. This option does not appear for history log searches.
Subject	Enter all or part of the subject line of the email message as it appears in the log message. This option appears only for history log searches.

GUI item	Description
Message-ID	Enter all or part of the message ID in the log message.
From	Enter all or part of the sender's email address as it appears in the log message. This option does not appear for event log searches.
Header From	Enter all or part of the email header from address. This option does not appear for event log searches.
To	Enter all or part of the recipient's email address as it appears in the log message. This option does not appear for event log searches.
Session ID	Enter all or part of the session ID in the log message.
Client location (History log search only)	Select a geographical location by country from the dropdown menu.
Client name/IP (History log search only)	Enter all or part of the domain name or IP address of the SMTP client. For email users connecting to send email, this is usually an IP address rather than a domain name. For SMTP servers connecting to deliver mail, this may often be a domain name.
Classifier	Enter the classifier in the log message. The classifier field displays which FortiMail scanner applies to the email message. For example, *Banned Word* means the email messages was detected by the FortiMail banned word scanning. For information about classifiers, see Classifiers and dispositions in history logs on page 340.
Disposition	Enter the disposition in the log message. The disposition field specifies the action taken by the FortiMail unit. For information about dispositions, see Classifiers and dispositions in history logs on page 340.

5. Click *Search*.
   The FortiMail unit searches your currently selected log file for log messages that match your search criteria, and displays any matching log messages. For example, if you are currently viewing a history log file, the search locates all matching log messages located in that specific history log file.

To make an advanced log search

1. Go to *Monitor* > *Log* > *Log Search Task*.
2. Click *New*.
3. Configure the following settings:

GUI item	Description
Log type	Select one of the log type tabs: *History*, *Mail Event*, *AntiVirus*, *AntiSpam*, *Encryption*, or *System Event*.
Description	Enter an optional description for the log search task.
Time Range	Select a time range of log messages to include in the search results. Either search between two dates and times, or a custom time span.

GUI item	Description
	For example, you might want to search only log messages that were recorded during the last 10 days and 8 hours previous to the current date. In that case, you would select *Time span* and specify the number of days and hours before a specific end date and time.
Search Filter	Click *Add* to apply fields and operations (or match conditions) and define their values. For multiple search filter criterion, apply And/Or search logic under *Relationship*.
Search HA device	Enable and select under *Device Selection* which devices of the configured HA cluster you wish to include in the advanced log search task. Alternatively, leave disabled to only conduct the log search task locally.  This option is only available for domain level admin users, if history log access is granted (MSSP license required), and if HA is enabled. System level admin users can use the Centralized Monitor feature to conduct searches on HA devices. For more information, see Centrally monitoring the HA cluster on page 1.

4. Click *Search*.

   Alternatively, you can conduct the exact same advanced log search by going to *Monitor > Log > Log Search Task* and creating a new log search task, specifying the log type.

   The FortiMail unit searches your currently selected log file for log messages that match your search criteria, and displays any matching log messages. You can review the results of the search task by going to *Monitor > Log > Log Search Task*.

Cross-searching log messages

Because each log file type records different events, the same SMTP session (with one or more email messages sent during the session) or the same email message may be logged in multiple log files. For example, if the FortiMail unit detects a virus in an email messages, then this event will be logged in the:

- **History log**: Records the metadata of all sent and undelivered email messages.
- **AntiVirus log**: Records virus detections. The antivirus log has more descriptions of the virus than the history log.
- **Event log**: Records that the FortiMail unit's antivirus process has been started and stopped.

To find and display all log messages triggered by the same SMTP session or the same email message, you can use the cross-search feature.

Cross-search searches log files recorded five minutes before and after the log entry (this design is for performance reasons). It includes multiple log files but may not cover all of the related log files if any of them are recorded out of the ten minutes interval.

To do a cross-search of the log messages

1. Go to *Monitor* > *Log*.
2. When viewing a log message on the *History*, *System Event*, *Mail Event, AntiVirus*, or *AntiSpam* tab, right-click the log message that has a message ID. From the pop-up menu, select either:
   - *Cross Search (Session)*: Search for the log messages triggered by the same SMTP session. This may result in multiple email messages if multiple messages were sent in the same SMTP session.
   - *Cross Search (Message)*: Search for the log messages triggered by the same email message.

   You can also click the session ID of the log message to search for the log messages triggered by the same SMTP session. This is equivalent to the *Cross Search (Session)* pop-up menu.

   All correlating history, event, antivirus and antispam log messages will appear in a new tab.

For instances where the search is conducted within 60 minutes, it is recommended to conduct the cross search via SMTP session ID.

If the log is not in the same log file but in rotated log files, and it is also not within the 60 minute time frame, the cross search will not retrieve all the related logs.

If this occurs, search the antispam logs.

Managing the quarantines

You can quarantine email messages based on the message content, such as whether the email is spam or contains a prohibited word or phrase. FortiMail units have multiple types of quarantine:

- **Personal quarantine** — Quarantines email messages into separate folders for each recipient address in each protected domain. The FortiMail unit periodically sends quarantine reports to notify recipients, their designated group owner, and/or another email address of the email messages that were added to the quarantine folder for that recipient. See Managing the personal quarantines on page 43.
- **System quarantine** — Quarantines email messages into a system-wide quarantine. Unlike the per-recipient quarantine, the FortiMail unit does **not** send a quarantine report. The FortiMail administrator should review the quarantined email messages to decide if they should be released or deleted. See Managing the system quarantine on page 46.
- **Domain quarantine** — Quarantines email messages into separate folders for each protected domain, in the case of a multi-tenant environment. Unlike the per-recipient quarantine, the FortiMail unit does **not** send a quarantine report. The FortiMail administrator, assigned to their respective domain, should review the quarantined email messages to decide if they should be released or deleted. See Managing the domain quarantines on page 48.

  Domain quarantines are only available to FortiMail units with a valid advanced management feature license.

To quarantine spam and/or email with prohibited content, you must select a quarantine action in an antispam, antivirus, content, or DLP profile. For details, see:

- Configuring antispam profiles and actions on page 187
- Configuring antivirus profiles, file signatures, and actions
- Configuring content profiles and content action profiles on page 215
- Configuring content profiles and content action profiles

Spam samples may also be submitted to a special email account so it may either be reviewed by an administrator first (temporarily stored in a sample submission quarantine) or sent directly to FortiGuard. See Managing the spam sample submissions on page 49.

All FortiMail models can be configured to remotely store their quarantined email messages in a centralized quarantine hosted on a high end FortiMail model.

Managing the personal quarantines

The *Personal Quarantine* tab displays a list of personal quarantines, also called per-recipient quarantines.

In advanced mode, when incoming email matches a policy that directs quarantined email to the personal quarantine, the FortiMail unit will save the email to its hard drive and not deliver it to the recipient. Instead, the FortiMail unit will periodically send a quarantine report to email users, their designated group owner, or another recipient (if you have configured one using the advanced mode of the GUI).

In basic mode, incoming quarantined email also is kept on the FortiMail unit's hard drive.

The quarantine report, by default sent once a day at 9 AM, lists all email messages that were withheld since the previous quarantine report. Using the quarantine report, email users can review email message details and release any email messages that are false positives by clicking the link associated with them. The email message will then be released from quarantine and delivered to the email user's inbox. Using the GUI, FortiMail administrators can also manually release or delete quarantined email. For more information on deleting email that has been quarantined to the per-recipient quarantine, see Managing the personal quarantines on page 43. For information on configuring the schedule and recipients of the quarantine report, see Configuring global quarantine report settings on page 285.

You can configure the FortiMail unit to send email to the per-recipient quarantine by selecting *Quarantine* in action profiles, content profiles and antispam profiles. For more information, see Configuring antispam profiles and actions on page 187 and Configuring content profiles on page 216.

Unlike the system-wide quarantine, the per-recipient quarantine can be accessed remotely by email users so that they can manage their own quarantined email. For information on configuring remote per-recipient quarantine access, see How to enable, configure, and use personal quarantines on page 44.

To view the list of per-recipient quarantine folders for a protected domain

1. Go to *Monitor* > *Quarantine* > *Personal Quarantine*.
2. Select the name of a protected domain from *Domain*.
   You can view, delete, and release email that has been quarantined to each personal quarantine mailbox.

To reduce disk usage, regularly delete the quarantined email. Releasing quarantined email does not reduce disk usage.

Email users can also manage their own per-recipient quarantines through quarantine reports. For more information, see Releasing and deleting email via quarantine reports on page 290.

To view email messages inside a personal quarantine mailbox

1. Go to *Monitor* > *Quarantine* > *Personal Quarantine*.
2. Double-click the row corresponding to that mailbox.
3. To view an email in the mailbox, double-click it.

How to enable, configure, and use personal quarantines

In general, to use personal quarantines, you should complete the following:

1. Configure the host name and mail queue of the FortiMail unit.

   If you want to specify an alternate FQDN that will be used only by web release/delete URLs in HTML-formatted quarantine reports, see Web release host name/IP on page 286. This FQDN should be globally resolvable.
2. Select the recipients, delivery schedule, and release methods of the quarantine report. For details, see Configuring protected domains on page 92 for quarantine report settings that are domain-specific, or Configuring global quarantine report settings on page 285 for quarantine report settings that are system-wide.
3. If email users will release/delete email from their quarantine by sending email, configure the user name portion (also known as the local-part) for the quarantine control email addresses (the domain-part will be the local domain name of the FortiMail unit). For details, see Configuring the quarantine control options on page 293.
4. For gateway mode or transparent mode, configure authentication profiles that will allow email users to authenticate when accessing their per-recipient quarantine. Alternatively, if email users require only HTTP/HTTPS access, you may configure PKI user accounts.

   For server mode, configure the email user accounts. Email users can authenticate using this account to access their per-recipient quarantine.

   For details, see Workflow to enable and configure authentication of email users on page 230.
5. Enable quarantine reports in each email user's preferences. Both FortiMail administrators and email users can do this. For details, see Configuring user preferences on page 115, or the online help for FortiMail webmail and per-recipient quarantines.
6. If the FortiMail unit is operating in server mode and you want to enable web release/delete, configure resource profiles in which Webmail access on page 229 is enabled.
7. Enable the *Personal quarantine* and *Send quarantine report* option in incoming antispam and/or content profiles. If you want to allow email users to release and/or delete email from their quarantine by email or web release/delete, also enable *Email release* and *Web release*.

   For details, see Configuring antispam profiles and actions on page 187 and/or Configuring content action profiles on page 224.
8. Select the antispam and/or content profiles in incoming recipient-based policies. If you configured a resource profile in step If the FortiMail unit is operating in server mode and you want to enable web release/delete, configure resource profiles in which Webmail access on page 229 is enabled. on page 44, also select the resource profile.

   If the FortiMail unit is operating in gateway or transparent mode and you want to enable web release/delete, enable *Allow quarantined email access through webmail* in each incoming recipient-based policy.

   For details, see Controlling email based on sender and recipient addresses on page 163.
9. Either email users or FortiMail administrators can manage email in the per-recipient quarantines.

   For details, see Managing the personal quarantines on page 43 and Releasing and deleting email via quarantine reports on page 290.

Searching email in the personal quarantine

You can search the personal quarantine for email messages based on their contents, senders, recipients, and time frames, across any or all protected domains.

The search action involves the following steps:

- Create a search task, where you can specify search criteria.
- Execute and view the search results.

See below for detailed instructions.

To search the personal quarantine

1. Go to *Monitor* > *Quarantine* > *Personal Quarantine*.
2. Click *Search*. The *Personal Quarantine Search* tab appears, displaying all search tasks, if there are any.
3. Click *New* to add a search task.
4. Configure the search criteria, including *Time Range* to define the date/s and time of the search, various *Search Filter* criterion, and determine whether the search should be conducted across all or multiple domains.

   Email messages must match all criteria that you configure to be included in the search results. For example, if you configure *From* and *Subject*, only email messages matching **both** *From* and *Subject* will be included in the search results. Select from the list of available header options under *Field*:

   - *From*
   - *To*
   - *Cc*
   - *To or Cc*
   - *From, To or Cc*
   - *Subject*
   - *Text*
   - *Attachment*
   - *Message-ID*
   - *Client IP*
   - *Endpoint ID*
   - *Policy ID*
   - *Release Status*
   - *Custom Header*

   Wildcard header search support is also available.
5. Click *Search* to execute and save the task. The task name is the time when the task is created. The *Personal Quarantine Search* tab displays the search tasks and their search status as follows:
   - *Done*: The FortiMail unit has finished the search. You can click the *View Search Result* button to view the search results.
   - *Pending*: The search task is in the waiting list.
   - *Running*: The search task is still running. You can choose to stop the task by clicking the *Stop* button.
   - *Stopped*: The search task is stopped. You can choose to resume the task by clicking the *Resume* button.

Managing the system quarantine

The *System Quarantine* tab displays the system quarantine.

Unlike the per-recipient quarantine, the system quarantine cannot be accessed remotely by email users. Also, they do not receive quarantine reports for email held in the system quarantine and cannot manage the system quarantine themselves. A FortiMail administrator should periodically review the contents of the system quarantine. Alternatively, you can configure a special-purpose system quarantine administrator for this task. For more information, see Configuring the system quarantine setting on page 292.

To reduce disk usage, regularly delete the quarantined email. Releasing quarantined email does not reduce disk usage.

By default, the system quarantine is not used until you configure the FortiMail unit to send per-recipient quarantine to system quarantine by selecting *System quarantine* in antivirus action profiles, content action profiles, and antispam action profiles. For more information, see Configuring antivirus action profiles on page 213, Configuring antispam action profiles on page 206, and Configuring content action profiles on page 224.

To view and manage system quarantine folders

1. Go to *Monitor* > *Quarantine* > *System Quarantine*.
2. From the Folder dropdown list, select which type of quarantined email you want to view.

You can also configure a system quarantine administrator account whose exclusive purpose is to manage the system quarantine. For more information, see Configuring the system quarantine setting on page 292.

GUI item	Description
View (button)	Select a item in the table and click View to open item.
Delete (button)	Click to delete the selected item.
Compact (button)	Select the check boxes of each email user whose quarantine folder you want to compact and click *Compact*. For performance reasons, when you delete an email, it is marked for deletion but not actually removed from the hard disk at that time, and so still consumes some disk space. Compaction reclaims this hard disk space. **Note:** FortiMail updates folder sizes once an hour. The reduction in folder size is not immediately reflected after compacting.
Search (button)	Click to search the mail data.
Release (button)	Select a folder and batch release the email in the folder according to the criteria you specify: • Start date • End date • Message type: Either *Unreleased Only* or *All Messages*. • Release to: Original recipient(s) or other recipient(s) you specify.

GUI item	Description
Folder (dropdown list)	From the dropdown list, select a folder to view.
Folder	Lists the current folder. Older system quarantine mailboxes, also called rotated folders, are named according to their creation date and the rename date. For information on configuring rotation of the system quarantine mailbox, see Configuring the system quarantine setting on page 292. To view email messages quarantined in that mailbox, double-click its row. For more information, see Managing the system quarantine on page 46.
Size	Lists the size of the quarantine folder in kilobytes (KB). **Note:** Mailbox sizes are updated once an hour.
Message Count	Lists the total number of quarantined messages in the mailbox.

3. Double-click a system quarantine mailbox.
   You can view, delete, release, and forward email in the system quarantine.

GUI item	Description
View (button)	To view a message, either double-click it, or mark its check box and click *View*.
Delete (button)	Click to delete the selected item.
Release (button)	To release **all** email messages in the current view, mark the top check box and click *Release*. To release **individual** email messages, mark their check boxes and click *Release*. In the pop-up window, you can select to release email to the original recipient and/or to other recipients. If want to release email to other recipients, enter the email addresses. You can add up to five email addresses.
Back (button)	Click to return to viewing the list of system quarantine folders.
Filter	Use the filter to display the released or unreleased email only. By default, FortiMail only displays the unreleased email.
Search (button)	Click to search the system quarantine folder that you are currently viewing. For details, see Searching email in the system quarantine on page 48.
Subject	Lists the subject line of the email. Click to display the email message.
From	Lists the display name of the sender as it appears in the message header, such as `"User 1"`.
To	Lists the display name of the recipient as it appears in the message header, such as `"User 2"`.
Rcpt To	Lists the user name portion (also known as the local-part) of the recipient email address (`RCPT TO:`) as it appears in the message envelope, such as `user2` where the full recipient email address is user2@example.com.

GUI item	Description
Session ID	Lists the session ID of each email.
Received	Lists the time that the email was received.
Size	Lists the size of the email message in kilobytes (KB).

4. Double-click an email message to open it.
   The email message appears, including basic message headers such as the subject and date.
5. Select the action that you want to perform on the quarantined email.
   - To view additional message headers, click the + button, then click *Detailed Header*.
   - To release the email message to its recipient, click *Release*.
   - To download the email message from the quarantine, click *Download*.

Searching email in the system quarantine

You can search a system quarantine folder (content, virus or bulk) for email messages based on their message body content and message headers.

The search process is similar to the personal quarantine search. For details, see Searching email in the personal quarantine on page 45.

Managing the domain quarantines

The *Domain Quarantine* tab displays a list of quarantines for each domain on the FortiMail unit. Note that this is only available with a valid purchased advanced management license.

In multi-tenant environments with multiple domains, administrators are given per-domain permissions to view and perform actions on quarantined messages within their domain. Domain administrators are provided their privileges from the *Domain Quarantine* access control permission within their assigned admin profile. See Configuring administrator access profiles on page 70 for more information. Domain and domain-group administrators cannot access system quarantined messages.

Similarly to the system quarantine, domain quarantine administrators do not receive quarantine reports for email held in the domain quarantine and cannot manage the domain quarantine themselves. Domain administrators should periodically review the contents of the domain quarantine.

Options for viewing and managing the domain quarantine folders is similar to the options available for system quarantine. See To view and manage system quarantine folders on page 46 for more information.

Searching email in the domain quarantine

With a valid advanced management license, you can search the domain quarantine for email messages based on their contents, senders, recipients, and time frames, across any or all protected domains.

The search action involves the following steps:

- Create a search task, where you can specify search criteria.
- Execute and view the search results.

See below for detailed instructions.

To search the domain quarantine

1. Go to *Monitor* > *Quarantine* > *Domain Quarantine*.
2. Click *Search*. The *Domain Quarantine Search* tab appears, displaying all search tasks, if there are any.
3. Click *New* to add a search task.
4. Configure the search criteria, including *Time Range* to define the date/s and time of the search, various *Search Filter* criterion, the particular domain to search, and determine whether the search should be conducted across all or multiple folders, or mailboxes.

   Email messages must match all criteria that you configure to be included in the search results. For example, if you configure *From* and *Subject*, only email messages matching **both***From* and *Subject* will be included in the search results. Select from the list of available header options under *Field*:

   - *From*
   - *To*
   - *Cc*
   - *To or Cc*
   - *From, To or Cc*
   - *Subject*
   - *Text*
   - *Attachment*
   - *Message-ID*
   - *Client IP*
   - *Endpoint ID*
   - *Policy ID*
   - *Custom Header*

   Wildcard header search support is also available.
5. Click *Search* to execute and save the task. The task name is the time when the task is created. The *Domain Quarantine Search* tab displays the search tasks and their search status as follows:
   - *Done*: The FortiMail unit has finished the search. You can click the *View Search Result* button to view the search results.
   - *Pending*: The search task is in the waiting list.
   - *Running*: The search task is still running. You can choose to stop the task by clicking the *Stop* button.
   - *Stopped*: The search task is stopped. You can choose to resume the task by clicking the *Resume* button.

Managing the spam sample submissions

When FortiMail receives a submitted sample email (see Configuring spam sample submission service on page 88), you can search for it based on whether it was submitted as spam, non-spam (or ham), or if it was detected to contain spam by FortiGuard Antispam.

Depending on the email addresses defined to receive these submissions, emails are placed into the *Spam* or *Ham* (non-spam) folders. Any emails that FortiGuard Antispam detected as spam are placed into the *Spam_detected* folder.

The *All* folder is limited to displaying only the current day's messages.

To view all historically submitted messages, you must select the appropriate folder (either *Spam*, *Ham*, or *Spam_detected*).

To view and manage sample submission folders

1. Go to *Monitor* > *Quarantine* > *Sample Submission*.
2. From the *Folder* dropdown list, select which type of spam sample submission email you want to view:

GUI item	Description
View (button)	Select a item in the table and click View to open item.
Delete (button)	Click to delete the selected item.
Compact (button)	Select the check boxes of each email user whose quarantine folder you want to compact and click *Compact*. For performance reasons, when you delete an email, it is marked for deletion but not actually removed from the hard disk at that time, and so still consumes some disk space. Compaction reclaims this hard disk space. **Note:** FortiMail updates folder sizes once an hour. The reduction in folder size is not immediately reflected after compacting.
Search (button)	Click to search the mail data.
Submit (button)	Select a folder and batch submit the email in the folder to FortiGuard Antispam labs or other recipients, according to the criteria you specify: • *Start date* • *End date* • *Message type*: Either *Not Submitted Only* or *All Messages*. • *Submit to*
Folder (dropdown list)	From the dropdown list, select a folder to view.
Folder	Lists the current folder. Older system quarantine mailboxes, also called rotated folders, are named according to their creation date and the rename date. For information on configuring rotation of the system quarantine mailbox, see Configuring the system quarantine setting on page 292.
Size	Lists the size of the quarantine folder in kilobytes (KB). **Note:** Mailbox sizes are updated once an hour.
Message Count	Lists the total number of quarantined messages in the mailbox.

3. Double-click a spam sample submission folder.

   You can view, delete, submit, and filter sample submissions.

GUI item	Description
Filter	Use the filter to display the submitted or unsubmitted email only. By default, FortiMail only displays the unsubmitted email.
Subject	Lists the subject line of the email. Click to display the email message.

GUI item	Description
From	Lists the display name of the sender as it appears in the `From:` message header, such as `"User 1"`.
To	Lists the display name of the recipient as it appears in the `To:` message header, such as `"User 2"`.
Rcpt To	Lists the user name portion (also known as the local-part) of the recipient email address (`RCPT TO:`) as it appears in the SMTPenvelope, such as `user2` where the full recipient email address is `user2@example.com`.
Session ID	Lists the session ID of each sample submission.
Received	Lists the time that the email was received.
Size	Lists the size of the email message in kilobytes (KB).

4. Double-click an email message to open it.
   The email message appears, including basic message headers such as the subject and date.

Managing the mail queues

FortiMail units prioritize email delivery according to mail queues:

- **Regular mail queues**
  When the FortiMail unit's 1st attempt to deliver an email fails, then the email is moved to a normal priority mail queue: default, incoming, or outgoing.
- **Slow mail queues**
  If more delivery retries fail, then the email is moved to a slow mail queue. (The threshold between normal and slow queues is a CLI-only setting.) Slow queues also try to use Time interval for retry, but if FortiMail is busy and system resource usage is high, then slow queues have a lower priority than normal queues, so a retry in a slow queue might not occur exactly at the interval time. This allows the FortiMail unit to send valid email more quickly, instead of wasting system resources frequently retrying email that may be invalid (for example, email destined to an invalid MTA) or for an MTA that is too busy or undergoing maintenance.

After an undelivered email is in a deferred queue for 5 minutes, then the email appears in *Monitor > Mail Queue > Mail Queue*. Email that has been deferred for less than 5 minutes does not appear.

Delivery failure can be caused by temporary reasons such as high system resource usage or interruptions to network connectivity. FortiMail units will periodically retry delivery. (Administrators can also manually initiate a retry.)

If the retry succeeds, then the FortiMail unit removes the email from the queue. It does not notify the sender.

But if delivery continues to be delayed, then the FortiMail unit eventually sends an initial delivery status notification (DSN) email message to notify the sender that delivery has not yet succeeded.

Finally, if the FortiMail unit cannot send the email message by the retry time limit, then the FortiMail unit sends a final DSN to notify the sender about the delivery failure and deletes the email message from the deferred queue.

If the sender cannot receive this notification(for example, if the sender's SMTP server is unreachable or if the sender address is invalid or empty), then the FortiMail unit saves the email in the dead mail folder. See Managing undeliverable mail on page 53.

However, if you manually delete a deferred email in the queue, FortiMail will not send a notification to the sender.

To view, delete, or resend an email in the deferred mail queue, go to *Monitor > Mail Queue > General*.

GUI item	Description
View (button)	Select a message and click *View* to see its contents.
Delete (button)	Click to deleted the selected item.
Resend (button)	Mark the check boxes of the rows corresponding to the email messages that you want to immediately retry to send, then click *Resend*. To determine if these retries succeeded, click *Refresh*. If a retry succeeds, the email will no longer appear in either the deferred mail queue or the dead mail folder. Otherwise, the retry has failed.
Type	Select the directionality and priority level of email to filter the mail queue display. • *Default*: For FortiMail email process usage. • *Incoming*: Displays email to protected domains after a failed delivery attempt. After more failed retries, the email may be moved to *Incoming-slow*. (The threshold between normal and slow queues is a CLI-only setting.) • *Outgoing*: Displays email to unprotected domains after a failed delivery attempt. After more failed retries, the email may be moved to *Outgoing-slow*. • *IBE*: Displays IBE email after a failed delivery attempt. After more failed retries, the email may be moved to the *IBE-slow*.For information about IBE email, see Configuring IBE encryption on page 324. • *Default-slow*: For FortiMail email process usage. • *Incoming-slow*: Displays incoming email for which retries failed. • *Outgoing-slow*: Displays outgoing email for which retries failed. • *IBE-slow*: Displays IBE email for which retries failed. • *Delivery control*: Displays email throttled by delivery control policies (see Rate limiting for delivery on page 158). After 3 attempts, the mail will be moved to *Outgoing-slow*.
Search (button)	Select to filter the mail queue display by entering criteria that email must match in order to be visible.
Client IP	Lists the client IP addresses.
Location	Lists the geographic locations or country names associated with the IP address.
Envelope From	Lists the sender (`MAIL FROM:`) of the email.
Envelope To	Lists the recipient (`RCPT TO:`) of the email.
Subject	Lists the email subjects.
First Processed	Lists the date and time that the FortiMail unit first tried to send the email.

GUI item	Description
Last Processed	Lists the date and time that the FortiMail unit last tried to send the email.
Tries	Lists the number of times that the FortiMail unit has tried to send the email.

Viewing the FortiGuard spam outbreak protection mail queue

If you enable Spam outbreak protection in an antispam profile, and if the FortiGuard Antispam check (blocked IP and/or URL filter) returns no result, then FortiMail temporarily holds the email. After the specified wait time, FortiMail queries FortiGuard again. This provides an opportunity for the FortiGuard Antispam service to update its database when a spam outbreak occurs, so that it can give a query result.

To view the email on hold, go to *Monitor* > *Mail Queue* > *Spam Outbreak*.

Viewing the FortiGuard virus outbreak protection mail queue

If you enabled antivirus outbreak protection in an antivirus profile, FortiMail will temporarily hold suspicious email for a certain period of time (configurable on *System* > *FortiGuard* > *AntiVirus*). After the specified time interval, FortiMail will query the antivirus database for the second time. This provides an opportunity for the FortiGuard antivirus service to update its database in cases a virus outbreak occurs.

To view the email on hold, go to *Monitor* > *Mail Queue* > *Virus Outbreak*.

Viewing the FortiSandbox mail queue

The FortiSandbox unit is used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus profiles (see Configuring antivirus profiles on page 209). If the file exhibits risky behavior, or is found to contain a virus, the result will be sent back to FortiMail and a new virus signature is created and added to the FortiGuard antivirus signature database as well.

To view the email waiting to be sent to FortiSandbox, go to *Monitor* > *Mail Queue* > *FortiSandbox*.

Managing undeliverable mail

The *Dead Mail* tab displays the list of email messages in the dead mail folder.

Unlike the deferred mail queue, the dead mail folder contains copies of delivery status notification (DSN) email messages, also called non-delivery reports (NDR).

DSN messages are sent from the FortiMail unit ("postmaster") to an email's sender when the email is considered to be more permanently undeliverable because all previous retry attempts of the deferred email message have failed. These email include a copy of the original email message for which the DSN was generated.

If an email cannot be sent nor a DSN returned to the sender, it is usually because both the recipient and sender addresses are invalid. Such email messages are often sent by spammers who know the domain name of an SMTP server but not the names of its email users, and are attempting to send spam by guessing at valid recipient email addresses.

The FortiMail unit can automatically delete old dead mail.

Alternatively, to prevent dead mail to invalid recipients, enable recipient address verification to reject email with invalid recipients. Rejecting email with invalid recipients also prevents quarantine mailboxes for invalid recipients from consuming hard disk space. For details, see Configuring recipient address verification on page 97.

To view or delete undeliverable email, go to *Monitor* > *Mail Queue* > *Dead Mail*.

Configuring mail queue search tasks

Similar to the quarantine search functionality, you can configure mail queue tasks that provide options to execute various actions, including the sending or deletion of mail, or delivery to an alternative host.

Delivery of mail to alternative host is only available for *General* mail queue search tasks.

To configure a mail queue search task:

1. Go to *Monitor* > *Mail Queue* > *Mail Queue Search Task* and select *New*.
2. Select a *Queue type*. Additionally, set a *Subtype* for general mail queue searches.
3. Define the *Time Range* start and end times for the search to take place.
4. For more granularity, use the *And*/*Or* logic filters under *Search Filter* and click *Add* to add relationship settings.
5. Under *Search Result*, define the action to take place for search results.
6. When finished configuring, click *Search*.

From the list of mail queue search tasks, you can *Stop*, *Resume*, and *Rerun* search tasks as necessary.

Viewing the mail queue size

Mail queue size status can be viewed, including incoming, outgoing, IBE, spam and virus outbreak, and FortiSandbox queues.

To view the mail queue size status in the GUI, go to *Dashboard* > *Status* and find the *Queue Status* widget.

Viewing DMARC report statistics

If you have enabled both:

- DMARC report analysis
- DMARC report generation, either system-wide or for protected domains (see DMARC section on page 193 and DMARC Report Setting on page 104)

then the FortiMail unit collects statistics about them.

These statistics can be useful to monitor your SPF alignment and DMARC setup because it shows how well other mail servers on the Internet are capable of DMARC and SPF, and if they are successful at validating emails from your protected domains. This includes how many email were sent to each recipient domain name, and how many of those email failed verification. A high failure rate can indicate a misconfiguration, and comparing statistics from different domains can be useful to isolate the cause.

Alternatively, DMARC reports can be generated on demand. See On-demand DMARC reports on page 90.

Viewing the DMARC and SPF report summary

For an overview of DMARC and SPF report results and ongoing monitoring, you can use the statistics summary.

1. Go to *Monitor* > *DMARC Analysis* > *Analysis Summary*.
2. From the dropdown list at the top left, select either the name of a protected domain that sends email, or *System* (all protected domains on the FortiMail unit, not filtered).

   If the protected domain has not recently sent email, or DMARC is recently enabled, then you may need to wait until FortiMail can collect some statistics about those DMARC reports. Click the *Refresh* icon on each chart when new DMARC reports become available. Alternatively, reload the page in your web browser.
3. For each of the charts (*Last 30 Days*, *Last 12 Months*, and *Last 10 Years*), click the *Setting* icon and select which category to display:

GUI item	Description
DMARC Capable	How many recipient domains were capable of DMARC verification. If many email were sent to one recipient domain during a specific time range, and the DMARC report statistics indicate that it is not capable, then that domain's administrator may not have configured DMARC verification on their servers.
DMARC Aligned	How many email DMARC verifications succeeded or failed. If many or all DMARC verifications are failing for a protected domain, then its DMARC record may not be correct. To inspect them, see Viewing details about DMARC and SPF report statistics on page 56.
SPF Aligned	How many email SPF verifications succeeded or failed.

4. To view details about any bar on the chart, click it.

   A pie chart appears in a new dialog. If you prefer a table format instead, click the *Show Table* icon in the dialog's title bar.

   For more details, instead see Viewing details about DMARC and SPF report statistics on page 56.

Viewing details about DMARC and SPF report statistics

For troubleshooting DMARC and SPF with individual protected domains, it can be useful to inspect DMARC records and to analyze results based on more detailed criteria, such as by country, DMARC report ID, or by each SMTP client IP address.

To inspect a DMARC or SPF record

1. Go to *Monitor > DMARC Analysis > Analysis Detail*.
2. From the *Domain* dropdown list, select either the name of a protected domain that sends email, or *System* (all protected domains on the FortiMail unit, not filtered).

   If the protected domain has not recently sent email, or DMARC is recently enabled, then you may need to wait until FortiMail can collect some statistics about those DMARC reports. Click the *Refresh* icon on each chart when new DMARC reports become available. Alternatively, reload the page in your web browser.
3. Click *DMARC/SPF Record*.

   The FortiMail unit gets the record from the public DNS server, and displays the result. If the record does not exist or is not correct, then DMARC and SPF verifications will fail on recipient email servers. For details, see DMARC section on page 193.

To export DMARC or SPF report details

1. Go to *Monitor > DMARC Analysis > Analysis Detail*.
2. From the *Domain* dropdown list, select either the name of a protected domain that sends email, or *System* (all protected domains on the FortiMail unit, not filtered).

   If the protected domain has not recently sent email, or DMARC is recently enabled, then you may need to wait until FortiMail can collect some statistics about those DMARC reports. Click the *Refresh* icon on each chart when new DMARC reports become available. Alternatively, reload the page in your web browser.
3. From the *Duration* dropdown list, select either *Last 7 Days* or *Last 30 Days*.

   Charts and a list of DMARC reports appear. If you want to filter and only export specific individual reports, then click their rows in the table. To select multiple rows, either:
   - Hold down the Ctrl key while you select each individual row.
   - Click the first row and then hold down the Shift key while you select the last row. This selects all rows in a continuous range
4. Click *Export* and then select either *Export All* or *Export Selected* (if you selected only specific rows).

Viewing the greylist statuses

The *Greylist* submenu lets you monitor automatic greylisting exemptions, and email currently experiencing temporary failure of delivery due to greylisting.

Greylisting exploits the tendency of legitimate email servers to retry email delivery after an initial temporary failure, while spammers will typically abandon further delivery attempts to maximize spam throughput. The greylist scanner replies with a temporary failure for all email messages whose combination of sender email address, recipient email address, and SMTP client IP address is unknown. If an SMTP server retries to send the email message after the required greylist delay but before expiry, the FortiMail unit accepts the email and adds the combination of sender email address, recipient email address, and SMTP client IP address to the list of those

known by the greylist scanner. Subsequent **known** email messages are accepted. For details on the greylisting mechanism, see About greylisting on page 300.

To use greylisting, you must enable the greylist scan in the antispam profile. For more information, see Configuring antispam profiles on page 187.

Enabling greylisting can improve performance by blocking most spam before it undergoes other, more resource-intensive antispam scans.

Greylisting is bypassed if the SMTP client establishes an authenticated session (see Controlling email based on sender and recipient addresses on page 163, and Controlling email based on IP addresses on page 159), **or** if the matching access control rule's *Action* is *RELAY* (see Order of execution for antispam scans on page 22).

You can configure the initial delay associated with greylisting, and manually exempt senders. For details, see Configuring the greylist TTL and initial delay on page 304 and Manually exempting senders from greylisting on page 305.

Viewing the pending and individual automatic greylist entries

The *Display* tab lets you view pending and individual automatic greylist entries.

- Pending greylist entries are those whose *Status* is **not** *PASSTHROUGH*. For email messages matching pending greylist entries, the FortiMail unit will reply to delivery attempts with a temporary failure code until the greylist delay period, indicated by *Time to passthrough*, has elapsed.
- Individual greylist entries are those whose *Status* is *PASSTHROUGH*. For email messages matching pending greylist entries, the greylist scanner will allow the delivery attempt, and may create a consolidated automatic greylist entry. For information on consolidated entries, see Viewing the consolidated automatic greylist exemptions on page 59.

To view the greylist, go to *Monitor* > *Greylist* > *Display*.

Viewing the list of pending and individual greylist entries

GUI item	Description
Search (button)	Click to filter the displayed entries. For details, see Filtering pending and individual automatic greylist entries on page 58.
IP	Lists the IP address of the SMTP client that delivered or attempted to deliver the email message. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Location	Lists the GeoIP locations/country names.

GUI item	Description
Sender	Lists the sender email address in the message envelope (`MAIL FROM:`), such as user1@example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Recipient	Lists the recipient email address in the message envelope (`RCPT TO:`), such as user1@example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Status	Lists the current action of the greylist scanner when the FortiMail unit receives a delivery attempt for an email message matching the entry. • *TEMPFAIL*: The greylisting delay period has not yet elapsed, and the FortiMail unit currently replies to delivery attempts with a temporary failure code. For information on configuring the greylist delay period, see Configuring the greylist TTL and initial delay on page 304. • *PASSTHROUGH*: The greylisting delay period has elapsed, and the greylist scanner will allow delivery attempts.
Time to passthrough	Lists the time and date when the greylisting delay period for a pending entry is scheduled to elapse. Delivery attempts after this date and time confirm the pending greylist entry, and the greylist scanner converts it to an individual automatic greylist entry. The greylist scanner may also consolidate individual greylist entries. For information on consolidated entries, see Viewing the consolidated automatic greylist exemptions on page 59. *N/A* appears if the greylisting period has already elapsed.
Expire	Lists the time and date when the entry will expire. The greylist entry's expiry time is determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings` (for details, see the FortiMail CLI Reference). The default initial expiry time is 4 hours. If the initial expiry time elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. • TTL: Between the entry's PASSTHROUGH time and initial expiry time, if the entry is hit again (the sender retries to send the message again), the entry's expiry time will be reset by adding the TTL value (time to live) to the message's "Received" time. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. For information on configuring the TTL, see Configuring the greylist TTL and initial delay on page 304.

Filtering pending and individual automatic greylist entries

You can filter the greylist entries on the *Display* tab based on sender email address, recipient email address, and/or the IP address of the SMTP client.

To filter the greylist entries

1. Go to *Monitor* > *Greylist* > *Display*.
2. Click *Search*.
   A dialog appears.
3. Configure one or more of the following:

GUI item	Description
Field	Select one of the following columns in the greylist entries that you want to use to filter the display. • IP • Sender • Recipient
Operation	Select how the column's contents will be matched, such as whether the row must contain the *Value*.
Value	Enter a pattern or exact value based on your selection in *Field* and *Operation*. • *IP*: Enter the IP address of the SMTP client, such as `172.16.1.10`. • *Sender*: Enter the complete sender email address in the message envelope (`MAIL FROM:`), such as `user1@example.com`. • *Recipient*: Enter the complete recipient email address in the message envelope (`RCPT TO:`), such as `user1@example.com`.
Case Sensitive	Enable for case-sensitive filtering.

   Use an asterisk (`*`) to match multiple patterns, such as typing `user*` to match `user1@example.com`, `user2@example.net`, and so forth. Blank fields match any value. Regular expressions are not supported.
4. Click *Search*.
   The *Display* tab appears again, but its contents are restricted to entries that match your filter criteria. To remove the filter criteria and display all entries, click the *Display* tab to refresh its view.

Viewing the consolidated automatic greylist exemptions

The *Auto Exempt* tab displays consolidated automatic greylist entries.

The FortiMail unit creates consolidated greylist entries from individual automatic greylist entries that meet consolidation requirements. For more information on individual automatic greylist entries, see Viewing the pending and individual automatic greylist entries on page 57. For more information on consolidation requirements, see Automatic greylist entries on page 303.

To view the list of consolidated entries, go to *Monitor* > *Greylist* > *Auto Exempt*.

Auto Exempt tab options

GUI item	Description
Search (button)	Click to filter the displayed entries.

GUI item	Description
IP	Lists the /24 subnet of the IP address of the SMTP client that delivered or attempted to deliver the email message. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Location	Lists the GeoIP locations/country names.
Sender	Lists the domain name portion of the sender email address in the message envelope (`MAIL FROM:`), such as example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Expire	Lists the time and date when the entry will expire, determined by adding the TTL value to the time the last matching message was received. For information on configuring the TTL, see Configuring the greylist TTL and initial delay on page 304.

Viewing sender, authentication and endpoint reputation

FortiMail tracks and displays the reputation statuses of SMTP clients (sender reputation), login accesses (authentication reputation), and carrier end points (endpoint reputation).

Viewing sender reputation statuses

The FortiMail unit tracks SMTP client behavior to limit deliveries of those clients sending excessive spam messages, infected email, or messages to invalid recipients. Should clients continue delivering these types of messages, their connection attempts are temporarily or permanently rejected. Sender reputation is managed by the FortiMail unit and requires no administration.

Monitor > *Reputation* > *Sender Reputation* displays the sender reputation score for each SMTP client.

For more information on enabling sender reputation and configuring the score thresholds, see Configuring sender reputation options on page 173.

To view the sender reputation scores, go to *Monitor* > *Reputation* > *Sender Reputation*.

Viewing the sender reputation statuses

GUI item	Description
Search (button)	Click to filter the displayed entries. For more information, see Filtering sender reputation score entries on page 62.
Clear (button)	Click to remove any search filter conditions.

GUI item	Description
IP	The IP address of the SMTP client.
Location	Lists the GeoIP locations/country names.
Score	The SMTP client's current sender reputation score.
State	Lists the action that the sender reputation feature is currently performing for delivery attempts from the SMTP client. • *Score controlled*: The action is determined by comparing the current *Score* value to the thresholds in the session profile.
Last Modified	Lists the time and date the sender reputation score was most recently modified.

Sender reputation is a predominantly automatic antispam feature, requiring little or no maintenance. For each connecting SMTP client (sometimes called a sender), the sender reputation feature records the sender IP address and the number of ***good*** email and ***bad*** email from the sender.

In this case, bad email is defined as:

- Spam
- Virus-infected
- Unknown recipients
- Invalid DKIM
- Failed SPF check

The sender reputation feature calculates the sender's current reputation score using the ratio of good email to bad email, and performs an action based on that score.

The FortiMail unit calculates the sender reputation score using statistics up to 12 hours old, with more recent statistics influencing the score more than older statistics. The sender reputation score decreases (improves) as time passes where the sender has not sent spam. The score itself ranges from 0 to 100, with 0 representing a completely acceptable sender, and 100 being a totally unacceptable sender.

To determine which action the FortiMail unit will perform after it calculates the sender reputation score, the FortiMail unit compares the score to three score thresholds which you can configure in the session profile:

1. **Throttle client at:** For scores less than this threshold, senders are allowed to deliver email without restrictions. For scores greater than this threshold but less than the temporary fail threshold, senders are rate-limited in the number of email messages that they can deliver per hour, expressed as either an absolute number or as a percentage of the number sent during the previous hour. If a sender exceeds the limit and keeps sending email, the FortiMail unit will send temporary failure codes to the sender. See descriptions for *Temporary fail* in Configuring sender reputation options on page 173.
2. **Temporarily fail:** For scores greater than this threshold but less than the reject threshold, the FortiMail unit replies to senders with a temporary failure code, delaying delivery and requiring senders to retry later when their score is reduced.
3. **Reject:** For scores greater than this threshold, the FortiMail unit replies to senders with a rejection code.

If the SMTP client does not attempt any email deliveries for more than 12 hours, the SMTP client's sender reputation entry is deleted, and a subsequent delivery attempt is regarded as a new SMTP client by the sender reputation feature.

Although sender reputation entries are used for only 12 hours after last delivery attempt, the entry may still appear in list of sender reputation scores.

Filtering sender reputation score entries

You can filter sender reputation score entries that appear on the *Display* tab based on the IP address of the SMTP client, the score, state, and date/time of the last score modification.

To filter the sender reputation score entries

1. Go to *Monitor* > *Reputation* > *Sender Reputation*.
2. Click *Search*.
   A dialog appears.
3. Configure one or more of the following:

GUI item	Description
Field	Select one of the following in the entries that you want to use to filter the display. • IP • Score • State • Last Modified
Operation	Select how to match the field's contents, such as whether the row must contain the contents of *Value*.
Case Sensitive	Enable for case-sensitive filtering.
Value	Enter a pattern or exact value, based on your selection in *Field* and *Operation*. • *IP*: Enter the IP address of the SMTP client, such as `172.16.1.10`, for the entry that you want to display. • *Score*: Enter the minimum and maximum of the range of scores of entries that you want to display. • *State*: Select the *State* of entries that you want to display. • *Last modified*: Select the year, month, day, and/or hour before or after the *Last Modified* value of entries that you want to display.

   Blank fields match any value. Regular expressions and wild cards are not supported.
4. Click *Search*.
   The *Display* tab appears again, but its contents are restricted to entries that match your filter criteria. To remove the filter criteria and display all entries, click *Clear*.

Viewing authentication reputation statuses

FortiMail tracks login attempt failures of CLI, mail and web access. To configure the authentication tracking settings, see Configuring authentication reputation.

To view the authentication reputation statuses

1. Go to *Monitor* > *Reputation* > *Authentication Reputation*.
2. If *Authentication Reputation* is set to *Enable* or *Monitor only* (see Configuring authentication reputation on page 1), this page displays the following information:

GUI item	Description
IP	Lists the blocked IP addresses.
Location	Lists the GeoIP locations/country names.
Violation	List the violation reasons.
Access	Lists the access type: CLI, Mail, or Web. For details see Configuring authentication reputation on page 1.
Expiry Time	If *Authentication Reputation* is set to *Enable* under *Security > Authentication Reputation > Setting*, this column displays when the blocking period will end. The blocking period is also configurable under *Security > Authentication Reputation > Setting*. If *Authentication Reputation* is set to *Monitor only*, this column displays *To be blocked*.

Viewing endpoint reputation statuses

Go to *Monitor > Reputation > Endpoint Reputation* to view the current list of carrier end points (by their MSISDN, subscriber ID, or other identifier) that were caught by FortiMail for sending spam. For general procedures about how to configure endpoint reputation, see Configuring endpoint reputation.

The *Endpoint Reputation* tab is not enabled by default. You must use the following CLI commands to enable the feature and then the tab will appear on the GUI:

```
config antispam settings
   set carrier-endpoint-status enable
end
```

If a carrier end point has attempted to deliver during the automatic blocklisting window a number of spam text messages that is greater than the automatic endpoint blocklisting threshold, FortiMail unit adds the carrier end point to the automatic endpoint block list for the duration configured in the session profile. While the carrier end point is on the automatic block list and it does not expire, all text messages or email messages from it will be rejected. For information on configuring the automatic block list window, see Configuring the endpoint reputation score window. For information on enabling the endpoint reputation scan and configuring the automatic block list threshold in a session profile, see Configuring session profiles on page 171.

You can alternatively blocklist MSISDNs/subscriber IDs manually. For more information, see Manually blocklisting endpoints.

You can exempt MSISDNs/subscriber IDs from automatic blocklisting. For more information, see Exempting endpoints from endpoint reputation.

To view the automatic endpoint reputation block list, go to *Monitor > Reputation > Endpoint Reputation*.

GUI item	Description
Move (button)	To move entries to the manual endpoint block list or safe list, in the check box column, mark the check boxes of entries that you want to move, then click *Move*.
Search (button)	Click to filter the displayed entries. For more information, see Filtering automatic endpoint block list entries on page 64.
Clear (button)	Click to remove any search filter conditions.
Endpoint ID	Lists the mobile subscriber IDSN (MSISDN), subscriber ID, login ID, or other unique identifier for the carrier end point.
Score	Lists the number of text messages or email messages that the FortiMail has detected as spam or infected from the MSISDN/subscriber ID during the automatic endpoint block list window.
Expire	Lists the time at which the automatic endpoint blocklisting entry expires and is removed from the list. *N/A* appears if the endpoint ID has not reached the threshold yet.

Filtering automatic endpoint block list entries

You can filter automatic endpoint block list entries that appear on the *Endpoint Reputation* tab based on the MSISDN, subscriber ID, or other sender identifier.

To filter the endpoint block list entries

1. Go to *Monitor* > *Reputation* > *Endpoint Reputation*.
2. Click *Search*.

GUI item	Description
Field	Displays one option: *Endpoint ID*.
Operation	Select how to match the field's contents, such as whether the row must contain the contents of *Value*.
Value	Enter the identifier of the carrier end point, such as the subscriber ID or MSISDN, for the entry that you want to display. A blank field matches any value. Use an asterisk (*) to match multiple patterns, such as typing 46* to match 46701123456, 46701123457, and so forth. Regular expressions are not supported.
A? (Case Sensitive)	Enable for case-sensitive filtering.

3. Click *Search*.
   The *Auto Blocklist* tab appears again, but its contents are restricted to entries that match your filter criteria. To remove the filter criteria and display all entries, click *Clear*.

Viewing reports

FortiMail units can generate reports either:

- automatically, according to the schedule that you configure in the report profile
- manually, when you select a report profile and click *Generate*

For details, see Configuring report profiles and generating reports on page 346.

Once the reports have been generated, you can view and/or download generated reports.

To reduce the amount of disk space consumed by reports, download generated reports and then delete them from the FortiMail unit.

To view reports

1. If you want to view reports about mailboxes or domain-level mail statistics, purchase the feature license and enable the feature. See Mailbox accounting service on page 1 and Domain mail statistics on page 1.
   By default, their corresponding areas of the GUI are hidden and disabled.
2. Go to either:
   - *Monitor > Report > Mail Statistics*
   - *Monitor > Report > Mailbox Statistics*
   - *Monitor > Report > Domain Mail Statistics*

GUI item	Description
Delete (button)	Click to delete the selected item.
Download (button)	Click to create a PDF version of the report.
Domain	Select which domain's reports to view. This dropdown list only appears on *Monitor > Report > Domain Mail Statistics*.
Directory	Lists the report names of generated reports. To view an individual section of the report in HTML format, click + next to the report name to expand the list of HTML files that comprise the report, then double-click one of the file names.
Creation Time	Lists the date and time when the FortiMail unit completed the generated report.
Size (Byte)	Lists the file size in bytes of the report in HTML format.

3. To view the report in PDF file format, mark the check box in the corresponding row and click *Download*. On the pop-up menu, select *Download PDF*.
4. To view the report in HTML file format, you can view all sections of the report together, or you can view report sections individually.
   - To view **all** report sections together, select the report name, such as `treportprofile-2011-06-27-1039`, then click the *Download* dropdown list and select *Download*

HTML. Your browser downloads a file with an archive (.tgz.gz) file extension to your management computer. To view the report, extract the report files from the archive, and then open the HTML files in your web browser.

- To view **one** report section, in the row corresponding to the report that you want to view, click *+* next to the report name to expand the list of sections, then double-click the file name of the section that you want to view, such as `Statistics.html`. Each *Query Selection* in the report becomes a separate HTML file.

Configuring system settings

The *System* menu lets you administrator accounts, and configure network settings, system time, SNMP, RAID, high availability (HA), certificates, and more.

Configuring administrator accounts and access profiles

The *Administrator* submenu configures administrator accounts and access profiles.

About administrator account permissions

Depending on the account that you use to log in to the FortiMail unit, you may not have complete access to all CLI commands or areas of the GUI.

Admin profile and *Access level* together control which commands and areas an administrator account can access. **Permissions result from an interaction of both.**

The *Access level* is the scope to which an administrator is assigned, either:

- **System**
  The administrator can access areas regardless of whether it is the FortiMail unit itself (system-wide) or a protected domain. Every administrator's permissions are restricted only by their *Admin profile*.
- **Domain**
  The administrator can **only** access areas that are specifically assigned to that protected domain. With a few exceptions, the administrator **cannot** access system-wide settings, files, statistics, nor most settings that can affect other protected domains, regardless of whether access to those items would otherwise be allowed by the administrator's access profile. The administrator **cannot** access the CLI, nor the basic mode of the GUI For more information on the display modes of the GUI, see Basic mode versus advanced mode on page 1.
- **Domain group**
  With an advanced management license, domain groups can be created and used to allocate domain-level administrators to potentially manage multiple domains, and all log entries associated with their domains. Domain-level administrators can search history logs, with the results filtered based on the user's domain.

There are exceptions. Domain administrators can configure IP-based policies, the global block list, the global safe list, the blocklist action, and the global Bayesian database. If you do not want to allow this, do **not** provide *Read-Write* permission to those categories in the *Admin profile* for domain administrators.

Areas of the GUI that domain administrators cannot access

Monitor **except**: • *Personal Quarantine* • *Log* (with advanced management license) • *Domain Quarantine* (with advanced management license)
System **except** for: • *Administrator*
Domain & User **except**: • *Domain*, including its subdomains and associated domains • *Address Map* • *User Alias* • *User > User Preference* • *User > Imported User* (with advanced management license) • *User Import Profile* (with advanced management license)
Policy **except**: • *Recipient Policy > Inbound* • *Recipient Policy > Outbound*
Profile **except**: • *AntiSpam* • *AntiVirus* • *Content* • *File Filter* • *Resource* • *Authentication* • *Dictionary* • *Email* • *Group* • *Notification*
Security **except**: • *Block/Safe List > Domain* • *Block/Safe List > Personal* • *Option > Bayesian*
Encryption
Data Loss Prevention
Email Archiving
Log & Report
Microsoft &Google API

Configuring administrator accounts

The *Administrator* tab displays a list of the FortiMail unit's administrator accounts and the trusted host IP addresses that administrators are allowed to use to log in (if configured).

By default, FortiMail units have one administrator account, `admin`. For more granular control over administrative access, you can create more administrator accounts that are restricted to a specific protected domain and permissions. For details, see About administrator account permissions on page 67.

Depending on the type of your FortiMail administrator account, this list may not display all administrator accounts.

For all cloud administrators, only the administrators with lower level access profile will be displayed.

If you configured a system quarantine administrator account, this account does **not** appear in the list of standard FortiMail administrator accounts. For details, see Configuring the system quarantine setting on page 292.

To configure administrator accounts

1. Go to *System* > *Administrator* > *Administrator* or *Cloud Administrator* (for FortiMail Cloud users).
2. Either click *New* to add an account or double-click an account to modify it.
3. Configure the following and then click *Create*:

GUI item	Description
Enable	Enable or disable the account. If disabled, the account cannot access FortiMail.
Administrator	Enter the name for this administrator account. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
Access level	Select the access level of this administrator account: • *System*: System-wide access, including all protected domains. • *Domain*: This administrator's own account and domain settings only. • *Domain Group*: This administrator's own account and domain group settings only. For details, see About administrator account permissions on page 67 and Configuring protected domains on page 92.  If *Access level* is *Domain* or *Domain Group*, this administrator cannot use the CLI console nor the basic mode of the GUI.
Domain	Select the name of a protected domain. This setting is available only if *Access level* is *Domain*.
Domain Group	Select the name of a group of protected domains. This setting is available only if *Access level* is *Domain group*.

GUI item	Description
Admin profile	Select the name of an administrator profile that determines which functional areas the administrator account may view or affect. Click New to create a new profile or Edit to modify the selected profile. For details, see Configuring administrator access profiles on page 70.
Trusted host	Enter an IPv4 or IPv6 address or subnet from which this administrator can log in. You can add up to 10 trusted hosts. If you want the administrator to access the FortiMail unit from any IP address, use `0.0.0.0/0.0.0.0`. Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiMail unit from your private network by typing `192.168.1.0/255.255.255.0`.  For additional security, restrict all trusted host entries to administrator computers on your trusted private network. For information on restricting administrative access protocols that can be used by administrator computers, see Editing network interfaces on page 1.

Configuring administrator access profiles

The *Admin Profile* tab displays a list of access profiles.

Administrator profiles, in conjunction with the *Access level* to which an administrator account is assigned, govern which areas of the GUI and CLI that an administrator can access, and whether or not they have the permissions to change the configuration or modify items in each area.

To configure an administrator access profile

1. Go to *System* > *Administrator* > *Admin Profile*.
2. Either click *New* to add an account or double-click an access profile to modify it.
3. For *Profile name*, enter the name for this access profile.
4. Optionally enter a comment.
5. For *Access Control* > *Permission*, you can either set all GUI area access to one permission level, or set different permissions to each area.
   - *None*: No permissions to view or configure settings.
   - *Read*: View-only privilege; no modifications are allowed.
   - *Read/Update*: Privilege to view and modify existing configurations. But creation or deletion of table objects is not allowed.
   - *Read/Write*: Full privilege to view and modify settings.
   - *Custom*: If there are sub menus under the main menu, you can specify different permission for different sub menus.
6. Optionally, select the *Privilege level*:
   - *Low*: No access to `diagnose` and `config system xxx` commands in the CLI.
   - *Medium*: Normal access except for super admin privileges. This is the default setting.

- *High*: Same as medium.

Configuring system time

For many features to work, including scheduling, logging, encryption, and certificate validation, the FortiMail system time must be accurate.

Go to *System* > *Configuration* > *Time* to configure the system time and date of the FortiMail unit.

You can either manually set the FortiMail system time or configure the FortiMail unit to automatically keep its system time correct by synchronizing with Network Time Protocol (NTP) servers.

NTP is recommended to achieve better time accuracy. See also Appendix: Port Numbers on page 375.

FortiMail units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

Customizing custom messages, and email templates

Configuring custom messages

Go to *System* > *Customization* > *Custom Message* to view and reword custom messages.

Custom messages are used in many places such as login pages, IBE messages, disclaimer messages, email templates, and other system-related messages. Content, DLP, and antivirus replacement messages used in the action profiles are configured under *Profile* > *Replacement Message* > *Replacement Message*. For details, see Configuring replacement message profiles and variables on page 227, Customizing email templates on page 79, and Configuring global disclaimers on page 1.

The message list organizes replacement messages into a number of types (for example, *System*, *Reject*, etc.). Use the expand arrow beside each type to display the replacement messages for that category. Double-click each custom message to customize that message for your requirements.

You can change the content of the custom message by editing the text and HTML code and by working with custom message variables. For descriptions of the default custom message variables, see Default custom message variables on page 73.

All message groups can be edited to change text, or add text and variables.

1. Go to *System* > *Customization* > *Custom Message*.
2. To edit a message, double-click it or select it and click *Edit*.
3. In the *Content* area, enter the custom message.

   Disclaimer messages include additional settings such as *Tag subject*, *Insert header*, and *Add content*.

   There is a limit of 8191 characters for each custom message.

   For HTML content, if you want to add color, you can either enter the hexadecimal or RGB value directly in the HTML tag, such as:

   ```
   <tr bgcolor="#3366ff">
   ```

   or:

   a. Place the cursor in the attribute. Attribute names vary by the HTML tag.
   b. Click *Insert Color Code*.
   c. Click the color in the palette to insert its numerical value.
4. If custom variables exist, you can add them to the text. To do so:
   a. Click *Insert Variable*. A pop-up window appears.
   b. Place your mouse cursor in the text message at the insertion point for the variable.
   c. Click the name of the variable to add. It appears at the insertion point.
   d. Click the *Close* (X) icon to close the window.

   If no custom variables exist, the *Insert Variable* link does not appear. Some message types include predefined variables. You can create variables. See Creating new variables on page 72.
5. Click *OK*, or click *Reset To Default* to revert the custom message to its default text.

Creating new variables

In addition to the predefined variables, you can create new ones to customize custom messages and email templates. Typically, these variables represent text that you will use multiple times.

Many predefined variables exist, and you cannot edit their values or rename them. Variables cannot be reused in other messages or email templates. For a list of predefined variables and which templates they can be used in, see the default variables for custom messages.

1. To create new variables to be used in custom messages, go to *System* > *Customization* > *Custom Message*.

   To create new variables to be used in email templates, go to *System* > *Customization* > *Custom Email Template*.
2. Select a custom message or email template where you want to add a new variable, and click *Edit Variable*.
3. Click *New*.
4. Configure the following:
   - In *Name*, enter the variable name to use in the custom message.

     For example, if you enter `COMPANY-NAME`, this variable will appear as `%%COMPANY-NAME%%` in the custom message if you insert it. This is also the name of the variable as it appears in the CLI. (The GUI uses *Display name* instead.)
   - In *Display Name*, enter a label that will appear in the variable list when you click *Insert Variables* in the GUI while customizing a message or creating a variable. For example, you could enter `Company Name` for the variable `%%COMPANY-NAME%%`.
   - In *Content*, enter the variable's value.
5. Click *Create* and then *Close*.

To use the new variable, edit the contents of the custom message or email template. See Configuring custom messages on page 71 or Customizing email templates on page 79.

Default custom message variables

Variable	Description	Location
%%FILE%%	The name of the file that is infected with a virus.	System > Customization > Custom Message > Reject > Virus message
%%VIRUS%%	The name of the virus that has infected the file.	
%%FILE_TYPE%%	The file type of the infected file. This variable is only applicable to files with extensions.	
%%FILE%%	The name of the file that was removed from the email.	System > Customization > Custom Message > Reject > Suspicious message
%%EMAIL_ID%%	The ID that FortiMail assigns to the quarantined email. Note that this email ID is different from the standard message ID in the email header.	System > Customization > Custom Email Template > Report > Quarantine summary
%%MESSAGE_ID%%	The standard message ID in the header of the quarantined email.	
%%ORIG_ENVELOPE_FROM%%	The original envelope sender address (MAIL FROM:) of the quarantined email.	
%%ORIG_ENVELOPE_TO%%	The original envelope recipient address (MAIL TO:) in the SMTP envelope of the quarantined email.	
%%QMSG_EMAIL_DELETE%%	Under email actions in the quarantine summary, the *Delete* link that, if it is clicked, sends an email request to delete the quarantined message.	
%%QMSG_FROM%%	The email address of the sender of the quarantined email	
%%QMSG_WEB_DELETE%%	Under web actions in the quarantine summary, the Delete link that, if being clicked, sends a HTTP or HTTPS request to delete the quarantined message.	
%%QUARANTINE_FROM%%	The start time of the quarantine summary.	

Variable	Description	Location
%%QUARANTINE_TO%%	The end time of the quarantine summary.	System > Customization > Custom Email Template > Report > Quarantine summary
%%SPAM_DELETE_ALL_EMAIL%%	Under email actions in the quarantine summary, the Click Here link that, if being clicked, sends an email to delete all quarantined messages.	
%%SPAM_DELETE_ALL_URL%%	Under spam web actions in the quarantine summary, the Click Here link that, if being clicked, sends a HTTP or HTTPS request to delete all quarantined messages.	
%%SPAM_DELETE_SUBJECT%%	The subject of the email that is sent to delete a quarantined message when you click Delete under email actions in the quarantine summary.	
%%SPAM_RELEASE_EMAIL%%	The email address, such as release-ctrl@example.com, used to release an email from the recipient's personal quarantine. For details, see Configuring the quarantine control options on page 293.	
%%QMSG_DATE%%	The date and time when a message was quarantined.	
%%QMSG_EMAIL_RELEASE%%	Under email actions in the quarantine summary, the Release link that, if being clicked, sends an email to have a quarantined message sent to you.	
%%QMSG_SUBJECT%%	The subject of a quarantined message.	
%%QMSG_WEB_RELEASE%%	Under web actions in the quarantine summary, the Release link that, if being clicked, releases the message to your inbox.	
%%QUARANTINE_MESSAGES_COUNT%%	The number of quarantined messages in this summary.	

Variable	Description	Location
%%SPAMREPORT_SENDER%%	The email address, such as release-ctrl-svr@example.com, used to send quarantine summaries.	System > Customization > Custom Email Template > Report > Quarantine summary
%%SPAM_DELETE_ALL_SUBJECT%%	The subject of the email that is sent to delete all quarantined messages when you select Click Here under email actions in the quarantine summary.	
%%SPAM_DELETE_EMAIL%%	The email address, such as delete-ctrl@example.com, used to delete an email from the recipient's personal quarantine. For details, see Configuring the quarantine control options on page 293.	
%%SPAM_PREFERENCE%%	The *Click Here* link under *Other* in the quarantine summary that, if it is clicked, opens your entire quarantine inbox for you to manage your preferences.	
%%SPAM_RELEASE_SUBJECT%%	The subject of the email that is sent to release a quarantined message when you click *Release* under email actions in the quarantine summary.	
%%SERVICE_NAME%%	Copyright information of the secure message.	System > Customization > Custom Message > Secure message > Secure message footer
%%SERVICE_NAME%%	The From:, To:, and subject lines of the secure message.	System > Customization > Custom Message > Secure message > Secure message header
%%DISCLAIMER_REPLY_TO%%	The disclaimer reply to address.	System > Customization > Custom Message > Email Content Resources > Disclaimer insertion message
%%FILE%%	The name of the file that was removed from the email.	
%%FILE_TYPE%%	The file type of the suspicious file. This variable is only applicable to files with extensions.	
%%MESSAGE_ID%%	The standard message ID in the header of the email.	
%%ORIG_ENVELOPE_FROM%%	The original envelope sender address (MAIL FROM:) of the email.	
%%ORIG_FROM%%	The sender email address in the message header (From:) of the original email.	
%%ORIG_FROM_DOMAIN%%	The domain in the sender email address in the message header (From:) of the original email.	
%%VIRUS%%	The name of the virus that has infected the file.	

Variable	Description	Location
%%ADMIN_SENDER%%	The sender's address of this notification email.	System > Customization > Custom Email Template > Secure message > Account reset notification
%%LAST_NAME%%	The last name of the notification receiver.	
%%MONTH%%	The month when the link in the notification to reset the account will expire.	
%%TIME%%	The time when the link in the notification to reset the account will expire.	
%%DAY%%	The day when the link in the notification to reset the account will expire.	System > Customization > Custom Email Template > Secure message > Account reset notification
%%LINK_URL%%	The link in the notification that you can click to complete the account reset.	
%%SERVICE_NAME%%	Signature of the notification.	
%%YEAR%%	The year when the link in the notification to reset the account will expire.	
%%ADMIN_SENDER%%	The sender's address of this notification email.	
%%LAST_NAME%%	The last name of the notification recipient.	
%%RECIPIENT%%	The email address of the notification recipient.	
%%YEAR%%	The year when the notification was sent.	
%%DAY%%	The day when the notification was sent.	
%%MONTH%%	The month when the notification was sent.	
%%SERVICE_NAME%%	Signature of the notification.	
%%DAY%%	The day when the link in the notification to reset the password will expire.	System > Customization > Custom Email Template > Secure message > Password reset notification
%%LAST_NAME%%	The last name of the notification recipient.	
%%MONTH%%	The month when the link in the notification to reset the password will expire.	
%%TIME%%	The time when the link in the notification to reset the password will expire.	
%%URL_HELP%%	The Help link in the notification about secure email.	
%%FIRST_NAME%%	The first name of the notification recipient.	

Variable	Description	Location
%%LINK_URL%%	The link in the notification that you can click to complete the password reset.	System > Customization > Custom Email Template > Secure message > Password reset notification
%%SERVICE_NAME%%	Signature of the notification.	
%%URL_ABOUT%%	The About link in the notification about secure email.	
%%YEAR%%	The year when the link in the notification to reset the password will expire.	
%%ADMIN_SENDER%%	The sender's address of this notification email.	
%%LAST_NAME%%	The last name of the notification recipient.	
%%RECIPIENT%%	The email address of the notification recipient.	
%%YEAR%%	The year when the notification was sent.	
%%DAY%%	The day when the notification was sent.	
%%MONTH%%	The month when the notification was sent.	
%%SERVICE_NAME%%	Signature of the notification.	
%%ADMIN_SENDER%%	The sender's address of this notification email.	System > Customization > Custom Email Template > Secure message > Secure message notification - Pull
%%EMAIL_SUBJECT%%	The subject of the notification.	
%%URL_HELP%%	The Help link in the notification about secure email.	
%%LINK_URL%%	The link in the notification that you can click to open the secure message.	
%%URL_ABOUT%%	The *About* link in the notification about secure email.	
%%ADMIN_SENDER%%	The sender's address of this notification email.	System > Customization > Custom Email Template > Secure message > Secure message notification - Push
%%URL_ABOUT%%	The *About* link in the notification about secure email.	System > Customization > Custom Email Template > Secure message > Secure message notification - Push
%%EMAIL_SUBJECT%%	The subject of the notification.	
%%URL_HELP%%	The *Help* link in the notification about secure email.	

Variable	Description	Location
%%ADMIN_SENDER%%	The sender's address of this notification email.	System > Customization > Custom Email Template > Secure message > User registration notification
%%LAST_NAME%%	The last name of the notification recipient.	
%%RECIPIENT%%	The email address of the notification recipient.	
%%YEAR%%	The year when the notification was sent.	
%%DAY%%	The day when the notification was sent.	
%%MONTH%%	The month when the notification was sent.	
%%SERVICE_NAME%%	Signature of the notification.	
%%ATTENDEE_ACTION%%	The action (accept, tentative, or reject) taken by the event attendee.	System > Customization > Custom Email Template > Notification > Calendar event notification
%%CALENDAR_SENDER%%	The email address from where the notification is sent.	
%%CALENDAR_URL_NO%%	The event is rejected.	
%%EVENT_FREQUENCY%%	The frequency of the event.	
%%EVENT_ORGANIZER%%	the email address of the event organizer.	
%%EVENT_TYPE%%	The type of the event.	
%%TIME_END%%	The ending time of the event.	
%%CALENDAR_ATTENDEE%%	The name of the person invited to this event.	
%%CALENDAR_URL_MAYBE%%	The event is set to tentative by the attendee.	
%%CALENDAR_URL_YES%%	The event is accepted by the attendee.	
%%EVENT_LOCATION%%	The location where the event is to be held.	System > Customization > Custom Email Template > Notification > Calendar event notification
%%EVENT_TITLE%%	The nature of the event. For example, meeting or party.	
%%TIME_BEGIN%%	The starting time of the event.	
%%LOCAL_HOST_NAME%%	Host name of the FortiMail unit which sends out the notification.	System > Customization > Custom Email Template > Notification
%%LOCAL_DOMAIN_NAME%	Domain name of the Fortimail unit which sends out the notification.	

Customizing email templates

The FortiMail unit may send notification email for:

- quarantine reports (see Configuring email quarantines and quarantine reports on page 285)
- IBE (see FortiMail IBE configuration workflow on page 325)
- repackaging virus-infected email with new email body (see Configuring antivirus action profiles on page 213)
- notifying the recipient for any FortiMail actions (see Configuring notification profiles on page 274)

You can customize the email templates for all of these email/report types.

Due to Microsoft 365 API limitations, customization of the From field in the notification email templates is not supported if FortiMail runs in MS365 mode.

To customize notification email templates

1. Go to *System* > *Customization* > *Custom Email Template*.
2. To edit a template, double-click it or select it and click *Edit*.
3. Enter the replacement message and click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

   Email templates include additional settings, such as *Subject*, *From*, *To*, and *Envelope from*, and *Envelope to*. You can either enter text directly, or insert a variable such as `%%SUBJECT%%` or `%%POSTMASTER%%`.
4. To format replacement messages in HTML, use HTML tags, such as `<b>some bold text</b>`.

   There is a limit of 250 characters for the *Subject* field, 60 characters for the *From* field, and 4000 characters for *HTML* and *Text* messages each in the *Content* field.
5. To add a variable:
   - Select *Insert Variables* next to the area to insert a variable. A pop-up window appears.
   - Place your mouse cursor in the text message at the insertion point for the variable.
   - Click the name of the variable to add. It appears at the insertion point.
   - To add another variable, click the message area first, then click the variable name.
   - Click the *Close* (X) icon to close the window.
6. To insert a color:
   - Click *Insert Color Code*. A pop-up window of color swatches appears.
   - Place your mouse cursor in the text at the insertion point for the color code, or highlight an existing color code to change.
   - Click a color in the color swatch. For example, to replace the color code in the HTML tag `<tr bgcolor="#3366ff">`, you can highlight `"#3366ff"`, then select the color you want from the color palette.

   To add a new color code, include it with HTML tags as applicable, such as `<tr bgcolor="#3366ff">`.
7. To determine if your HTML and color changes are correct, click *Preview*. The replacement message appears in HTML format.
8. Click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

Configuring single sign-on (SSO)

Single sign-on (SSO) can save time for users by reducing the number of times that they must log in when using many network services. Once they log in, they can access all other authorized services that use SSO until their session expires.

FortiMail Cloud supports SSO for webmail users.

CalDAV and WebDAV authentication

When SSO is enabled for webmail users, CalDAV and WebDAV authentication will not function. They only support simple local password authentication.

In Security Assertion Markup Language (SAML) SSO, you must configure both of these to connect and authenticate with each other:

- FortiMail, which is the service provider (SP)
- FortiAuthenticator or other remote authentication server, which is the identity provider (IdP)

In addition to SSO, FortiMail also supports single log off (SLO). When someone logs out of FortiMail, they will also be logged out of all services that use the same federated SSO authentication.

To configure SAML SSO

- On the IdP server:
  a. Download its IdP metadata XML. Alternatively, copy the URL where FortiMail can download it.
  b. The email address that the user must give when they authenticate is stored in an attribute on the IdP server. This attribute has an object identifier (OID). If this OID is different than the default setting of Attribute used to identify email address on FortiMail, then copy the IdP server's OID. For example
  ```
  urn:oid:0.9.2342.19200300.100.1.3
  ```
- On FortiMail:
  a. If you are integrating with FortiAuthenticator or Ping Identity, then on FortiMail, use the CLI to enable Security Fabric and the administrator account named `admin_sso`:
  ```
  config system csf
     set status enable
  end
  config system admin
     edit admin_sso
        set status enable
  end
  ```
  The `admin_sso` account acts as a wildcard, so that you do not need to configure all FortiMail accounts on the IdP too. The Security Fabric provides communication for this feature.
  b. Go to *System* > *Single Sign On* > *Profile*.
  c. Click *New*, or select a row and click *Edit* to edit an existing profile.
  d. Configure the following:

GUI Item	Description
Profile name	Enter a unique name for the profile.

GUI Item	Description
Comment	Optional. Enter a descriptive comment.
Metadata	Enter the IdP metadata. To do this, either: • Paste the metadata XML into the text area. • Click *Upload* and select a file that contains the XML. • Click *Retrieve from URL*, and then enter the URL where FortiMail can download the XML.
Attribute used to identify email address	Enter the OID of user email addresses on the IdP server.

e. Click *Create* or *OK*.Now FortiMail automatically generates its SP metadata, entity ID, and ACS URL. (You might need to navigate away from the tab and return in order for it to display.)

f. Go to *System* > *Single Sign On* > *Setting*.

g. Copy the following:

GUI Item	Description
Single sign on	Enable or disable SSO.
Allow dynamic IP from IdP	Enable if the IdP uses dynamic client IP addresses, even within the same SAML session. (This can be useful, for example, if the IdP is deployed behind a load balancer.) Then enter the IdP's client IP addresses or subnet in CIDR or dotted decimal format. Separate multiple IP addresses or subnets with a comma. Spaces are not allowed. If no IP range is specified, then any IP address is allowed.  For better security, only allow IdP communications from known IP addresses.
Use different service provider for admin and webmail access	Enable to use different service provider metadata for FortiMail admin and webmail access, so that both the FortiMail admin URL (https://fortimail_hostname_or_ip/admin) and the webmail URL (https://fortimail_hostname_or_ip) can be supported on the IDP.
Service Provider Metadata	If you enable the above option, choose which user access you will configure the service provider metadata for: `Admin` or `Webmail`, then configure the following settings.
Entity ID	A globally unique identifier for FortiMail when it connects to the IdP, such as: `https://FortiMail.example.com/sp`
Signature	The hash algorithm(for example, `SHA256`) that will be used by the signature.
ACS URL	The URL where FortiMail will receive authentication responses from the IdP (the assertion consumer service (ACS)), such as: `https://FortiMail.example.com/sso/SAML2/POST`
Metadata	Click *Download* to retrieve the FortiMail SP metadata XML file.

- On the IdP server:
  a. Paste the entity ID, SP metadata URL, and ACS URL from FortiMail.
  b. Select to identify users by their email addresses attribute, and then enter the attribute object identifier (OID) that authentication requests from FortiMail use:`urn:oid:0.9.2342.19200300.100.1.3`
  c. Optionally, enable and configure multi-factor authentication (MFA).
  d. If required, add the FortiMail unit's certificate to the list of trusted CAs ("trust store").(Skip this step if your IdP already trusts the certificate, directly or indirectly, via a CA certificate signing chain.)
- On FortiMail, go to *System > Administrator > Administrator*. For each administrator or protected domain (webmail users), configure *Configuring administrator accounts and access profiles* and *Configuring administrator accounts and access profiles*, and/or *Webmail single sign on*, so that person can use SAML SSO to log in. To test SSO, authenticate on FortiMail using one of those accounts. Then access another service that also uses SSO. If successful, the other service should not prompt you to log in again.

Using FortiNDR malware inspection

FortiNDR (formerly FortiAI) is the first Fortinet Network Detection and Response product from Fortinet. Apart from the Virtual Security Analyst™ with sub-second malware detection technology based on neural networks, FortiNDR is built on FortiAI's technology with extended and added features to detect Network Anomalies with auto and manual mitigation techniques. FortiNDR is renamed from FortiAI with additional Network Detection and Response functionality, with the original FortiAI malware analysis features.

FortiNDR is the next generation of Fortinet's malware detection technology, using Artificial Neural Networks (ANN) which can deliver sub-second malware detection and verdicts. You can send suspicious email attachments to FortiNDR for inspection when you configure antivirus profiles (see Configuring antivirus profiles on page 209). If the file exhibits risky behavior, or is found to contain a malware, the result will be sent back to FortiMail and you can take actions according to the verdict.

For more information, see the FortiNDR Administration Guide.

For FortiMail and FortiNDR to communicate, both sides must have the Fortinet certificate installed.

To add a FortiNDR service

1. Go to *System > FortiNDR > FortiNDR*.
2. Configure the following settings:

GUI item	Description
Status	Enable FortiNDR protection.
Base URL	Enter the FortiNDR base URL.
API key	Enter the API key that you generated on FortiNDR. For details, see the FortiNDR Administration Guide.

GUI item	Description
Test Connection	Click to test the network connection to the URL.
Upload timeout	Specify the timeout (in seconds) for uploading email attachments. Default setting is 10 seconds.
Rating timeout	Specify the timeout (in seconds) for FortiNDR to scan the uploaded files. Default setting is 10 seconds.

Using FortiSandbox antivirus inspection

The FortiSandbox appliance and FortiSandbox cloud service are used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus profiles (see Configuring antivirus profiles on page 209). If the file exhibits risky behavior, or is found to contain a virus, the result will be sent back to FortiMail and a new virus signature is created and added to the FortiGuard antivirus signature database as well.

If email attachments are sent to FortiSandbox, and the "reject" action is configured in the action profile, the actual action will fallback to "system quarantine" if spam or viruses are detected afterward.

Spam URLs already detected by FortiGuard will not be submitted to FortiSandbox.

To add a FortiSandbox unit

1. Go to *System* > *FortiSandbox* > *FortiSandbox*.
2. Enable the *FortiSandbox Inspection* and configure the following settings:

GUI item	Description
FortiSandbox type	If you use an appliance, specify the appliance's host name or IP address; If you use the regular or enhanced cloud service, see FortiCloud service on page 84.
Server name/IP	Enter the FortiSandbox host name or IP address. The port to use is 514. If you have a firewall in between FortiMail and FortiSandbox, make this port is allowed.
Notification email	This is the email address that FortiSandbox will use to send out notifications and reports. If you want to receive such email, enter your email address. For details, see the FortiSandbox documentation.
Statistics interval	Specify how long FortiMail should wait to retrieve some high level statistics from FortiSandbox. The default interval is 5 minutes. The statistics include how many malware are detected and how many files are clean among all the files submitted.

GUI item	Description
Scan timeout	Specify how long FortiMail will wait to get the scan results. If you receive timeouts and want to wait longer for the results, you can increase the timeout.
Scan result expires in	Specify how long FortiMail will cache the results. 0 means no local cache.
File Scan Setting	
File types	Select what types of attachment files will be uploaded to FortiSandbox for scanning.
File patterns	Create your own file pattern that will be uploaded to FortiSandbox, for example, *.txt.
File size	Specify the maximum file size to upload to FortiSandbox. You may want to limit the file size to improve performance.
URL Scan Setting	
URL selection	Specify a URL category profile or click *New* to create one. You can also click *Edit* to modify the selected profile.
Upload URL on rating error	Sometimes, FortiMail may not be able to get results from the FortiGuard queries (for example, ratings errors due to network connection failures). In this case, you can choose whether to upload those URLs to FortiSandbox for scanning. Choosing not to upload those URLs may help improving the FortiSandbox performance.
Bypass one-time URL	When enabled, any URLs that are in the personal or business category and are a pre-defined filter pattern, or if the URL is locally defined, bypass URL submission to FortiSandbox.
Number of URLs per email	Specify how many URLs will be scanned in one email message. **Note**: If the FortiSandbox type is set to *Appliance*, the valid range is 1 to 100; if it is set to *Cloud* or *Enhanced Cloud*, the valid range is 1 to 12.

FortiCloud service

If you have a valid FortiMail Cloud Sandbox entitlement, select *Regular* or *Enhanced Cloud* when configuring the service for use with the FortiMail appliance.

Depending on your FortiCare contract, FortiMail Cloud Sandbox provides two operational modes:

- Regular cloud service: You will share the Cloud Sandbox service with other users.
- Enhanced cloud service: You will have dedicated Cloud Sandbox service and enjoy better performance.

If you have a hosted FortiSandbox Cloud deployment in FortiCloud, or are using a hardware or virtual FortiSandbox appliance, FortiMail should be configured in *appliance mode*. Check to ensure FortiMail can communicate with FortiSandbox over TCP port 514.

To use the FortiCloud service

1. Go to *Dashboard > Status*.
2. Under *License Information*, click *Activate* besides *FortiCloud*.
3. In the popup dialog box, enter the email address and password for the FortiCloud account.
4. Click *OK* to log on to FortiCloud.
   Now the *License Information* should display as *Paid Contract* (if you use a demo unit, it displays as *Trial License)*.
5. Go to *System > FortiSandbox > FortiSandbox* and select *Cloud* or *Enhanced Cloud* for *FortiSandbox type* depending on your FortiCare contract. Also configure other scan settings (see Using FortiSandbox antivirus inspection on page 83).
6. After you activate FortiCloud and configure the FortiSandbox scan settings, you can access the FortiCloud web portal by going to *Dashboard > Status* and clicking *Launch Portal* besides *FortiCloud* under *License Information*.
   The portal allows you view the FortiMail file submission status and FortiSandbox cloud scan results.
7. If you upgrade from older releases, a reminder will appear on the dashboard, telling you to activate FortiCloud (that is, to create an FortiCloud account) before you can access the FortiCloud portal.

If you are running FortiMail HA, you must activate FortiCloud service on the primary and secondary units. For active-passive HA, this is to ensure that the secondary unit can continue to use the FortiCloud service in case of HA failover. For active-active HA, this is because all the units need to access the service.

See also

Viewing the mailbox backup/restoration status

Backing up and restoring the mailboxes

Configuring mailbox backups

Configuring FortiGuard services

Go to *System > FortiGuard > License* to view your current licenses and service status, and the most recent updates to FortiGuard Antivirus engines, antivirus definitions, and FortiGuard Antispam definitions (antispam heuristic rules).

FortiMail units receive updates from the FortiGuard Distribution Network (FDN), a world-wide network of FortiGuard Distribution Servers (FDS). FortiMail units connect to the FDN by connecting to the FDS nearest to the FortiMail unit by its configured time zone.

In addition to manual update requests, FortiMail units also support scheduled updates, by which the FortiMail unit periodically polls the FDN to determine if there are any available updates.

For FortiGuard Antispam and FortiGuard Antivirus update connectivity requirements and troubleshooting information, see Troubleshoot FortiGuard connection issues.

Configuring FortiGuard Antivirus service

You can configure the FortiMail unit to periodically request updates from the FDN or override servers for the FortiGuard Antivirus engine and virus definitions.

For example, you might schedule updates every night at 2 AM or weekly on Sunday, when email traffic volume is light.

Before configuring scheduled updates, first verify that the FortiMail unit can connect to the FDN or override server.

To configure FortiGuard Antivirus options

1. Go to *System* > *FortiGuard* > *AntiVirus*.
2. Configure the following and then click *Apply*.

GUI item	Description
Virus outbreak protection	When a virus outbreak occurs, the FortiGuard antivirus database may need some time to get updated. Therefore, you can choose to defer the delivery of the suspicious email messages and scan them for the second time. • *Disable*: Do not query FortiGuard antivirus service. • *Enable*: Query FortiGuard antivirus service. • *Enable with Defer*: If the first query returns no results, defer the email for the specified time and do the second query.
Virus outbreak protection period	If Virus outbreak protection is *Enable with Defer*, enter how many minutes later a second query will be done.
Virus database	Depending on your models, FortiMail supports three types of antivirus databases: • *Default*: The default FortiMail virus database contains most commonly seen viruses and should be sufficient enough for regular antivirus protection. For the current release, FortiMail VM00 model supports the default virus database only. • *Extended*: Some high-end FortiMail models support the usage of an extended virus database, which contains viruses that are not active any more. For the current release, FortiMail VM01/VM02/200F/400F models support both the default and extended virus databases. • *Extreme*: Some high-end models also support the usage of an extreme virus database, which contains more virus signatures than the default and extended databases. For the current release, FortiMail VM04/900F and above models support all three types of virus databases
Scheduled update	Enable to perform updates according to a schedule, then select one of the following as the frequency of update requests. When the FortiMail unit requests an update at the scheduled time, results appear in *Last Update Status*. • *Every*: Select to request to update once every 1 to 23 hours, then select the number of hours between each update request. • *Daily*: Select to request to update once a day, then select the hour of the day to check for updates.

GUI item	Description
	• *Weekly*: Select to request to update once a week, then select the day of the week and the hour of the day to check for updates.
Server location	Use FortiGuard servers either in the United States only, or in any location in the world.

See also

Configuring FortiGuard services

Configuring FortiGuard Antivirus service

Manually requesting updates

Troubleshoot FortiGuard connection issues

Manually requesting updates

You can manually trigger the FortiMail unit to connect to the FDN or override server to request available updates for its FortiGuard antivirus packages.

You can manually initiate updates as an alternative or in addition to other update methods.

To manually request updates

Before manually initiating an update, first verify that the FortiMail unit can connect to the FDN or override server.

1. Go to *System* > *FortiGuard* > *AntiVirus*.
2. Click *Update Now*.

Updating FortiGuard Antivirus definitions can cause a short disruption in traffic currently being scanned while the FortiMail unit applies the new signature database. To minimize disruptions, update when traffic is light, such as during the night.

3. After a few minutes, click the *System* > *FortiGuard* > *License* tab to check the update status. If an update was available, new version numbers appear for the packages that were updated. If you have enabled logging, messages are recorded to the event log indicating whether the update was successful or not. For details, see Logs, reports, and alerts on page 336.

Configuring FortiGuard Antispam service

You can connect to the FDN to use the FortiGuard Antispam service. You can also use your own override server, such as a FortiManager unit, for antispam service.

To configure the FortiGuard Antispam options

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. Under *FortiGuard AntiSpam*, verify that *Status* is enabled.
3. Specify a spam outbreak protection level. Higher level means more strict filtering.
4. Optionally enable cache and specify the cache TTL time. Enabling cache can improve performance.

5. Use FortiGuard servers either in the United States only, or in any location in the world.
6. Click *Apply*.

About spam outbreak protection from FortiGuard

This feature temporarily hold email for a certain period of time (spam outbreak protection period) if the enabled FortiGuard Antispam check (block IP and/or URL filter) returns no result (see FortiGuard section on page 189). After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard Antispam service to update its database in cases a spam outbreak occurs.

FortiMail uses its internal algorithms to determine the suspicious level of an email. For example, the following email is treated as highly suspicious because it contains a phishing URL that might not be known to FortiGuard at the time.

```
Received: from linux-2543.local ([64.78.154.244])by mail.example.com with ESMTP id 31AmE8tP018352-
      31AmE8tQ018352 for <bob@example.com>; Fri, 10 Feb 2023 14:14:09 -0800
From: "American Express Online" <info@american-express.com>
To: bob@example.com
Reply-To: <spammer@gmail.com>
Subject: New secure email message from American Express
Date: 10 Feb 2023 15:14:08 -0700
Message-ID: <20230210151408.e4253c5C355132EB@givemeyourmoney.com>
MIME-Version: 1.0
Content-Type: text/plain
For your protection, the content of this message has been sent securely by American Express using
      encryption technology
To view the secure message, for your security reason
Copy paste below the link in your browser and follow the instruction
https://american.express.vds.xxxxxx.com/secure_email
The secure message expire on February 15 .2023 @ 9:01 PM(GMT)!!!
Do not reply to the notification message, the message was auto generated by the sender's Security
      system
```

Configuring spam sample submission service

Users can submit samples of spam and non-spam that were not detected correctly. Special email addresses on FortiMail receive each type of sample. Then administrators can either review them first, or they can be sent directly to the FortiGuard Antispam service labs. This information can be used to improve the FortiGuard Antispam catch rate.

Once you have configured FortiMail to receive spam samples, you can install a plugin on your users' email clients to make it easier for them to submit samples. For details, see:

- FortiMail Outlook Spam Submission Plugin Deployment Guide
- FortiMail Outlook Spam Submission Plugin for Web or Mobile App Deployment Guide

To configure the spam sample submissions service

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. In the *Sample Submission* section, enable *Status*.

3. If you have multiple protected domains, enable *Domain submission* if you want to allow domain administrators to view spam sample submissions for their own domain..
4. In *Submission handling type*, select whether you want an administrator to manually review spam sample submissions (see Managing the spam sample submissions on page 49), or you want them to be sent directly to FortiGuard.
5. In *Retention period*, enter a number of days between 0-60, after which the sample spam submission will be deleted.
6. In *Email account to receive spam* and *Email account to receive non-spam*, enter the email addresses that will receive spam and non-spam ("ham") sample submissions.

Sample submission email addresses must:

- Not be the same.
- Receive only samples of spam and non-spam; they should not receive any other email. They cannot be the same as the quarantine control accounts, email archiving accounts, Bayesian training accounts, and any other email accounts.

7. Click *Apply*.

System utility

Go to *System* > *Utility* to use various system utilities.

FortiGuard query

Go to *System* > *Utility* > *FortiGuard Query* if you need to manually query the FortiGuard Antispam service by entering an IP address, URL, or a hash value of an email message. See also Configuring FortiGuard Antispam service on page 87.

Traffic capture

When troubleshooting networks, it helps to examine packet headers. This determines whether the destination, listening port numbers, route, and more are all what you expect.

To perform a packet trace, go to *System* > *Utility* > *Traffic Capture*. For details, see `diagnose sniffer` commands in the FortiMail CLI Reference.

Regular expression validator

Go to *System* > *Utility* > *Regex Validator* to validate and test regular expressions and string text. See also Syntax on page 381.

Message file converter

Go to *System* > *Utility* > *Msg Converter* to convert .msg files to .eml files. Since .msg is only used by Microsoft Outlook, you can use the converter to allow other email programs to work with the .msg file content, once converted to the more universal .eml format.

To evade email attachment inspection, a sender may use the Outlook file format .msg to hide malicious links that other email clients and scanners cannot read.

On-demand DMARC reports

If DMARC checks and DMARC reports are enabled (see DMARC section on page 193 and DMARC Report Generation on page 314), then FortiMail automatically periodically sends DMARC reports.

If you have the feature license for it (see DMARC report analysis on page 1), then you can also manually trigger FortiMail to generate the report at any time. Additional report settings are also available.

To send a DMARC report

1. Go to *System* > *Utility* > *DMARC*.
2. Configure the following settings:

GUI item	Description
Date	Select a date from within the previous month. This filters the report so that it only shows email that FortiMail processed on this date. After 30 days, DMARC data expires and is not available for reports anymore.
Policy domain	Select a sender domain name that matched a policy where DMARC was applied. This filters the report so that it only shows email from this sender domain. Available options vary by your selection in Date.
Report from domain	Select the domain name that the FortiMail unit will use as its sender email address (`From:`) when it sends the DMARC report email. Available options vary by your selection in Date and Policy domain. (In the original email that had a DMARC check, the sender tried to send email to one or more protected domains. Available options are one of those recipient protected domains.)
Report from address	Optional. Enter the local part (username) that the FortiMail unit will use as its sender email address (`From:`) when it sends the DMARC report email. Default is `noreply`. Change it if, for example, an administrator wants replies about this DMARC report. For the equivalent setting in DMARC reports that are sent automatically, see Sender address local part on page 314 or From address local part on page 105.
Report to address	Select which recipient email address to send the DMARC report to, either: • *RUA Address* — FortiMail automatically queries the DNS server about the sender domain in Policy domain to determine that domain's authorized DMARC report recipient. **Note:** If a sender does not have a valid DMARC RUA/RUF configured in the domain's DNS `TXT` record, then FortiMail cannot send them because there is no report recipient email address.

GUI item	Description
	• *Other Address* — Manually configure another DMARC report recipient in Email address. **Tip:** This option can be useful if, for example, the sender domain's DMARC record is misconfigured, and you want to send a report to show them how many email were rejected due to failed DMARC checks.
Email address	Enter the recipient email address where FortiMail will send the DMARC report. This setting applies only if Report to address is *Other Address*.

3. Click *Send Report*.
   This button is not available until you have configured all required settings.

Trace log

If Fortinet Technical Support requests a trace log for system analysis purposes, you can download one using the GUI.

Trace logs are compressed into an archive (.gz), and contain information that is supplementary to debug-level log files.

To download a trace file

1. Go to *System* > *Utility* > *Trace Log*.
2. At the bottom of the tab, click *Download Trace Log*.

Configuring domains and users

The *Domains & User* menu allows you to configure the protected domains and users.

Configuring protected domains

The *Domain* tab displays the list of protected domains and domain groups.

As the FortiMail Cloud administrator, you have to add protected domains on the FortiMail Cloud Admin Portal. For details, see the FortiMail Cloud Portal Guide. Then you can edit the protected domains on the FortiMail Admin GUI.

Protected domains define connections and email messages for which the FortiMail unit can perform protective email processing by describing both the:

- IP address of an SMTP server
- domain name portion (the portion which follows the @ symbol) of recipient email addresses in the SMTP envelope (`RCPT TO:`)

The FortiMail unit uses both parts to compare to connections and email messages when looking for traffic that involves the protected domain.

For FortiMail units operating in server mode, protected domains list only the domain name, not the IP address: the IP address of the SMTP server is the IP address of the FortiMail unit itself.

For example, if you wanted to scan email from email addresses such as `user.one@example.com` hosted on the SMTP server 10.10.10.10, you would configure a protected domain of `example.com` whose SMTP server is `10.10.10.10`.

Aside from defining the domain, protected domains contain settings that apply specifically to all email destined for that domain, such as mail routing and disclaimer messages.

With an advanced management feature license, domain groups can be created and used to associate to domain-level administrators, allowing administrators to potentially manage multiple domains and all log entries associated with their domains. Domain-level administrators may search history logs, with the results filtered based on the user's domain.

Many FortiMail features require that you configure a protected domain. For example, when applying recipient-based policies for email messages incoming to the protected domain, the FortiMail unit compares the domain name of the protected domain to the domain name portion of the recipient email addresses.

When FortiMail units operating in transparent mode are proxying email connections for a protected domain, the FortiMail unit will pass, drop or intercept connections destined for the IP address of an SMTP server associated with the protected domain, and can use the domain name of the protected domain during the SMTP greeting.

Usually, you have already configured at least one protected domain during installation of your FortiMail unit; however, some configurations may not require any protected domains. You can add more domains or modify the settings of existing ones if necessary.

If you have many mail domains that will use identical settings, instead of creating many protected domains, you may want to create one protected domain, and then configure the others as associated domains. For details, see Domain Association on page 101.

If the FortiMail unit is operating in gateway mode, you must change the MX entries for the DNS records for your email domain, referring email to the FortiMail unit rather than to your email servers. If you create additional protected domains, you must modify the MX records for each additional email domain. Similarly, MX records must also refer to the FortiMail unit if it is operating in server mode.

To configure a protected domain

1. Go to *Domain & User > Domain > Domain*.
   The tab varies with the operation mode.

GUI item	Description
Delete (button)	Click *Delete* to remove the protected domain. **Caution:** This also deletes all associated email user accounts and preferences.
Domain FQDN	The fully qualified domain name (FQDN) of the protected domain. If the protected domain is a subdomain or domain association, click the + next to a domain entry to expand the list of subdomains and domain associations. To collapse the entry, click the -.
Relay Type (gateway mode only)	How the SMTP server will receive email from the FortiMail unit for the protected domain, either: • *Host* • *MX Record (this domain)* • *MX Record (alternative domain)* • *IP Group* • *LDAP Domain Mail Host*
SMTP server (gateway mode only)	The host name or IP address and port number of the mail exchanger (MX) for the protected domain.

GUI item	Description
	If Relay type is *MX Record (this domain)* or *MX Record (alternative domain)*, this information is determined dynamically by querying the MX record of the DNS server, and this field will be empty.
Recipient Verification (gateway mode only)	The SMTP server or LDAP server used for recipient address verification, if it is enabled.
Sub (gateway mode only)	The number of subdomains for each protected domain.
Association (gateway mode only)	The number of domain associations for the protected domain. See also Domain Association on page 101.
MTA Status (gateway mode only)	The status of the SMTP server for the protected domain.
Active User	The number of .active mailboxes. See Active mailbox user list on page 30.
Disk Usage (%) (gateway mode only)	The disk space used by quarantine reports in kilobytes (KB).

2. Either click *New* to create a new protected domain, or click a row to modify it.
   A dialog appears. Its options vary with the operation mode.
3. Configure the settings that apply to the operation mode and your choice for relay type:

GUI item	Description
Domain name	Enter the fully qualified domain name (FQDN) of the protected domain. For example, if you want to protect email addresses such as `user1@example.com`, you would enter the protected domain name `example.com`. Generally, your protected domain will use a valid, globally-resolvable top-level domain (TLD) such as `.com`. Exceptions could include testing scenarios, where you have created a `.lab` mail domain on your private network to prevent accidental conflicts with live mail systems legitimately using their globally-resolvable FQDN.
Is subdomain	Mark this check box to indicate the protected domain you are creating is a subdomain of an existing protected domain, then also configure Main domain. Subdomains, like their parent protected domains, can be selected when configuring policies specific to that subdomain. Unlike top-level protected domains, however, subdomains will appear as grouped under the parent protected domain when viewing the list of protected domains. This option is available only when another protected domain exists to select as the parent domain.

GUI item	Description
Main domain	Select the protected domain that is the parent of this subdomain. For example, lab.example.com might be a subdomain of example.com. This option is available only when Is subdomain is enabled.
Relay type (gateway mode only)	Select from one of the following methods of defining which SMTP server will receive email from the FortiMail unit that is destined for the protected domain: • *Host*: Configure the connection to one protected SMTP server or, if any, one fallback. Also configure SMTP server and Fallback SMTP server. • *MX Record (this domain)*: Query the DNS server's MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. • *MX Record (alternative domain):* Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. Also configure Alternative domain name. • *IP Group:* Configure the connection to rotate among one or **many** protected SMTP servers for load balancing. Also configure IP group. • *LDAP Domain Mail Host*: Query the LDAP server for the FQDN or IP address of the SMTP server. Also configure LDAP profile (see Configuring LDAP profiles on page 234). **Note:** If an MX option is used, you may also be required to configure the FortiMail unit to use a private DNS server whose MX and/or A records differ from that of a public DNS server. Requirements vary by the topology of your network and by the operating mode of the FortiMail unit.
	• In gateway mode, a private DNS server is required. On the **private** DNS server, configure the MX record with the FQDN of the SMTP server that you are protecting for this domain, causing the FortiMail unit to route email to the protected SMTP server. This is different from how a **public** DNS server should be configured for that domain name, where the MX record usually should contain the FQDN of the FortiMail unit itself, causing external SMTP servers to route email through the FortiMail unit. Additionally, if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall, on the **private** DNS server, configure the protected SMTP server's A record with its private IP address, while on the **public** DNS server, configure the FortiMail unit's A record with its public IP address. • In transparent mode, a private DNS server is required if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall. On the **private** DNS server, configure the protected SMTP server's A record with its private IP address. On the **public** DNS server, configure the protected SMTP server's A record with its public IP address. Do not modify the MX record. • For performance reasons, DNS lookups are skipped in gateway and server mode unless the sending domain is blank.
SMTP server (gateway mode only)	Enter the fully qualified domain name (FQDN) or IP address of the primary SMTP server for this protected domain, then also configure Port and Use SMTPS.

GUI item	Description
	If you have an internal mail relay that is located on a physically separate server from your internal mail server, this could be your internal mail relay, instead of your internal mail server. Consider your network topology, directionality of the mail flow, and the operation mode of the FortiMail unit. For more information, see Inbound versus outbound email on page 145 and Avoiding scanning email twice. This field appears only if Relay type is *Host*.
Fallback SMTP server (gateway mode only)	Enter the fully qualified domain name (FQDN) or IP address of the secondary SMTP server for this protected domain, then also configure Port and Use SMTPS. This SMTP server will be used if the primary SMTP server is unreachable. This field appears only if Relay type is *Host*.
IP group (gateway mode only)	Select the name of the IP group that is the range of IP addresses. Also configure Port and *Use SMTPS*. This field appears only if Relay type is *IP Group*.
LDAP profile (gateway mode only)	Select the name of the LDAP profile that has the FQDN or IP address of the SMTP server you want to query. Also configure Port and *Use SMTPS*. This field appears only if Relay type is *LDAP Domain Mail Host*.
Port	Enter the port number on which the SMTP server listens. If you enable Use SMTPS, Port automatically changes to the default port number for SMTPS, but can still be customized. This field appears only if Relay type is *Host*, *IP Group* or *LDAP Domain Mail Host*. See also Appendix: Port Numbers on page 375.
Alternative domain name (gateway mode only)	Enter the domain name to use when querying the DNS server for MX records. This option appears only if Relay type is *MX Record (alternative domain name)*.
LDAP User Profile (server mode only)	Select the name of an LDAP profile in which you have configured (see Configuring LDAP profiles on page 234), enabling you to authenticate email users and expand alias email addresses or replace one email address with another by using an LDAP query to retrieve alias members.
Use SMTPS	Enable to use SMTPS for connections originating from or destined for this protected server. This field appears only if Relay type is *Host*, *IP Group* or *LDAP Domain Mail Host*.
Relay Authentication	To test relay authentication, enable it and enter an email user name and password pair that exists on the mail server. Also specify the authentication type.
Test (button)	After you have entered the relay server information, you can click the *Test* button to test if the relay server is accessible. To further test mail delivery, click *Advanced Group*, and enter the SMTP `HELO`/`EHLO`, sender (`MAIL FROM:`), and recipient (`RCPT TO:`) information. Click *Test*. The test results will be displayed. **Note:** STARTTLS is not supported for relay host testing.

To configure domain groups

1. Purchase the feature license and enable the feature. See Domain group support on page 1.
2. Go to *Domain & User* > *Domain* > *Domain Group*.
3. Click *New*, or select a row and click *Edit* to edit an existing group.
4. Enter a *Group Name*.
5. Click the domains that you want to add to the domain group from the *Available* text area, and click the right-arrow to bring them to the *Members* text area.
6. Click *Create*.
7. Configure the following sections:
   - Configuring recipient address verification
   - Configuring protected domains
   - Configuring removal of invalid quarantine accounts
   - LDAP Option section
   - Advanced Setting section
   - Mail Migration Settings section

Configuring recipient address verification

This section does not apply to server mode.

Select a method of confirming that the recipient email address in the message envelope (`RCPT TO:`) corresponds to an email user account that actually exists on the protected email server. If the recipient address is invalid, the FortiMail unit will reject the email. This prevents quarantine email messages for non-existent accounts, thereby conserving quarantine hard disk space.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click New to create a new protected domain, or click an row to modify it.
   A dialog appears. Its options vary with the operation mode.
3. Expand the recipient address verification section.
4. Configure the following:

GUI item	Description
Disable	Do not verify that the recipient address is an email user account that actually exists.
SMTP Server	Query the SMTP server using either the SMTP `VRFY` command or `RCPT` command to verify that the recipient address is an email user account that actually exists. `RCPT` is the default command. If you want to query an SMTP server other than the one you have defined as the protected SMTP server, also enable Use alternative server, then enter the IP address or FQDN of the server in the field next to it. Also configure *Port* with the port number on which the SMTP server listens, and enable *Use SMTPS* if you want to use SMTPS for recipient address verification connections with the server. See also Appendix: Port Numbers on page 375.

GUI item	Description
	In case you want to use different sender email addresses in the SMTP envelope (`MAIL FROM:`) for different domains, set *Mail from address* to *Use domain setting* and specify the address to use. If you select *Use system setting* (the default setting), FortiMail will use an emtpy sender email address unless you specify a global one with the following CLI commands: `config mailsetting smtp-rcpt-verification` `set mail-from-addr <sender_email>` `end` **Note**: Microsoft 365 does not accept an empty MAIL FROM for SMTP recipient verification. You must specify an envelope from address if FortiMail is protecting Microsoft 365 domains. Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).
LDAP Server	Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. For more information on configuring LDAP profiles, see Configuring LDAP profiles on page 234. Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).
Imported User	Query an LDAP or Microsoft 365 server to verify that the imported users actually exist. For more information, see Managing imported users on page 118 Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).

Configuring removal of invalid quarantine accounts

This section does not apply to server mode.

Select a method by which to periodically remove quarantined spam for which an email user account does not actually exist on the protected email server.

If you select either SMTP or LDAP server, the FortiMail unit queries the server daily (at 4:00 AM daily unless configured for another time in the CLI; see the FortiMail CLI Reference) to verify the existence of email user accounts. If an email user account does not currently exist, the FortiMail unit removes all spam quarantined for that email user account.

In some instances, recipient verification is not always feasible via SMTP or LDAP. Select *Purge Inactive* to remove any inactive accounts.

If you have also enabled Recipient Address Verification (see Configuring recipient address verification on page 97), the FortiMail unit does not form quarantine accounts for email user accounts that do not exist on the protected email server. In that case, invalid quarantine accounts are never formed, and this option may not be necessary, except when you delete email user accounts on the protected email server. If this is the case, you can improve the performance of the FortiMail unit by disabling this option.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click *New* to create a new protected domain, or click an row to modify it.
   A multi-section dialog appears. Its options vary with the operation mode.
3. Expand the *Automatic Removal of Invalid Quarantine Accounts* section.
4. Configure the following:

GUI item	Description
Disable	Do not verify that the recipient address is an email user account that actually exists.
SMTP Server	Query the SMTP server to verify that the recipient address is an email user account that actually exists.
LDAP Server	Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. For more information on configuring LDAP profiles, see Configuring LDAP profiles on page 234.
Purge Inactive	Checks how many days an email user account has been inactive. If the account has been inactive for more than the designated *Retention period*, the account is purged.

LDAP Option section

Use this section to configure the LDAP service usages.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click *New* to create a new protected domain, or click an row to modify it.
   A multisection dialog appears. Its options vary with the operation mode.
3. Expand the *LDAP Option* section.
4. Configure the following:

GUI item	Description
User alias / address mapping profile (gateway mode only)	Select the name of an LDAP profile in which you have enabled and configured, enabling you to expand alias email addresses or replace one email address with another by using an LDAP query to retrieve alias members and/or address mappings. To use this option make sure that the email alias and/or address mappings do exist on the LDAP server. If the alias cannot be retrieved or LDAP server is not accessible, the email will be temp failed (451 error). For more information, see Configuring LDAP profiles on page 234.
Mail routing LDAP profile	Enable to perform mail routing, then click the arrow to expand the options and select the name of an LDAP profile in which you have enabled and configured. For more information, see Configuring LDAP profiles on page 234.
Scan override profile	Enable to query an LDAP server for an email user's preferences to enable or disable antispam, antivirus, and/or content processing for email messages destined for them, then select the name of an LDAP profile in which you have enabled and configured. For more information, see Configuring LDAP profiles on page 234.

Advanced Setting section

Go to *Domain & User* > *Domain* > *Domain* and expand the *Advanced Setting* section to configure the following domain settings:

- Quarantine Report Setting
- Domain Association
- DKIM and ARC Setting
- DMARC Report Setting
- Disclaimer
- Sender Address Rate Control
- Other

Quarantine Report Setting

The *Quarantine Report Setting* section that appears when configuring a protected domain lets you configure quarantine report settings. You can choose either to use the system-wide quarantine report settings or to configure domain-wide settings.

For information on system-wide quarantine report settings and quarantine reports in general, see Configuring global quarantine report settings on page 285 and Customizing custom messages, and email templates on page 71.

To configure per-domain quarantine report settings

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click New to create a protected domain or double-click a domain to modify it.
3. Expand the *Advanced Setting* section.
4. Click *Quarantine Report Setting*.
   A new dialog appears.
5. Configure the following:

GUI item		Description
Report destination		
	Original recipient	Enable to send the quarantine report to all recipients. For more information, see Managing the personal quarantines on page 43.
	Other recipient	Select to send the quarantine report to a recipient other than the individual recipients or group owner. For example, you might delegate quarantine reports by sending them to an administrator whose email address is not locally deliverable to the protected domain, such as `admin@lab.example.com`.
	LDAP group owner based on LDAP profile	Enable to send the quarantine report to a group owner, rather than individual recipients, then select the name of an LDAP profile in which you have enabled and configured the group query options (see Group Query on page 238.

GUI item	Description
	Also configure the following two options for more granular control: • Only when original recipient is group • When group owner is found, do not send to original recipient
Report schedule	Click the arrow to expand the options.
Schedule	Select the schedule to use when sending quarantine reports. • *System settings*: Use the system-wide quarantine report schedule. For more information, see Configuring global quarantine report settings on page 285. • *Domain settings*: Use a quarantine report schedule that is specific to this protected domain. Also configure These Hours and These Days.
These Hours	Select which hours to send the quarantine report for this protected domain. This option is available only when Schedule is *Use domain settings*.
These Days	Select which days to send the quarantine report for this protected domain. This option is available only when Schedule is *Use domain settings*.
Report template	Select an email template to use. If you choose to use the system settings, you can view the template but cannot edit from this page. But you can edit the system-wide template by going to *System* > *Customization* > *Custom Email Template*. If you choose to use the domain settings, you can click *Edit* to modify the template.

Replacement messages often include variables, such as the MIME type of the file that was overwritten by the replacement message.

Typically, you will customize text, but should not remove variables from the replacement message. Removing variables may result in an error message and reduced functionality. For example, removing `%%SPAM_DELETE_URL%%` would make users incapable of using the quarantine report to delete email individually from their personal quarantines.

6. Click *Create* or *OK*.

Domain Association

When configuring a protected domain, you can configure associated domains. An associated domain uses the settings of the protected domain or subdomain with which it is associated.

Domain associations can be useful for saving time when you have multiple domains, and you would otherwise need to configure multiple protected domains with identical settings.

For example, if you have one SMTP server handling email for ten domains, you could:

- Create ten separate protected domains and configure each with identical settings.
- Create one protected domain and list the nine other domains as domain associations.

The advantage of using the second method is that you do not have to repeatedly configure the same things when creating or modifying the protected domains. This saves time and reduces chances for error. Changes to one protected domain automatically apply to all of its associated domains.

The maximum number of domain associations that you can create is separate from the maximum number of protected domains.

Domain associations do not appear if FortiMail is operating in server mode.

To configure domain associations

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Click *New* to create a protected domain or double-click a domain to modify it.
3. Under *Advanced Setting*, click *Domain Association*.
4. If the relay type of this protected domain uses MX record (this domain) or MX record (alternative domain), for the MX record lookup option of the domain associations, you can choose to use the domain association's (self) MX record, or this protected domain's (parent) MX record.

   To create a domain association, click *New* and enter the fully qualified domain name (FQDN) of a mail domain that will use the same settings as the same protected domain. You can use wildcard, such as `*.example.com`.
5. Click *Create*.

   The name of the associated domain appears in the *Members* area.
6. Repeat the previous steps for all domains that you want to associate with this protected domain.
7. Click *Create* or *OK*.

DKIM and ARC Setting

To prove that an email's message headers and body content have not been tampered with during transit, you can sign outgoing email using DomainKeys Identified Mail (DKIM; RFC 4871) and/or Authenticated Received Chain (ARC; RFC 8617).

RFC 1918 private network addresses are not globally unique, cannot be resolved by public DNS on the Internet, and therefore their email cannot be signed by DKIM or ARC.

With DKIM, the sender's MTA (such as FortiMail) adds a `DKIM-signature:` message header which contains a:

- Checksum/hash (`bh=` value) of the original email's content and message headers. Proves integrity.
- Signature (`b=` value) of the hash by the MTA. Proves authenticity.

DKIM signatures (and its predecessor, DomainKeys) use a public-private key pair. Private keys are used by the sender's MTA to sign email. Public key are stored in each domain name's DNS `TXT` record. To validate an email's DKIM signature, the recipient's email server queries the public DNS server about the domain and gets the public keys.

To determine which private key to sign with, FortiMail looks at the domain name in the:

1. Sender email address in the message headers (`From:`), or, if none,
2. Sender email address in the SMTP envelope (`MAIL FROM:`).

For associated domains, there is no separate key pair; FortiMail instead reuses the parent domain's private key. Public DNS records therefore have the same public key too.

DKIM does not always work, however.

Sometimes email is not delivered directly to recipients' email servers. Mail relays and proxies **between** the sender and recipient ("hops") may have legitimate reasons to change the original email, such as:

- tagging the subject line
- adding disclaimers and unsubscribe links
- bundling multiple email together into mailing list digests
- sending from a different source IP address (forwarding service)

and this invalidates the original SPF and/or DKIM hash and signatures.

To solve this problem, ARC sealing extends the DKIM solution. The relay or proxy validates the original SPF and/or DKIM authentication results on behalf of the recipient, and then provides an alternative signature.

After processing email, the relay or proxy adds ARC headers:

- `ARC-Authentication-Results:` Result of the original SPF and/or DKIM signature verification, before processing invalidated them.
- `ARC-Message-Signature:` Similar to DKIM, a checksum/hash of the email's message headers and body, except for ARC headers.
- `ARC-Seal:` Signature of the results and hash by the relay or proxy (or, if there are multiple relays and proxies, a signing chain similar to a certificate signing chain). Used to validate the previous ARC headers.

Then recipients or other relays and proxies can query a public DNS server to validate the ARC signature, and may use those results instead of SPF or DKIM. (For example, on FortiMail, you can enable ARC override.)

To configure DKIM and/or ARC validation and signing

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Double-click to modify a protected domain.
   DKIM and ARC settings do not appear until after you save a new domain.
3. Expand the *Advanced Setting* section.
4. Click *DKIM and ARC Setting*.
5. Click *New*.
   In *New selector*, enter a unique name for the key pair, such as `example_com_v2`.
   In *Key*, select either:
   - *Auto Generation*: Generate a public-private key pair on the FortiMail unit.
   - *Manual Import*: Upload an existing public key and private key file in PEM format. If the private key file was encrypted with a password, you must enter it in *Password* so that FortiMail can decrypt and use it.

     Private key backups must be stored in a secure location, similar to passwords. Ideally the private key file should be encrypted while at rest. Unauthorized access could allow others to sign email with your key, compromising security.

   Click *OK*.
6. Click the new selector and then click *Download*.
   Alternatively, click the down arrow next to the*Download* button to select either *Multi-string format* or *Single-string format*.

7. On the domain name's authoritative public DNS server, put the public key in the TXT record. For details, see the documentation for your DNS server. For example:

   ```
   example_com._domainkey IN TXT "t=y; k=rsa;
         p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5xvUazqp2sBovpfumPuR5xC+yDvGbfndyHZuVQdSHhwdKAdsf
         iyOa03iPniCfQEbuM0d+4/AoPyTXHHPFBBnChMMHkWgHYlRDm5UMjrH5J1zDT5OyFxUEur+NtfS6LF29Te+6vSS+D3
         asfZ85V6WJDHSI9JV0504uwDeOOh/aewIDAQAB"
   ```

   Wait for the DNS records to propagate. Time required varies but is often less than 24 hours. Recipients cannot validate signatures until this occurs.

   Do not remove old public keys if recipients still need them to validate previously sent email.
8. On FortiMail, select the new key and then click *Activate*. (Only one key pair can be selected to sign with at a time.)

   In *DKIM signing option* and *ARC sealing option*, select either:

   - *Disable*:Do not sign.
   - *Incoming*:Sign email sent between users in the same protected domain.
   - *Outgoing*:Sign email sent from a protected domain to other external or protected domains. This includes email released from quarantine.
   - *All*: Sign both incoming and outgoing email.

   For example, if an IP-based policy matches both directions, but you only want to sign outgoing email, then select *Outgoing*.

   Click *OK*.
9. Click *OK*.
10. In the profile used by policies that match email that you want to DKIM or ARC sign, enable sender validation.

    Depending on the policy type, you may be able to use either:

    - **Antispam profile:** Enable SPF section, DKIM section, DMARC section, and/or ARC section. Use this method if you must validate existing ARC signatures from other relays or proxies before FortiMail adds its own signature to the signing chain.
    - **Session profile:** Enable SPF check and/or Enable DKIM check.

    When FortiMail validates SPF, DKIM, and/or ARC signatures, if the email direction matches *DKIM signing option* or *ARC sealing option*, then validation results are automatically signed.

DMARC Report Setting

You can configure DMARC report settings that are system-wide (see DMARC Report Generation on page 314), or specific to this protected domain.

To configure per-domain DMARC report and statistics

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click *New* to create a protected domain or double-click a domain to modify it.
3. Click to expand *Advanced Setting*.
4. Click *DMARC Report Setting*.
5. Configure the following:

GUI item	Description
Report Generation	

GUI item	Description
Status	Select whether or not to send DMARC reports, and which settings to use: • *Enable* — Collect DMARC check data. Each day, for each sender domain that matched a policy where DMARC checks are enabled, send a report to that domain's authorized DMARC report recipient. Also configure From address local part. **Note:** If a sender does not have a valid DMARC RUA/RUF configured in the domain's DNS `TXT` record, then even if you enable DMARC reports, FortiMail cannot send them to that domain because there is no report recipient email address. **Tip:** If you have the DMARC report analysis feature license, then you can instead use charts with statistics about DMARC reports.You can also generate DMARC reports on demand, and send them to other recipients. See Viewing DMARC report statistics on page 55, and the Status setting for analysis. • *Disable* — Do not collect DMARC check data. Do not generate a report. • *Monitor Only* — Collect DMARC check data, but do not generate a report. • *Use System Setting* — Use the system-wide setting.
From address local part	Enter the local part (username) that the FortiMail unit will use as its sender email address (`From:`) when it sends DMARC report email. Default is `noreply`. Change it if, for example, an administrator wants replies about DMARC reports. Also configure Status for report generation.
Report Analysis	
Status	Select whether or not to include data from this protected domain in charts with current DMARC statistics that FortiMail administrators can use when they log in (see Viewing DMARC report statistics on page 55), either: • *Enable* — Include data from this protected domain. • *Disable* — Do not include data from this protected domain. • *Use System Setting* — Use the system-wide setting.

Disclaimer

You can configure disclaimer messages that are system-wide (see Configuring global disclaimers on page 1), or specific to each protected domain.

A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential, or other information required by law, such as unsubscribe links or physical addresses. For disclaimers added to outgoing messages, you must configure an IP-based policy or an outgoing recipient-based policy.

Disclaimer messages can be appended for either or both incoming or outgoing email messages.

Disclaimer insertion may invalidate existing DKIM signatures, requiring an alternative ARC signature. See DKIM and ARC Setting on page 102.

To configure a per-domain disclaimer messages

1. Go to *System* > *Mail Setting* > *Disclaimer*.
2. Enable *Allow per-domain settings*.
3. If FortiMail is operating in transparent mode, also enable clients to send email using their specified SMTP server. For more information, see Use client-specified SMTP server to send email on page 1.
4. Go to *Domain & User* > *Domain* > *Domain*.
5. Either click *New* to create a protected domain or double-click a domain to modify it.
6. Expand the *Advanced Setting* section.
7. Click *Disclaimer*.
   A new dialog appears.
8. Configure the following:

GUI item	Description
Setting	Select which type of disclaimer message to append. • *Disable*: Do not append disclaimer messages. • *Use system setting*: Append the system-wide disclaimer message. • *Use domain setting*: Append the disclaimer messages configured specifically for this protected domain. For information about how to configure disclaimer messages, see Configuring global disclaimers on page 1. This option is only available only if you have enabled per-domain disclaimer messages. See Configuring global disclaimers on page 1.

Sender Address Rate Control

For users in each protected domain, you can rate control how much email each user can send.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click *New* to create a protected domain or double-click a domain to modify it.
3. Expand the *Advanced Setting* section.
4. Click *Sender Address Rate Control*.
   A new dialog appears.
5. Configure the following:

GUI item	Description
Status	Enable or disable the following rate limits.
Action	Select which action to apply when a user exceeds any of the following rate limits. For details about actions, see Action on page 161.
Exempt List	Click to define which SMTP clients are exceptions, and the rate limits in this protected domain do not apply to them.
Maximum number of messages per half hour	Enter the maximum number of emails per user in each 30 minute time interval.

GUI item	Description
Maximum number of recipients per half hour	Enter the maximum number of unique email recipient addresses per user in each 30 minute time interval.
Maximum data size per half hour (MB)	Enter the maximum size, in megabytes (MB), per user in each 30 minute time interval.
Maximum number of spam messages per half hour	Enter the maximum number of spam email per user in each 30 minute time interval. If the sender's email are often detected as spam, then it is probable that they are intentionally sending unwanted email (not by accident).
Send notification upon rate control violation	If the user directly connects to FortiMail to send email, then Action will indicate to the user that their email was not accepted. Otherwise (or if you want to provide a detailed explanation), configure this option to send an explanation email to the user. See Configuring notification profiles on page 274.

See also

Use client-specified SMTP server to send email

Allow per-domain settings

Incoming versus outgoing email

Configuring protected domains

Other

This section contains miscellaneous settings for the protected domain.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click New to create a new protected domain, or click an row to modify it.
   A multi-section dialog appears. Its options vary with the operation mode.
3. Expand the *Advanced Setting* section.
4. Click *Other*.
   A new dialog appears.
5. Configure the following:

GUI item	Description
Webmail theme	Either use the system setting or choose a color to overwrite the system setting.

GUI item	Description
Webmail language	Select either to use the default system language or a different language that the FortiMail unit will use to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same language as the GUI. For more information, see Customizing custom messages, and email templates on page 71.
Disk quota (GB)	Enter the disk quota in gigabytes (GB). If the maximum disk quota of this domain is exceeded, users of this domain will no longer receive any new email. If the disk quota reaches 90% threshold, a warning email is sent to the domain customer email. For instances where a resource profile disk quota is set to 0, the domain quota is enforced. Setting any value on resource profile higher than the domain quota value results in the domain quota value being imposed. Resource profile quota values are imposed instead when they are lower than the domain quota. **Note:** This option is only available in server mode.
Webmail single sign on	For webmail SSO, enable the service and select an SSO profile from the dropdown menu. For more information, see Configuring single sign-on (SSO) on page 80.
Maximum message size (KB)	Enter the limit in kilobytes (KB) of the message size. Email messages over the threshold size are rejected. **Note**: If the same email message is sent to recipients in multiple protected domains and the maximum message size limits in the domain settings are different, the smallest size setting will take effect and thus the email won't be delivered to any recipients. In this case, you can use the maximum message size setting in the content profile instead (under *Profile* > *Content* > *Content*). However, you can use the reject action only for separate SMTP sessions, not for one same session. **Note:** When you configure session profile settings under *Profile* > *Session* > *Session*, you can also set the message size limit. Here is how the two settings work together: • For outgoing email, only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. The smaller size will be used.
SMTP greeting (EHLO/HELO) Name (As Client)	Select how the FortiMail unit will identify itself during the `HELO` or `EHLO` greeting when delivering mail to the protected SMTP server as a client. • *Use this domain name*: The FortiMail unit will identify itself using the domain name for this protected domain. If the FortiMail unit will handle internal email messages (those for which both the sender and recipient addresses in the envelope contain the domain name of the protected domain), to use this option, you must also configure your protected SMTP server to use its host name for SMTP greetings. Failure to do this will result in dropped SMTP sessions, as both the FortiMail unit and the protected SMTP server will be using the same domain name when greeting each other. • *Use system host name*: The FortiMail unit will identify itself using its own host name. This is the default setting.

GUI item	Description
	• *Use other name*: Specify a greeting name if you want to use a customized host name. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.
Remove received header of outgoing email	Enable to remove the `Received:` message headers from email whose: • sender email address belongs to this protected domain • recipient email address is outgoing (that is, does not belong to this protected domain); if there are multiple recipients, only the first recipient's email address is used to determine whether an email is outgoing Alternatively, you can remove this header from any matching email using session profiles. See Received: on page 183.
Use global Bayesian database	Enable to use the global Bayesian database instead of the Bayesian database for this protected domain. If you do not need the Bayesian database to be specific to the protected domain, you may want to use the global Bayesian database instead in order to simplify database maintenance and training. Disable to use the per-domain Bayesian database. **Note:** Train the global or per-domain Bayesian database before using it. If you do not train it first, Bayesian scan results may be unreliable. For more information on Bayesian database types and how to train them, see Types of Bayesian databases on page 315 and Training the Bayesian databases on page 316.
Bypass bounce verification	Mark this check box to disable bounce verification for this protected domain. This option appears only if bounce verification is enabled. For more information, see Configuring bounce verification and tagging on page 308.

Service Settings section

If you are a managed security service provider (MSSP) which host multiple domains for multiple customers, for billing purpose, the super admin may want to limit usage of FortiMail resources by each protected domain. Domain administrators are not allowed to modify these settings.

These features are available only if FortiMail is operating in server mode.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click *New* to create a new protected domain, or click an row to modify it.
3. Expand the *Advanced Setting* section.
4. Click *Other*.
   A new dialog appears.
5. Expand the *Service Setting* section.
6. Configure the following:

GUI item	Description
Enable domain level service settings	Select to enable the domain-level server controls.
Email account limit	Specify the maximum number of email account are allowed on this domain.
Max user quota (MB)	Specify the maximum disk quota for each user.
Mail access	Specify the allowed mail access protocol for the users: POP3, IMAP, or Webmail.
Webmail service type	For webmail access, if you select *Limited Service*, the users will be only able to change their passwords and configure mail forwarding. All other features will not be available.

Customer Information section

In each protected domain, you can make notes about the associated customer account.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Either click New to create a new protected domain, or click an row to modify it.
   A multi-section dialog appears. Its options vary with the operation mode.
3. Expand the *Customer Information* section.
4. Configure the following:

GUI item	Description
Name	Enter the customer name.
Email	Enter the customer email address.
Account limit	Enter the user account limit.
Description	Optional. Enter a description or comment.

Mail Migration Settings section

If FortiMail is operating in server mode, and you enable the mail migration feature, this section will appear. For details, see Migrating email from other mail servers (server mode only) on page 141.

Managing users

The User menu enables you to configure email user-related settings, such as user preferences and PKI authentication. If the FortiMail unit is operating in server mode, the User menu also enables you to add email

user accounts.

Configuring local user accounts (server mode only)

When operating in server mode, the FortiMail unit is a standalone email server. The FortiMail unit receives email messages, scans for viruses and spam, and then delivers email to its email users' mailboxes. External MTAs connect to the FortiMail unit, which itself is also the protected email server.

When the FortiMail unit operates in server mode and the GUI operates in advanced mode, the User tab is available. It lets you configure email user accounts whose mailboxes are hosted on the FortiMail unit. Email users can then access their email hosted on the FortiMail unit using webmail, POP3 and/or IMAP. For information on webmail and other features used directly by email users, see Setup for email users on page 366.

To view email user accounts, go to *Domain & User* > *User* > *User*.

GUI item	Description
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of each mailbox, and empty or delete mailboxes as required. The SecureMail mailbox contains the secured email for the user. The Bulk mailbox contains spam quarantined by the FortiMail unit. Click Back to return to the Users tab.
Export .CSV (button)	Click to download a backup of the email users list in comma-separated value (CSV) file format. The user passwords are encoded for security. **Caution:** Most of the email user accounts data, such as mailboxes and preferences, is not included in the .csv file. For information on performing a complete backup, see Backup and restore.
Import .CSV (button)	In the field to the right of Import .CSV, enter the location of a CSV-formatted email user backup file, then click Import .CSV to upload the file to your FortiMail unit. The import feature provides a simple way to add a list of new users in one operation. See Importing a list of users on page 113. Before importing a user list or adding an email user, you must first configure one or more protected domains to which the email users will belong. For more information, see Configuring protected domains on page 92. You may also want to back up the existing email user accounts. For details, see Backup and restore.
Password (button)	Select a user and click this button to change a user's password. A dialog appears. Choose whether to change the user password or to switch to LDAP authentication. You can create a new LDAP profile or edit an existing one. For details, see Configuring LDAP profiles on page 234.
Domain	Select the protected domain to display its email users, or to select the protected domain to which you want to add an email user account before clicking New. You can see only the domains that are permitted by your administrator profile.
Search user	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users displays again with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.

GUI item	Description
User Name	Displays the user name of an email user, such as `user1`. This is also the local portion of the email user's primary email address.
Type	Displays the type of user: local, LDAP, or RADIUS.
Display Name	Displays the display name of an email user, such as `"J Smith".` This name appears in the `From:` field in the message headers of email messages sent from this email user.
Disk Usage (KB)	Displays the disk space used by mailboxes for the email user in kilobytes (KB).

Configuring users in server mode

You can create users one at a time or import a list of users. Before importing a user list or adding an email user, you must first configure one or more protected domains to which the email users will belong. For more information, see Configuring protected domains on page 92.

To configure an email user account

1. Go to *Domain & User* > *User* > *User*.
2. From *Domain*, select the name of the protected domain to which you want to add an email user. You can also set the domain on the user dialog.
3. Either click *New* to add an email user or double-click an email user to modify it.
   A dialog appears.
4. In *User name*, enter the name of the account in the selected domain whose email will be locally deliverable on the FortiMail unit.
   For example, an email user may have numerous aliases, mail routing, and other email addresses on other systems in your network, such as `accounting@example.com`. However, the user name you enter in the *New User* dialog reflects the email user's account that they will use to log in to this FortiMail unit at the selected domain; such as, `jsmith` if the email address is `jsmith@example.com`.
5. You can change the user's domain if it necessary. In the dropdown menu to the right of the `@` symbol, select the name of the protected domain to which the email user belongs.
6. For *Authentication type*, select one of the following:
   - select *Local* and then enter the password for this email account
   - select *LDAP* and select the name of an existing LDAP profile in the dropdown list
   - select *RADIUS* and select the name of an existing RADIUS profile in the dropdown list.

   If no profile exists, click *New* to create one.
   If a profile exists but needs modification, select it and click *Edit*.

   The LDAP option requires that you first create an LDAP profile in which you have enabled and configured user authentication options. See User Authentication on page 240.
7. In *Display Name*, enter the name of the user as it should appear in the `From:` field in the message header. For example, an email user whose email address is `user1@example.com` may prefer that their *Display Name* be `"J Zang"`.
8. Click *OK*.

For a new user, the FortiMail unit creates the account. Authentication is not yet enabled and a policy may not exist that allows the account to send and receive email.

Complete the next two steps as applicable.

9. To enable the user account, create a recipient-based policy that both matches its email address and uses a resource profile in which User account status on page 229 is enabled. For details, see Workflow to enable and configure authentication of email users on page 230 and Configuring resource profiles on page 228.
10. To allow the user account to send and receive email, configure an access control rule and either an IP-based policy or an incoming recipient-based policy. For details, see Configuring policies on page 144.

If you rename an existing user account to a new user account name using the CLI command, all the user's preferences and mail data will be ported to the new user. However, due to the account name change, the new user will not be able to decrypt and read the encrypted email that is sent to the old user name before.

Importing a list of users

The import feature provides a simple way to add a list of new local users in one operation. You can create a CSV file in any spreadsheet and import the data as long as the columns match the FortiMail format.

To create and import user records

1. Go to *Domain & User* > *User* > *User*.
2. Create at least one local (not LDAP) user.
3. Select that user and click Export .CSV.
4. Save the file on your local computer.
5. Open the CSV file in a spreadsheet editor, such as Microsoft Excel.
6. Enter user records in the pre-existing columns so the new users exactly match the exported format (delete the original exported user record).

Sample CSV format:

	A	B	C
1	User name	Password	Display
2	user12@example.com	user12	user12
3	user13@example.com	user13	user13

7. Use the Save As feature to save the file in plain CSV format.
8. On the User tab, click Import.
   A dialog appears.
9. Click Browse to locate the CSV file to import and click Open.
10. Click OK.
    A field appears showing the percentage of import completion.
    A dialog appears showing the number of imported records.

The import feature does not overwrite existing records.

To change the password of multiple email user accounts

This procedure sets the same password for one or more email user accounts, which can result in reduced security of the email users' accounts. To reduce risk, set a strong password and notify each email user whose password has been reset to configure a unique, strong password as soon as possible.

1. Go to *Domain & User* > *User* > *User*.
2. From Domain, select the name of the protected domain in which you want to change email user account passwords.
3. To change the passwords of **all** email user accounts for the protected domain, mark the check box located in the check box column heading.
   To change the passwords of **individual** email user accounts, in the check box column, mark the check boxes of each email user account whose password you want to change.
4. Click Password.
5. Select either:
   - Password, then enter the password for this email account, or
   - LDAP, then select the name of an LDAP profile in which you have enabled and configured the User Auth Options query, which enables the FortiMail unit to query the LDAP server to authenticate the email user.

   You can create LDAP profiles using the advanced mode of the GUI. For more information, see Configuring LDAP profiles on page 234.
6. Click OK.

See also

Managing the disk usage of email users mailboxes

Configuring user preferences

Configuring user aliases

Configuring address mappings

Managing users

Configuring LDAP profiles

Managing the disk usage of email users mailboxes

If your email users often send or receive large attachments, email users' mailboxes may rapidly consume the hard disk space of the FortiMail unit. You can manage the disk usage of email users' mailboxes by monitoring the size of the folders, and optionally deleting their contents.

For example, if each email user has a mailbox folder named "Spam" that receives tagged spam, you might want to periodically empty the contents of these folders to reclaim hard disk space.

Alternatively, you can assign email users' disk space quota in their resource profile. For details, see Configuring resource profiles on page 228.

To empty a mailbox folder

1. Go to *Domain & User > User > User*.
2. Select the check box for the user.
3. Click Maintenance.
   A list of mailbox folder names with their hard disk usages appears.
4. Select the mailbox folder that you want to empty, such as Trash, then click Empty.
   A confirmation dialog appears.
5. Click OK.

See also

Configuring local user accounts (server mode only)

Configuring resource profiles

Configuring user preferences

The User Preferences tab lets you configure preferences for each email user, such as per-user safe lists and preferred webmail quarantine language.

Preferences apply to email user accounts in all operation modes but vary slightly in implementation. For example:

- Out-of-office status messages and mail forwarding can only be configured when the FortiMail unit is operating in server mode.
- In server mode, user accounts are stored on the FortiMail unit.
- With gateway or transparent mode, user accounts are stored hosted on your protected SMTP server.

Although you may have created a local user account, the user's preferences may not be created. You can either wait for an event that requires it to be automatically initialized using the default values, or you can manually create and modify it.

Administrators can modify preferences for each email user through the GUI. Email users can modify their own preferences by logging in to the FortiMail webmail or email quarantine.

To view and manage existing user preferences

1. Go to *Domain & User > User > User Preference*.

GUI item	Description
Delete User Data (button)	Select the user and then click this button to delete the user preference settings and mail data.
Maintenance (button)	Click to reveal a dropdown menu with preference management options. • *Clear Safe List*

GUI item	Description
	• *Clear Block List* • *Enable Safelisting Outgoing Recipient* • *Disable Safelisting Outgoing Recipient* • *Enable Adding Recipient of Sent Email to Personal Address Book* • *Disable Adding Recipient of Sent Email to Personal Address Book* • *Global Edit (user preferences of) Selected User(s)/All Domain Users* • *Reset* (resets preferences to their defaults)
Domain	Select the protected domain to display its email users, or to select the protected domain to which you want to add an email user account before clicking New. You can see only the domains that are permitted by your administrator profile.
Search user	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users redisplays with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
User Name	Displays the user name of an email user, such as `user1`.
Display name (server mode only)	Displays the display name of the email user.
Language	Displays the language in which this email user prefers to display their quarantine and, if the FortiMail unit is operating in server mode, webmail. By default, this language preference is the same as the system-wide default webmail language preference. For more information, see Customizing custom messages, and email templates on page 71.
Safe List	The icon in this column indicates whether or not a personal safe list currently exists for this email user. Hover the mouse pointer over the list icon to determine its status: • New: A personal safe list does not exist for this email user. • Edit: A personal safe list exists for this email user. Click the icon to open a dialog where you can configure, back up, or restore the personal safe list. Safe lists include sender IP addresses, domain names, and email addresses that the email user wants to permit. **Note:** System-level lists take precedence over domain-level lists while domain-level lists take precedence over personal-level lists. For more information on safe lists and block lists, see Managing the personal block lists and safe lists on page 298.
Block List	The icon in this column indicates whether or not a personal block list currently exists for this email user. Hover the mouse pointer over the list icon to determine its status: • New: A personal block list does not exist for this email user. • Edit: A personal block list exists for this email user. Click the icon to open a dialog where you can configure, back up, or restore the personal block list. Block lists include sender IP addresses, domain names, and email addresses that the email user wants to block **Note:** System-level lists take precedence over domain-level lists while domain-level lists take precedence over personal-level lists.

GUI item	Description
	For more information on safe lists and block lists, see Managing the personal block lists and safe lists on page 298.
Secondary Accounts	The icon in this column indicates whether or not this email user will also handle quarantined email messages for other email addresses. Hover the mouse pointer over the list icon to determine its status: • New: A secondary access list does not exist for this email user. • Edit: A secondary access list exists for this email user. A list of email accounts in sub-domains that are linked to a user on the parent domain. For example, if user1@example.com can have that email address linked to the following secondary accounts: user1@one.example.com, and user1@two.example.com. Select the New or Edit icon to add accounts to the secondary accounts for this user. Note that any accounts must first be created before they can be added to this list. Click the icon to open a dialog where you can add or remove secondary accounts. The addresses must exist in one of the existing FortiMail domains to be added.
Outgoing Recipient Safelisting (icon)	The icon indicates whether or not the FortiMail unit will automatically add recipient addresses in outgoing email sent by this email user to their per-user safe list, if it is allowed in the antispam profile. • A green check mark icon indicates automatic per-user safelisting is enabled. • A red X icon indicates automatic per-user safelisting is disabled. Email users can change this setting in their webmail preferences. For more information, log in to the FortiMail webmail, then click Help. This setting can be initialized manually or automatically. FortiMail administrators can manually create and configure this setting when configuring email user preferences. If the setting has not yet been created when either: • an email user logs in to FortiMail webmail • an email user sends outgoing email through the FortiMail unit • a FortiMail administrator configures the email user's personal block or safe list (see Managing the personal block lists and safe lists on page 298) then the FortiMail unit will automatically initialize this setting as disabled.
Preference	The green check mark indicates that the user preference has been configured and the settings will be used. The red check mark indicates that the user preference has not be configured and the default settings will be used.
Disk Usage	Displays how much disk space each user mailbox is using.

2. Either click New or double-click the user's preferences to modify them.
   A dialog appears that varies depending on the operation mode.
3. Configure the user preferences as required.

See also

Configuring local user accounts (server mode only)

Configuring user preferences

Configuring user aliases

Configuring address mappings

Managing imported users

Go to *Domain & User > User > Imported User* to manually create users and/or groups, and to import and export users and/or groups via .CSV file.

Currently, you can periodically synchronize users from an LDAP server (such as Azure AD) or Microsoft 365 cloud server in order to verify mailbox count information. This feature is particularly beneficial for automatically maintaining up-to-date remote server information, as remote user/group records change over time.

All user email addresses (primary and secondary if applicable) can be synchronized, including distribution lists and alias addresses. Profiles are created and assigned to remote users/groups to configure synchronization schedules.

Note: If the delivered email address is a secondary address of the synced account, it will not be counted as a new mailbox.

Note: This advanced management feature is only available when *User management* is enabled. See Configuring advanced management features (license required) on page 1.

To view and manage imported users

Go to *Domain & User > User > Imported User*.

GUI item	Description
Import (button)	Select to import users/groups by uploading a .CSV file.
Export (button)	Select to export the selected imported users/groups to .CSV format, allowing you to review the information elsewhere.
Type	Select whether the view individual imported users or groups.
Domain	Select the protected domain to display its imported email users/groups, or to select the protected domain to which you want to add an email user/group before clicking New. You can see only the domains that are permitted by your administrator profile.
Status	A green check mark icon indicates that the imported user/group is enabled.
Display Name	Display name of the imported email user/group. This name appears in the `From:` field in the message headers of email messages sent from this email.
Email	Displays the email address of the imported email user/group.
Type	Displays the entity type: *User* or *Group*.
Profile	Displays the user import profile the recipient belongs to. See Configuring user import profiles on page 118 for more information.

Configuring user import profiles

You can map remote users/groups to maintain a synchronization schedule with LDAP or Microsoft 365 servers.

To configure user import profiles

1. Purchase the feature license and enable the feature. See User management on page 1.
2. Go to *Domain & User* > *User* > *User Import Profile*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone*. Enter a name and apply a domain for the new profile, and click *OK*.
Sync Now (button)	Click to prompt a synchronization between the FortiMail unit and the LDAP and/or Microsoft 365 servers to retrieve up-to-date user data.
Domain	Select the protected domain to display its user import profiles, or to select the protected domain to which you want to add a user import profile before clicking New. You can see only the domains that are permitted by your administrator profile.
Name	Displays the user import profile name.
Domain	Displays the protected domain the user import profile is assigned to.
Type	Displays whether the user import profile is for LDAP or Microsoft 365.
Description	Displays the description of the user import profile.
Schedule	Displays at what time intervals the user import profile conducts user import synchronizations.
Sync Status	Displays the current synchronization status.
Last Sync	Displays the last time a successful user import synchronization occurred.

3. Click *New* to add a profile or double-click a profile to modify it.
4. Configure the following general settings:

GUI item	Description
Profile name	For a new profile, enter its name.
Domain	Select the name of a protected domain to apply to the user import profile. You can see only the domains that are permitted by your administrator profile.
Search timeout	Define the synchronization query timeout period in seconds. Set the value between 60-600.
Type	Define the remote server type, either *LDAP* or *Microsoft 365*.
Tenant ID	Enter the Microsoft 365 tenant ID.
Application ID	Enter the Microsoft 365 application ID.
Application secret	Enter the Microsoft 365 application secret.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.
Port	Enter the port number where the LDAP server listens. The default port number varies by Secure LDAP connection.

GUI item	Description
	See also Appendix: Port Numbers on page 375.
Secure LDAP connection	Enable to connect to the LDAP servers using an encrypted connection.
Protocol version	Select the LDAP server protocol version.
Scope	Define the search scope of the LDAP server, either *Base*, *One Level*, or *Subtree*.
Description	Optionally enter a description for the profile.
Default Bind Option	Click to expand and configure the following: • *Base DN*: Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for user objects, such as `ou=People,dc=example,dc=com`. User objects should be child nodes of this location. • *Bind DN*: Enter the bind DN, such as `cn=fortimail,dc=example,dc=com`, of an LDAP user account with permissions to query the Base DN. • *Bind password*: Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in Base DN, or, if you have not yet entered a *Base DN*, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your *Base DN*, or need to look up attribute names. For example, if the *Base DN* is unknown, browsing can help you to locate it. Before using, first configure *Server name/IP*, *Secure LDAP connection*, *Bind DN*, *Bind password*, and *Protocol version*, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.
User Query Option	Click to expand and configure the following: • *User query*: Enter the LDAP query string to get all users.For example, *(mail=*)* if using OpenLDAP. • *Display name attribute*: Enter the LDAP display name attribute, such *CN*. • *Primary address attribute*: Enter the LDAP user's primary email address attribute, such as *mail*. • *Secondary address attribute*: Enter the LDAP user's secondary email address attribute.
Group Query Option	Click to expand and configure the following: • *Group query*: Enter the LDAP query string to get all groups. • *Display name attribute*: Enter the LDAP group/mailinglist display name attribute. • *Primary address attribute*: Enter the LDAP group's primary email address attribute. • *Secondary address attribute*: Enter the LDAP group's secondary email address attribute.

GUI item	Description
Schedule	Click to expand and configure the following: • *Schedule*: Define a synchronization schedule of either Daily, Weekly, or Monthly (or none). If setting a weekly or monthly schedule, set the days of the week or days of the month that you wish to schedule synchronizations to occur. • *At hour*: Define the hour of the day at which synchronization will occur.

Configuring user aliases

The User Alias tab lets you configure email address aliases for protected domains.

Aliases sometimes act as distribution lists; that is, they translate one email address into the email addresses of several recipients, called members. An alias can also be a literal alias; that is, it is an alternative email address that resolves to the real email address of a single email user.

For example, groupa@example.com might be an alias that the FortiMail unit will expand to user1@example.com and user2@example.com, having the effect of distributing an email message to all email addresses that are members of that alias, while john.smith@example.com might be an alias that the FortiMail unit translates to j.smith@example.com. In both cases, the FortiMail unit converts the alias in the recipient fields of incoming email messages into the member email addresses of the alias, each of which are the email address of an email user that is locally deliverable on the SMTP server or FortiMail unit.

Members of an alias can include the email address of the alias itself.

Aliases can contain both or either local and non-local email addresses as members of the alias. For example, if the local protected domain is mail.example.com, you could create an email address alias whose members are:

- user1@mail.example.com, which is locally deliverable to the protected domain
- user1@external.example.net, which is **not** locally deliverable to the protected domain

Alternatively to configuring aliases locally, you can configure the FortiMail unit to query an LDAP directory. For details, see Configuring LDAP profiles on page 234.

Unlike address maps, aliases can be one-to-many relationships between the alias and its members, but cannot be bidirectional — that is, recipient email addresses that are aliases are translated into their member email addresses, but sender email addresses that are members are **not** translated into aliases.

To view and configure alias addresses

1. Go to *Domain & User* > *User Alias* > *User Alias*.

GUI item	Description
Domain	Select the name of a protected domain to view email address aliases for that protected domain. You can see only the domains that are permitted by your administrator profile.
Alias Name	Displays the email address of the alias, such as `teama@example.com`.
Members	Displays the email addresses to which the alias will translate, which may be the email addresses of one or more local or non-local email users. Multiple email addresses are comma-delimited.
Count	Displays the number of members.

2. Either click *New* to add an alias or double-click an alias to modify it.
3. A dialog appears. Its features vary with the operation mode.
4. For a new alias in all operation modes, enter the local-part (the part before the `@` symbol) of the email address alias in *Alias name*.
5. If the FortiMail unit is operating in gateway or transparent mode, do the following:
   - Select the name of its protected domain from the dropdown list next to *Alias name*.
   - For example, for the alias `group1@example.com`, you would enter `group1` and select `example.com`.
   - To add members to the alias, in the field to the left of the right arrow button, enter the email address, then click the right arrow button. The email address appears in the *Members* area.
   - To remove members from the alias, in the *Members* area, select one or more email addresses, then click *Remove Selected*.
6. If the FortiMail unit is operating in server mode, do the following:
   - Select a protected domain in *Select an internal domain*.
   - The email addresses of users from the selected domain (that is, local users) appear in the *Available user* area.
   - To add **local** email addresses as members to the alias, select one or more email addresses in the Available users area, then click ->. The email addresses are moved to the *Member* area.
   - To add **non-local** email addresses as members to the alias, enter the email address in the *External Email address* field, then click -> next to the field. The email address appears in the *Member* area.
   - To remove members from the alias, select one or more email addresses in the *Members* area, then click the <- arrow. The email addresses are removed from the *Members* area. Local email addresses return to the *Available user* area.
7. Click *Create* or *OK*.

See also

Configuring address mappings

User Alias

Mail Routing

Configuring address mappings

Address mappings are bidirectional, one-to-one or many-to-many mappings. They can be useful when:

- you want to hide a protected domain's true email addresses from recipients
- a mail domain's domain name is not globally DNS-resolvable, and you want to replace the domain name with one that is
- you want to rewrite email addresses

Like aliases, address mappings translate email addresses.

Unlike aliases:

- Mappings cannot translate one email address into many.
- Mappings cannot translate an email address into one that belongs to an unprotected domain (this restriction applies to locally defined address mappings only; it is not enforced for mappings defined on an LDAP server).
- Mappings are applied bidirectionally, when an email is outgoing as well as when it is incoming to the protected domain.
- Mappings may affect both sender and recipient email addresses, and may affect those email addresses in both the message envelope and the message header, depending on the match condition.

The following table illustrates the sequence in which parts of each email are compared with address mappings for a match, and which locations' email addresses are translated if a match is found.

Both `RCPT TO:` and `MAIL FROM:` email addresses are always evaluated for a match with an address mapping. If both `RCPT TO:` and `MAIL FROM:` contain email addresses that match the mapping, both mapping translations will be performed.

Match evaluation and rewrite behavior for email address mappings

Order of evaluation	Match condition	If yes...	Rewrite to...
1	Does `RCPT TO:` match an **external** email address?	Replace `RCPT TO:`.	Internal email address
2	Does `MAIL FROM:` match an **internal** email address?	For each of the following, if it matches an internal email address, replace it: • `MAIL FROM:` • `RCPT TO:` • `From:` • `To:` • `Return-Path:` • `Cc:` • `Reply-To:` • `Return-Receipt-To:` • `Resent-From:`	External email address

Order of evaluation	Match condition	If yes...	Rewrite to...
		• `Resent-Sender:` • `Delivery-Receipt-To:` • `Disposition-Notification-To:`	

For example, you could create an address mapping between the internal email address `user1@marketing.example.net` and the external email address `sales@example.com`. The following effects would be observable on the simplest case of an outgoing email and an incoming reply:

- For email from `user1@marketing.example.net` to other users, `user1@marketing.example.net` in both the message envelope (`MAIL FROM:`) and many message headers (`From:`, `Cc:`, etc.) would then be replaced by `sales@example.com`. Recipients would only be aware of the email address `sales@example.com`.
- For email to `sales@example.com` from others, the recipient address in the message envelope (`RCPT TO:`), but **not** the message header (`To:`), would be replaced with `user1@marketing.example.net`. The recipient `user1@marketing.example.net` would be aware that the sender had originally sent the email to the mapped address, `sales@example.com`.

You can alternatively create address mappings by configuring the FortiMail unit to query an LDAP server that contains address mappings. For more information, see Configuring LDAP profiles on page 234.

To view and configure an address map list

1. Go to *Domain & User* > *Address Map* > *Address Map*.

GUI item	Description
Domain	Select the name of a protected domain to view address maps whose internal email address belongs to that protected domain. You can see only the domains that are permitted by your administrator profile.
Internal Email Address	Displays either an email address, such as `user1@admissions.example.edu`, or an email address pattern, such as `*@example.com`, that exists in a protected domain.
External Email Address	Displays either an email address, such as `admissions@example.edu`, or an email address pattern, such as `*@example.net`, that exists in a protected domain.

2. Either click *New* to add an address mapping or double-click a mapping to modify it.
A dialog appears.
3. Configure the following:

GUI item	Description
Internal email address	Enter either an email address, such as `user1@example.com`, or an email address pattern, such as `*@example.com`, that exists in a protected domain. This email address is hidden when passing to the external network by being rewritten into the external email address according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 123.
External email address	Enter either an email address, such as `sales@example.com`, or an email address pattern, such as `*@example.net`, that exists in a protected domain.

GUI item	Description
	This email address is visible to the internal network, but will be rewritten into the internal email address according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 123. The external email address must **not** be within the same protected domain as the internal address. Otherwise, it may cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable.

Note: If you use wildcards (* or ?) in the name, you must enter a pattern using the same wild card in the external email address. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the external address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, * mapped to ? or the opposite), then this substitution will fail.

See also

Configuring user aliases

Address Mapping

Mail Routing

Configuring IBE users

You can send secured email with Identity Based Encryption (IBE) through the FortiMail unit. The IBE User option lets you manage the IBE mail users and IBE domains. For details about how to use IBE service, see FortiMail IBE configuration workflow on page 325.

Configuring active users

The Active User tab lets you enable, delete, maintain, and reset the following secured mail recipients:

- recipients who have received secured mail notifications from the FortiMail unit
- recipients who have registered or authenticated on the FortiMail unit

To view and manage active users, go to *Domain & User > IBE User > Active User*..

GUI item	Description
Delete (button)	Select to remove a selected user in the list. A deleted user cannot access the FortiMail unit.
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of a mailbox and empty a mailbox as required.

GUI item	Description
	The SecureMail mailbox contains the secured email for the user. The encrypted email are put into this mailbox if Pull is selected to retrieve IBE mail. The Bulk mailbox contains spam that are quarantined by the FortiMail unit.
Reset User (button)	Click to reset a mail user and require new login information to access the FortiMail unit. Resetting a user sends the user a new notification and the user needs to re-register on the FortiMail unit.
IBE domain	Select the name of an IBE domain to view its active users. For more information about IBE domain, see Configuring IBE authentication on page 128.
Search	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users refreshes with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
Enabled	Select the check box to activate a mail user. A disabled user cannot access the FortiMail unit.
Email	Displays the email address of mail users.
First Name, Last Name	Displays the first and last name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Recovery Email	Displays the recovery email address of the mail users.
Status	The mail user has four status possibilities: • *Pre-registered*: The FortiMail unit encrypts an email and sends a notification to the recipient. • *Activated*: The mail recipient registers on the FortiMail unit. • *Password reset*: When a mail recipient who is provided with new password to access the FortiMail unit has actually changed the password, this status appears. • *LDAP*: When a mail recipient. who belongs to an IBE domain bound with an LDAP profile authenticates on the FortiMail unit, this status appears. For more information about IBE domain, see Configuring IBE authentication on page 128.
Creation Time	Displays when IBE user was registered and created.
Last Access	Displays the time stamp when: • the FortiMail unit sends a notification (*Pre-registered* status) • the mail recipient registers on the FortiMail unit (*Activated* status) • a mail user changes the password (*Password reset* status) • a mail recipient, who belongs to an IBE domain, authenticates on the FortiMail unit (*LDAP* status)

Configuring expired users

Depending on the configuration of User registration expiry time and User inactivity expiry time in the IBE service, if email recipients fail to register or authenticate on the FortiMail unit, or fail to access the FortiMail unit after registration for a certain period of time, they become expired users. For more information about IBE service configuration, see Configuring IBE encryption on page 324.

The *Expired User* tab displays the same information as the Active User tab except that the users in this list have expired. These users need to re-register on the FortiMail unit when a new notification arrives to become active.

GUI item	Description
Delete (button)	Select to remove a selected user in the list. A deleted user cannot access the FortiMail unit.
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of a mailbox and empty a mailbox as required. The *SecureMail* mailbox contains the secured email for the user. The encrypted email are put into this mailbox if *Pull* is selected to retrieve IBE mail. The *Bulk* mailbox contains spam that are quarantined by the FortiMail unit.
Re-activate	Select the expired IBE user record(s) you wish to re-activate and select *Re-activate*. Any re-activated IBE users will move to the *Active User* tab.
Export	Select from the dropdown menu if you wish to *Export All* or *Export Selected* expired IBE users in comma-separated value (CSV) file format. **Note:** *Export All* will export all records on the current page. If you wish to export a larger number of records, set *Records per page* to a higher value (maximum of 500).
Records per page	Define the maximum number of expired IBE user records appear on the current page.
IBE domain	Select the name of an IBE domain to view its active users. For more information about IBE domain, see Configuring IBE authentication on page 128.
Search	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users redisplays with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
Email	Displays the email address of mail users.
First Name, Last Name	Displays the first name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Last Name	Displays the last name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Status	The mail user has four status possibilities: • *Pre-registered*: The FortiMail unit encrypts an email and sends a notification to the recipient. • *Activated*: The mail recipient registers on the FortiMail unit. • *Password reset*: When a mail recipient who is provided with new password to access the FortiMail unit has actually changed the password, this status appears. • *LDAP*: When a mail recipient. who belongs to an IBE domain bound with an LDAP profile authenticates on the FortiMail unit, this status appears. For more information about IBE domain, see Configuring IBE authentication on page 128.
Expiry Time	Displays when the user's registration expired.
Last Access	Displays the time stamp when the user was last active.

Configuring IBE authentication

When mail recipients of the IBE domains access the FortiMail unit after receiving a secure mail notification:

- recipients of the IBE domains without LDAP authentication profiles need to register to view the email
- recipients of the IBE domains with LDAP authentication profiles just need to authenticate because the FortiMail unit can query the LDAP servers for authentication information based on the LDAP profile

In both cases, the FortiMail unit will record the domain names of the recipients who register or authenticate on it under the *IBE Domain* tab. For details, see Viewing and managing IBE domains on page 129.

Go to *Domain & User > IBE User > IBE Authentication* to bind domains with LDAP authentication profiles with which the FortiMail unit can query the LDAP servers for authentication, email address mappings, and more. For more information about LDAP profiles, see Configuring LDAP profiles on page 234.

To configure IBE authentication rules

1. Go to *Domain & User > IBE User > IBE Authentication*.
2. Click *New* and configure the following:

GUI item	Description
Status	Select to enable this rule.
Domain pattern	Enter a domain name that you want to bind to an LDAP authentication profile. If you want all IBE users to authenticate through an LDAP profile and do not want other users to be registered, you can use a wildcard * for the domain name and then bind it to an LDAP profile. For more information about LDAP profiles, see Configuring LDAP profiles on page 234.
LDAP profile	Select the LDAP profile you want to use to authenticate the domain users.

User registration process with two-factor authentication

Two-factor authentication, via email and/or SMS text message, can be used with IBE.

See Configuring IBE services on page 326 for more information on configuring two-factor authentication settings.

The user verification process for receiving and reading a secure message varies depending on which method is chosen.

IBE user registration and check email process via email:

1. When a secure message is sent to a user, the user receives a notification directing them to their inbox.
2. The user opens the registration email and clicks the registration link.
3. The user registers, providing their *Language*, *Time zone*, *First name*, and *Last name*.
4. When the user clicks *Next*, they must confirm their *Verification email* address, then click *OK*.
5. The user then receives a one-time password or token via email.
6. Upon entering the token correctly, the user receives a successful registration notification email.

   Now that registration is complete, the user may only open the secure message once they have requested a token.

7. The user clicks the secure message link and then clicks *Request Token*. The token is sent via email to the user.
8. The user enters the token and clicks *Verify Token*.
9. After the token is verified, the user is granted access to the secure message.

IBE user registration and check email process via SMS:

1. When a secure message is sent to a user, the user receives a notification. The user clicks *Register*.
   A registration email is sent to the user.
2. The user opens the registration email and clicks the registration link.
3. The user registers, providing their *Language*, *Time zone*, *First name*, and *Last name*.
4. When the user clicks *Next*, they must confirm their *Verification phone number*, then click *OK*.
5. The user then receives a one-time password or token via SMS.
6. Upon entering the token correctly, the user receives a successful registration notification email.
   Now that registration is complete, the user may only open the secure message once they have requested a token.
7. The user clicks the secure message link and then clicks *Request Token*. The token is sent via email to the user.
8. The user enters the token and clicks *Verify Token*.
9. After the token is verified, the user is granted access to the secure message.

IBE user registration and check email process via email and SMS:

1. When a secure message is sent to a user, the user receives a notification. The user clicks *Register*.
   A registration email is sent to the user.
2. The user opens the registration email and clicks the registration link.
3. The user registers, providing their *Language*, *Time zone*, *First name*, and *Last name*.
   Since the user has selected both email and SMS as token delivery methods, they must verify their email address and Mobile Station International Subscriber Directory Number (MSISDN). Note that a token is not required for the registration of the user's own email address.
4. When the user clicks *Next*, they must confirm their *Verification email* address, then click *OK*.
5. The user must then confirm their *Verification phone number* and request a token.
6. The user then receives a one-time password or token via SMS.
7. Upon entering the token correctly, the user receives a successful registration notification email.
   Now that registration is complete, the user may only open the secure message once they have requested a token.
8. The user clicks the secure message link. Before the user clicks *Request Token*, they must select a *Token method* option: either *SMS* or *Email*. The token is sent via the selected option to the user.
9. The user enters the token and clicks *Verify Token*.
10. After the token is verified, the user is granted access to the secure message.

Viewing and managing IBE domains

The FortiMail unit records the domain names of the recipients who register or authenticate on FortiMail.

To view those domains, go to *Domain & User > IBE User > IBE Domain*.

GUI item	Description
Delete (button)	Select to remove a selected domain. Deleting a domain also disables all its users. These users cannot access the FortiMail unit until they receive new secure mail notifications from the FortiMail unit.
Remove All Users (button)	Select to delete all mail users in a selected domain. These users cannot access the FortiMail unit until they receive new secure mail notifications from the FortiMail unit.
Search (button)	Select to search IBE domains. A search dialog appears.
Active User Count	Displays the active mail users in a domain. For more information about active users, see Configuring active users on page 125.
Expired User Count	Displays the expired mail users in a domain. For more information about active users, see Configuring expired users on page 126.

Configuring the address book

You can create contacts and group them for a shared address book. FortiMail webmail users can use it when writing an email. For information on how to use the shared address book in FortiMail webmail, log in to FortiMailwebmail and click *Help*.

Adding contacts to the address book

Address book contacts for FortiMail webmail can be created either:

- manually
- via import of comma-separated values (CSV) or vCard files, from third-party address book or email client software, such as Address Book on Apple iPhone
- via import from a directory server via LDAP, either on-demand or with scheduled synchronization

To replace existing entries:

1. Select those entries, then click *Delete*.
2. Import the address book that contains the replacements.

The FortiMail unit compares the`Webmail_ID` value of each entry in the address book file, and will not overwrite existing entries.

Alternatively, you can create contacts while creating a contact group. See Grouping contacts on page 132.

To batch edit or back up the address book, you can export to CSV or vCard files.

Domain & User > *Address Book* > *Contact* and other related tabs appear only if either:

- in server mode
- in gateway and/or transparent mode, if *Email Continuity* is enabled.

To manually add contacts

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Either click *New* or double-click an entry to modify it.
3. Configure the following:

GUI item	Description
Domain	Select either *System* or the name of a protected domain to which the contact belongs. See Configuring protected domains on page 92.
First name	Enter a first name (given name).
Last name	Enter a last name (family or surname).
Display name	
Email	Enter an email address. The email address field is optional and can be in any format.
Phone	

4. If you want to include more fields such as *Company name or Address*, click *Additional Fields* and then enable those fields.
5. Click *Create* or *OK*.
6. To group multiple contacts together into an address book, see Grouping contacts on page 132.

To import contacts from a CSV or vCard file

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Click *More* and then select *Import* > *CSV* or *Import* > *vCard*.
3. Click *Browse*, find the file that you want to import, and then click *OK*.

To import contacts from an LDAP server on demand

Alternatively, you can schedule FortiMail to automatically periodically synchronize with the directory. See Synchronizing the address book via LDAP on page 134.

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Click *More* and then select *Import* > *LDAP*.
3. Configure the following:

GUI item	Description
Select LDAP profile	Select an LDAP profile that queries the LDAP server to import contacts, or click the **+** button to create a new profile. See Configuring LDAP profiles on page 234.
Select LDAP mapping	Select an LDAP attribute mapping template, or click the **+** button to create a new template. The FortiMail unit will import contacts from the LDAP server based on this template. See Configuring LDAP attribute mapping for the address book on page 133.

4. Click *OK*.
   The FortiMail unit starts importing contacts from the LDAP server. When complete, a *Status* field appears with information on whether the import was successful.
5. To group multiple contacts together into an address book, see Grouping contacts on page 132.

To back up or export contacts

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Click *More* and then select *Export* > *CSV* or *Export* > *vCard*.

To batch edit many contacts at once, you can edit the CSV file in spreadsheet software such as Microsoft Excel, and then import the CSV file. Imports can also be used to restore backups. See To import contacts from a CSV or vCard file on page 131.

Grouping contacts

Contact groups are a common set of address book information that FortiMail webmail users have access to when they compose email. For details on how to use contact groups, log in to FortiMailwebmail and click *Help*.

Domain & User > *Address Book* > *Contact* and other related menus appear only if either:
- in server mode
- in gateway and/or transparent mode, if *Email Continuity* is enabled.

To configure a contact group

1. Go to *Domain & User* > *Address Book* > *Contact Group*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Domain	Select either *System* or the name of a protected domain to which the contact group belongs. See Configuring protected domains on page 92.
Name	Enter a unique name

4. Click *Create*.
   The contact group now exists, but does not contain any contacts yet.
5. If you created the group in a protected domain, then from the *Domain* dropdown list, select the name of the protected domain to which the contact group belongs. (Otherwise, initially the group does not appear because by default, *Domain* is *System*.)
6. Double-click the group to enter it.
   The tab now displays a filtered list, showing only the contacts that are in the group. If you want to return to the list of groups and select another, click the *Back* button at the top left of the tab.
7. Select one or more contacts.
   If you need to add contacts, either click *New* or *More* > *Import*. For details, see Adding contacts to the address book on page 130.

If you have many contacts, and need to find an existing contact in the group, click *Search*, type text that matches one of the fields (for example, the display name or last name), and then press Enter. The group is filtered to show only the search results.

8. Click the *More* button and then select either *Manage Group* > *Add to Group* or *Manage Group* > *Delete From Group*.

If you delete a contact on *Domain & User* > *Address Book* > *Contact Group*, contacts are not removed from everywhere on FortiMail — only removed from the group.

9. Configure the following:

GUI item	Description
Domain	Select either *System* or the name of a protected domain to which the contact group belongs. The list in Available group(s) is filtered by this selection.
Available group(s)	If you want to add a contact to the group, then select the contact group, then click the **>** button to move it to Selected group(s).
Selected group(s)	If you want to remove a contact from the group, then click the **<** button to return it to Available group(s).

Configuring LDAP attribute mapping for the address book

You can import information in your directory server to create an address book on FortiMail. Before you do this, you must map LDAP attributes to the equivalent field of contacts in the FortiMail address book.

Domain & User > *Address Book* > *Contact* and other related menus appear only if either:

- in server mode
- in gateway and/or transparent mode, if *Email Continuity* is enabled.

To configure an LDAP-to-address-book mapping

1. If required, on your LDAP server, configure the schema so that it works with a FortiMail LDAP profile query. For details, see Preparing your LDAP schema for FortiMail LDAP profiles on page 250.

   Also test the query results. If it contains data that you do not want to import into the address book, then you must configure LDAP query filter later.
2. Go to *Domain & User* > *Address Book* > *LDAP Mapping*.
3. Either click *New* or double-click an entry to modify it.
4. Configure the following:

GUI item	Description
Mapping name	Enter a unique name.
Mapping content	If you need to add a mapping, click the **+** button, and then configure Contact Field and LDAP Attribute. If you need to delete a mapping, select a mapping's checkbox, and then click the **-** button.

GUI item	Description
Contact Field	Select an attribute in FortiMail address book contacts (such as *Email*, *First name*, *Last name*, or *Mobile*) that you want to map to an LDAP attribute. **Note:** The *Email* attribute must be mapped.
LDAP Attribute	Select the name of the LDAP attribute on the directory server that corresponds to each Contact Field. For example, the `cn` (common name) attribute might be mapped to *Display name*, and the `mail` attribute might be mapped to *Email*.
LDAP query filter	If the query in the LDAP profile returns some results that you do not want to import into the address book, enter an LDAP query filter. For example, to select only results that have an email address, the filter might be: `(mail=*)`

5. Click *Create*.
6. To apply the LDAP attribute mapping, select it either while importing contacts on demand, or in a regularly scheduled address book synchronization. For details, see Adding contacts to the address book on page 130 and Synchronizing the address book via LDAP on page 134.

Synchronizing the address book via LDAP

You can configure synchronization of the FortiMail webmail address book with your directory server. Synchronization can be regularly scheduled, or on demand.

Each contact is identified by its email address. If a new contact is created on the directory server, then synchronization adds it to the address book. If the same contact already exists in the address book, then synchronization updates it with current data from the directory server. If the contact does not exist on the directory server, then synchronization deletes that contact from the address book.

Domain & User > Address Book > Contact and other related menus appear only if either:
- in server mode
- in gateway and/or transparent mode, if *Email Continuity* is enabled.

To configure LDAP synchronization of the address book

1. Go to *Domain & User > Address Book > LDAP Sync*.
2. Either click *New* or double-click an entry to modify it.
3. Configure the following:

GUI item	Description
Name	Enter a unique name.
Description	Enter a comment or description.
LDAP profile	Select an LDAP profile that defines the base query and connection to the directory server. See also Configuring LDAP profiles on page 234.
LDAP mapping	Select an LDAP attribute-to-address-book mapping that defines which contact

GUI item	Description
	information will be synchronized. See also Configuring LDAP attribute mapping for the address book on page 133.
Sync type	Select how much to synchronize from the directory to the address book, either: • *Full* — All data that matches the LDAP query and has an address book mapping. • *Incremental* — Only data that changed since the most recent synchronization. For example, you might have both a daily incremental sync task (it's smaller, so it can run every night), and also a full sync task (it runs every weekend).
Sync to	Select the protected domain whose address book you want to synchronize, or select *System* to synchronize the global address book. **Note:** Once the LDAP synchronization task is created, this selection cannot be changed.
Schedule	Select the time interval between each LDAP synchronization, either *Not scheduled*, *Daily*, *Weekly*, or *Monthly*. If you select *Not scheduled*, then you can use this profile to import the address book from the directory server at any time, on demand. See Adding contacts to the address book on page 130. Otherwise, select when FortiMail automatically synchronizes: which hour, day of the week, or day of the month.

4. Click *Create*.

Sharing calendars and address books (server mode only)

FortiMail supports calendar sharing and LDAP-based address book sharing. The calendar, meeting schedule, free-busy time, and resources like meeting rooms, projectors, and other equipment usage are also supported.

To be specific, the following features are supported:

- FortiMail internal calendar sharing from/to FortiMail webmail users
- Internet calendar sharing from/to FortiMail webmail users
- Calendar sharing from/to Microsoft Outlook users using WebDAV (Outlook does not support CalDAV)
- Calendar sharing from/to Mozilla Thunderbird users using WebDAV or CalDAV
- Address book query from Outlook using LDAP
- Address book query from Thunderbird using LDAP
- Option to manually send reminders (organizer only)
- Organizer display name support

Other email clients may also be supported if they support the standard WebDAV and CalDAV protocols.

Calendar sharing

To share calendars, you must first enable the service on FortiMail and then configure the webmail or mail client settings.

FortiMail calendar settings

To enable the WebDAV and CalDAV services

1. Go to *Domain & User* > *Calendar* > *Setting*.
2. Select *Enable WebDAV* and *Enable CalDAV*.
3. Click *Apply*.

To create a calendar resource for sharing

1. Go to *Domain & User* > *Calendar* > *Resource*.
2. Click *New*.
3. Fill out the information and click *Create*.

FortiMail webmail settings

FortiMail webmail users can perform calendar publishing, subscribing, and sharing operations with other mail clients, such as Microsoft Outlook and Thunderbird Lightning.

To access the WebDAV and CalDAV service URL

1. Log on to FortiMail webmail.
2. On the upper right corner, click the *Settings* dropdown list and select *Preferences*.
3. Under *Account Settings* > *Service URL*, click *[View]* to access the FortiMail WebDAV, CalDAV and CardDAV service URLs.

Thunderbird settings

Thunderbird Lightning users can publish and subscribe calendars to/from the FortiMail WebDAV server. They can also subscribe the shared calendar via the CalDAV protocol which facilitates calendar sharing and synchronization between FortiMail and Thunderbird Lightning.

Thunderbird users can schedule an event or meeting based on the free/busy information shared and stored on FortiMail WebDAV server. Before scheduling a meeting, the free/busy settings must be configured.

To publish a calendar to FortiMail WebDAV service

1. In Thunderbird, go to *Events and Tasks* > *Calendar*.
2. Right-click on a calendar and select *Publish Calendar*.

3. For *Publishing URL*, enter the URL you get from the FortiMail webmail (see FortiMail webmail settings on page 136).
4. Enter the user name and password required for FortiMail authentication.
5. Click *Publish*.
6. Enter the user name and password required for FortiMail authentication.
7. Click *OK*.

To subscribe a calendar from FortiMail CalDAV service

1. In Thunderbird, go to *File* > *New* > *Calendar*.
2. Select *On the Network*.
3. For *Format*, select *CalDAV*.
4. Enter the publicly shared calendar location you get from the FortiMail webmail (see FortiMail webmail settings on page 136).
5. Enter the display name and other settings, then click *Next*.
6. Enter the user name and password required for FortiMail authentication.
7. The new calendar will appear in the left calendar pane. And it can be synchronized with the FortiMail CalDAV service automatically or manually.

To configure the free/busy settings in Thunderbird

1. Go to *Tools* > *Free/Busy*.
2. Click the *Settings* tab.
3. Enter the email address and the matching free/busy URL. Thunderbird users get the FB URL from the FortiMail administrator, who gets the URL from the calendar settings on the FortiMail GUI.
4. Create a new event and invite attendees.
5. Enter the email address of the attendees. The free/busy information will be retrieved from FortiMail.

With the free/busy settings configured, Thunderbird users can schedule a meeting with the right time.

To schedule a meeting in Thunderbird

1. Go to *Events and Tasks* > *New Event*.
2. Enter the event contents and click *Invite Attendees*.
3. Enter the email address of the attendees. Their free/busy information will be retrieved from the FortiMail server and displayed in different colors.

Outlook settings

Outlook users can publish and subscribe calendars to/from FortiMail WebDAV service (Outlook does not support CalDAV). They can also schedule meetings based on the free/busy information shared and stored on the FortiMail WebDAV server.

Outlook users can schedule an event or meeting based on the free/busy information shared and stored on FortiMail WebDAV server. Before scheduling a meeting, the free/busy settings must be configured.

To publish a calendar to FortiMail WebDAV service

1. In Outlook, go to *Go* > *Calendar*.
2. Right-click on a calendar and select *Publish to Internet*.
3. Select *Publish to WebDAV Server*.
4. In the popup window, enter the URL you get from the FortiMail webmail (see FortiMail webmail settings on page 136).
5. Specify a time span and permission.
6. Enter the user name and password required for FortiMail authentication.
7. Click *OK*.
8. Enter the user name and password required for FortiMail authentication.
9. Click *OK*.

To subscribe a calendar from FortiMail WebDAV service

1. In Outlook, go to *Tools* > *Account Setting*.
2. Click the *Internet Calendars* tab.
3. Click *New*.
4. Enter the publicly shared calendar location you get from the FortiMail webmail (see FortiMail webmail settings on page 136).
5. Specify the folder name and description.
6. Click *OK*.

To configure the free/busy settings in Outlook 2007

1. Go to *Tools* > *Options*.
2. Then go to *Calendar Options* > *Free/Busy Options*.
3. Enter free/busy URL. Outlook users get the FB URL from the FortiMail administrator, who gets the URL from the calendar settings on the FortiMail GUI.
4. Note that *Publish at my location* is not supported. Do not select this option.
5. Click *OK*.

With the free/busy settings configured, Outlook users can schedule a meeting with the right time.

To schedule a meeting in Outlook 2007

1. Go to *New* > *Meeting Request*.
2. Click *Scheduling*.
3. Enter the email address of the attendees. Their free/busy information will be retrieved from the FortiMail server and displayed in different colors.
4. Click Appointment to arrange and send the meeting request.

Address book sharing

With the LDAP service enabled, users can search and download address books stored in FortiMail from within their mail clients, such Thunderbird and Outlook.

FortiMail settings

First, you need to enable the LDAP service on FortiMail.

To enable the LDAP service

1. Log on to FortiMail CLI console.
2. Enter the following commands (available in server mode only:

```
config system global
   set ldap-server-sys-status enable
end7
```

By default, the LDAP service is enabled.

For the users to access the FortiMail address book from mail clients via LDAP, you must create a resource profile and a policy to allow the access.

To create a policy

1. Go to *Policy* > *Recipient Policy* > *Inbound*.
2. Click *New*.
3. Specify the sender and recipient patterns, and other settings.
4. For Resource profile, click *New*.
5. In the resource profile configuration, select Domain address book, Global address book, or both.

Thunderbird settings

Thunderbird users can access the address books stored on FortiMail via the LDAP protocol.

To configure the address book LDAP settings in Thunderbird

1. Open the address book in Thunderbird.
2. From File, select New LDAP Directory.
3. Select the General tab.
4. Enter a name.
5. Enter the hostname of FortiMail.
6. Enter the base DN.
7. Enter the port number. See also Appendix: Port Numbers on page 375.
8. Enter the Bind DN.
9. Click OK.

Note that SSL is not supported. Do not select *Use secure connection*.

To search contacts FortiMail address books

1. Go to *Edit > Advanced address book search*.
2. Specify the address book to be searched.
3. Enter the user name.
4. Click *Search*.

To download contacts from FortiMail address books

1. Open the address book in Thunderbird.
2. Click *Properties* of an address book.
3. Click *Offline*.
4. Click *Download Now*.
5. Enter the password of the binding user required for FortiMail authentication.

Outlook settings

Outlook users can access the address books stored on FortiMail via the LDAP protocol.

To configure the address book LDAP settings in Outlook 2007

1. Go to *Tools > Account Setting*.
2. Select *Address Books*.
3. Click *New*.
4. Enter the server name or IP address of FortiMail.
5. Enter the user name and password.
   For example, User name: cn=user1,ou=people, dc=example, dc=com, assuming your user name is `user1`, your domain name is `example.com`.
   In this example, `user1` is a user under the protected domain `example.com` in FortiMail. The password is the same password used for `user1`'s domain.
6. Select *More Settings*.
7. Select the *Connection tab*.
8. Specify the display name and connection port.
9. Switch to the *Search* tab, and specify the *Search Base* to *Custom*: dc=example, dc=com.
10. Click *OK*.

To access FortiMail address books

1. Open the address book in Outlook.
2. Select the target address book.
3. Enter the user name you want to find.
4. Click *Go*.

Migrating email from other mail servers (server mode only)

If you already have other mail servers, such as Exchange or FortiMail server, and you want to consolidate the mail user and data into one FortiMail server, you can do so by migrating the users and data to your FortiMail unit.

The email migration process involves the following procedures:

1. **Preparation**
   a. Enable the mail migration feature using the following CLI commands (available in server mode only):
   ```
   config system global
      set email-migration-status enable
   end
   ```

   By default, the email migration feature does not appear on the GUI until you enable it with the above CLI commands.

   b. Define the remote mail server settings. For details, see Defining a remote mail server for mail migration on page 142.
   c. Create a domain for the to-be-migrated users. For details, see Creating domains for mail migration on page 142.
2. **User migration**
   Because FortiMail will act as an IMAP client on behalf of the users to get their email from the remote mail server, you must import the user/password information first. To do this, you can use one of the following methods:
   - If you only need to migrate email for a few users and you know the users' login credentials, you can manually enter their user name/password information by going to *Domain & User > Mail Migration > Migration User* and click *New*.
   - If you can export the user name/non-encrypted password list into a CSV file, you can import the CSV file by going to *Domain & User > Mail Migration > Migration User* and click *Action > Import > From .CSV File*.
   - If the to-be-migrated users already have accounts on the FortiMail server, you can import/copy the local user list to the migration user list by going to *Domain & User > Mail Migration > Migration User* and click *Action > Import > From Local Domain*.
   - If the user passwords are encrypted, you have to collect their passwords through FortiMail webmail login or SMTP client login. To do this:
     i. Create an authentication profile that uses the remote mail server as the authentication server. For details, see Configuring authentication profiles on page 231.
     ii. Create a recipient-based policy that includes the migration users as senders and also includes the authentication profile. For details, see the Controlling email based on sender and recipient addresses on page 163.
     iii. Use one of the following two methods to collect user passwords:
       i. Through FortiMail webmail login: Inform the users to log in to the FortiMail webmail portal, using their email addresses of the remote domain (the domain part needs to match proper authentication policy) and their passwords. Upon successful login, the users will be shown an

empty webmail mailbox. This is because the email data has not been migrated yet and this step is only meant to collect user passwords.

ii. Through SMTP client login: Inform the users to use the FortiMail host name as their outgoing mail server.

After you have done the above, when the users try to send email, they will have to authenticate through FortiMail. Then FortiMail will record the user names and passwords into the migration user list under *Domain & User > Mail Migration > Migration User*.

3. **Mail data migration**

   After you have migrated the users, you can start to migrate the their mail boxes from the remote server. To do this:

   a. Go to *Domain & User > Mail Migration > Migration User*.
   b. From the *Action* dropdown list, select *Migrate > Selected Users* or *All Users*.
   c. If needed, you can click the *Stop* and *Start* button to control the migration process.
   d. After the user's mail data is successfully migrated, you can export the user to the local user list by clicking *Action > Export > Selected Users* or *All Users*. The exported users will appear as local users under *User > User*.

Defining a remote mail server for mail migration

This is one of the email migration procedures. For the entire procedures, see Migrating email from other mail servers (server mode only) on page 141.

1. Go to *Domain & User > Mail Migration > Remote Mail Server*.
2. Click *New*.
3. Enter a name for the remote server.
4. Enter the host name or IP address of the remote server.
5. For Protocol, select either IMAP or IMAPS, FortiMail will act as an IMAP client on the users' behalf to get email from the remote server.
6. Enter the IMAP port number. See also Appendix: Port Numbers on page 375.
7. Click *Create*.

Creating domains for mail migration

This is one of the email migration procedures. For the entire procedures, see Migrating email from other mail servers (server mode only) on page 141.

1. Go to *Domain & User > Domain > Domain*.
2. Click *New*.
3. Configure the settings as described in Configuring protected domains on page 92.

In v5.0 release, the created domain name on FortiMail must be the same as the users' domain on the remote mail server. Beginning from v5.0.1 release, the domain names can be different.

4. Since you have enabled mail migration, a new section called Mail Migration Settings appears at the bottom of the domain settings page. Expand this section and configure the following settings.
5. Check *Enable mail migration*.
6. Specify the remote mail server from the dropdown list. See Defining a remote mail server for mail migration on page 142.
7. Click *Create*.

See also:

Configuring protected domains

Configuring LDAP profiles

Configuring policies

The Policy menu lets you create policies that use profiles to filter email.

It also lets you control who can send email through the FortiMail unit, and stipulate rules for how it will deliver email that it proxies or relays.

Modify or delete policies and policy settings with care. Any changes made to a policy take effect immediately.

This section includes:

What is a policy?

A policy defines which way traffic will be filtered. It may also define user account settings, such as authentication type, disk quota, and access to webmail.

After creating the antispam, antivirus, content, authentication, TLS, or resource profiles (see Configuring profiles on page 171), you need to apply them to policies for them to take effect.

FortiMail units support three types of policies:

- Access control and delivery rules that are typical to SMTP relays and servers (see Controlling SMTP access and delivery on page 148)
- Recipient-based policies (see Controlling email based on sender and recipient addresses on page 163)
- IP-based policies (see Controlling email based on IP addresses on page 159)

Recipient-based policies versus IP-based policies

- Recipient-based policies

  The FortiMail unit applies these based on the recipient's email address or the recipient's user group. May also define authenticated webmail or POP3 access by that email user to their per-recipient quarantine. Since version 4.0, the recipient-based policies also check sender patterns.

- IP-based policies

The FortiMail unit applies these based on the SMTP client's IP address (server mode or gateway mode), or the IP addresses of both the SMTP client and SMTP server (transparent mode).

Inbound versus outbound email

There are two types of recipient-based policies: inbound and outbound. The FortiMail unit applies inbound policies to the incoming mail messages and outbound policies to the outgoing mail messages.

Whether the email is inbound or outbound is decided by the domain name in the recipient's email address. If the domain is a protected domain, the FortiMail unit considers the message to be inbound and applies the first matching inbound recipient-based policy. If the recipient domain is not a protected domain, the message is considered to be outbound, and applies outbound recipient-based policy.

To be more specific, the FortiMail unit actually matches the recipient domain's IP address with the IP list of the protected SMTP servers where the protected domains reside. If there is an IP match, the domain is deemed protected and the email destined to this domain is considered to be inbound. If there is no IP match, the domain is deemed unprotected and the email destined to this domain is considered to be outbound.

IP-based policies are not divided into inbound and outbound types. The client IP address and, for transparent mode, the server IP address are only used to determine whether or not the IP-based policy matches.

See also

How to use policies

Controlling SMTP access and delivery

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

How to use policies

FortiMail has multiple types of policies:

- **Access control receiving rules and delivery rules** control which SMTP clients can send email through FortiMail, and how to deliver email that it proxies or relays.
- **IP-based policies** control SMTP sessions based on the IP address of the SMTP client and, if the FortiMail unit is operating in transparent mode, the SMTP server. They may apply various features such as antispam.
- **Recipient-based policies** control individual email messages based on the recipient's email address and, for outbound email, the sender's email address. They may apply various features such as antispam.

Depending on each email and your configuration, multiple policies may apply. Effects vary by the order of execution for policies, and which policies matched.

Whether to use IP-based or recipient-based policies

Many of the same features can be applied in IP-based and recipient-based policies. Which type of policy should you use?

You can use either or both.

Exceptions include the following scenarios, which require IP-based policies:

- mail hosting service providers
  There is a great number of domains, and it is not feasible to configure them all as protected domains on the FortiMail unit.
- Internet service providers (ISPs)
  Mail domains of customers are not known.
- session control
  Even if protected domains are known and configured on the FortiMail unit, an IP-based policy must be created in order to apply a session profile. Session profiles are only available in IP-based policies.
- differentiated services based on the network of origin
  To apply antispam and antivirus protection based on the IP address of the SMTP client or based on a notion of the internal or external network, rather than the domain in a recipient's email address, you must use an IP-based policy.

As a general rule, it is simpler to use IP-based policies. Use recipient-based policies only where they are required, such as when the policy must be tailored for a specific email address.

For webmail login, select an Authentication type and Authentication profile when configuring an inbound recipient-based policy. This option is only available when the FortiMail unit is operating in either gateway or transparent mode.

IP-based policy authentication does not support webmail login.

For example, if your company is an ISP, you can use recipient-based policies to apply antispam and antivirus profiles for only the customers who have paid for those services.

If both a recipient-based policy and an IP-based policy match the email, unless you have enabled Take precedence over recipient based policy match in the IP-based policy, the settings in the recipient-based policy will have precedence.

See also

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

Order of execution of policies

Use Policy Lookup to test which policies will match, and which profile settings will apply. This can save time if you have many policies and domains.

During each SMTP session that FortiMail receives, it looks for matching policies and applies their profile settings in a specific order:

1. Find a matching access control receiving rule.
2. Find a matching IP-based policy.
3. Find a matching recipient-based policy.
   Multiple policy IDs may apply if:
   - The email has multiple recipients. See also Which policy/profile is applied when an email has multiple recipients? on page 147.
   - The SMTP client requests authentication. This requires an authentication profile, so FortiMail searches the IP-based or recipient-based policy lists again to find a matching policy ID with an authentication profile, if any.
4. If either:
   - No matching recipient-based policy exists.
   - A matching recipient-based policy exists, but no protection profiles are selected there. Instead, they are in the IP-based policy.
   - Take precedence over recipient based policy match on page 163 is enabled in the IP-based policy.

   then apply the protection profiles which are in the matching IP-based policy.
   Otherwise apply the protection profiles in the matching recipient-based policy.

If SMTP traffic is allowed by access control receiving rules, but does not match any IP-based or recipient-based policy, it is allowed. However, no antivirus, antispam, or other protection profile is applied.
If you configured policies to match and allow all required traffic, then you can tighten security by adding an IP-based policy at the bottom of the list to reject all other, unwanted connections.

For each policy type, FortiMail looks for a match in order, from the top to the bottom of the list — not by ID number. Disabled policies are skipped. Once a match is found, match evaluation stops. Therefore you should put more specific policies before more generic policies. Otherwise evaluation does not reach more specific policies, and they are not used.

For example, an inbound recipient-based policy that matches all recipients (*@*) is the most general policy possible because it matches all email. If you create more specific policies (for example, `user1@example.com`), then you must move them above. Otherwise, the general policy always matches, and so the other policies would never be applied.

See also

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

Order of execution for antispam scans

Which policy/profile is applied when an email has multiple recipients?

When applying recipient-based policies, an email with multiple recipients is treated as if it were multiple email messages, each with one recipient. This allows a fine degree of control for each recipient, but also means that

separate recipient-based policies may block the email for some recipients but allow it for others.

Exceptions include use of an antivirus profile. In this case, the FortiMail unit will treat an email with multiple recipients as a single email. Starting with the first recipient email address, the FortiMail unit looks for a matching recipient-based policy. If none is found, FortiMail continues by looking for a matching IP-based policy.

See also

Controlling email based on sender and recipient addresses

Controlling SMTP access and delivery

The *Policy > Access Control* submenu lets you configure access control and delivery policies for SMTP sessions.

Unlike proxy/implicit relay pickup, access control rules take effect after the FortiMail unit has initiated or received an IP and TCP-level connection at the application layer of the network.

Other protocols can also be restricted if the connection's destination is the FortiMail unit. For details, see Configuring the network interfaces on page 1.

Access control policies, also called ACLs, are categorized based on whether they affect either:

- receipt (the FortiMail unit is the destination of the SMTP session)
- delivery (the FortiMail unit is the source of the SMTP session)

This is different from the idea of incoming vs. outgoing direction in IP-based and recipient policies. For example, delivery policies can affect both incoming and outgoing mail; receiving policies can, too.

Configuring access control receiving policies

The *Receiving* tab displays a list of access control rules that apply to SMTP sessions being **received** by the FortiMail unit (initiated by SMTP clients).

Access control policies, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages in SMTP sessions.

When an SMTP client tries to send email through the FortiMail unit, the FortiMail unit compares each access control policy to the commands used by the SMTP client during the SMTP session, such as the:

- sender email address in the SMTP envelope (`MAIL FROM:`)
- recipient email address in the SMTP envelope (`RCPT TO:`)
- domain name of the SMTP client that is delivering the email (`HELO`/`EHLO`)
- authentication (`AUTH`)
- session encryption (`STARTTLS`)

Policies are evaluated for a match in sequential order, from top to bottom of the list. If all attributes of a policy match, then the FortiMail unit applies the action in the policy or TLS profile, and stops match evaluation. Remaining access control policies, if any, are not applied.

Only one access control policy is applied to an SMTP session.

If no access control rules exist, or none match, then the action varies by whether the SMTP client authenticated:

- **Authenticated**: Email is relayed/proxied.
- **Not authenticated**: Default action is performed.

The default action varies by whether or not the recipient email address in the SMTP envelope (`RCPT TO:`) is a member of a protected domain:

- **Protected domain**: Relay/proxy with greylisting.
- **Not protected domain**:Reject.

See also Configuring protected domains on page 92.

Rejecting unauthenticated SMTP clients that send email to unprotected domains prevents your email service from becoming an open relay. Open relays are abused by spammers, and therefore DNSBLs block them, so this FortiMail behavior helps to protect the reputation of your email server. Senders can deliver email incoming to your protected domains, but cannot deliver email outgoing to unprotected domains

If you want to allow your email users or email servers to send email to unprotected domains, then you must configure at least one access control policy. You may need to configure more access control rules if, for example, you want to discard or reject email from specified:

- email addresses, such as ones that no longer exist in your protected domain
- SMTP clients, such as a spammer that is not yet known to public blocklists

Like IP-based policies, access control rules can reject connections based on IP address.

Unlike IP-based policies, however, access control rules **cannot** affect email in ways that occur after the session's `DATA` command, such as by applying antispam profiles. Access control rules also cannot be overruled by recipient-based policies, and cannot match connections based on the SMTP server (which is always the FortiMail unit itself, **unless** the FortiMail unit is operating in transparent mode). For more information on IP-based policies, see Controlling email based on IP addresses on page 159.

For information about the sequence in which access control rules are used relative to other antispam methods, see Order of execution for antispam scans on page 22.

Do **not** create an access control policy where:

- Sender is *
- Recipient is *
- Reverse DNS is *
- Forged IP check is *Any*
- Authentication status is *Any*
- TLS profile is *None*
- Action is *Relay*

This creates an **open relay**, which could result in other MTAs and DNSBL servers blocklisting your protected domain.

To configure an access control rule

1. Go to *Policy* > *Access Control* > *Receiving*.
2. Either click *New* to add a policy, or double-click a policy to modify it.
3. Configure the following:

GUI item	Description
Status	Enable or disable the policy.
Sender	Select how you will define the sender email addresses that match the policy, either: • *External*: Email addresses that are **not** at a protected domain. • *Email Group*: Select a group of email addresses configured on the FortiMail unit. See also Configuring email groups on page 272. • *Internal*: Email addresses that are at a protected domain. • *LDAP Group*: Enter the name of a group of email addresses configured on a directory server such as Microsoft Active Directory, then select the LDAP profile used for the query. See also Configuring LDAP profiles on page 234. • *LDAP Verification*: Select the LDAP query to a directory server such as Microsoft Active Directory. See also Configuring LDAP profiles on page 234. **Note**: Use `$s` in the query string to match sender addresses. For example, to reject senders that are not in the recipient's allowed sender list: **a.** Create an ACL policy and select LDAP verification in Sender. **b.** Select an LDAP profile where this user query string is used: `&(mail=$m)(!(allowedSenders=$s)))` **c.** In Action, select *Reject*. For each recipient (`$m`), this will match a sender (`$s`) that is not (`!`) in their `allowedSenders` list, and the action will reject it. • *User (wildcard)* Enter a complete or partial email address. Wild card characters can be used to match multiple email addresses. An asterisk (`*`) represents one or more characters. A question mark (`?`) represents any single character. For example: `*@example.???` matches all email addresses at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • *User (regex* Enter a regular expression that can match multiple email addresses. To validate the expression and verify correct matching, click *Validate*. See also Appendix: Wildcards and regular expressions on page 380 and Using wildcards and regular expressions with access control on page 153.
Recipient	Select how you will define the recipient email addresses that match the policy. Options are the same as Sender. **Note:** For *LDAP Verification*, use `$m` in the query string to match recipient addresses. See also User Query on page 237.
Source	Select how you will define the source IP address of SMTP clients that match this policy, either: • *IP/Netmask*: Enter an IP address and netmask. For example, you can enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. In the policy list, this appears as `10.10.10.0/24`, with the `0` indicating that any value is matched in that position of the address.

GUI item	Description
	Similarly, if you enter `10.10.10.10/32`, it appears as `10.10.10.10/32` because a 32-bit netmask only matches one address, 10.10.10.10 specifically. To match any IPv4 address, enter `0.0.0.0/0`; to match any IPv6 address, enter `::/0`; to match both IPv4 and IPv6 addresses, you must create two separate rules. • *IP Group*: Select an IP address group. See also Configuring IP groups on page 272. • *GeoIP Group*: Select a geographic IP address group. See also Configuring GeoIP groups on page 273. • *ISDB*: Select a service name. The Internet Service Database (ISDB) from FortiGuard is an automatically updated list of IP addresses and subnets used by popular services such as 8x8, Akamai, Microsoft 365, and more. • *LDAP*: Select the LDAP query to a directory server such as Microsoft Active Directory. See also Hostname/IP Lookup on page 248. **Note**: Use `$h` in the query string to match the IP address.
Reverse DNS	Select how you will define the FQDN of SMTP clients that match this policy, either: • *User Defined (wildcard)*: Enter a complete or partial domain name. Wild card characters can be used to match multiple FQDNs. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • *User Defined (regex)*: Enter a regular expression. **Tip:** To verify syntax and correct matching, click *Validate*. See also Appendix: Wildcards and regular expressions on page 380 and Using wildcards and regular expressions with access control on page 153. • *LDAP*: Select the LDAP query to a directory server such as Microsoft Active Directory. See also Hostname/IP Lookup on page 248. **Note**: Use `$h` in the query string to match the FQDN. Because the domain name in the SMTP session greeting (`HELO/EHLO`) is self-reported by the connecting SMTP client, it could be fake and the FortiMail unit does not trust it. Instead, the FortiMail does a reverse DNS (`PTR` record) lookup of the SMTP client’s IP address to discover its real domain name. This is compared to the pattern or LDAP query results. If the domain name does not match, or if the reverse DNS query fails, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, “.lab” is not valid because it is reserved for testing on RFC 1918 **private** networks, not the Internet. Thus a reverse DNS query to **public** DNS servers on the Internet will always fail.
Forged IP check	FortiMail examines the reverse DNS (`PTR` record) and FQDN (`A` or `AAAA` record). Normally, these records should agree. Select whether to match this policy if the DNS records agree, either: • *Pass*: Match this policy if the DNS records agree.

GUI item	Description
	• *Fail*: Match this policy if the DNS records do **not** agree. • *Any*: Ignore DNS query results. If the DNS queries fail, or the result does not match this setting, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, ".lab" is not valid because it is reserved for testing on RFC 1918 **private** networks, not the Internet. Thus a reverse DNS query to **public** DNS servers on the Internet will always fail.
Authentication status	Select whether to match this policy if the SMTP client has authenticated with the FortiMail unit, either: • *Any*: Ignore authentication status. • *Authenticated*: Match this policy if the SMTP client has authenticated. • *Not Authenticated*: Match this policy if the SMTP client has **not** authenticated.
TLS profile	If you want to allow or reject the connection based on whether the session attributes matches TLS profile, then select the TLS profile. • *Match*: Action occurs. • *No Match*: Action on failure in the TLS profile occurs. See Configuring TLS security profiles on page 266.
Action	Select which delivery action the FortiMail unit will perform for SMTP sessions that match this policy. • *Reject*: Reject delivery of the email (SMTP reply code `550 Relaying denied`). • *Discard*: Accept the email (SMTP reply code `250 OK`), but then silently delete it and do not deliver it. • *Relay*: Accept the email (SMTP reply code `250 OK`), regardless of authentication or protected domain. **Do not greylist**, but continue with remaining antispam and other scans. • *Safe*: Accept the email (SMTP reply code `250 OK`) if the sender authenticates or recipient belongs to a protected domain. **Greylist**, but skip remaining antispam scans. Continue other scans such as antivirus. Otherwise, if the sender does not authenticate, or the recipient does not belong to a protected domain, then reject delivery of the email (SMTP reply code `554 5.7.1 Relaying denied`). In older FortiMail versions, this setting was named *Bypass*. • *Safe & Relay*: Like *Relay*, **do not greylist**, but also skip remaining antispam scans. • *Receive*: Like *Relay*, but **greylist**, and require authentication or protected domain. Otherwise, if the sender does not authenticate or the recipient does not belong to a protected domain, then FortiMail rejects (SMTP reply code `554 5.7.1 Relaying denied`). **Tip:** *Receive* is usually used when you need to apply a TLS profile, but do not want to safelist nor allow outbound, which *Relay* does. If you do **not** need to apply a TLS profile, then a policy with this action is often not required because by default, email inbound to protected domains is relayed/proxied.
Comment	Optional. Enter a description or comment. If a comment exists, it is displayed as a tool tip when you mouse-over the ID column in the list of rules in the GUI.

4. Click *Create*or *OK*.
5. If you want your new policy to be evaluated before another policy, click *Move* and put your new policy before the other policy in the list.

Initially, the policy appears at the end of the list of policies. List order indicates order of evaluation. As a result, the new policy will match an SMTP session only if no previous policy matches.

The policy *ID* number may be different from the order of evaluation.

Using wildcards and regular expressions with access control

In the list of rules on *Policy > Access Control > Receiving* and *Policy > Access Control > Delivery*, the prefix in each column indicates if a regular expression was used:

- `R/` prefix: Regular expression syntax to describe matching patterns.
- `-/` prefix: Not a regular expression.

Before you enable a policy that uses a regular expression, in the policy, click *Validate* to verify that it matches everything that you intend, and nothing that you do not intend. See also Syntax on page 381 and Example regular expressions on page 383.

When you configure access control policies, **do not leave any pattern fields blank**. Instead, if you want the FortiMail unit to ignore a pattern:

- If a regular expression is **not selected** for the setting, enter an asterisk (*) in the pattern field.
- If a regular expression is **selected** for the field, enter a dot-star (`.*`) character sequence in the pattern field.

For example, if you enter an asterisk (*) in *Recipient* and do not select a regular expression, then the asterisk matches all recipient addresses, and therefore all SMTP sessions can match the policy (unless one of the other criteria does not match).

Example: Access control rules with wild cards

If your protected domain, `example.com`, contains email addresses in the format of `user1@example.com`, `user2@example.com`, and so on, and you want to allow those email addresses to send email to any external domain if they authenticate their identities and use TLS according to `tlsprofile1`, then you might configure the following access control rule:

Status	Enable
Sender	user*@example.com
Recipient	*
Source	0.0.0.0/0
Reverse DNS	*
Forged IP check	Any
Authentication status	Authenticated

TLS profile	tlsprofile1
Action	Relay

Example: Access control rules with regular expressions

Example Corporation uses a FortiMail unit operating in gateway mode, and that has been configured with only one protected domain: example.com. The FortiMail unit was configured with the access control rules illustrated in the following table.

ID	Sender	Recipient	Source	Reverse DNS	Forged IP check	Authentication status	Action
1	-/*	-/user932@example.com	0.0.0.0/0	-/*	Any	Any	Reject
2	R/^\s*$	-/*	0.0.0.0/0	-/*	Any	Any	Reject
3	-/*	-/*@example.com	172.20.120.0/24	-/mail.example.org	Any	Any	Relay
4	-/*@example.org	-/*	0.0.0.0/0	-/*		Any	Reject
5	-/*	R/^user\d*@example\.com$	0.0.0.0/0	-/*		Any	Relay

Policy 1

The email account of former employee `user932` receives a large amount of spam. Since this employee is no longer with the company and all of the user's external contacts now email the replacement employee instead, email to the former employee's address must be spam.

Policy 1 uses only Recipient and Action. All other settings are configured to match any value. This policy rejects all messages sent to the `user932@example.com` recipient email address. Rejection at the access control stage prevents these messages from being scanned for spam and viruses, saving FortiMail system resources for other email that need more complex evaluation.

This policy is placed first because it is the most specific access control policy in the list. It applies only to SMTP sessions for that single recipient address. SMTP sessions sending email to any other recipient do not match it. If a policy that matched all messages were placed at the top of the list, no policy after the first would ever be checked for a match, because the first would always match.

SMTP sessions that do not match this policy are compared to the next policy.

Policy 2

Much of the spam received by Example Corporation has no sender email address specified in the SMTP envelope. Most valid email have a sender email address.

Policy 2 uses only Sender and Action. The regular expression `^\s*$` matches sender email addresses that are empty or contain only spaces (look empty). If any non-space character appears in the sender string, then this policy does not match. The rule's action rejects email with no sender.

Not all email without a sender are spam, however. Delivery status notification (DSN) messages often have no specified sender. Bounce notifications are the most common type of DSN messages. These are legitimate email, but the FortiMail administrators at Example Corporation decided that the advantages of this policy outweigh the disadvantages.

SMTP sessions that do not match this policy are compared to the next policy.

Policies 3 and 4

Recently, Example Corporation has been receiving spam that appears to be sent by `example.org`. The FortiMail log files revealed that the source IP address is being spoofed (the address in the SMTP greeting does not match) and the email are sent from servers operated by spammers. Because spam servers often change IP addresses to avoid being blocked, the FortiMail administrators decided to use two rules to block all mail from `example.org` unless delivered from a server at the legitimate IP address and host name.

When legitimate, email messages from `example.org` are sent from one of multiple mail servers. All these servers have IP addresses within the 172.20.120.0/24 subnet and have a domain name of `mail.example.org` that can be verified using a reverse DNS query.

Policy 3 uses Recipient, Source, Reverse DNS, and Action. This policy will relay messages to email users of `example.com` sent from a client whose verified domain name is `mail.example.org` and source IP address is between 172.20.120.1 and 172.20.120.255.

SMTP sessions that do not match this policy are compared to the next policy.

Policy 4 works with policy 3. It uses only Source and Action. Policy 4 rejects all messages from `example.org`, but because it is positioned after policy 3 in the list, policy 4 affects only messages that were not already proven to be legitimate by policy 3, thereby rejecting only email messages with a fake sender.

Policies 3 and 4 must appear in that order. If their order were reversed, then all mail from `example.org` would be rejected. The more specific policy 3 (accept valid mail from `example.org`) must be before the more general policy 4 (reject all mail from `example.org`).

SMTP sessions that do not match this policy are compared to the next policy.

Policy 5

An administrator of `example.com` has noticed that during peak traffic, a flood of spam using random user names causes the FortiMail unit to devote a significant amount of resources to recipient address verification. Verification is performed by an LDAP query to their directory server which also expends significant resources servicing these requests. Example Corporation email addresses start with `user`, followed by the user's employee number, and end with `@example.com`.

Policy 5 uses only Recipient and Action. The regular expression matches email addresses that follow that pattern. SMTP sessions that match this policy are relayed.

Default implicit rules

For SMTP sessions that do not match any policy, the FortiMail unit will perform the default action, which varies by whether or not the recipient email address in the SMTP envelope (`RCPT TO:`) is a member of a protected

domain.

- For protected domains, the default action is delivery (with greylisting).
- For unprotected domains, the default action is *Reject*.

Configuring delivery rules

The *Delivery* tab displays a list of delivery rules that apply to SMTP sessions being **initiated** by the FortiMail unit in order to deliver email.

Delivery rules can be used to encrypt each connection with TLS, and/or to encrypt each email with secure MIME (S/MIME) (also called IBE).

When the FortiMail unit initiates an SMTP session, each delivery policy is compared to the domain name in the recipient email address (`RCPT TO:`) and sender email addresses (`MAIL FROM:`) in the SMTP envelope. Policies are evaluated for a match in order, from top to bottom of the list. If a match does not exist, then the email is delivered. If a match does exist, then the connection attributes are compared to the TLS profile. Depending on the result, either the email is delivered (with encryption profile settings, if selected, and to the specified destination IP address) or the connection is not allowed. No subsequent delivery rules are applied. Only one delivery policy is ever applied to each SMTP session.

If you apply S/MIME encryption, the destination can be any email gateway or server, if either the:

- destination's MTA or mail server
- recipient's MUA

supports S/MIME and has the sender's certificate and public key, which is necessary to decrypt the email. Otherwise, the recipient cannot read the email.

To configure a delivery rule

1. Go to *Policy* > *Access Control* > *Delivery*.
2. Either click *New* to add a policy, or double-click a policy to modify it.
3. Configure the following:

GUI item	Description
Status	Enable or disable the policy.
Sender	Select how you will define the sender email addresses (`MAIL FROM:`) in the SMTP envelope that match the policy, either: • *Email Group*: A group of email addresses configured on the FortiMail unit. In the dropdown list below this setting, select the group name. See also Configuring email groups on page 272. • *LDAP Group*: A group of email addresses configured on a directory server such as Microsoft Active Directory. In the text field and dropdown list below this setting, enter the group of recipient email addresses that is in the directory server, and select the LDAP profile that is used for the query. See also Configuring LDAP profiles on page 234. **Note**: In the LDAP query string, use `$m` to match sender email addresses. • *User (wildcard)*: An email address or wild card pattern that can match multiple email addresses. In the text field below the dropdown list, enter the pattern.

GUI item	Description
	Wild card characters can be used to match multiple email addresses. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*@example.???` matches all email addresses at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • *User (regex)*: A regular expression that can match multiple email addresses. In the text field below the dropdown list, enter the regular expression. **Tip:** To verify that the regular expression is valid and only matches the email addresses that you intend, click *Validate* See also Appendix: Wildcards and regular expressions on page 380 and Using wildcards and regular expressions with access control.
Recipient	Select how you will define the recipient email addresses (`RCPT TO:`) in the SMTP envelope that match the policy. Options are the same as Sender. **Note**: For the *LDAP Group* option, use `$m` in the LDAP query string to match recipient email addresses.
Destination	If you configured TLS profile, then select how you will define the destination IP addresses and netmasks that match the policy, either: • *IP/Netmask*: Enter the IP address and netmask. For example, you can enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. In the policy list, this appears as `10.10.10.0/24`, with the `0` indicating that any value is matched in that position of the address. Similarly, if you enter `10.10.10.10/32`, it appears as `10.10.10.10/32` because a 32-bit netmask only matches one address, 10.10.10.10 specifically. To match any IPv4 address, enter `0.0.0.0/0`; to match any IPv6 address, enter `::/0`; to match both IPv4 and IPv6 addresses, you must create two separate rules. • *IP Group*: Select an IP address group. See also Configuring IP groups on page 272.
TLS profile	If you want to allow or reject the connection based on whether the TLS profile matches the session, select a profile. • **Match**: Processing continues and delivery may occur. • **No match**: Action on failure in the TLS profile occurs. For details, see Configuring TLS security profiles on page 266.
Encryption profile	If you want to apply S/MIME or IBE encryption to the email, select a profile. See also Configuring encryption profiles on page 268, Configuring certificate bindings on page 328, and Configuring content action profiles on page 224. **Note:** If you select IBE in the content action profile (*Encrypt with profile*) but S/MIME in *Encryption profile*, then IBE is overridden and not used. *Destination* does not affect whether to apply *Encryption profile*.
Comment	Optional. Enter a description or comment. If a comment exists, it is displayed as a tool tip when you mouse-over the *ID* column in the list of rules in the GUI.

4. Click *Create*or *OK*.
5. If you want your new policy to be evaluated before another policy, click *Move* and put your new policy before the other policy in the list.

Initially, the policy appears at the end of the list of policies. List order indicates order of evaluation. As a result, the new policy will match an SMTP session only if no previous policy matches.

The policy *ID* number may be different from the order of evaluation.

Rate limiting for delivery

Administrators often block MTA IP addresses that send email at a high rate because this is a common trait of spammers. Because of this, marketing mail campaigns can accidentally cause your protected domains to be registered in a DNSBL.

To prevent this problem, you can rate limit email delivery, either for a specific sender email address in a protected domain (see Sender Address Rate Control on page 106), for an entire protected domain, or all domains protected by FortiMail.

When the FortiMail unit initiates an SMTP session, each delivery rate limit policy is compared to the domain name in the recipient email address (`RCPT TO:`) in the SMTP envelope. Policies are evaluated for a match in order, from top to bottom of the list. If a match does not exist, then the email is delivered with no rate control. If a match does exist, then the rate limit is applied. No subsequent delivery rate limit policies are applied. Only one delivery rate limit policy is applied to each SMTP session.

To configure a delivery control policy

1. Go to *Policy* > *Access Control* > *Delivery Control*.
2. Either click *New* to add a policy, or double-click a policy to modify it.
3. Configure the following settings, and then click *Create*.

GUI item	Description
Status	Enable or disable the policy.
Recipient domain	Enter a complete or partial domain name in recipient email addresses. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name.
Restrict the number of concurrent connections	Enter the maximum concurrent SMTP connections, or enter 0 to disable the limit. Valid range is 0-100.

GUI item	Description
Restrict the number of messages per connection	Enter the maximum number of email per SMTP connection, or enter 0 to disable the limit. Valid range is 0-1000.
Restrict the number of recipients per period (30 minutes)	Enter the maximum recipients per 30 minute time span, or enter 0 to disable the limit. Valid range is 0-1000000000.
Restrict the number of recipients per message	Enter the maximum recipients per email, or enter 0 to disable the limit. Valid range is 0-1000.

Controlling email based on IP addresses

The *IP Policies* section of the Policies tab lets you create policies that apply profiles to SMTP connections based on the IP addresses of SMTP clients and/or servers.

Due to the nature of relay in SMTP, an SMTP client is not necessarily always located on an email user's computer. The SMTP client is the connection initiator; it could be, for example, another email server or a mail relay attempting to deliver email. The SMTP server, however, is always a mail relay or email server that receives the connection.

For example, if computer A opened a connection to computer B to deliver mail, A is the client and B is the server. If computer B later opened a connection to computer A to deliver a reply email, B is now the client and A is now the server.

Like access control rules, IP-based policies can reject connections based on IP address.

Unlike access control rules, however, IP-based policies can affect email in many ways that occur **after** the session's `DATA` command, such as by applying antispam profiles. IP-based policies can also be overruled by recipient-based policies, and, if the FortiMail unit is operating in server mode, may match connections based on the IP address of the SMTP server, not just the SMTP client. For more information on access control rules, see Configuring access control receiving policies on page 148.

IP-based policies can apply in addition to recipient-based policies, although recipient-based policies have precedence if the two conflict **unless** you enable Take precedence over recipient based policy match.

To find both IP-based and recipient-based policies that match, see Policy Lookup on page 164.

For information about how recipient-based and IP-based policies are executed and how the order of policies in the list affects the order of execution, see How to use policies on page 145.

If SMTP traffic does not match any IP-based or recipient-based policy, it is allowed. However, no antivirus or antispam protection may be applied.
If you are certain that you have configured policies to match and allow all required traffic, you can tighten security by adding an IP policy at the bottom of the policy list to reject all other, unwanted connections.
To do this, create a new IP policy, enter `0.0.0.0/0` as the client IP/netmask, and set the action to *Reject*. See the following procedures about how to configure an IP policy. Then, move the policy to the very bottom of the IP policy list. Because this policy matches any connection, all connections that do not match any other policy will match this final policy, and be rejected.

Profiles used by the policy, if any, are listed in the policy table, and appear as linked text. To modify profile settings, click the name of the profile.

Domain administrators can create and modify IP-based policies. Because they can affect any IP address, a domain administrator could therefore create a policy that affects another domain. If you do not want to allow this, do **not** grant Read-Write permission to the Policy category in domain administrators' access profiles.

For details, see About administrator account permissions on page 67.

To configure an IP-based policy

1. Go to *Policy* > *IP Policy* > *IP Policy*.
2. Select New to add a policy or double-click a policy to modify it.
   A dialog appears that varies with the operation mode.
3. Configure the following settings and then click *Create*.

GUI item	Description
Enable	Enable or disable the policy.
Source	You can use the following types of IP addresses of the SMTP clients to whose connections this policy will apply: • IP address and subnet mask • IP group. See Configuring IP groups on page 272. • GeoIP group. See Configuring GeoIP groups on page 273. • ISDB To match all IPv4 clients, enter `0.0.0.0/0`; to match all IPv6 clients, enter `::/0`; to match both IPv4 and IPv6 clients, you must create two separate policies.
Reverse DNS pattern	To define which SMTP clients match this policy, depending on whether you enable *Regular Expression*, enter either a: • Complete or partial domain name. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other "example" domain ending with a three-letter top-level domain name.

GUI item	Description
	• Regular expression. **Tip:** To verify syntax and correct matching, click *Validate*. See also Appendix: Wildcards and regular expressions on page 380 and Using wildcards and regular expressions with access control on page 153. Because the domain name in the SMTP session greeting (`HELO/EHLO`) is self-reported by the connecting SMTP client, it could be fake and the FortiMail unit does not trust it. Instead, the FortiMail does a reverse DNS lookup of the SMTP client's IP address to discover its real domain name. This is compared to the pattern. If the domain name does not match the pattern, or if the reverse DNS query fails, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, `.lab` is not valid because it is reserved for testing on private networks, not the Internet, and thus a reverse DNS query to DNS servers on the Internet will always fail.
Destination	***Warning***: For FortiMail Cloud users, keep the default setting as 0.0.0.0/0. Do not configure this field.
Action	Select whether to: • *Scan*: Accept the connection and perform any scans configured in the profiles selected in this policy. • *Reject*: Reject the email and respond to the SMTP client with SMTP reply code 550, indicating a permanent failure. • *Fail Temporarily*: Reject the email and respond to the SMTP client with SMTP reply code 451, indicating to try again later. • *Proxy Bypass*: Bypass the FortiMail proxy without scanning. This action is available only if FortiMail is in transparent mode.
Comment	Optional. Enter a description or comment. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.

Profile		
	Session	Select the name of a session profile to have this policy apply. This option is applicable only if Action is *Scan*. **Caution**: If you are configuring an IP-based policy in transparent mode, you **must** select a session profile for the policy to work.
	AntiSpam	Select the name of an antispam profile to have this policy apply. This option is applicable only if Action is *Scan*.
	AntiVirus	Select the name of an antivirus profile to have this policy apply. This option is applicable only if Action is Scan.
	Content	Select the name of a content profile to have this policy apply. This option is applicable only if Action is *Scan*.
	DLP (if DLP is enable on GUI)	Select the name of a DLP profile to have this policy apply. This option is applicable only if Action is *Scan*.
Authentication and Access (not available in server mode)		This section appears only if the FortiMail unit is operating in gateway or transparent mode. For server mode, select a resource profile instead.

		For more information on configuring authentication, see Workflow to enable and configure authentication of email users on page 230.
	Authentication type	If you want the email user to authenticate using an external authentication server, select the authentication type of the profile (SMTP, POP3, IMAP, RADIUS, or LDAP). **Note:** In addition to specifying an authentication server for SMTP email messages that this policy governs, configuring Authentication profile on page 169 also allows email users to authenticate when accessing their per-recipient quarantine using HTTP or HTTPS. For more information, see How to enable, configure, and use personal quarantines on page 44.
	Authentication profile	Select an existing authentication profile to use with this policy. Click New to create on or Edit to modify the selected profile.
	Allow SMTP authentication	Enable to allow the SMTP client to use the SMTP `AUTH` command, and to use the server defined in Authentication profile on page 169 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile on page 169. **Note:** Enabling this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication. For details, see Configuring access control receiving policies on page 148.
Miscellaneous		
	Reject different SMTP sender identity for authenticated user	Enable to require that the sender uses the same identity for: authentication name, SMTP envelope `MAIL FROM:`, and header `FROM:`. Disable to remove such requirements on sender identities. By default, this feature is disabled.
	Sender identity verification with LDAP server	In some cases, while you do not want to allow different SMTP sender identities for an authenticated user, you still want to: • allow users to authenticate with their identities (for example, user1@example.com) and send email from their proxy email addresses (for example, user1.name@example.com and user1name@example.com) • or to allow users in an alias group to authenticate with their own identities (for example, salesperson1@example.com) and send email from their alias group address (for example, sales@example.com) Then you can choose to verify the sender identity with the LDAP server. If the verification is successful, the sender will be allowed to send email with different identities. **Note**: When the above rejection option is enabled, even though the authentication identity can be different from the sender identity upon successful LDAP verification. the envelope (`MAIL FROM:`)address is never allowed to be different from the header `FROM:`)address. And the two addresses cannot be empty either.

Take precedence over recipient based policy match	Enable to omit use of recipient-based policies for connections matching this IP-based policy. For information on how policies are executed, see How to use policies on page 145. Note that if there is no authentication profile in a recipient based policy, but there is an authentication profile in an IP-based policy, SMTP authentication can still succeed without this feature enabled. This option is applicable only if Action is *Scan*. **Note:** Enabling this option also causes the FortiMail unit to ignore the option Configuring protected domains on page 92 in the protected domain.

See also

Example: Strict and loose IP-based policies

Example: Strict and loose IP-based policies

You have a FortiMail unit running in gateway mode to protect your internal mail server (192.168.1.1). The FortiMail unit receives email incoming to, and relays email from, the internal mail server.

You can create two IP-based policies:

- Policy 1: Enter `192.168.1.1/32` as the source IP address and `0.0.0.0/0` as the destination to match outgoing email connections from the mail server, and select a **loose** session profile, which may have sender reputation and other similar restrictions disabled, since the sender (that is, source IP) will always be your mail server.
- Policy 2: Enter `0.0.0.0/0` as the source IP address and `0.0.0.0/0` as the destination IP address to match incoming email connections from all other mail servers, and select a **strict** session profile, which has all antispam options enabled.

You would then move policy 1 above policy 2, as policies are evaluated for a match with the connection in order of their display on the page.

See also

Controlling email based on IP addresses

Controlling SMTP access and delivery

Controlling email based on sender and recipient addresses

Go to *Policy* > *Recipient Policy* > *Inbound* or *Policy* > *Recipient Policy* > *Outbound* to create recipient-based policies based on the incoming or outgoing directionality of an email message with respect to the protected domain.

Recipient-based policies have precedence if an IP-based policy is also applicable, but conflicts. Exceptions include IP-based policies where you have enabled Take precedence over recipient based policy match on page 163. For information about how recipient-based and IP-based policies are executed and how the order of polices affects the execution, see How to use policies on page 145.

If the FortiMail unit protects many domains, and therefore creating recipient-based policies would be very time-consuming, such as it might be for an Internet service provider (ISP), consider configuring **only** IP-based policies. For details, see Controlling email based on IP addresses on page 159.
Alternatively, consider configuring recipient-based policies **only** for exceptions that must be treated differently than indicated by the IP-based policy.

Profiles used by the policy, if any, are listed in the policy table, and appear as linked text. To modify profile settings, click the name of the profile.

GUI item	Description
Move (button)	Arrange policies in the policy list by placing the most specific policy at the top and more general policies at the bottom. See also Order of execution of policies on page 146. To move a policy in the policy list: **1.** In Domain, select a protected domain or system-wide scope. **Note**: If *Domain* is *All*, then the *Move* button is disabled. To move domain-level policies, you must disable *Show system policy*. See also About the default system-level recipient policy on page 170. **2.** Click a policy to select it. **3.** Click *Move*, then select either: • *Up* or *Down* (the direction in which to move the selected policy), or • *After* or *Before*, then in *Move right after* or *Move right before* indicate the policy's new location by entering the ID of another policy. **4.** To test whether email will match the policy in the new position, use Policy Lookup.
Policy Lookup (button)	Click to test which recipient and/or IP-based policy will match an email or SMTP connection. **1.** In *Lookup option*, select the either *Email Scan* or *Authentication & Resource* to simulate a policy match for either protection profile or authentication and webmail resource purposes. **2.** Configure the following: • *Sender IP address*: Enter a source IP address, or, to find policies that match any IP address, enter `0.0.0.0` (for IPv4) or `::` (for IPv6). • *Sender email address*: Enter an email address, or, to find policies that match multiple email addresses, enter a partial address with a wild card (`*@example.com`). This setting appears only If *Lookup option* is *Email Scan*. • *Recipient email address*: Enter an email address, or, to find policies that match multiple email addresses, enter a partial address with a wild card (`*@example.com`). **Note:** During authentication, email is sent from a protected domain, and so *Recipient email address* is actually compared to the sender email address —

GUI item	Description
	not the recipient. **Tip:** Do not enter a wild card only(*) in *Recipient email address*. It is a valid expression, but in reality, each email address has a direction (inbound or outbound) and therefore will match a different recipient-based policy: inbound or outbound. To test accurately, try both directions: • a wild card then an external domain name (outbound) • a wild card then a protected domain name (inbound) **3.** Click *OK*. Results show the matching IP-based and/or recipient-based policies, if any. To view a policy, click its link. **Note:** Policy lookup results do not include policies whose *Status* is *Disabled*. Results may be different for *Email Scan* or *Authentication & Resource*, even if the *Sender IP address* and *Recipient email address* search criteria are the same. For details, see Order of execution of policies on page 146.
Domain (dropdown list)	Select which policies to display, either: • *All*: Both system-level and domain-level policies (unless you disable Show system policy). • *System*: Only system-wide policies. • Only the policies that belong to a specific protected domain. If you are an administrator that is assigned to a protected domain, then you can only see the policies that are permitted by your administrator profile.
Show system policy	Enable or disable to show or hide system-wide policies when you view the list of policies. This button appears only if Domain is *All*or a protected domain.
Enabled	Select whether or not the policy is currently in effect.
ID	Displays the number identifying the policy. If a comment is added to this rule when the rule is created, the comment will show up as a mouse-over tool-tip in this column. **Note:** The ID may be different from the order in the list, which indicates order of comparison for a match. For details, see Order of execution of policies on page 146
Domain Name (column)	Indicates which part the policy is used for: either system wide or a specific protected domain.
Sender Pattern	A sender email address (`MAIL FROM:`) as it appears in the envelope or a regular expression pattern to match sender email addresses. See also Syntax on page 381.
Recipient Pattern	A recipient email address (`RCPT TO:`) as it appears in the envelope or a regular expression pattern to match recipient email addresses. See also Syntax on page 381.
AntiSpam	Displays the antispam profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring antispam profiles on page 187.
AntiVirus	Displays the antivirus profile selected for the matching recipients.

GUI item	Description
	To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring antivirus profiles, file signatures, and actions on page 209.
Content	Displays the content profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring content profiles on page 216.
DLP (if DLP is enable on GUI)	Displays the DLP profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring data loss prevention on page 332.
Resource (server mode and gateway mode)	Displays the resource profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring resource profiles on page 228.
Authentication (not in server mode; inbound only)	Displays the authentication profile selected for the matching recipients. To modify or view a profile, click its name.The profile appears in a pop-up window. For details, see Configuring authentication profiles on page 231 or Configuring LDAP profiles on page 234.

To configure recipient-based policies

1. Before you can configure a recipient policy, you must configure:
   - at least one protected domain (see Configuring protected domains on page 92)
   - at least one user group or LDAP profile with a configured group query, if you will use either to define which recipient email addresses will match the policy (see Managing users on page 110 or Configuring LDAP profiles on page 234)
   - at least one PKI user, if you will allow or require email users to access their per-recipient quarantine using PKI authentication (see Managing users on page 110)
2. Go to *Policy* > *Recipient Policy* > *Inbound* or .*Policy* > *Recipient Policy* > *Outbound*.
3. Either click *New* to add a policy or double-click a policy to modify it.
4. Select *Enable* to determine whether or not the policy is in effect.
5. For *Domain*, select either *System* or the protected domain name that this profile belongs to.
6. Optionally, enter a comment.
   The comment will appears as a mouse-over tool-tip in the ID column of the rule list.
7. Configure the following sections:
   - Configuring the sender and recipient patterns on page 166
   - Configuring the profiles section of a recipient policy on page 168
   - Configuring authentication for inbound email on page 168
   - Configuring the advanced settings of inbound policies on page 169

Configuring the sender and recipient patterns

Configure the *Sender* and *Recipient* sections.

GUI item	Description
Type	Select one of the following ways to define sender or recipient email addresses that match this policy: • *User (wildcard)*: Enter a sender/recipient email address. Wild card characters allow you to enter patterns that can match multiple email addresses. The asterisk (*) represents one or more characters and the question mark (?) represents any single character. • *User (regex)*: Enter a sender/recipient as a regular expression pattern, such as: `.*@example\.com` Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. See also Syntax on page 381. • *Local group (server mode only)*: Select the name of a protected domain in the second dropdown list, then select the name of a user group in the first dropdown list. • *LDAP Group*: Select an LDAP profile in which you have enabled and configured a group query, then enter either the group's full or partial membership attribute value as it appears in the LDAP directory. Depending on your LDAP directory's schema, and whether or not you have enabled Use group name with base DN as group DN, this may be a value such as `1001`, `admins`, or `cn=admins,ou=Groups,dc=example,dc=com`. • *Email Group*: Select an email group from the dropdown list. For details about creating an email group, see Configuring email groups on page 272.
Option	This option appears only if you have the Advancement Management license and enable it with the following CLI command: `config system advanced-management` `set recipient-policy-sender-option {envelope-from-only | envelope-or-header-from}` `end` By default, the recipient policy uses Envelope From as the sender. If `envelope-or-header-from` is set, you can choose to use either Envelope From or Header From as the sender for recipient policy match.

Configuring the recipient exclusion list

If you want to exclude any recipients from the policy, add them to the exclusion list under the *Recipient Exclusion* section.

GUI item	Description
Status	Enable/disable the exclusion list.
Type	Select one of the following ways to define recipient email addresses to be excluded from this policy: • *User (wildcard)*: Enter the recipient email address.Wild card characters allow you to enter patterns that can match multiple email addresses. The asterisk (*) represents one or more characters and the question mark (?) represents any single character.

GUI item	Description
	• *User (regex)*: Enter a recipient as a regular expression pattern, such as: `.*@example\.com` Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. See also Syntax on page 381. • *Email Group*: Select an email group from the dropdown list. For details about creating an email group, see Configuring email groups on page 272.

Configuring the profiles section of a recipient policy

Select the profiles that you want to apply to the policy. If you have created a system profile and a domain profile with the same profile name, the profile that appears in the profile dropdown lists is the domain profile, not the system profile. Thus, only the domain profile will be selected.

GUI item	Description
AntiSpam	Select which antispam profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring antispam profiles on page 187. **Tip:** You can use an LDAP query to enable or disable antispam scanning on a per-user basis.
AntiVirus	Select which antivirus profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring antivirus profiles, file signatures, and actions on page 209.
Content	Select which content profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring content profiles on page 216.
DLP (if enabled)	Select which DLP profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring DLP profiles on page 334.
Resource (server mode and gateway mode)	Select which resource profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click *New* to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click *Edit*. For details, see Configuring resource profiles on page 228.

Configuring authentication for inbound email

The Authentication and Access section appears only for inbound policies.

When FortiMail authenticates a user, it checks the authentication profile in the matching recipient policy.

Note that for outbound email, when FortiMail requires authentication with the sender, FortiMail will lookup authentication profiles for the defined recipient patterns within inbound policies.

For more information on configuring an authentication profile, see Workflow to enable and configure authentication of email users on page 230.

GUI item	Description
Authentication type	If you want the email user to authenticate using an external authentication server, select the type of the authentication profile (SMTP, POP3, IMAP, RADIUS, LDAP, or LOCAL for server mode). **Note:** In addition to specifying an authentication server for SMTP email messages that this policy governs, configuring Authentication profile on page 169 also allows email users to authenticate when accessing their per-recipient quarantine using HTTP or HTTPS. For more information, see How to enable, configure, and use personal quarantines on page 44.
Authentication profile	Select an existing authentication profile to use with this policy.
Allow SMTP authentication (gateway and transparent mode only)	Enable to allow the SMTP client to use the SMTP `AUTH` command, and to use the server defined in Authentication profile to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile. **Note:** Enabling this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication. For details, see Configuring access control receiving policies on page 148.

Configuring the advanced settings of inbound policies

The Advanced Setting section appears for both inbound and outbound policies.

GUI item	Description
Reject different SMTP sender identity for authenticated user	Enable to require that the sender uses the same identity for: authentication name, SMTP envelope `MAIL FROM:`, and header `FROM:`. Disable to remove such requirements on sender identities. By default, this feature is disabled.
Sender identity verification with LDAP server for authenticated user	In some cases, while you do not want to allow different SMTP sender identities for an authenticated user, you still want to: • allow users to authenticate with their identities (for example, user1@example.com) and send email from their proxy email addresses (for example, user1.name@example.com and user1name@example.com) • or to allow users in an alias group to authenticate with their own identities (for

GUI item	Description
	example, salesperson1@example.com) and send email from their alias group address (for example, sales@example.com) Then you can choose to verify the sender identity with the LDAP server. If the verification is successful, the sender will be allowed to send email with different identities. **Note**: When the above rejection option is enabled, even though the authentication identity can be different from the sender identity upon successful LDAP verification. the envelope (`MAIL FROM:`)address is never allowed to be different from the header `FROM:`)address. And the two addresses cannot be empty either.
Enable PKI authentication for web mail access **(Inbound policy only)**	Enable if you want to allow web mail users to log in by presenting a certificate rather than a user name and password. Also configure Certificate validation is mandatory on page 170. For more information on configuring PKI users and what defines a valid certificate, see Managing users on page 110.
Certificate validation is mandatory **(Inbound policy only)**	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enable this option.

About the default system-level recipient policy

In *Domain*, if you select *All*, and then enable *Show system policy*, then system-level policies are visible. There is a default system-level policy. If its position is above other policies, then when an email arrives, the default policy will be evaluated for a match before other policies, and other policies will not apply.

Like other system-level policies, an administrator with system-wide permissions can edit this default policy. This provides the following conveniences:

- If many domains need identical policies, it can be simpler and faster to modify a system-level policy instead.
- When troubleshooting, you can temporarily move this system-level policy before other policies to use it for all protected domains while you examine other profiles and policies.

Configuring profiles

The *Profile* menu lets you configure many types of profiles. These are a collection of settings for antispam, antivirus, authentication, or other features.

After creating and configuring a profile, you can apply it either directly in a policy, or indirectly by inclusion in another profile that is selected in a policy. Policies apply each selected profile to all email messages and SMTP connections that the policy governs.

Creating multiple profiles for each type of policy lets you customize your email service by applying different profiles to policies that govern different SMTP connections or email users. For instance, if you are an Internet service provider (ISP), you might want to create and apply antivirus profiles only to policies governing email users who pay you to provide antivirus protection.

Configuring session profiles

Session profiles focus on the connection and envelope portion of the SMTP session. This is in contrast to other types of profiles that focus on the message header, body, or attachments.

To configure session profiles

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to add a profile or double-click a profile to modify it.
3. For a new session profile, type the name in *Profile name*. The profile name is editable later.
4. Configure the following sections:
   - Configuring connection settings on page 171
   - Configuring sender reputation options on page 173
   - Configuring endpoint reputation options on page 175
   - Configuring sender validation options on page 176
   - Configuring session settings on page 177
   - Configuring unauthenticated session settings on page 179
   - Configuring SMTP limit options on page 181
   - Configuring error handling options on page 182
   - Configuring header manipulation options on page 182
   - Configuring list options on page 183
   - Configuring advanced MTA control settings on page 184

Configuring connection settings

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Expand the *Connection Setting* section. The options vary with the operation mode.
4. Configure the following options to restrict the number and duration of connections to the FortiMail unit. When any of these limits are exceeded, the FortiMail unit blocks further connections.

GUI item	Description
Hide this box from the mail server (transparent mode only)	Enable to preserve the IP address or domain name of the SMTP client in the: • SMTP greeting (`HELO`/`EHLO`) and in the `Received:` message headers of email messages • client IP in email header This masks the existence of the FortiMail unit to the protected SMTP server. Disable to replace the SMTP client's IP addresses or domain names with that of the FortiMail unit. **Note:** Unless you enabled *Take precedence over recipient based policy match* in the IP-based policy, the *Hide the transparent box* option in the protected domain supersedes this option, and may prevent it from applying to incoming email messages. **Note:** For full transparency, also enable Configuring protected domains on page 92.
Restrict the number of connections per client per 30 minutes to	Specify the maximum connections per client IP address in a period of 30 minutes. 0 means no limit.
Restrict the number of messages per client per 30 minutes to	Specify the maximum email messages (number of senders in the SMTP envelope (`MAIL FROM:`)) a client can send in a period of 30 minutes. 0 means no limit.
Restrict the number of recipients per client per 30 minutes to	Specify the maximum recipients (number of recipients in the SMTP envelope (`RCPT TO:`)) a client can send email to for a period of 30 minutes. 0 means no limit.
Maximum concurrent connections for each client	Enter the maximum number of concurrent connections per client. 0 means no limit.
Connection idle timeout (seconds)	Enter a limit to the number of seconds a client may be idle before the FortiMail unit drops the connection. Set the value between 5-1200.
Do not let client connect to blocklisted SMTP servers (transparent mode only)	Enable to prevent clients from connecting to SMTP servers that have been blocklisted in antispam profiles or, the FortiGuard AntiSpam service if enabled. **Note:** This option applies only if you have enabled Use client-specified SMTP server to send email, and only for outgoing connections.

Configuring sender reputation options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

You can also view the sender reputation statuses by going to *Monitor* > *Sender Reputation*. See Viewing sender reputation statuses on page 60.

To configure sender reputation options

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click to expand *Sender Reputation*.

   Sender reputation is a predominantly automatic antispam feature, requiring little or no maintenance. For each connecting SMTP client (sometimes called a sender), the sender reputation feature records the sender IP address and the number of good email and bad email from the sender.

   In this case, bad email is defined as:

   - Spam
   - Virus-infected
   - Unknown recipients
   - Invalid DKIM
   - Failed SPF check

   Sender reputation scores can be affected by sender validation results.

   Enabling sender reputation can improve performance by rejecting known spammers before more resource-intensive antispam scans are performed.

4. Configure the following:

GUI item	Description
Enable sender reputation	Enable to accept or reject email based upon sender reputation scores. The following options have no effect unless this option is enabled. This option may not function well for SMTP clients with dynamic IP addresses. Instead, consider “Enable Endpoint Reputation” on page 316.
Throttle client at	Enter a sender reputation score over which the FortiMail unit will rate limit the number of email messages that can be sent by this SMTP client. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increases or decreases the sender reputation scores accordingly.

GUI item		Description
		The enforced rate limit is either *Restrict number of emails per hour to n* or *Restrict email to n percent of the previous hour*, whichever value is greater. After the sender reaches the limit, no more incoming email will be accepted.
	Restrict number of email per hour to	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client.
	Restrict email to ... percent of the previous hour	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client, as a percentage of the number of email messages that the SMTP client sent during the previous hour.
	Temporarily fail client at	Enter a sender reputation score over which the FortiMail unit will return a temporary failure error when the SMTP client attempts to initiate a connection. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increase or decrease the sender reputation scores accordingly.
	Reject client at	Enter a sender reputation score over which the FortiMail unit will reject the email and reply to the SMTP client with SMTP reply code 550 when the SMTP client attempts to initiate a connection. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increase or decrease the sender reputation scores accordingly.
FortiGuard IP reputation check		If you want the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted, enable this option. If the SMTP client IP address is a private one, the FortiMail unit will query the FortiGuard Antispam service to determine if the first public IP address in the header is blocklisted. • *Use AntiSpam profile settings*: In an antispam profile, you can also enable or disable FortiGuard IP reputation checking. This action happens after the entire message has been received by FortiMail. For details, see FortiGuard section on page 189. • *Use AntiSpam profile settings (no authentication)*: Use antispam profile settings but disable SMTP authentication when the client IP reputation score triggers the threshold. • *When client connects*: Enable to query the FortiGuard Antispam Service to determine if the IP address of the SMTP server is blocklisted. And this action will happen during the connection phase. Therefore, if this feature is enabled in a session profile and the action is reject, the performance will be improved. FortiGuard categorizes the blocklisted IP addresses into three levels -- level 3 has bad reputation; level 2 has worse reputation; and level 1 has the worst reputation. To help prevent false positives, you can choose which level to block with the following CLI commands:

GUI item	Description
	``config system fortiguard antispam set threshold-ip-connect <integer> end``` <integer> is the level number: 1, 2, or 3. The default setting is 3, which means all levels will be blocked. If you want to block level 1 and level 2 but not level 3, then you set it to 2. • *Disable*: Skip FortiGuard IP reputation check, even this is enabled in an antispam profile.

Configuring endpoint reputation options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Endpoint Reputation*.

   The *Endpoint Reputation* settings let you restrict, based upon its endpoint reputation score, the ability of an MSISDN or subscriber ID to send email or MM3 multimedia messaging service (MMS) messages from a mobile device. The MSISDN reputation score is similar to a sender reputation score.

   For more on endpoint reputation-based behavior, see About endpoint reputation.

   Enabling endpoint reputation can improve performance by rejecting known spammers before more resource-intensive antispam scans are performed.

4. Configure the following:

GUI item	Description
Enable Endpoint Reputation	Enable to accept, monitor, or reject email based upon endpoint reputation scores. This option is designed for use with SMTP clients with dynamic IP addresses. It requires that your RADIUS server provide mappings between dynamic IP addresses and MSISDNs/subscriber IDs to the FortiMail unit. If this profile governs sessions of SMTP clients with static IP addresses, instead see Configuring sender reputation options on page 173.
Action	Select either: • *Reject*: Reject email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed *Auto blocklist score trigger value*. • *Monitor*: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed *Auto blocklist score trigger value*. Entries appear in the history log.

GUI item	Description
Auto blocklist score trigger value	Enter the MSISDN reputation score over which the FortiMail unit will add the MSISDN/subscriber ID to the automatic blocklist. The trigger score is relative to the period of time configured as the automatic blocklist window. For more information on the automatic blocklist window, see Configuring the endpoint reputation score window.
Auto blocklist duration	Enter the number of minutes that an MSISDN/subscriber ID will be prevented from sending email or MMS messages after they have been automatically blocklisted.

Configuring sender validation options

Validation results are used to adjust the sender reputation scores, MSISDN reputation scores, and deep header scans. Failure to validate does not guarantee that an email is spam, just as successful validation does not guarantee that an email is not spam, but it may help to indicate spam.

Enable sender validation to improve performance by rejecting invalid senders before more resource-intensive antispam scans are performed.

Sender validation may examine signatures in the email's message headers and/or the domain name's DNS records. If they do not exist, then the result cannot be determined, and therefore FortiMail skips that check.

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to modify it.
3. Expand *Sender Validation*.
4. Configure the following:

GUI item	Description
SPF check	Select either: • *Enable*: Validate the SMTP client IP address using SPF. For details, see SPF section on page 191. • *Disable*: Do not use SPF validation, unless SPF section is enabled in the antispam profile. • *Bypass*: Do not use SPF validation.
Enable DKIM check	Enable to validate the DKIM signature. For details, see DKIM and ARC Setting on page 102.
Enable DKIM signing for outgoing message	Enable to sign **outgoing** email with a DKIM signature. For details, see DKIM and ARC Setting on page 102.

GUI item	Description
Enable DKIM signing for authenticated sender only	Enable to sign **outgoing** email with a DKIM signature only if the sender is authenticated.
Enable domain key check	Enable to validate the DomainKeys signature. DomainKeys is a predecessor of DKIM and works in the same way. For details, see DKIM and ARC Setting on page 102. Because some domains still use DomainKeys validation, it is provided for backward compatibility.
Bypass bounce verification check	Enable to omit verification of bounce address tags on **incoming** bounce messages. **Note:** This setting does not omit bounce address tagging of **outgoing** messages. See also Configuring bounce verification and tagging on page 308.
Sender address verification with LDAP	Enable to validate sender email addresses with a query an LDAP server, then select an LDAP profile from the dropdown list. See also Configuring LDAP profiles on page 234.

Configuring session settings

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Session Setting*.
4. Configure the following:

GUI item	Description
Session action	Select an action profile or click *New* to create a new one. The session action profile uses the content action profile. For more information about actions, see Configuring content action profiles on page 224.
Message selection	The action can be applied to All messages or Accepted messages only. For example, for header manipulation, tagging, some other actions, you can choose to apply them to the accepted message only.
Reject EHLO/HELO command with invalid character in the domain	Enable to return SMTP reply code 501, and to reject the SMTP greeting, if the client or server uses a greeting that contains a domain name with invalid characters. To avoid disclosure of a real domain name, spammers sometimes spoof an SMTP greeting domain name with random characters, rather than using a valid domain name. The following example shows invalid command in bold: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT` **`EHLO ^^&^&^#$`** `501 5.0.0 Invalid domain name` Valid characters for domain names include: • alphanumerics (A to Z and 0 to 9)

GUI item	Description
	• brackets ([and]) • periods (.) • dashes (-) • underscores (_) • number symbols(#) • colons (:)
Rewrite EHLO/HELO domain to [n.n.n.n] IP string of the client address (transparent mode only)	Enable to rewrite the domain name in the SMTP greeting (HELO/EHLO) to the IP address of the client to prevent domain name spoofing.
Rewrite EHLO/HELO domain to (transparent mode only)	Enable to rewrite the domain name in the SMTP greeting (HELO/EHLO) to the specified value.
Prevent encryption of the session (transparent mode only)	Enable to block STARTTLS/MD5 commands so that email connections cannot be TLS-encrypted. **Caution:** Disable this option only if you trust that SMTP clients connecting using TLS through the FortiMail unit will not be sources of viruses or spam. FortiMail units operating in transparent mode cannot scan encrypted connections traveling through them. Disabling this option could thereby permit viruses and spam to travel through the FortiMail unit.
Allow pipelining for the session	Enable to allow SMTP command pipelining. This lets multiple SMTP commands to be accepted and processed simultaneously, improving performance for high-latency connections. Disable to allow the SMTP client to send only a single command at a time during an SMTP session.
Enforce strict RFC compliance (transparent mode only)	Enable to limit pipelining support to strict compliance with RFC 2920, SMTP Service Extension for Command Pipelining. This option is effective only if *Allow pipelining for the session* is enabled.
Perform strict syntax checking	When the client or server uses SMTP commands with syntax errors (such as incorrect command sequences, invalid email addresses, and extra spaces in parameters), FortiMail returns an SMTP reply code and reject the SMTP command. When strict syntax checking is enabled, FortiMail also checks if the MAIL FROM: and RCPT TO: addresses are inclosed with angle brackets, such as <user@example.com>: `RCPT TO:user@example.com` `553 5.1.2 user@example.com... Invalid email address`

GUI item	Description
Switch to SPLICE mode after (transparent mode only)	Enable to use splice mode. Enter threshold value based on time (seconds) or data size (kilobytes). Splice mode lets the FortiMail unit simultaneously scan an email and relay it to the SMTP server. This increases throughput and reduces the risk of server timeout. If it detects spam or a virus, it terminates the server connection and returns an error message to the sender, listing the spam or virus name and infected file name.
ACK EOM before AntiSpam check	Enable to acknowledge the end of message (EOM) signal immediately after receiving the carriage return and line feed (CRLF) characters that indicate the EOM, rather than waiting for antispam scanning to complete. If the FortiMail unit does not complete antispam scanning within 4 minutes, it returns SMTP reply code `451(Try again later)`, resulting in no permanent problems, since according to RFC 2821, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail unit to acknowledge the EOM command. Enabling this option prevents those rare cases.

Configuring unauthenticated session settings

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Unauthenticated Session Setting* section.
4. Configure the following:

GUI item	Description
Check HELO/EHLO domain	Enable to return SMTP reply code 501, and reject the SMTP command, if the domain name accompanying the SMTP greeting is not a domain name that exists in either MX or A records.In the following example, the invalid command is highlighted in bold: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT` **`EHLO example.com`**
Check sender domain	Enable to return SMTP reply code 421, and reject the SMTP command, if the domain name portion of the sender address is not a domain name that exists in either MX or A records. The following example shows the invalid command in bold italics: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT` `EHLO` `250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you` **`MAIL FROM:<user1@example.com>`** `421 4.3.0 Could not resolve sender domain.`
Check recipient domain	Enable to return SMTP reply code 550, and reject the SMTP command, if the domain name portion of the recipient address is not a domain name that exists in either MX or A records.

GUI item	Description
	The following example shows the invalid command in bold italics: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:48:32 GMT` `EHLO example.com` `250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you` `MAIL FROM:<user1@fortinet.com>` `250 2.1.0 <user1@fortinet.com>... Sender ok` **`RCPT TO:<user2@example.com>`** `550 5.7.1 <user2@example.com>... Relaying denied. IP name lookup failed [192.168.1.1]`
Reject empty domain	Enable to return SMTP reply code 553, and reject the SMTP command, if the `HELO`/`EHLO` greeting does not have a domain, or the sender address (`MAIL FROM:`) is empty. The following example shows the invalid command in bold: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 20 Nov 2013 10:42:07 -0500` **`ehlo`** `250-FortiMail-400.localdomain Hello [172.20.140.195], pleased to meet you` `250-ENHANCEDSTATUSCODES` `250-PIPELINING` `250-8BITMIME` `250-SIZE 10485760` `250-DSN` `250-AUTH LOGIN PLAIN` `250-STARTTLS` `250-DELIVERBY` `250 HELP` `mail from:aaa@333` `550 5.5.0 Empty EHLO/HELO domain.` `quit` `221 2.0.0 FortiMail-400.localdomain closing connection`
Prevent open relaying (transparent mode only)	Enable to prevent clients from using open relays to send email by blocking sessions that are unauthenticated (Unauthenticated sessions are assumed to be occurring to an open relay). If you permit SMTP clients to use open relays to send email, email from your domain could be blocklisted by other SMTP servers. This option is effective only if you have enabled Use client-specified SMTP server to send email for outgoing mail. Otherwise, the FortiMail unit forces clients to use the gateway you have defined as a relay server (see Configuring SMTP relay hosts), if any, or the MTA of the domain name in the recipient email address (`RCPT TO:`), as determined using an MX lookup, so it is not possible for them to use an open relay.
Reject if recipient and helo domain match but sender domain is different	Enable to reject the email if the domain name in the SMTP greeting (`HELO`/`EHLO`) and recipient email address (`RCPT TO:`) match, but the domain name in the sender email address (`MAIL FROM:`) does not. Mismatching domain names is sometimes used by spammers to mask the true identity of their SMTP client. **Note**: This option should not be used if you have Microsoft 365 and would like to send email to other Microsoft 365 tenants (private or business).

Configuring SMTP limit options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *SMTP Limit*.
   Setting any of these values to 0 disables the limit.
4. Configure the following:

GUI item	Description
Restrict number of EHLO/HELOs per session to	Enter the limit of SMTP greetings that a connecting SMTP server or client can perform before the FortiMail unit terminates the connection. Restricting the number of SMTP greetings allowed per session makes it more difficult for spammers to probe the email server for vulnerabilities (more attempts results in a greater number of terminated connections, which must then be re-initiated).
Restrict number of email per session to	Enter the limit of email messages per session to prevent mass mailing.
Restrict number of recipients per email to	Enter the limit of recipients to prevent mass mailing.
Cap message size (KB) at	Enter the limit of the message size. Messages over the threshold size are rejected. **Note:** When you configure domain settings under *Domain & User* > *Domain*, you can also set the message size limit. Here is how the two settings work together: • For outgoing email (for information about email directions, see Inbound versus outbound email on page 145), only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. FortiMail will use the smaller size.
Cap header size (KB) at	Enter the limit of the message header size. Messages with headers over the threshold size are rejected.
Maximum number of NOOPs allowed for each connection	Enter the limit of `NOOP` commands permitted per SMTP connection. Some spammers use `NOOP` commands to keep a long connection alive. Legitimate connections usually require few `NOOP`s.

GUI item	Description
Maximum number of RSETs allowed for each connection	Enter the limit of RSET commands permitted per SMTP connection. Some spammers use RSET commands to try again after receiving error messages such as unknown recipient. Legitimate connections should require few RSETs.

Configuring error handling options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Error Handling*.

   Configure *Error Handling* to specify how the FortiMail unit should handle connections from SMTP clients that are error-prone. Errors sometime indicate attempts to misuse the server. You can impose delays or drop connections if there are errors. Setting any of these values to 0 disables the limit.

   Configuring error handling can improve performance by dropping connections with error-prone SMTP clients.

4. Configure the following:

GUI item	Description
Number of 'free' errors allowed for each connection	Enter the number of errors permitted before the FortiMail unit imposes a delay.
Delay for the first non-free error (seconds)	Enter the delay time for the first error after the number of **free** errors is reached.
Delay increment for subsequent errors (seconds)	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.
Maximum number of errors allowed for each connection	Enter the total number of errors the FortiMail unit accepts before dropping the connection. By default, five errors are permitted before the FortiMail unit drops the connection.

Configuring header manipulation options

Email processing software can add lines to the message header of each email message. When multiple lines are added, this can significantly increase the size of the email message. You can configure FortiMail to delete message headers that are not needed. This can improve the speed of email throughput and reduce disk space usage.

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Expand the *Header Manipulation* section.
4. Configure the following:

GUI item	Description
Received:	Enable to remove all `Received:` message headers that have been inserted by other MTAs (not this FortiMail). Alternatively, you can remove this header with a per-domain setting. For details, see Remove received header of outgoing email on page 109.
Custom	If the below *Header inserted by this unit* option is not enabled, enable this option to remove other headers that have been inserted by other MTAs (not this FortiMail). If the below *Header inserted by this unit* option is also enabled, enable this option to remove any headers that have been inserted by other MTAs AND this FortiMail. Then click *Edit* to enter the name (key) of a header that you want to remove, such as `X-Custom`. Do not include the colon (`:`) after the key. Multiple similar headers can be matched by using a regular expression pattern (see Syntax on page 381, except that character classes that use a colon such as `[[:alnum:]]` are not supported). Regular expression matching is automatically enabled if the entry contains any of the following special characters: `.^$*+?{}[]\\|()` Otherwise FortiMail compares with a simple literal match.
Header inserted by this unit	Enable this option and the above *Custom* option to remove the headers that are inserted by this FortiMail system, except `DKIM-Signature:`. **Warning**: If only this option is enabled but the above *Custom* option is not, this option will not work. **Note**: For backwards compatibility, if you upgrade the firmware and both of the related settings *Received:* and *Custom* were enabled, then this setting will be enabled by default.

Configuring list options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Lists*.

   Configure the sender and recipient block lists and safe lists, if any, to use with the session profile. Block and safe lists are separate for each session profile, and apply only to traffic controlled by the IP-based policy to which the session profile is applied.

Email addresses in each block list or safe list are arranged in alphabetical order. For more information on how blocklisted email addresses are handled, see Order of execution for antispam scans on page 22.

If you require regular expression support for safelisting and blocklisting sender and recipient email addresses in the envelope, do not configure safe and block lists in the session profile. Instead, configure access control rules and message delivery rules. For more information, see Configuring the address book on page 130.

Use safe lists and block lists with caution. They can increase incorrect results.

For example, a session safe list entry for `0.0.0.0/0` allows email from *all* email servers. The result is that all spam from any email server — normal or spammer — would **bypass later antispam scans**.

4. Configure the following:

GUI item	Description
Enable sender safe list checking	Enable to check the sender addresses in the SMTP envelope (`MAIL FROM:`), message header (`From:`) and (`Reply-to:`) against the safe list in the SMTP sessions to which this profile is applied, then click *Edit* to define the safelisted email addresses.
Enable sender block list checking	Enable to check the sender addresses in the SMTP envelope (`MAIL FROM:`), message header (`From:`) and (`Reply-to:`) against the block list in the SMTP sessions to which this profile is applied, then click *Edit* to define the blocklisted email addresses.
Allow recipients on this list	Enable to check the recipient addresses in the SMTP envelope (`RCPT TO:`) against the safe list in the SMTP sessions to which this profile is applied, then click *Edit* to define safelisted email addresses.
Disallow recipients on this list	Enable to check the recipient addresses in the SMTP envelope (`RCPT TO:`) against the block list in the SMTP sessions to which this profile is applied, then click *Edit* to define blocklisted email addresses.

Configuring advanced MTA control settings

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 171.

In addition to global MTA settings, you can configure the following MTA settings in a session profile. These session-specific MTA settings will override the global settings.

1. Purchase the feature license and enable the feature. See MTA advanced control on page 1.

   By default, this feature is disabled and hidden. After this feature is enabled, the following options will appear in the session profile settings. In addition, four new tabs will appear: *Profile* > *Session* > *Address Rewrite*, *Mail Routing*, *Access Control*, and *DSN*.
2. Go to *Profile* > *Session* > *Session*.
3. Click *New* to create a new session profile or double click on an existing profile to edit it.

4. Click the + to expand *Advanced Control*.
5. Configure the following settings:

GUI item	Description
Email queue	Select which email queue to use for the matching sessions. For other general queue settings, see Configuring mail queue setting.
Rewrite sender address	Select an address rewrite profile to rewrite the sender address and specify which sender address to rewrite: *Envelope From*, *Header From*, or *Header Reply-to*. Select *Use Envelope From value for selected headers* if you want to use the sender email address in the SMTP envelope (`MAIL FROM:`) to rewrite the sender in the message header (`From:` and/or `Reply-to:`). Click *New* to create a new profile. For details about configuring Address Rewrite profiles, see Configuring address rewrite profiles in the session profile on page 185.
Rewrite recipient address	Select an Address Rewrite profile to rewrite the recipient address and specify which recipient address to rewrite: *Envelope recipient* or *Header To and CC*. Note that if you set to deliver or quarantine the unmodified copy of email when you configure the action profile preferences, the recipient (`RCPT TO:`) in the SMTP envelope will still be rewritten. Click *New* to create a new profile. For details about configuring Address Rewrite profiles, see Configuring address rewrite profiles in the session profile on page 185.

Configuring address rewrite profiles in the session profile

If you enable the advanced MTA control feature in session profiles (see Configuring advanced MTA control settings on page 184), the *Address Rewrite* tab will appear.

To configure an address rewrite profile to be used in a session profile

1. Go to *Profile* > *Session* > *Address Rewrite*.
2. Click *New*.
3. Enter a profile name.
4. Click *New* to enter the address rewrite rules.
   - For *Rewrite type*, select *Local* if you are configuring direct rewrite from the original address to another specific address. Then specify the original address and the address you want to rewrite to. If you want to keep the local part or the domain part of the original address, click *Insert Variable* to insert the variable for the local part or the domain part.
   - Select *LDAP* if you want to rewrite the original address to the user's external email address and display name that are stored on an LDAP server when the `MAIL FROM:` in the SMTP envelope or `From:` or `Reply-To:` in the message header matches a sender rewrite pattern. Then specify the original address and the LDAP profile. For information about LDAP server configuration, see Address Mapping on page 245.
5. Click *Create*.

Configuring mail routing profiles in a session profile

If you enable the advanced MTA control feature in session profiles (see Configuring advanced MTA control settings on page 184), the *Mail Routing* tab will appear.

To configure a mail routing profile to be used in a session profile

1. Go to *Profile* > *Session* > *Mail Routing*.
2. Click *New*.
3. Enter a profile name.
4. Click *New* to configure the mail routing settings.
5. In the popup window, specify the sender pattern, recipient pattern, and the relay type:
   - *Host*: Relay the matched sessions to the specified SMTP server.
   - *MX Record (alternative domain):* Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. Also specify the alternate domain name.
   - *MX Record (this domain)*: Query the DNS server's MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them.
   - *Relay Host*: Relay to a pre-defined relay host.
6. Enter the SMTP port number. See also Appendix: Port Numbers on page 375.
7. Click *Create*.

Configuring access control profiles in a session profile

If you enable the advanced MTA control feature in session profiles (see Configuring advanced MTA control settings on page 184), the *Access Control* tab will appear.

To configure an access control profile to be used in a session profile

1. Go to *Profile* > *Session* > *Access Control*.
2. Click *New*.
3. Enter a profile name.
4. Click *New* to configure the access control rule.
5. In the popup window, configure the rule settings. These setting are identical to the system-wide access control rule settings. For details, see Configuring access control receiving policies on page 148.
6. Click *Create*.

Configuring DSN profiles in a session profile

If you enable the advanced MTA control feature in session profiles (see Configuring advanced MTA control settings on page 184), the *DSN* tab will appear. Configure this setting to overwrite the global setting configured in Configuring mail queue setting.

To configure a DSN profile to be used in a session profile

1. Go to *Profile* > *Session* > *DSN*.
2. Click *New*.
3. Enter a profile name.
4. Specify if you want to send DSN email and the maximum number of retries.
5. Click *Create*.

Configuring antispam profiles and actions

The *AntiSpam* submenu lets you configure antispam profiles and the action profiles that they use.

Configuring antispam profiles

FortiMail units can use many methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, and more. Antispam profiles can save you time: you can configure a group of scans in a profile, and then reuse that profile in multiple policies.

For information on the order in which FortiMail units perform each type of antispam scan, see Order of execution for antispam scans on page 22.

You can use an LDAP query to enable or disable antispam scanning on a per-user basis. For details, see Configuring LDAP profiles on page 234 and Scan Override on page 246.

To manage incoming antispam profiles

1. Depending on the type of antispam scan, before you select it in a profile, you may need to enable the feature, validate its license, or configure its system-wide settings. See Configuring FortiGuard services on page 85.
2. Go to *Profile* > *AntiSpam* > *AntiSpam*.
3. Either click *New* or *Clone* to add a profile, or double-click a profile to modify it.
   Alternatively, see Batch editing antispam profiles on page 200.
4. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.
Default action	Select the action profile to apply when the antispam profile detects spam. For each scan in the antispam profile, you can use its *Action* setting to override this default and select a more specific behavior. See also Configuring antispam action profiles on page 206.

5. Depending on which scans you want to use, enable and expand to configure the following:
   - FortiGuard section
   - Greylist section
   - SPF section

- DKIM section
- DMARC section
- ARC section
- Behavior analysis section
- Header analysis section
- Business email compromise section
- Heuristic section
- SURBL section
- DNSBL section
- Banned word section
- Safelist word section
- Dictionary section
- Image spam section
- Bayesian section
- Newsletter and suspicious newsletter sections

6. Expand the *Scan Option* section, and configure the following:

GUI item	Description
Max message size to scan	Enter the maximum size of each email, in bytes, that the FortiMail unit will scan for spam. Larger email are not scanned for spam. To disable the limit so that all email are scanned, enter `0`.  If spam is usually smaller, then you can reduce this limit to improve performance. (More system resources are required to scan larger email.)
Bypass scan on SMTP authentication	Enable to bypass spam scanning for authenticated SMTP connections. This option is enabled by default.  If authenticated SMTP clients are not a source of spam, then you can enable this option to improve performance.
Scan PDF attachment	Enable to inspect PDF attachments with the heuristic, banned word, and/or image spam scans (if you have enabled them). See also Heuristic section on page 195, Banned word section on page 197, and Image spam section on page 199. If *Attachment images* is enabled in QR code URL scan, then FortiMail also scans QR code images in the PDF. See Configuring preferences on page 312. Spammers may attach a PDF file to an email with an empty body to try to bypass spam scans. Because the body has no text to scan, it cannot determine spam status. However the PDF content is still spam. This option detects this type of spam.
Apply default action without scan upon policy match	Enable to perform the action in Default action immediately, without applying other antispam filters, if the email matches the IP or recipient policy.

7. Click *Create* or *OK*.
8. To apply the antispam profile, select it in a policy.

FortiGuard section

The FortiMail unit can query the FortiGuard Antispam service and custom threat feeds to determine spam status. Before you select FortiGuard scans in an antispam profile, you must enable and configure FortiGuard Antispam rating queries.

In general, for the FortiGuard section, if *Action* is *None*, then by default, for all sub-scans, FortiMail still scans and logs FortiGuard Antispam results, but **does not** perform an action.

However if you then select a different specific action for sub-scans such as *IP Reputation*, then it overrides and FortiMail**does** apply that action.

When both *IP Reputation* and *URL Category* scans detect spam, then the URL category's action takes precedence.

For example, if the *Action* is *Tag* for *IP Reputation*, but *Reject* for *URL Category*, then the email is rejected.

If the *FortiGuard*scans are enabled, you may improve performance and the spam catch rate by also enabling *Block IP*.

GUI item		Description
IP Reputation		Examine if the SMTP client's IP address is blocklisted.
	Level 1 **Level 2** **Level 3**	FortiGuard Antispam service categorizes blocklisted IP addresses into: • *Level 3*: Bad reputation. • *Level 2*: Worse reputation. • *Level 1*: Worst reputation. Enable each level that you want to apply an *Action* to.  To avoid false positives, you can select a different action for each level. Strict actions, such as reject or discard, are usually effective for *Level 1*, but less strict actions, such as quarantine or tag, usually can be used with *Level 3*.
	Threat feed	Use custom lists of IP addresses that are known sources of spam, and then select an *Action*. For details, see Configuring a threat feed on page 279.

GUI item		Description
	Extract IP from Received Header	If the SMTP client has a **private** network IP address (which is not guaranteed to be a unique identifier), then the FortiMail unit will query about the first **public** IP address in the header instead. (If you want to examine **all** public IP addresses in the `Received:` lines of the message header, enable *Extract IP from Received Header*.) FortiGuard Antispam scans do not examine private network addresses as defined in RFC 1918 because different private networks may use the same IP address ranges, and therefore it does not accurately identify specific SMTP clients.
URL Category		Determine if any uniform resource identifiers (URI) in the message body are associated with spam. FortiGuard groups URLs into various rating categories, such as phishing, drug abuse, etc. If you have configured custom categories, these can also be used. You can configure how FortiMail detects URLs. For details see About URL types on page 278.
	Primary **Secondary**	You can split categories into *Primary* and *Secondary* to select a separate *Action* for each, such as to exempt URLs from spam filtering. For details, see Configuring URL filter profiles on page 276.  If an email matches URL categories in both *Primary* and *Secondary*, then the *Action* that you select for *Primary* takes precedence. To reduce false positives, unrated IP addresses are ignored.

GUI item	Description
Spam outbreak protection	Select *Enable* to temporarily hold suspicious email if the FortiGuard Antispam scan for blocklisted IP addresses and/or URL category returns no result. This provides an opportunity for the FortiGuard Antispam service to update its database if a spam outbreak has just started and is not yet confirmed. To configure the hold time period, enter the CLI commands: `config profile antispam` `  set spam-outbreak-protection` `config system fortiguard antispam` `  set outbreak-protection-period` To view the email currently being held, go to *Monitor* > *Mail Queue* > *Spam Outbreak*. After the time interval, FortiMail queries the FortiGuard server again to determine the final result and apply the matching action.  *Spam outbreak protection* uses the *Action* that you select for *FortiGuard*, not the *Default action* for the whole antispam profile. If spam outbreak protection needs to temporarily hold the email (so the SMTP client is no longer connected and a *Reject* action is not technically possible anymore), and spam status is confirmed later, then the FortiMail instead applies the *System Quarantine* action. If the *Secondary* URL category is matched, then the email will be deferred in the spam outbreak queue. If you select *Monitor only*, then email is not deferred. Instead, FortiMail logs the email and inserts this message header: `X-FEAS-Spam-outbreak: monitor-only`

Greylist section

See Configuring greylisting on page 300.

Greylisting can improve performance by blocking most spam before it undergoes other resource-intensive antispam scans.

SPF section

You can enable Sender Protection Framework (SPF) verification to compare the SMTP client's IP address to the list of authorized senders for the domain name in its public DNS record (RFC 4408). If SPF information does not exist in the DNS record, then IP address validation is omitted.

If you disable SPF verification, but you enable the DMARC section, then SPF will still occur. This is because DMARC requires SPF.

Invalid SPF results may be normal in some cases, and require ARC signature validation instead (see ARC section on page 194). For details, see DKIM and ARC Setting on page 102.

Unlike SPF verification by a session profile, SPF verification by an antispam profile does **not** increase the SMTP client's reputation score if the check fails.

RFC 1918 private network addresses are not globally unique, cannot be resolved by public DNS on the Internet, and therefore their email cannot be validated by SPF.

If SPF check is *Bypass* in the session profile or if a safe list matches (see Configuring the block lists and safe lists on page 294), then even if you enable SPF in the antispam profile, FortiMail skips SPF verification.

GUI item	Description
Fail	Select which *Action* to perform if SPF indicates that the SMTP client is not authorized to send email for that domain name.
Soft Fail	Select which *Action* to perform if SPF indicates that the SMTP client is not authorized to send email for that domain name, but there is no strong statement.
Permanent Error	Select which *Action* to perform if the DNS server returned an invalid SPF record when FortiMail made the DNS query.
Temporary Error	Select which *Action* to perform if the DNS server returned `Temp error` when FortiMail made the DNS query.
Pass	Select which *Action* to perform if SPF verification succeeds, and the SMTP client is an authorized sender.
Neutral	Select which *Action* to perform if a valid SPF record exists, but there is no definitive assertion.
No Record	Select which *Action* to perform if a SPF record does not exist on the DNS server.

DKIM section

You can verify DomainKeys Identified Mail (DKIM) signatures to prove that email has not been tampered with in transit.

If you disable DKIM verification, but you enable the DMARC section, then DKIM will still occur. This is because DMARC requires DKIM.

Invalid DKIM signatures may be normal in some cases, and require ARC signature validation instead (see ARC section on page 194). For details, see DKIM and ARC Setting on page 102.

If a safe list matches (see Configuring the block lists and safe lists on page 294), then even if you enable DKIM in the antispam profile, FortiMail skips DKIM.

GUI item	Description
Fail	Select which *Action* to perform if DKIM verification detects an invalid signature or body hash.
Temporary Error	Select which *Action* to perform if the DNS server returned `Temp error` when FortiMail made the DNS query.
Pass	Select which *Action* to perform if DKIM verification succeeds.
No Record	Select which *Action* to perform if no DKIM information exists in the DNS record, or the record could not be parsed.

DMARC section

Domain-based Message Authentication, Reporting & Conformance (DMARC) performs email authentication with SPF and DKIM.

If either the SPF or DKIM verification succeeds, then DMARC verification succeeds. If both of them fail, then DMARC verification fails. You do not need to enable SPF section or DKIM section before you enable DMARC verification. Because DMARC depends on their results, those checks are performed automatically, even if they are disabled.

FortiMail also verifies sender alignment, where at least one of the domains authenticated by SPF or DKIM must match the sender's domain name in the message header (`From:`). If they do not align, then the DMARC check fails. See also RFC 7489.

GUI item	Description
Fail	Select which *Action* to perform if DMARC verification fails. Furthermore, you can set individual actions for the following DMARC DNS record policy (P tags): • *None* • *Quarantine* • *Reject*
Temporary Error	Select which *Action* to perform if the DNS server returned `Temp error` when FortiMail made the DNS query.
Pass	Select which *Action* to perform if DMARC verification succeeds.
No Record	Select which *Action* to perform if no DMARC information exists in the DNS record, or the record could not be parsed.
DMARC override	Enable *SPF* and/or *DKIM* if you want the DMARC result to take precedence over SPF and DKIM results. For example, if DMARC verification succeeds, then the SPF fail and soft fail won't take effect anymore.

You can generate DMARC reports automatically, or manually (on demand), or administrators can log into FortiMail to view current statistics. See Viewing DMARC report statistics on page 55.

ARC section

You can enable Authenticated Received Chain (ARC) validation if the email was modified in transit by a relay or proxy. For details, see DKIM and ARC Setting on page 102.

If you enable *ARC override* for SPF, DKIM, and/or DMARC, then the ARC result has priority over them. This can be useful when a policy matches indirectly delivered email (via mailing list, forwarding service, etc.) that, during normal processing, always invalidates SPF or DKIM signatures. The override allows FortiMail to validate the email using the alternative ARC signature instead.

Behavior analysis section

Behavior analysis (BA) uses a database to analyze similarities between known spam and undetermined email to determine if an email is spam.

The BA database is a gathering of spam email caught by FortiGuard Antispam service. Therefore, the accuracy of the FortiGuard Antispam service has a direct impact on the BA accuracy.

You can adjust the BA aggressiveness using the following CLI commands:

```
config antispam behavior-analysis
   set analysis-level {high | medium | low}
end
```

The high setting means the most aggressive while the low setting means the least aggressive. The default setting is medium.

You can also reset (empty) the BA database using the following CLI command:

```
diagnose debug application mailfilterd behavior-analysis update
```

Header analysis section

Enable this option to examine the entire message header for spam characteristics.

Business email compromise section

To better protect against business email compromise (BEC) spam attacks, FortiMail can scan for cousin domains, suspicious characters, sender alignment, action keywords, and URL categories. To avoid false positives and false negatives, you can adjust ("weight") the scores of each type of suspicious behavior, and the total score threshold that an email must reach to be categorized as spam.

GUI item	Description
Weighted analysis	Enable to apply a weighted analysis profile and assign an appropriate action. See also Configuring weighted analysis profiles on page 204.
Impersonation analysis	Enable to automatically learn and track the mapping of display names and internal email addresses to prevent spoofing attacks. See also Configuring impersonation profiles on page 201.

GUI item	Description
Cousin domain	Enable to scan for domain names that are deliberately misspelled in order to appear to come from a trusted domain. Additionally, enable *Header Detection*, *Body Detection*, and/or *Auto Detection* if you wish to scan for cousin domain names either within the email header, the email body, and/or automatically (respectively). See also Configuring cousin domain profiles on page 202.
Sender alignment	Enable to scan for sender email address and name mismatches. Sender alignment compares the message header `From:` (and any others you select in *Apply to*, that is, *Reply-To* and *Display name*) with the SMTP envelope `MAIL FROM:` to look for a mismatch, which is typical of spam.

Heuristic section

Heuristic scans can use many rules. Each rule has an individual score used to calculate the total score for an email. If an email matches the rule, then its score is added to the total. For example, if the subject line of an email contains “As seen on national TV!”, then it might match a heuristic rule that increases the heuristic scan score towards the threshold.

- **Spam:** Total score equals or exceeds the threshold.
- **Not spam:** Total score is less than the threshold.

A default heuristic rule set is included with the firmware. Update your FortiGuard Antispam packages regularly to get current heuristic rules for the most accurate heuristic score.

Heuristic scanning is resource intensive. If spam detection rates are acceptable without heuristic scanning, consider disabling it or limiting its application to policies for problematic hosts.

You can also apply heuristic scans to PDF attachments. See Scan PDF attachment on page 188.

GUI item	Description
Threshold	Enter the score at which the FortiMail unit considers an email to be spam. The default value is recommended.
The percentage of rules used	Enter the percentage of the total number of heuristic rules to use to calculate the heuristic score for an email.

SURBL section

In addition to supporting Fortinet’s FortiGuard Antispam SURBL service, the FortiMail unit supports third-party Spam URL Realtime Block Lists (SURBL) servers. You can specify which public SURBL servers to use as part of an antispam profile. Consult the third-party SURBL service providers for any conditions and restrictions.

The SURBL section of antispam profiles lets you configure the FortiMail unit to query one or more SURBL servers to determine if any of the uniform resource identifiers (URL) in the message body are associated with spam. If a URL is blocklisted, the FortiMail unit treats the email as spam and performs the associated action. You can configure how FortiMail detects URLs. See About URL types on page 278.

To add a SURBL server

1. In the *SURBL* section of an antispam profile, click *Configuration*.
   A pop-up window appears that displays a list of SURBL servers.
2. Click *New* and type the address of a SURBL server.
   Servers are queried from top to bottom. Therefore you may want to put the reliable servers with less traffic at the top of the list.
3. Click *OK*.
   The pop-up window closes.

   When you close the pop-up window, it does **not** save. Before navigating to another part of the GUI, you must click *OK* in the antispam profile in order to save it and the list.

4. Click *Create* or *OK*.

DNSBL section

In addition to supporting Fortinet's FortiGuard Antispam DNSBL service, the FortiMail unit can query third-party DNS blocklist servers to determine if an SMTP client is blocklisted. Consult the third-party DNSBL service providers for any conditions and restrictions.

Carefully select your DNSBL providers and review their operations. Fortinet recommends that all email administrators utilize services which have clearly defined and rational listing policies and do not charge for delisting. Services that block whole subnets and AS numbers and have a business model which charges for delisting should be viewed with heavy caution. Fortinet cannot delist IP addresses blocklisted by other vendors.

DNSBL scans examine the IP address of the SMTP client that is currently delivering the email message. If the *Enable Block IP to query for the blocklist status of the IP addresses of all SMTP servers appearing in the Received: lines of header lines.* option in the *Deep header* section is enabled, DNSBL scan will also examine the IP addresses of all other SMTP servers that appear in the `Received:` lines of the message header.See FortiGuard section on page 189.

DNSBL scans do not examine private network addresses as defined in RFC 1918 because different private networks may use the same IP address ranges, and therefore it does not accurately identify specific SMTP clients.

To add a DNSBL server

1. In the *DNSBL* section of an antispam profile, click *Configuration*.
   A pop-up window appears that displays a list of DNSBL servers.
2. Click *New* and type the address of a DNSBL server.

Servers are queried from top to bottom. Therefore you may want to put the reliable servers with less traffic at the top of the list.

3. Click *OK*.

   The pop-up window closes.

When you close the pop-up window, it does **not** save. Before navigating to another part of the GUI, you must click *OK* in the antispam profile in order to save it and the list.

4. Click *Create* or *OK*.

Banned word section

The *Banned word* section of antispam profiles lets you configure the FortiMail unit to consider email messages as spam if the subject line and/or message body contain a prohibited word.

When banned word scanning is enabled and an email is found to contain a banned word, the FortiMail unit adds `X-FEAS-BANNEDWORD:` to the message header, followed by the banned word found in the email. The header may be useful for troubleshooting purposes, when determining which banned word or phrase caused an email to be blocked.

You can use wildcards in banned words. But unlike dictionary scans, banned word scans do **not** support regular expressions. For details, see Appendix: Wildcards and regular expressions on page 380.

You can also apply this scan to PDF attachments. See Scan PDF attachment on page 188.

To add banned words

1. In the *Banned word* section of an antispam profile, click *Configuration*.

   A pop-up window appears that displays a list of banned words.
2. Click *New*.
3. In *Banned Word*, enter the word or phrase.

   If you want to scan email subject lines for the word, enable *Subject*. If you want to scan the message body, enable *Body*.
4. Repeat the previous step until you have added all of the words.
5. Click *OK*.

   The pop-up window closes.

When you close the pop-up window, it does **not** save. Before navigating to another part of the GUI, you must click *OK* in the antispam profile in order to save it and the list.

6. Click *Create* or *OK*.

Safelist word section

Safelist word scans let you exempt email from being categorized as spam if they contain specific key words or phrases.

You can use wildcards to match multiple safelist words. Unlike dictionary scans, safelist word scans do **not** support regular expressions. For details, see Appendix: Wildcards and regular expressions on page 380.

To configure safelist words

1. In the *Safelist word* section of an antispam profile, click *Configuration*.
   A pop-up window appears that displays a list of banned words.
2. Click *New*.
3. In *Safelist Word*, enter the word or phrase.
   If you want to scan email subject lines for the word, enable *Subject*. If you want to scan the message body, enable *Body*.
4. Repeat the previous step until you have added all of the words.
5. Click *OK*.
   The pop-up window closes.

   When you close the pop-up window, it does **not** save. Before navigating to another part of the GUI, you must click *OK* in the antispam profile in order to save it and the list.

6. Click *Create* or *OK*.

Dictionary section

Dictionary scans use dictionary profiles (see Configuring dictionary profiles on page 262.) to determine if the email is spam.

If an email has a dictionary word, FortiMail units add `X-FEAS-DICTIONARY:` to the message header, followed by the dictionary word or pattern found in the email. The header may be useful for troubleshooting purposes, when determining which dictionary word or pattern caused an email to be blocked.

Compared to banned word scans, dictionary scans are more resource-intensive. If you do not require dictionary features such as regular expressions, consider using a banned word scan instead.

GUI item	Description
With dictionary group	Select the name of a group of dictionary profiles to use with the dictionary scan. Alternatively, configure With dictionary profile.
With dictionary profile	Select the name of a dictionary profile to use with the dictionary scan.

GUI item	Description
Minimum dictionary score	Enter the number of dictionary term matches above which the email will be considered to be spam. **Note:** Score value is based on individual dictionary profile matches, not the dictionary group matches.

Image spam section

Image spam scans analyze the contents of GIF, JPG, and PNG graphics to determine if the email is spam. This may be useful if the message body of an email contains graphics but no text, and therefore text-based antispam scans cannot determine spam status.

GUI item	Description
Aggressive	Enable to inspect image file attachments in addition to embedded graphics.  If you do not require this feature, disable it to improve performance. Enabling this option increases workload when scanning email messages that contain image file attachments. This option applies only if you enable Scan PDF attachment.

Bayesian section

Bayesian scans use a trained database to determine if the email is spam.FortiMail units can maintain multiple Bayesian databases: global, and specific to each protected domain.

- For **outgoing** email, the FortiMail unit uses the global Bayesian database.
- For **incoming** email, which database will be used when performing the Bayesian scan varies by configuration of the incoming antispam profile and the configuration of the protected domain.

Before using Bayesian scans, you must train one or more Bayesian databases in order to teach the FortiMail unit which words indicate probable spam. If a Bayesian database is not sufficiently trained, it can increase false positive and/or false negative rates. You can train the Bayesian databases of your FortiMail unit in several ways. For more information, see Training the Bayesian databases on page 316.

 If you do not continue to train it, Bayesian scanning becomes significantly less effective over time. Therefore Fortinet does not recommend enabling this feature.

GUI item	Description
Accept training messages from user	Enable to accept training messages from email users.

GUI item	Description
	Training messages are email messages that email users forward to the email addresses of control accounts, such as `is-spam@example.com`, in order to train or correct Bayesian databases. For information on Bayesian control account email addresses, see Configuring the quarantine control options on page 293. FortiMail units apply training messages to either the global or per-domain Bayesian database depending on your configuration of the protected domain to which the email user belongs. Disable to discard training messages. This option is available only if *Direction* is *Incoming* (per-domain Bayesian databases cannot be used when the recipient does not belong to a protected domain, which defines outgoing email).
Use other techniques for auto training	Enable to use scan results from FortiGuard, SURBL, and per-user and system-wide safelists to train the Bayesian databases. This option is available only if *Direction* is *Incoming* (domain-level Bayesian databases cannot be used when the recipient does not belong to a protected domain, which defines outgoing email).

Newsletter and suspicious newsletter sections

Although newsletters and marketing campaigns are often opt-in and therefore are technically not spam in some geographic regions, some users may find them annoying. It can save time to tag the subject line, so that they can apply rules in their email client to filter out newsletters. Administrators may not want to waste system resources on processing or storing newsletters, either. Some newsletters are suspicious, too, because they may actually be disguised spam.

Enable these options to detect both real and fake newsletters, and then in *Action*, select an action profile. If both types are enabled, and if a FortiMail detects that an email is suspicious, then it applies the action for suspicious newsletters only.

Batch editing antispam profiles

You can apply changes to multiple antispam profiles at once.

1. Go to *Profile* > *AntiSpam* > *AntiSpam*.
2. In the row corresponding to existing profiles whose settings you want to modify, hold Ctrl and select the profiles that you want to edit.

   You cannot batch edit antispam profiles predefined profiles.
3. Click *Batch Edit*.
4. Modify the profile, as explained in Configuring antispam profiles on page 187, changing only those settings that you want to apply to all selected profiles.
5. Click *Apply To All* to save the changes and remain on the dialog, or click *OK* to save the changes and return to the *AntiSpam* tab.

Configuring impersonation profiles

Email impersonation is a type of email spoofing attack. It forges the email header to deceive the recipient because the message appears to be from a different source than the actual address.

To use this feature, you must have a license for the Fortinet Enterprise Advanced Threat Protection (ATP) bundle.

To fight against email impersonation, you can map high valued target display names with correct email addresses and FortiMail can check for the mapping. For example, an external spammer wants to impersonate the CEO of your company(`ceo@company.com`). The spammer will put `From: CEO ABC <ceo@external.com>` in the email header, and send such email to a user(`victim@company.com`). If FortiMail has been configured with a manual entry "`CEO ABC`"/"`ceo@company.com`" in an impersonation analysis profile to indicate the correct display name/email pair, or it has learned display name/email pair through the dynamic process, then such email will be detected by impersonation analysis, because the spammer uses an external email address and an internal user's display name.

Impersonation analysis inspects both the `From:` and `Reply-To:` message headers.

Entries can be mapped either:

- **Manually**: You enter mappings between display names and email addresses.
- **Dynamically**: The FortiMail mail statistics service automatically learns the mappings.

To create an impersonation analysis profile

1. Go to *Profile* > *AntiSpam* > *Impersonation*.
2. Either click *New* or *Clone* to add a profile, or double-click a profile to modify it.
   Alternatively, see Batch editing antispam profiles on page 200.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name.
Comment	Enter a comment or description.

4. In the *Impersonation* section, select either *Match Rule* or *Exempt Rule*.

To avoid false positives, impersonation analysis also follows some other exemptions.

5. Click *New* and then configure the following:

GUI item	Description
Display name pattern	Enter the display name to be mapped to the email address. You can use a wildcard or regular expression.
Pattern type	Select either: • *Wildcard* • *Regular expression* See Appendix: Wildcards and regular expressions on page 380.
Email address	Enter the email address to be mapped to the display name. The email address can be from protected/internal domains or unprotected/external domains. If the email address is from an external domain, such as gmail.com or hotmail.com, the display name matching the external email address will be passed. Otherwise, it will be caught by impersonation analysis.

6. Click *Create*.
7. Repeat the previous step until all rules have been created.
8. Click *Create* or *OK*.
9. To apply impersonation profile, select it in an antispam profile. For details, see Business email compromise section on page 194.

Enabling impersonation analysis dynamic scanning

You can manually enter mappings and create impersonation analysis profiles, but the FortiMail mail statistics service also can automatically, dynamically learn and track the mapping of display names and internal email addresses.

By default, FortiMail uses manual analysis only. You can use manual, dynamic, or both.

To select which methods to use, and to enable the mail statistics service, use these CLI commands:

```
config antispam settings
   set impersonation-analysis {dynamic manual}
end
config system global
   set mailstat-service enable
end
```

After the service is enabled, you can search the automatic mappings. Go to *Profile* > *AntiSpam* > *Impersonation* and click *Impersonation Lookup*. Enter the email address. If a record exists, the corresponding display name will be displayed.

Configuring cousin domain profiles

Similar to impersonation profiles, cousin domain profiles help to mitigate domain impersonation risks. Similar to impersonation profiles that map display names, cousin domain profiles can map both inbound and outbound domain names to either be scanned or exempt from scanning. Domain names may be deliberately misspelled, either by character removal, substitution, and/or transposition, in order to make emails look as though they originate from trusted internal sources.

For example, if you configure a regular expression for the sender domain `f?rtinet.com`, it will match `f0rtinet.com`, but the legitimate and trusted sender domain `fortinet.com` will also be detected as a cousin domain. To avoid this, you can add `fortinet.com` into the exempt rules setting to avoid detecting it as spam.

To configure a cousin domain profile

1. Go to *Profile* > *AntiSpam* > *Cousin Domain*.
2. Either click *New* or *Clone* to add a profile, or double-click a profile to modify it.
   Alternatively, see Batch editing antispam profiles on page 200.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.

4. In the *Domain Pattern* section, select *From*, *To*, or *Exempt*.
5. Click *New* and then configure the following:

GUI item	Description
Domain name pattern	Enter the domain name to be mapped to the email address. You can use wildcard or regular expression.
Pattern type	Select either: • *Wildcard* • *Regular expression* • *Look-alike* A look-alike pattern can be configured to specifically check for instances of recipient domain typos. For example, if a domain such as `fortinet.com` is configured with pattern type set to look-alike, any similar misspelled domains, such as `fort1net.com`, are caught. See also Syntax on page 381.  Since auto-detection is not applicable to outgoing policies, look-alike patterns are best suited for catching misspelled domains.

6. Repeat the previous step until you have entries that match all cousin domains.
7. Click *Create* or *OK*.
8. To apply a cousin domain profile, select it in an antispam profile. For details, see Business email compromise section on page 194.

Configuring weighted analysis profiles

You can create weighted analysis profiles containing of one or more score weighted rules configured to scan for various categories, including intelligent analysis.

To create a weighted analysis profile

1. Go to *Profile* > *AntiSpam* > *Weighted Analysis*.
2. Either click *New* or *Clone* to add a profile, or double-click a profile to modify it.
   Alternatively, see Batch editing antispam profiles on page 200.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.

4. In the *Rule* section, click *New*and then configure the following:

GUI item	Description
Status	Enable or disable the rule.
Name	Enter the name of the rule.
Action (dropdown list)	Specify an action for the rule.
Threshold	Enter the threshold at which the current rule is to be triggered. This score will be allocated to the categories below.
Score Weight	Enter the score weight thresholds of the following factors: • *Relationship strength*: Set score for strong or weak relation result obtained from querying FortiGuard Sender and Recipient Relation (SRR). FortiGuard Social Database contains the social mapping of the email communication flow. For example, if user1@1.example.com and user2@2.example.com have regular communication, then their SRR is strong; if they have no history of communication before, then their SRR is weak. • *Intelligent analysis*: Multiple factors contribute to intelligent analysis in order to reduce false positives, including: • SPF • DKIM • DMARC • matching of sender addresses in the message headers (`From:`

GUI item	Description
	and `Reply-To:`) • newly registered domain names that do not have a FortiGuard Antispam rating yet • header analysis • malformed email detection • *Cousin domain*: Detects domain impersonation. See Configuring cousin domain profiles on page 202. • *Suspicious character*: Detects internationalized domain name (IDN) homograph attacks. If domain names in URLs, sender email addresses, or recipient email addresses have Unicode characters that are from different languages yet look similar (for example, `A` looks similar in Cyrillic, Greek, and Latin alphabets), then an attacker could trick the user into using a fraudulent website or email. FortiMail detects these as suspicious. • *Sender alignment*: Compares the domain name of the sender email address in the message header (`From:`) and SMTP envelope (`MAIL FROM:`) to look for a mismatch, which is typical of spam. • *Action keyword*: Select the name of a dictionary profile that contains words or phrases that typically only spam has. Keywords are often a "call to action" that motivates the user to reply or click a hyperlink. For example, "Click here", "transfer", "money", "dollars", "bank account", "conference attendee", etc. • *Dictionary profile*: Select the dictionary profile. See Configuring dictionary profiles on page 262. • *Minimum dictionary score*: Enter the threshold for dictionary profile matches. When the dictionary profile scans an email, it counts the number of matching words or phrases, and adjusts this total according to the pattern weight and maximum pattern weight in the dictionary profile. If the result equals or exceeds this threshold, then FortiMail applies the weighted score defined in *Action keyword*. • *URL category*: Detects spam or phishing URLs in the email. • *Malformed email*: Detects malformed data in the email structure, header, or body. For more information, see RFC 7103.

5. Repeat the previous step until all rules are configured.
6. Click *Create* or *OK*.
7. To apply a weighted analysis profile, select it in an antispam profile. See Business email compromise section on page 194.

Configuring antispam action profiles

The *Action* tab in the *AntiSpam* submenu lets you define one or more things that the FortiMail unit should do if the antispam profile determines that an email is spam.

For example, assume you configured a default antispam action profile, named `quar_and_tag_profile`, that both tags the subject line and quarantines email detected to be spam. In general, all antispam profiles using the default action profile will quarantine the email and tag it as spam. However, you can decide that email failing to pass the dictionary scan is always spam and should be rejected so that it does not consume quarantine disk space. Therefore, for the antispam profiles that apply a dictionary scan, you could override the default action by configuring and using a second action profile, named `rejection_profile`, which rejects such email.

The specific action profile will override the default action profile when `mailfilterd` scans the email and take disposition (action) against the email. When the email is out of the process of `mailfilterd`, any remaining actions, such as spam report, web release, and sender safelisting, will still be taken based on the default action profile.

To configure an antispam action profile

1. Go to *Profile* > *AntiSpam* > *Action*.
2. Either click *New* or *Clone* to add a profile, or double-click a profile to modify it.
   Alternatively, see Batch editing antispam profiles on page 200.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.
Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[spam]`. The FortiMail unit will prepend this text to the subject line of spam before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.
Insert header	Enable and enter the message header key in the field, and the values in the *With value* field. The FortiMail unit adds this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.

GUI item	Description
	Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as spam by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. Starting from FortiMail 6.0.1, you can add multiple headers by adding them to the header table. You can also insert the predefined variables to the header value.
Insert disclaimer	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System > Mail Setting > Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email. **Note:** If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile and ignores *Relay server name* and *Use this domain's SMTP server to deliver the mail*.
Deliver to original host	Enable to deliver email to the original host.
FortiGuard spam outbreak protection	Enable to manually defer emails and place email in the spam defer queue. **Note:** The *Spam outbreak protection* option in the FortiGuard settings under *Profile > AntiSpam > AntiSpam* does not affect this feature.
Defer delivery	Enable to defer delivery of emails that may be resource intensive and reduce performance of the mail server, such as large email messages, or lower priority email from certain senders (for example, marketing campaign email and mass mailing).
BCC	Enable to send a blind carbon copy (BCC) of the email. You can specify an *Envelope from address* so that, in the case the email is not deliverable and bounced back, it will be returned to the specified envelope from address, instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. Click *New* to add BCC recipients.
Notify with profile	Enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification email is customizable and will tell the users what happened to the email message. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.

GUI item		Description
Final action		For details about final and non-final actions, see Order of execution for antispam scans on page 22.
	Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
	Reject	Enable to reject the email and reply to the SMTP client with SMTP reply code 550. However, if email messages are held for FortiGuard spam outbreak protection or FortiGuard virus outbreak protection, or sent to FortiSandbox, the actual action will fallback to "system quarantine".
	Personal quarantine	For incoming email, enable to redirect the email to the recipient's personal quarantine. For more information, see Managing the personal quarantines on page 43. For outgoing email, this action will fallback to the system quarantine.
	System quarantine	Enable to redirect spam to the system quarantine and then select the quarantine folder. For more information, see Managing the system quarantine on page 46. You can also enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification recipients will be able to release the quarantined email using the URL in the notification email. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
	Domain quarantine	Enable to redirect spam to the domain quarantine and then select the quarantine folder. For more information, see Managing the domain quarantines on page 48. You can also enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification recipients will be able to release the quarantined email using the URL in the notification email. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
	Rewrite recipient email address	Enable to change the recipient address of any email message detected as spam. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the @ symbol). For each part, select either: • *None*: No change. • *Prefix*: Prepend the part with text that you have entered in the *With* field. • *Suffix*: Append the part with the text you have entered in the *With* field. • *Replace*: Substitute the part with the text you have entered in the *With* field.

4. Click *Create* or *OK*.

5. To apply an antispam action profile, select it in an antispam profile. For details, see Default action on page 187.

Configuring antivirus profiles, file signatures, and actions

The *AntiVirus* submenu lets you configure antivirus profiles and related action profiles.

Configuring antivirus profiles

Go to *Profile* > *AntiVirus* > *AntiVirus* to create antivirus profiles that you can select in a policy in order to scan email for viruses.

The FortiMail unit scans email header, body, and attachments (including compressed files, such as ZIP, PKZIP, LHA, ARJ, and RAR files) for virus infections. If the FortiMail unit detects a virus, it will take actions as you define in the antivirus action profiles. For details, see Configuring antivirus action profiles on page 213.

FortiMail keeps its antivirus scan engine and virus signature database up-to-date by connecting to Fortinet FortiGuard Distribution Network (FDN) antivirus services.

To configure an antivirus profile

1. Go to *Profile* > *AntiVirus* > *AntiVirus*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.
Default action	Select the action profile to apply when the profile detects a virus. For each scan in the profile, you can use its *Action* setting to override this default and select a more specific behavior. See also Configuring antivirus action profiles on page 213.

4. Click the arrows to expand each section and configure the following:

GUI item		Description
AntiVirus		Enable to perform antivirus scanning.
	Malware/virus Outbreak	Instead of using virus signatures, malware outbreak protection uses data analytic from the FortiGuard Service. For example, if a threshold volume of previously unknown attachments are being sent from known malicious sources, they are treated as suspicious viruses. This feature can help quickly identify new threats. Because the infected email is treated as virus, the virus replacement message will be used, if the replacement action is triggered.
	Heuristic	Enable to use real-time malware analysis, or heuristic antivirus scan, when performing antivirus scanning.
	File signature check	Enable to scan for file signatures. For details, see Configuring file signatures on page 211.
	Grayware	Enable to scan for grayware, such as mail bomb detection.
FortiNDR		Enable this option to send potentially harmful attachments, such as executables, PDF, and OCX files, to FortiNDR for further malware analysis. For details about FortiNDR configuration, see Using FortiNDR malware inspection on page 82.
	Malicious/Virus **High risk** **Medium risk** **Low risk**	Specify the action to take if the FortiNDR analysis determines that the email messages have malware or other threat qualities. You can specify different actions according to the threat levels.
FortiSandbox		Select a scan mode to send potentially harmful URLs and attachments, such as executables, PDF, and OCX files, to FortiSandbox for further analysis. For details about FortiSandbox configuration, see Using FortiSandbox antivirus inspection on page 83.
	Scan mode	*Submit and wait for result*: Submit the attachments and URLs to FortiSandbox, then deliver the email or take the configured actions according to the scan results. *Submit only*: Submit the attachments and URLs to FortiSandbox, and deliver the email without waiting for scan results.
	Attachment analysis	Enable to send email attachments to FortiSandbox. If desired, configure different actions for different scan results.

GUI item		Description
	Malicious/Virus **High risk** **Medium risk** **Low risk** **No Result**	Specify the action to take if the FortiSandbox analysis determines that the email messages have virus or other threat qualities. You can specify different actions according to the threat levels.
URL analysis		Enable to send the URLs to FortiSandbox. If desired, configure different actions for different scan results.
	Email selection	Specify to scan URLs in all email or the suspicious email only.
	Malicious/Virus **High risk** **Medium risk** **Low risk** **No Result**	Specify the action to take if the FortiSandbox analysis determines that the email messages have virus or other threat qualities. You can specify different actions according to the threat levels.

Configuring file signatures

If you have the SHA-1or SHA-256 (Secure Hash Algorithm) hash values of some known virus-infected files, then you can add these values as file signatures and select the action to apply in the antivirus profile (see Configuring antivirus profiles on page 209).

Some file types do not contain viruses, so FortiMail file signature check only supports these attachment file types:

- .7z
- .bat
- .cab
- .dll
- .doc
- .docm
- .docx
- .dotm
- .exe
- .gz
- .hta
- .inf
- .jar
- .js
- .jse
- .msi
- .msp
- .ppsm
- .ppt
- .pptm
- .pptx
- .reg
- .scr
- .sldm
- .swf
- .tar
- .vbe
- .ws
- .wsc
- .wsf
- .wsh
- .xlam
- .xls
- .xlsm

- .pdf
- .pif
- .potm
- .ppam
- .xlsx
- .xltm
- .z
- .zip

File signatures can be added either individually, or batch imported via a threat feed, a list of checksums in CSV (comma-separated values), or a plain text file. File signatures also can be exported as a CSV file.

To add a new file signature manually or via threat feed

1. Go to *Profile* > *AntiVirus* > *File Signature*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Status	Enable or disable the profile.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.
Source	Select where the file signatures are stored, either: • *Local* — On the FortiMail unit. • *Remote* — A threat feed on an external server.

4. If Source is *Local*, then configure the following:

GUI item	Description
Type	Select either: • *SHA-1* • *SHA-256*
File Signature List	Click *New*. Enter the checksum value for a file, and then click *OK*. Repeat this step until you have entered all of the checksums.

Else if Source is *Remote*, then configure the following:

GUI item	Description
Threat feed	Select a threat feed that contains file signatures. (Its Resource type is *Malware Hash*.) See also Configuring a threat feed on page 279.

5. Click *Create*.

To import a signature list in CSV format

1. Go to *Profile* > *AntiVirus* > *File Signature*.
2. Click to select a profile.
3. Click *Import*.
4. Browse to the CSV file and click *OK*.
   The CSV file must contain SHA-1 or SHA-256 hash values, one per line.

To export file signatures in CSV format

1. Go to *Profile* > *AntiVirus* > *File Signature*.
2. Click to select a profile.
3. Click *Export*.

   Depending on your browser settings, your browser may prompt you for a file name and location before downloading the CSV file.

Configuring antivirus action profiles

Antivirus action profiles define what the FortiMail unit should do if the antivirus profile determines that an email is infected by viruses.

To configure antivirus action profiles

1. Go to *Profile* > *AntiVirus* > *Action*.
2. Either click New to add a profile or double-click an existing profile to modify it.
3. Configure the following:

GUI item	Description
Domain	Select which protected domain this profile belongs to, or *System* (all protected domains can use this profile). You can only see the domains that are permitted by your administrator profile. See About administrator account permissions on page 67.
Name	Enter a unique name for the profile.
Comment	Enter a comment or description.
Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[virus]`. The FortiMail unit will prepend this text to the subject line of spam before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.
Insert header	Enable and enter the message header key in the field, and the values in the With value field. The FortiMail unit adds this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as virus by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.

GUI item	Description
	Note: Do not enter spaces in the key portion of the header line. They are forbidden by RFC 2822. Starting from FortiMail 6.0.1 release, you can add multiple headers by adding them to the header table. You can also insert the predefined variables to the header value.
Insert disclaimer	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System > Mail Setting > Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email. **Note:** If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile and ignores Relay server name and Use this domain's SMTP server to deliver the mail.
Deliver to original host	Enable to route the email back to its original source destination.
BCC	Enable to send a blind carbon copy (BCC) of the email. You can specify a sender email address in the SMTP envelope (`MAIL FROM:`) so that, in the case the email is not deliverable and bounced back, it will be returned to the specified envelope from address, instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. Click *New* to add BCC recipients.
Replace infected/suspicious body or attachment (s)	Replaces the infected file with a replacement message that notifies the email user the infected file was removed. • For malware outbreak scans, virus replacement messages will be used. • For FortiSandbox scans, virus replacement messages will be used. • For heuristic scans, suspicious replacement messages will be used. You can customize replacement messages. For more information, see Customizing custom messages, and email templates on page 71.
Remove URL detected by FortiSandbox	Removes suspicious URLs from email, as detected by FortiSandbox.
Notify with profile	Enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification email is customizable and will tell the users what happened to the email message. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
Final action	Select one of the following actions: • *Discard*: Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.

GUI item	Description
	• *Reject*: Enable to reject the email and reply to the SMTP client with SMTP reply code 550. However, if email messages are held for FortiGuard spam outbreak protection or FortiGuard virus outbreak protection, or sent to FortiSandbox, the actual action will fallback to "system quarantine". • *System quarantine*: Enable to redirect email to the system quarantine. For more information, see Managing the system quarantine on page 46.You can choose to quarantine the original email or the modified email. • *Domain quarantine*: Enable to redirect email to the domain quarantine folder. For more information, see Managing the domain quarantines on page 48. • *Rewrite recipient email address*: Enable to change the recipient address of any infected email message. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). For each part, select either: • *None*: No change. • *Prefix*: Prepend the part with text that you have entered in the With field. • *Suffix*: Append the part with the text you have entered in the With field. • *Replace*: Substitute the part with the text you have entered in the With field. • *Repackage email with customized content*: Enable to forward the infected email as an attachment with the customized email body that you define in the custom email template. For example, in the template, you may want to say “The attached email is infected by a virus”. For details, see Customizing email templates on page 79. • *Repackage email with original text content*: Enable to forward the infected email as an attachment but the original email body will still be used without modification.

Configuring content profiles and content action profiles

The *Content* sub-menu lets you configure content profiles for incoming and outgoing content-based scanning. The available options vary depending on the chosen directionality.

Configuring content profiles

The *Content* tab lets you create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

Unlike antispam profiles, which deal primarily with spam, content profiles match any other type of email.

You can use content profiles to apply content-based encryption to email, or to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. You can apply content profiles to email that you want to protect and email that you want to prevent.

To view and configure content profiles

1. Go to *Profile* > *Content* > *Content*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone*. A single-field dialog appears. Enter a name for the new profile. Click *OK*.
Domain (dropdown list)	Select *System* to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain Name (column)	Displays either *System* or the name of a protected domain.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new profile, from the *Domain* dropdown, select either *System* to see profiles that apply to the entire FortiMail unit, or select the name of a protected domain.
4. For a new profile, enter its name. The profile name is editable later.
5. In *Action*, select a content action profile to use. For details, see Configuring content action profiles on page 224.
6. Configure the following sections:
   - Configuring attachment scan rules on page 217
   - Configuring scan options on page 217
   - Configuring content disarm and reconstruction (CDR) on page 218
   - Configuring archive handling on page 219
   - Configuring password decryption options on page 221
   - Configuring content monitor and filtering on page 221
7. Click *Create* or *OK* to save the content profile.

Configuring attachment scan rules

The attachment scan rules define what actions will be taken if the specified files types are found in email attachments.

Before you can configure the scan rule, you must configure the file filters. See Configuring file filters on page 222.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Attachment Scan Rule* section.
4. Click *New* to add a rule:

GUI item	Description
Enabled	Select to enable the rule.
File filter	Select the file filter. See Configuring file filters on page 222.
Operator	Select *Is* or *Is Not*. If *Is* is selected, the below action will be taken. If *Is Not* is selected, the below action will not be taken. You can use the *Is Not* option to safelist some attachment types. For example, if you want to reject all file types except for the PDF files, you can specify that *PDF Is Not Reject*.
Action	Specify the action. Or click *New* to create a new action profile.

Configuring scan options

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Scan Option* and configure the following:

GUI item	Description
Bypass scan on SMTP authentication	Enable to omit content profile scanning if the SMTP session is authenticated.
Detect fragmented email	Enable to detect and block fragmented email. Some mail user agents, such as Microsoft Outlook, can fragment big emails into multiple sub-messages. This is used to bypass oversize limits and scanning.
Detect password protected Office/PDF document	Enable to apply the block action configured in the content action profile if an attached Microsoft Office, OpenOffice, or PDF document is password-protected, and therefore cannot be decompressed in order to scan its contents.

GUI item	Description
Attempt to decrypt Office/PDF document	Enable to decrypt Microsoft Office, Open Office, or PDF attachments using the predefined or user-defined passwords. For details, see Configuring file passwords on page 223.
Detect embedded component	Specify which option(s) to use when scanning documents with embedded files such as Microsoft Office, Microsoft Visio, OpenOffice.org , and PDF documents. Similar to an archive, documents can sometimes contain video, graphics, sounds, and other files that are used by the document. By wrapping files within a document instead of linking to the file on a separate, external location, a document becomes more portable. However, it also means that documents with other files embedded can be used to hide infected files.
Policy match	Enable to defer mail delivery from specific senders configured in the policy. By sending low-priority, bandwidth-consuming email such as newsletter digest or marketing campaigns at scheduled times, you can conserve bandwidth at peak time so that high priority email can be sent more quickly. For information on policy, see How to use policies on page 145. For information on scheduling deferred delivery, see Configuring mail server settings on page 1.
Maximum number of attachment	Enter how many attachments are allowed in one email message. The valid range is from 1 to 100.
Maximum size	Enter the maximum size threshold in kilobytes for email or attachments.
Adult image analysis	If you have purchased the image scan feature license, you can enable the scan for image categories that you may want to block, such as violence and adult images. You can also configure the scan sensitivity and image fie size threshold. For details, see Configuring image analysis on page 1.

Configuring content disarm and reconstruction (CDR)

Configure these settings to sanitize email that contains hyperlinks and scripts, including in attachments, in order to reduce risk of spam, malware, and tracking. For more information about CDR, see Configuring content disarming and reconstruction on page 281.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *Content Disarm and Reconstruction* and configure the following:

GUI item	Description
Action	Select an action. See Configuring content action profiles on page 224.
HTML content	Enable to detect risky hypertext markup language (HTML) tags in an HTML email body, and then select how FortiMail will sanitize the email:

GUI item	Description
	• *Convert to text*: Convert the HTML email to plain text. • *Modify content*: Modify the HTML content, using the following settings: • *Active content*: Select to either *Keep* or *Remove*active content such as JavaScript. • *URL*: Select whether to: • *Keep*: Keep the URL or script. Do not remove or modify it. • *Remove*: Remove the URL or script. • *Redirect to FortiIsolator*: Redirect the user to FortiIsolator so that the user will be browsing indirectly, protected through FortiIsolator. To view the settings for URL click protection and FortiIsolator, click *View settings*. • *Redirect to Click Protection*: Rewrite the URL. If the user clicks on the URL, scan the URL and then perform click protection action configured in Configuring CDR URL click protection and removal options on page 282. • *Redirect to Click Protection + FortiIsolator*: Rewrite the URL and if the user clicks on it, redirect the URL to FortiMail for scanning. If the URL is malicious, it will be blocked; if the URL passes the scan, then it is rewritten to point to FortiIsolator, and the user will browse through FortiIsolator. • *Neutralize*: Modify the URL to make it inactive when clicked, but still easy to determine what the original URL was. For example, a link to: `https://www.example.com` is changed to: `hxxps:\\www[.]example[.]com` Then in *Apply to*, select whether CDR modifications should apply to either *Tag attribute* (for example, the `href` attribute in hyperlinks such as `<a href="https://example.com">`), *Tag text content*, or both. FortiMail will also add: `X-FEAS-ATTACHMENT-FILTER: Contains HTML tags.` to the message headers.
Text content	Enable to detect risky URLs in a plain text email body, and then in *URL*, select how FortiMail will sanitize the email (the options are similar to *URL* for HTML email).
MS Office	Enable to disarm and reconstruct Microsoft Office attachments. This also includes ZIP files that are compressed (nested compression is not supported).
PDF	Enable to disarm and reconstruct the PDF attachments. This also includes ZIP files that are compressed (nested compression is not supported).

Configuring archive handling

For email with archive attachments, you can decide what to do with them. Currently, FortiMail supports ZIP, PKZIP, GZIP, BZIP, TAR, RAR, JAR, CAB, 7Z, and EGG for content inspection.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *Archive Handling* and configure the following:

GUI Item	Description
Check archive content	Enable to determine which action to perform with the archive attachments. • blocking password protected archives if you have selected *Detect Password Protected Archive* • blocking archives that could not be successfully decompressed if you have selected *Detect on Failure to Decompress* • passing/blocking by comparing the depth of nested archives with the nesting depth threshold configured in *Max Level of Compression* By default, archives with less than 10 levels of compression will be blocked if they cannot be successfully decompressed or are password-protected. Depending on the nesting depth threshold and the attachment's depth of nested archives, the FortiMail unit may **also** consider the file types of files within the archive when determining which action to perform. For details, see the section below. If disabled, the FortiMail unit will perform the *Block*/*Pass* action solely based upon whether an email contains an archive. It will disregard the depth of nesting, password protection, successful decompression, and the file types of contents within the archive.
Detect archive bomb and decompression failure	Enable to apply the block action configured in the content action profile if an attached archive cannot be successfully decompressed, such as if the compression algorithm is unknown, and therefore cannot be decompressed in order to scan its contents. This option is available only if *Check archive content* is enabled.
Detect password protected archive	Enable to apply the block action configured in the content action profile if an attached archive is password-protected, and therefore cannot be decompressed in order to scan its contents. This option is available only if *Check archive content* is enabled.
Attempt to decrypt archive	Enable to decrypt and scan the archives, using the passwords configured in Configuring password decryption options on page 221. If it fails, the email will be passed. This option is available only if *Check archive content* is enabled.
Max level of compression	Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail unit uses one of the following methods to determine if it should block or pass the email. • *Max Level of Compression* is 0, or attachment's depth of nesting equals or is less than *Max Level of Compression*: If the attachment contains a file that matches one of the other file types, perform the action configured for that file type, either block or pass. • Attachment's depth of nesting is greater than *Max Level of Compression*: Apply the block action, unless you have deselected the check box for *Max Level of Compression*, in which case it will pass the file type content filter. Block actions are specified in the content action profile. The specified compression value is always considered if *Check Archive Content* is enabled, but has an effect only if the threshold is exceeded. This option is available only if *Check archive content* is enabled.

Configuring password decryption options

For password-protected PDF and archive attachments, if you want to decrypt and scan them, you can specify what kind of passwords you want to use to decrypt the files.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *File Password Decryption Options*.
4. Specify the type of passwords to use:
   - *Words in email content*: Enable and enter the *Number of adjacent word to keyword* to specify how many words before and after the keywords to try as the password for file decryption. For example, in an email, there could be a sentence such as: "To open the document, please use password 123456. If you cannot open it, please contact us." If you specify to use two words before and after the keyword, then "please", "use" (two words before the keyword "password"), "123456", and "If" (two words after the keyword "password") would be used as one by one as the password to decrypt the attachments. If no keyword exists, any words in the email body may be tried as the password.
   - *Built-in password list*: Enable this option to use the predefined passwords.
   - *User-defined password list*: Enable this option to use the passwords defined under *Profile* > *Content* > *File Password*. For details, see Configuring file passwords on page 223.

Configuring content monitor and filtering

The monitor profile uses the dictionary profile to determine matching email messages, and the actions that will be performed if a match is found.

You can also select to scan Microsoft Office, PDF, or archived email attachments.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 216.

To configure a content monitor profile

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Content Monitor and Filtering*.

GUI item	Description
Move (button)	Mark a check box to select a content monitor profile, then click this button. Choose *Up* or *Down* from the pop-up menu. Content monitor profiles are evaluated for a match in order of their appearance in this list. Usually, content monitor profiles should be ordered from most specific to most general, and from accepting or quarantining to rejecting.
Delete (button)	Mark a check box to select a content monitor profile, then click this button to remove it. **Note:** Deletion does not take effect immediately; it occurs when you save the content profile.

4. Click *New* for a new monitor profile or double-click an existing profile to modify it.

A dialog appears.

5. Configure the following:

GUI item	Description
Enable	Enable to use the content monitor to inspect email for matching email and perform the configured action.
Dictionary	Select either *Profile* or *Group*, then select the name of a dictionary profile or group from the dropdown list next to it. If no profile or group exists, click *New* to create one, or select an existing profile or group and click *Edit* to modify it. A dialog appears. For information on creating and editing dictionary profiles and groups, see Configuring dictionary profiles on page 262.
Minimum score	Displays the number of times that an email must match the dictionary profile before it will receive the action configured in *Action*. Note that the score value is based on individual dictionary profile matches, not the dictionary group matches.
Action	Displays action that the FortiMail unit will perform if the content of the email message matches words or patterns from the dictionary profile. If no action exists, click *New* to create one, or select an existing action and click *Edit* to modify it. A dialog appears. For information on action profiles, see Configuring content action profiles on page 224.
Scan Condition	Select the content type(s) to scan: • *PDF files* • *Microsoft Office files* • *Archived PDF and MS Office files*. If you select this option, you can also use the following CLI commands to specify the maximum levels to decompress and the maximum file size to decompress: `config mailsetting mail-scan-options` `set decompress-max-level <level_1-16>` `set decompress-max-size <MB_int>` `end`

6. Click *Create* or *OK*.

Configuring file filters

File filters are used in the attachment scan rules (see Configuring attachment scan rules on page 217. File filters defines the email attachment file types and file extensions to be scanned.

Wildcards can be used in file filters. For details, see Appendix: Wildcards and regular expressions on page 380.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles and content action profiles on page 215.

1. Go to *Profile* > *Content* > *File Filter*.
2. Click *New* to create a new filter or double click on an existing filter to edit it.

GUI item	Description
Domain	The new filter can applied to a domain or system wide.
Name	Enter a name for the filter.
Description	Optionally enter a description.
File Type	Either select from the predefined types and/or specify your own.
File Extension	Either select from the predefined extensions and/or specify your own.

Encrypted email content cannot be scanned for spam, viruses, or banned content.

Unlike other attachment types, archives may receive an action other than your *Block*/*Pass* selection, depending on your configuration in the *Scan Conditions* (see Action on page 175).

For each file type, you can use an action profile to overwrite the default action profile used by the content profile. For example, if you want to redirect encrypted email to a third party server (such as a PGP Universal Server) for decryption, You can:

1. Create a content action profile and enable the Send to alternate host option in the action profile. Enter the PGP server as the alternate host. For details about how create a content action profile, see Configuring content action profiles on page 224.
2. Select to block the `encrypted/pgp` file type under `document/encrypted`. “Block” means to apply an action profile.
3. Select the action profile for the `document/encrypted` file type. This action profile will overwrite the action profile you select for the entire content profile.

Configuring file passwords

When you configure a content profile, you can choose to decrypt documents (see Configuring scan options on page 217) and archived files (see Configuring archive handling on page 219). To decrypt the documents, you need passwords. See also Configuring password decryption options on page 221.

To configure user-defined passwords

1. Go to *Profile* > *Content* > *File Password*.
2. Click *New*.
3. Enter the password that will be used to decrypt documents.
4. Click *Create*.

Configuring content action profiles

The *Action* tab in the *Content* submenu lets you define content action profiles. Use these profiles to apply content-based encryption.

Alternatively, content action profiles can define one or more things that the FortiMail unit should do if the content profile determines that an email contains prohibited words or phrases, file names, or file types.

For example, you might have configured most content profiles to match prohibited content, and therefore to use a content action profile named `quar_profile` which quarantines email to the system quarantine for review.

However, you have decided that email that does not pass the dictionary scan named `financial_terms` is **always** prohibited, and should be rejected so that it does not require manual review. To do this, first configure a second action profile, named `rejection_profile`, which rejects email. You would then override `quar_profile` specifically for the dictionary-based content scan in each profile by selecting `rejection_profile` for content that matches `financial_terms`.

To view and manage the list of content action profiles

1. Go to *Profile* > *Content* > *Action*.

GUI item	Description
Domain (dropdown list)	Select *System*to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain (column)	Displays either *System* or a domain name.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click an existing profile to modify it.
   A dialog appears.
3. Configure the following:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter its name.
Tag subject	Enable and enter the text that will appear in the subject line of the email, such as `[PROHIBITED-CONTENT]`. FortiMail prepends this text to the subject line of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.

GUI item	Description
Insert header	Enable and click New to enter a message header key. The FortiMail unit adds this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Content-Filter: Contains banned word.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. You can add multiple headers by adding them to the header table. You can also insert the predefined variables to the header value. **Note**: Do not enter spaces in the key portion of the header line. These are forbidden by RFC 2822.
Remove header	Enable and click *New* to enter the message header name to be removed.
Insert disclaimer	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System* > *Mail Setting* > *Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email.
Deliver to original host	Enable to route the email to the original SMTP server or relay. Note the you can deliver email to both the original and alternate hosts. You can choose to deliver the original email or the modified email.
FortiGuard spam outbreak protection	Enable to send incoming email to the deferred mail queue. See also Configuring mail server settings on page 1.
Defer delivery	Enable to defer delivery of emails that may be resource intensive and reduce throughput of the mail server, such as large email messages, or mass email such as marketing campaign email and newsletter digest. See also. See also Configuring mail server settings on page 1.
BCC	Enable to send a blind carbon copy (BCC) of the email. Configure BCC recipient email addresses by entering each one and clicking *Create* in the BCC area.
Replace with message	Enable to replace the email's contents with a replacement message. Then select a replacement message from the dropdown list. For more information, see Customizing custom messages, and email templates on page 71.

GUI item	Description
Notify with profile	Enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification email is customizable and will tell the users what happened to the email message. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
Final action	Select one of the following final actions listed below for the content action profile.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
Reject	Enable to reject the email and reply to the SMTP client with SMTP reply code 550. However, if email messages are held for FortiGuard spam outbreak protection or FortiGuard virus outbreak protection, or sent to FortiSandbox, the actual action will fallback to "system quarantine".
Personal quarantine	For incoming email, enable to redirect the email to the recipient's personal quarantine. For more information, see Managing the personal quarantines on page 43. For outgoing email, this action will fallback to the system quarantine.
System quarantine	Enable to redirect spam to the system quarantine and then select the quarantine folder. For more information, see Managing the system quarantine on page 46. You can also enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification recipients will be able to release the quarantined email using the URL in the notification email. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
Domain quarantine	Enable to redirect spam to the domain quarantine and then select the quarantine folder. For more information, see Managing the domain quarantines on page 48. You can also enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification recipients will be able to release the quarantined email using the URL in the notification email. For details about notification profiles and email templates, see Configuring notification profiles on page 274 and Customizing email templates on page 79.
Rewrite recipient email address	Enable to change the recipient address of any email that matches the content profile. Configure rewrites separately for the local-part (the portion of the email address before the @ symbol, typically a user name) and the domain part (the portion of the email address after the @ symbol). For each part, select either: • *None*: No change. • *Prefix*: Prepend the part with text that you have entered in the *With* field. • *Suffix*: Append the part with the text you have entered in the *With* field. • *Replace*: Substitute the part with the text you have entered in the *With* field.

GUI item	Description
Encrypt with profile	Enable to apply an encryption profile, then select which encryption profile to use. For details, see Configuring encryption profiles on page 268. Note that If you select an IBE encryption profile, it will be overridden if either S/MIME or TLS or both are selected in the message delivery rule configuration (*Policy > Access Control > Delivery > New*). For information about message delivery rules, see Configuring delivery rules on page 156.
Treat as spam	Enable to perform the *Actions* selected in the antispam profile of the policy that matches the email. See Configuring antispam profiles and actions on page 187.

4. To apply a content action profile, select it in the *Action* dropdown list of one or more antispam profiles. For details, see Configuring antispam profiles on page 187.

Configuring replacement message profiles and variables

Starting from v7.2.0, replacement message customization for content and DLP actions and variable customization has been moved from *System > Customization > Custom Message* to *Profile > Replacement Message*.

The replacement messages are used in the content/DLP action profiles when specifying the "Replace with message" action (see Configuring content profiles and content action profiles on page 215), and in the antivirus action profiles when you specifying the "Replace infected/suspicious body or attachment" action (see Configuring antivirus profiles, file signatures, and actions on page 209).

You can customize replacement messages for the subject, body, or attachment part, depending on which part triggers the content/DLP scanning. For virus-infected email, you can replace either the email body or attachments.

Modifying replacement messages

You can modify the text and HTML code within a replacement message to suit your requirements.

You can change the content of the replacement message by editing the text and HTML codes and by working with replacement message variables.

All message groups can be edited to change text, or add text and variables.

To customize replacement messages

1. Go to *Profile > Replacement Message > Replacement Message*.
2. Click New to add a message or click edit to modify an existing message.
3. Enter a name for the message.
4. Enter a description.

5. Under Replacement Message, click New.
6. Select a type.
7. In the Replacement massage area, enter the content. There is a limit of 8191 characters for each replacement message.
8. Click Insert Variables to include any other existing variables, if needed.
9. Place your mouse cursor in the text message at the insertion point for the variable.
10. Click the name of the variable to add. It appears at the insertion point.
    For example, you may enter :
    `The file %%FILE%% has been detected containing virus %%VIRUS%%, and has been removed. File type is %%FILE_TYPE%%.`
    where `%%FILE%%` is the file name, `%%VIRUS%%` provides the virus name, and `%%FILE_TYPE%%` is the file type of the infected file.
11. To add a color code, use HTML tags, such as `<tr bgcolor="#3366ff">`. You can select a color code, such as `"#3366ff"` in the HTML tag, from the color palette after selecting Insert Color Code.
    Some message types include predefined variables.
12. Click OK, or click Reset To Default to revert the replacement message to its default text.

Creating variables

In addition to the predefined variables, you can create new ones to customize replacement messages and email templates. Typically, these variables represent messages that you will use frequently. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

To create a new variable

1. To create new variables to be used in the replacement messages, go to *Profile* > *Replacement Message* > *Variable*.
2. Click New.
   A dialog appears.
3. Configure the following:
   - In Name, enter the variable name to use in the replacement message. Its format is: `%%<variable_name>%%`. For example, if you enter the word `virus`, this variable will appear as `%%virus%%` in the replacement message if you select to insert it. This is usually a simple and short form for a variable.
   - In Display Name, enter words to describe the variable. For example, use `virus name` for the variable `virus`. The display name appears in the variable list when you select Insert Variables while customizing a message or creating a variable.
   - In Content, enter the variable's content.
4. Click Create.

Configuring resource profiles

Go to *Profile* > *Resource* > *Resource* to configure miscellaneous aspects of the email user accounts, such as disk space quota.

For more information on settings that can be applied to email user accounts, see Configuring local user accounts (server mode only) on page 111 and Configuring user preferences on page 115.

To configure resource profiles

1. Go to *Profile* > *Resource* > *Resource*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Domain (dropdown list)	Select System to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain Name (column)	Displays either System or a domain name.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile, or double-click a profile to modify it.
3. Configure the following:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter the name of the profile. The profile name is editable later.
Disk quota (MB)	Enter the disk space quota in megabytes for this profile. Valid values are 0-60000. Default value is 1000. This option is only available in server mode.
User account status	Enable email user accounts using this resource profile. If not enabled, the user will have no access to FortiMail system, including webmail, address book, quarantine, or any other functions.
Webmail access	Enable to allow email users to access FortiMail webmail and other webmail features, such as auto-reply and address books: • *User preference access*: Determine whether users can access preferences such as the idle session timeout and ability to automatically check for new messages. For information about idle sessions in webmail, see the FortiMail Webmail Online Help and FortiMail CLI Reference. • *Address book access*: Determine whether users can access the domain address book and system address book. • *Quarantine attachment download*: Enable or disable attachment download for quarantined email. Note this option is only available for Server and Gateway

GUI item	Description
	mode. When disabled, all email within the *Bulk* folder (including subfolders) will have attachment download disabled. • *Mobile device access*: Enable for disable user mail access via mobile device.
Email Continuity	Enable to enforce email continuity for instances where the SMTP server is inaccessible. **Note:** This feature requires a valid feature license, and must be enabled. See Configuring email continuity on page 1. When the SMTP server is detected as inaccessible, recipient verification is skipped and emails are put into the email continuity queue. When the SMTP server is accessible again, the email is delivered. Note there is no DSN if the email is from an unknown user. Additionally, expand *Email continuity* and enable *BCC self*. When enabled, customers who log on to the webmail portal and who send email during a service disruption will have a copy of the mail sent back to them once service is restored.
Personal Quarantine	Specify the personal quarantine options, such as release method and safelisting.
Email Retention	Enter the number of days after which the FortiMail unit will automatically delete email that is locally hosted in each folder. 0 means not to delete email.

4. To apply the resource profile, you must select it in a policy. For details, see Controlling email based on sender and recipient addresses on page 163 and Controlling email based on IP addresses on page 159.

Workflow to enable and configure authentication of email users

In general, to enable and configure email user authentication, you should complete the following:

1. If you want to require authentication for SMTP connections received by the FortiMail unit, examine the access control rules whose sender patterns match your email users to ensure that authentication is required (*Authenticated*) rather than optional (*Any*).
   Additionally, verify that no access control rule exists that allows unauthenticated connections. For details, see Configuring access control receiving policies on page 148.
2. For secure (SSL/TLS) authentication:
   - Upload a local certificate. For details, see Managing local certificates.
   - Enable *SMTP over SSL/TLS*. For details, see Configuring mail server settings.
   - If you want to configure TLS, create a TLS profile, and select it in the access control rules. For details, see Configuring TLS security profiles on page 266 and Configuring access control receiving policies on page 148.
   - If the email user will use a personal certificate to log in to webmail or their per-recipient quarantine, define the certificate authority (CA) and the valid certificate for that user. If *OCSP* is enabled, you must

Managing users on page 110, Managing certificate authority certificates, and Managing OCSP server certificates on page 1.

3. If authentication will occur by querying an external authentication server rather than email user accounts locally defined on the FortiMail unit, configure the appropriate profile type, either:
   - SMTP, IMAP, or POP3 (gateway mode or transparent mode only; see Configuring authentication profiles on page 231)
   - LDAP (see Configuring LDAP profiles on page 234)
   - RADIUS (see Configuring authentication profiles on page 231)
4. For server mode, configure the email users and type their password, or select an LDAP profile. Also enable webmail access in a resource profile. For details, see Configuring local user accounts (server mode only) on page 111 and Configuring resource profiles on page 228.
5. For gateway mode or transparent mode, select the authentication profile in the IP-based policy or in the incoming recipient-based that matches that email user and enable Use for SMTP authentication. If the user will use PKI authentication, in the incoming recipient-based policy, also enable Enable PKI authentication for web mail spam access. For details, see Controlling email based on sender and recipient addresses on page 163 and Controlling email based on IP addresses on page 159.
   For server mode, select the resource profile in the incoming recipient-based policy, and if users authenticate using an LDAP profile, select the LDAP profile. For details, see Controlling email based on sender and recipient addresses on page 163.

Configuring authentication profiles

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS
- LDAP
- SSO

LDAP profiles can configure many features other than authentication. For details, see Configuring LDAP profiles on page 234.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine, and when authenticating with another SMTP server to deliver email.

For the general procedure of how to enable and configure authentication, see Workflow to enable and configure authentication of email users on page 230.

To configure an SMTP, IMAP, or POP3 authentication profile

1. Go to *Profile* > *Authentication* > *SMTP*, *IMAP*,or *POP3*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. Configure the following settings:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter the name of the profile. The profile name is editable later.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of a server that will be queried to authenticate email users if they authenticate to send email, or when they are accessing their personal quarantine.
Server port	Enter the port number on which the authentication server listens. See also Appendix: Port Numbers on page 375.
Use generic LDAP mail host if available (SMTP authentication only)	For gateway and transparent mode, select this option if your LDAP server has a mail host entry for the generic user. For more information, see Domain Lookup Query on page 247. If you select this option, the FortiMail unit will query the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will query the server you entered in the Server name/IP field.
Authentication mechanism	Select an authentication mechanism. For more information, consult the relevant RFCs.
Authentication options	
SSL/TLS	Enable if you want to use transport layer security (TLS) to authenticate and encrypt communications between the FortiMail unit and this server, and if the server supports it.
STARTTLS	Enable if you want to upgrade the existing insecure connection to the secure connection using SSL/TLS.
Secure authentication	Enable if you want to use secure authentication to encrypt the passwords of email users when communicating with the server, and if the server supports it.
Server requires domain	Enable if the authentication server requires that email users authenticate using their full email address (such as `user1@example.com`) and not just the user name (such as `user1`).

4. To apply the authentication profile, depending on the mode in which your FortiMail unit is operating, you may be able to select the profile in incoming recipient-based policies, IP-based policies, and email user accounts. For details, see Controlling email based on sender and recipient addresses on page 163, Controlling email based on IP addresses on page 159, and Configuring local user accounts (server mode only) on page 111.

To configure a RADIUS authentication profile

1. Go to *Profile* > *Authentication* > *RADIUS*.
2. Either click *New* to add a profile or double-click a profile to modify it.

3. Configure the following settings:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter the name of the profile.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of a server that will be queried to authenticate email users if they authenticate to send email, or when they are accessing their personal quarantine.
Server port	Enter the port number on which the authentication server listens. See also Appendix: Port Numbers on page 375.
Protocol	Select the authentication scheme for the RADIUS server.
NAS IP/Called station ID	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiMail interface uses to communicate with the RADIUS server will be applied.
Server secret	Enter the secret required by the RADIUS server. It must be identical to the secret that is configured on the RADIUS server.
Server requires domain	Enable if the authentication server requires that email users authenticate using their full email address (such as `user1@example.com`) and not just the user name (such as `user1`).
Advanced Setting	When you add a FortiMail administrator (see Configuring administrator accounts on page 69), you must specify an access profile (the access privileges) for the administrator. You must also specify a domain (either system or a protected domain) that the administrator is entitled to access. If you are adding a RADIUS account, you can override the access profile and domain setting with the values of the remote attributes returned from the RADIUS server. • *Enable remote access override*: Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing access profile. If there is no match, the specified access profile will still be used. • *Vender ID*: Enter the vender's registered RADIUS ID for remote access permission override. The default ID is `12356`, which is Fortinet. • *Attribute ID*: Enter the attribute ID of the above vender for remote access permission override. The attribute should hold an access profile name that exists on FortiMail. The default ID is `6`, which is `Fortinet-Access-Profile`. • *Enable remote domain override*: Enable to override the domain you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing protected domain. If there is no match, the specified domain will still be used. • *Vender ID*: Enter the vender's registered RADIUS ID for remote domain override. The default ID is `12356`, which is Fortinet. • *Attribute ID*: Enter the attribute ID of the above vender for remote domain override. The attribute should hold a domain name that exists on FortiMail. The default ID is `3`, which is `Fortinet-Vdom-Name`.

4. To apply the authentication profile, depending on the mode in which your FortiMail unit is operating, you may be able to select the profile in incoming recipient-based policies, IP-based policies, and email user accounts. For details, see Controlling email based on sender and recipient addresses on page 163, Controlling email based on IP addresses on page 159, and Configuring local user accounts (server mode only) on page 111.

Configuring LDAP profiles

The *LDAP* submenu lets you configure LDAP profiles which can query LDAP servers such as FortiAuthenticator, Microsoft Active Directory, Red Hat Directory Server, or Google Cloud Identity for authentication, email address mappings, and more.

Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server. When LDAP queries do not match with the server's schema and/or contents, unintended mail processing behaviors can result, including bypassing antivirus scans. For details on preparing an LDAP directory for use with FortiMail LDAP profiles, see Preparing your LDAP schema for FortiMail LDAP profiles on page 250.

LDAP profiles each contain one or more queries that retrieve specific configuration data, such as user groups, from an LDAP server. The LDAP profile list indicates which queries you have enabled in each LDAP profile.

To view the list of LDAP profiles, go to *Profile* > *LDAP* > *LDAP*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone*. A single-field dialog appears. Enter a name for the new profile. Click *OK*.
Name	Displays the name of the profile.
Comment	Displays the comment in the profile.
Server	Displays the domain name or IP address of the LDAP server.
Port	Displays the listening port of the LDAP server.
Group	Indicates whether *Group Query* is enabled.
Auth	Indicates whether *User Authentication* is enabled.
Alias	Indicates whether *User Alias* is enabled.
Routing	Indicates whether *Mail Routing* is enabled.
Address Map	Indicates whether *Address Mapping* is enabled.
Cache	Indicates whether query result caching is enabled.
Ref.	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

You can add an LDAP profile to define a set of queries that the FortiMail unit can use with an LDAP server. You might create more than one LDAP profile if, for example, you have more than one LDAP server, or you want to configure multiple, separate query sets for the same LDAP server.

After you have created an LDAP profile, LDAP profile options will appear in other areas of the FortiMail unit's configuration. These options let you to select the LDAP profile where you might otherwise create a reference to a configuration item stored locally on the FortiMail unit itself. These other configuration areas will only allow you to select applicable LDAP profiles — that is, those LDAP profiles in which you have enabled the query required by that feature. For example, if a feature requires a definition of user groups, you can select only from those LDAP profiles where *Group Query Option* are enabled.

To configure an LDAP profile

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to add a profile or double-click a profile to modify it.
3. Configure the following settings:

GUI item	Description
Name	For a new profile, enter a unique name.
Comment	Optional. Enter a descriptive comment.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. *Port*: Enter the port number where the LDAP server listens. The default port number varies by your selection in Use secure connection. See also Appendix: Port Numbers on page 375.
Fallback server name/IP	Optional. Enter the fully qualified domain name (FQDN) or IP address of an alternate LDAP server that the FortiMail unit can query if the primary LDAP server is unreachable. *Port*: Enter the port number where the fallback LDAP server listens. The default port number varies by your selection in Use secure connection. See also Appendix: Port Numbers on page 375.
Use secure connection	Select whether or not to connect to the LDAP servers using an encrypted connection. • *None*: Use a non-secure connection. • *SSL*: Use an SSL/TLS-secured (LDAPS) connection. If the LDAP server requires that clients such as the FortiMail unit present a client certificate to identify themselves during secure connections, then select the certificate from the *Client certificate* dropdown. Optionally, to authenticate using the selected certificate, enable *Use client certificate for TLS authentication*.This can be used instead of, or in addition to, a bind DN and password. See also Managing local certificates on page 1. Click *Test LDAP Query* to test the connection. A pop-up window appears. For details, see To verify a user query on page 258. **Note:** If your FortiMail unit is deployed in server mode, and you want to enable Enable webmail password change using an LDAP server that uses a Microsoft Active Directory-style schema, then you must select *SSL*. Active Directory servers require a secure connection for queries that change user passwords. **Note:** The certificate that FortiMail uses for client authentication must:

GUI item	Description
	• not be expired • not be revoked • be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail unit and that the server trusts (directly or indirectly, proven via a signing chain) Otherwise the secure connection will fail. Servers may have their own certificate validation requirements in addition to FortiMail requirements. For example, client certificates may require that `Key Usage` field allow client authentication. See your LDAP server's documentation.
Default Bind	
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for user objects, such as: `ou=People,dc=example,dc=com` User objects should be child nodes of this location.
Bind DN	Enter the bind DN of an LDAP user account with permissions to query the *Base DN*, such as: `cn=fortimail,dc=example,dc=com`
Bind password	Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in Base DN, or, if you have not yet entered a Base DN, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your Base DN, or need to look up attribute names. For example, if the Base DN is unknown, browsing can help you to locate it. **Note:** Before you click *Browse*, you must configure Server name/IP, Use secure connection, Bind DN, Bind password, and Protocol version, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection. When browsing the LDAP directory, you can search the directory for a specific DN. **Note**: • The search filter must follow the LDAP query syntax defined in RFC 2254, for example, `(|(cn=user1)(cn=*aaa*))`. • Wildcards are supported. • Search conditions: and (&), or (|) are supported. • The search filter applies only to the current level of the LDAP directory, not the sub directories.

4. Configure the following:
   - User Query
   - Group Query
   - User Authentication
   - User Alias
   - Mail Routing
   - Address Mapping

- Scan Override
- Domain Lookup
- Hostname/IP Lookup
- Remote Access Override
- LDAP Profile Chain
- Advanced

User Query

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *User Query* section.
4. Configure the query to retrieve the distinguished names (DN) of user objects by their email addresses:

GUI item	Description
Schema	Select a schema style. Then you can edit the schema or select *User Defined* and write your own schema.
User query	Enter an LDAP query filter that selects a set of user objects from the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects. For details, see Example: LDAP user query on page 238. For details on query syntax, refer to any standard LDAP query filter reference manual. **Warning**: To avoid user query confusion, this field cannot be empty.
Scope	Select which level of depth to query, starting from Base DN. • *One level:* Query only the one level directly below the base DN in the LDAP directory tree. • *Subtree*: Query recursively all levels below the base DN in the LDAP directory tree.
Derefer	Select the method to use, if any, when following the pointers of attributes whose values are references: • *Never*: Do not dereference. • *Always*: Always dereference. • *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.
Retrieve display name for webmail	If enabled, when a webmail user (authenticated using LDAP) composes email, the display name of the `From:` header will be automatically set to the value defined in LDAP, instead of the user preference.
Display name attribute	Enter the LDAP attribute of the display name to query. The default value is `cn`.

Example: LDAP user query

For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:

```
(& (objectClass=inetOrgPerson) (mail=$m))
```

where `$m` is the FortiMail variable for a user's email address.

If the email address (`$m`) as it appears in the message header is different from the user's email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the user by the email address (`$m`) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract `-spam` from the **end** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=inetOrgPerson) (mail=$m$
     {-spam}))
```

where `${-spam}` is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract `spam-` from the **beginning** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=inetOrgPerson) (mail=$m$
     {^spam-}))
```

where `${^spam-}` is the FortiMail variable for the tag to remove before performing the query.

For some schemas, such as Microsoft Active Directory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure *User Alias* to resolve aliases. For details, see User Alias on page 241.

Group Query

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *Group Query* section.
   For more information on determining user group membership by LDAP query, see Controlling email based on sender and recipient addresses on page 163 or Controlling email based on IP addresses on page 159.
4. Configure the following:

GUI item	Description
Use LDAP tree node as group	Enable to use objects within the Base DN of *User Query* as if they were members of a user group object. For example, your LDAP directory might not contain user group objects. In that sense, groups do not really exist in the LDAP directory. However, you could mimic a group's presence by enabling this option to treat all users that are child objects of the Base DN in *User Query* as if they were members of such a group.

GUI item	Description
Group membership attribute	Enter the name of the attribute, such as `memberOf` or `gidNumber`, whose value is the group number or DN of a group to which the user belongs. This attribute must be present in user objects. Whether the value must use common name, group number, or DN syntax varies by your LDAP server schema. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`.
Use group name with base DN as group DN	Enable to specify the base distinguished name (DN) portion of the group's full DN in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query. For example, you might find it more convenient in each recipient-based policy to type only the group name, `admins`, rather than typing the full DN, `cn=admins,ou=Groups,dc=example,dc=com`. In this case, you could enable this option, then configure Group base DN (`ou=Groups,dc=example,dc=com`) and Group name attribute (`cn`). When performing the query, the FortiMail unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the Group name attribute and the Group base DN configured in the LDAP profile. **Note:** Enabling this option is appropriate **only if** your LDAP server's schema specifies that the group membership attribute's value must use DN syntax. It is **not** appropriate if this value uses another type of syntax, such as a number or common name. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`. Because a group ID number does not use DN syntax, you would not enable this option.
Group base DN	Enter the base DN portion of the group's full DN, such as: `ou=Groups,dc=example,dc=com` This option is available only if Use group name with base DN as group DN is enabled.
Group name attribute	Enter the name of the attribute, such as `cn`, whose value is the group name of a group to which the user belongs. This option is available only if Use group name with base DN as group DN is enabled.
Max group expansion level	Enter how many levels of nested groups will be expanded for lookup. Valid range is 1-6. Default value is 1.
Lookup group owner	Enable to query the group object by its distinguished name (DN) to retrieve the DN of the group owner, which is a user that will receive that group's quarantine reports. Using that user's DN, the FortiMail unit will then perform a second query to retrieve that user's email address, where the quarantine report will be sent.

GUI item	Description
	For more information on sending quarantine reports to the group owner, see Quarantine Report Setting on page 100 and Managing the personal quarantines on page 43.
Group owner attribute	Enter the name of the attribute, such as `groupOwner`, whose value is the distinguished name of a user object. You can configure the FortiMail unit to allow that user to be responsible for handling the group's quarantine report. If Lookup group owner is enabled, this attribute must be present in group objects.
Group owner address attribute	Enter the name of the attribute, such as `mail`, whose value is the group owner's email address. If Lookup group owner is enabled, this attribute must be present in user objects.

User Authentication

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *User Authentication* section.
   For more information on authenticating users by LDAP query, see Controlling email based on sender and recipient addresses on page 163.
4. Configure the following:

GUI item	Description
Try UPN or mail address as bind DN	Select to form the user's bind DN by prepending the user name portion of the email address (`$u`) to the User Principle Name (UPN, such as `example.com`). By default, the FortiMail unit will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, enter that UPN in the field named *Alternative UPN suffix*. This can be useful if users authenticate with a domain other than the mail server's principal domain name.
Try common name with base DN as bind DN	Select to form the user's bind DN by prepending a common name to the base DN. Also enter the name of the user objects' common name attribute, such as `cn` or `uid` into the field. This option is preconfigured and read-only if, in *User Query*, you have selected from Schema any schema style other than *User Defined*.
Search user and try bind DN	Select to form the user's bind DN by using the DN retrieved for that user by *User Query*.

User Alias

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *User Alias* section.

   Resolving aliases to real email addresses enables the FortiMail unit to send a single quarantine report and maintain a single quarantine mailbox at each user's primary email account, rather than sending separate quarantine reports and maintaining separate quarantine mailboxes for each alias email address. For FortiMail units operating in server mode, this means that users need only log in to their primary account in order to manage their spam quarantine, rather than logging in to each alias account individually.
4. Configure the following:

GUI item	Description
Schema (dropdown list)	Click *Schema* to select a schema style. Then you can edit the schema or select *User Defined* and write your own schema.
Alias member attribute	Enter the name of the attribute, such as `mail` or `rfc822MailMember`, whose value is an email address to which the email alias resolves, such as `user@example.com`. This attribute must be present in either alias or user objects, as determined by your schema and whether it resolves aliases directly or indirectly. For more information, see Base DN on page 236. This option is preconfigured and read-only if, in *User Alias*, you have selected from Schema any schema style other than *User Defined*.
Alias member query	Enter an LDAP query filter that selects a set of either user or email alias objects, whichever object class contains the attribute you configured in *Alias member attribute*, from the LDAP directory. This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*. The query string filters the result set, and should be based upon any attributes that are common to all user/alias objects but also exclude objects that are not user/alias objects. For details, see Example: Alias member query on page 243. For more information on required object types and their attributes, see Preparing your LDAP schema for FortiMail LDAP profiles on page 250. For details on query syntax, refer to any standard LDAP query filter reference manual.
User group expansion In advance	Enable if your LDAP schema resolves email aliases indirectly. For more information on direct versus indirect resolution, see Base DN on page 236. When this option is **disabled**, alias resolution occurs using **one** query. The FortiMail unit queries the LDAP directory using the Base DN and the Alias member query, and then uses the value of each Alias member attribute to resolve the alias. When this option is **enabled**, alias resolution occurs using **two** queries: • The FortiMail unit first performs a preliminary query using the Base DN and Group member query, and uses the value of each Group member attribute as

GUI item	Description
	the base DN for the second query. • The FortiMail unit performs a second query using the distinguished names from the preliminary query (instead of the *Base DN*) and the Alias member query, and then uses the value of each Alias member attribute to resolve the alias. The two-query approach is appropriate if, in your schema, alias objects are structured like group objects and contain references in the form of distinguished names of member user objects, rather than directly containing email addresses to which the alias resolves. In this case, the FortiMail unit must first "expand" the alias object into its constituent user objects before it can resolve the alias email address. This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*.
Group member attribute	Enter the name of the attribute, such as `member`, whose value is the DN of a user object. This attribute must be present in alias objects only if they do not contain an email address attribute specified in Alias member attribute. This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*. If you have selected *User Defined*, this option is available only if User group expansion In advance is enabled.
Group member query	Enter an LDAP query filter that selects a set of alias objects, represented as a group of member objects in the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all alias objects but also exclude non-alias objects. For example, if alias objects in your directory have two distinguishing characteristics, their `objectClass` and `proxyAddresses` attributes, the query filter might be: `(&(objectClass=group) (proxyAddresses=smtp:$m))` where `$m` is the FortiMail variable for a recipient email address. (`$s` is a sender email address.) This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*. If you have selected *User Defined*, this option is available only if User group expansion In advance is enabled. For details on query syntax, refer to any standard LDAP query filter reference manual.
Max alias expansion level	Specify the maximum number of alias nesting levels that will be expanded for lookup. Valid range is 1-12 and the default value is 1.
Scope	Select which level of depth to query, starting from Base DN. • *One level*: Query only the one level directly below the base DN in the LDAP directory tree. • *Subtree:* Query recursively all levels below the base DN in the LDAP directory tree.
Derefer	Select the method to use, if any, when dereferencing attributes whose values are references. • *Never*: Do not dereference. • *Always*: Always dereference.

GUI item	Description
	• *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.
Use separate bind (configure the following if Default Bind is not what you want)	
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for either alias or user objects. User or alias objects should be child nodes of this location. Whether you should specify the base DN of either user objects or alias objects varies by your LDAP schema style. Schema may resolve alias email addresses directly or indirectly (using references). • With a direct resolution, alias objects directly contain one or more email address attributes, such as `mail` or `rfc822MailMember`, whose values are user email addresses such as `user@example.com`, and that resolves the alias. The Base DN, such as `ou=Aliases,dc=example,dc=com`, should contain alias objects. • With an indirect resolution, alias objects do **not** directly contain an email address attribute that can resolve the alias; instead, in the style of LDAP group-like objects, the alias objects contain only references to user objects that are "members" of the alias "group." User objects' email address attribute values, such as `user@example.com`, actually resolve the alias. Alias objects refer to user objects by possessing one or more "member" attributes whose value is the DN of a user object, such as `uid=user,ou=People,dc=example,dc=com`. The FortiMail unit performs a first query to retrieve the distinguished names of "member" user objects, then performs a second query using those distinguished names to retrieve email addresses from each user object. The Base DN, such as `ou=People,dc=example,dc=com`, should contain user objects.
Bind DN	Enter the bind DN of an LDAP user account with permissions to query the Base DN, such as: `cn=FortiMailA,dc=example,dc=com`
Bind password	Enter the password of the Bind DN.

Example: Alias member query

For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:

```
(& (objectClass=alias) (mail=$m))
```

where `$m` is the FortiMail variable for a user's email address.

If the email address (`$m`) as it appears in the message header is different from the alias email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the alias by the email address (`$m`) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract `-spam` from the **end** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=alias) (mail=$m${-spam}))
```

where `${-spam}` is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract `spam-` from the **beginning** of the user name portion of the recipient email address, you could use the query filter:

```
(& (objectClass=alias) (mail=$m${^spam-}))
```

where `${^spam-}` is the FortiMail variable for the tag to remove before performing the query.

Whether you should configure this query filter to retrieve user or alias objects depends on whether your schema resolves email addresses directly or indirectly (using references). For more information on direct versus indirect alias resolution, see Base DN on page 236.

If alias objects in your schema provide **direct** resolution, configure this query string to retrieve alias objects. Depending on your schema style, you can do this either using the user name portion of the alias email address (`$u`), or the entire email address (`$m`). For example, for the email aliases `finance@example.com` and `admin@example.com`, if your LDAP directory contains alias objects distinguished by `cn: finance` and `cn: admin`, respectively, this query string could be `cn=$u`.

If alias objects in your schema provide **indirect** resolution, configure this query string to retrieve user objects by their distinguished name, such as `distinguishedName=$b` or `dn=$b`. Also enable *User group expansion In advance*, then configure *Group member query* to retrieve email address alias objects, and configure *Group Member Attribute* to be the name of the alias object attribute, such as `member`, whose value is the distinguished name of a user object.

Mail Routing

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *Mail Routing* section.

The *Mail Routing* query occurs after recipient tagging processing. If you have enabled recipient tagging, the *Mail Routing* query will then be based on the tagged recipient address. If the tagged email address does not exist for the user in the LDAP directory, you may prefer to transform the recipient address by using the *User Alias*.

4. Configure the following:

GUI item	Description
Mail host attribute	Enter the name of the attribute, such as `mailHost`, whose value is the fully qualified domain name (FQDN) or IP address of the email server that stores email for the user's email account. This attribute must be present in user objects.
Mail routing port attribute	Enter the name of the attribute whose value is the listening port number of the mail host.
Mail routing address attribute	Enter the name of the attribute, such as `mailRoutingAddress`, whose value is the email address of a deliverable user on the email server, also known as the mail host.

GUI item	Description
	For example, a user may have many aliases and external email addresses that are not necessarily known to the email server. These addresses would all map to a real email account (mail routing address) on the email server (mail host) where the user's email is actually stored. A user's recipient email address located in the envelope or header portion of each email will be rewritten to this address. This attribute must be present in user objects.

Address Mapping

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile > LDAP > LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *Address Mapping* section.

   Mappings usually should not translate an email address into one that belongs to an unprotected domain. However, unlike locally defined address mappings, this restriction is not enforced for mappings defined on an LDAP server.

   After configuring a profile with this query, you must select it in order for the FortiMail unit to use it.

   Alternatively, you can configure email address mappings on the FortiMail unit itself.
4. Configure the following:

GUI item	Description
Internal address attribute	Enter the name of the LDAP attribute, such as `internalAddress`, whose value is an email address in the same or another protected domain. This email address will be rewritten to the value of the external address attribute according to the match conditions and effects. The name of this attribute may vary by the schema of your LDAP directory.
External address attribute	Enter the name of the attribute, such as `externalAddress`, whose value is an email address in the same or another protected domain. This email address will be rewritten to the value of the internal address attribute according to the match conditions and effects. The name of this attribute may vary by the schema of your LDAP directory.
Display name attribute	Enter the name of the attribute, such as `displayName`, whose value is the display name of the user. This display name will be inserted into the sender message header before the external email address, such as: `From: Display Name<externalAddress@example.com>` The name of this attribute may vary by the schema of your LDAP directory.

Scan Override

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+*to expand the *Scan Override* section.

If the *Scan Override* query fails, then the FortiMail unit will instead use the antispam, antivirus, and content processing settings defined in the profile for that policy.

4. Configure the following:

GUI item	Description
AntiSpam attribute	Enter the name of the attribute, such as `antispam`, whose value indicates whether or not to perform antispam processing for that user, and which antispam profile to use. Multiple syntax values are permissible. For details, see LDAP directory requirements for each FortiMail LDAP profile query on page 253. If enabled, this attribute setting takes precedence over the generic antispam attribute setting in the domain lookup options (see Domain Lookup on page 246). If you enable this option but leave the attribute field blank, the antispam profile in the matched recipient-based policy will be used.
AntiVirus attribute	Enter the name of the attribute, such as `antivirus`, whose value indicates whether or not to perform antivirus processing for that user and which antivirus profile to use. Multiple value syntaxes are permissible. For details, see LDAP directory requirements for each FortiMail LDAP profile query on page 253. If enabled, this attribute setting takes precedence over the generic antivirus attribute setting in the domain lookup options (see Domain Lookup on page 246). If you enable this option but leave the attribute field blank, the antivirus profile in the matched recipient-based policy will be used.
Content attribute	Enter the name of the attribute, such as `content`, whose value indicates whether or not to perform content processing for that user and which content profile to use. Multiple value syntaxes are permissible. For details, see LDAP directory requirements for each FortiMail LDAP profile query on page 253. If enabled, this attribute setting takes precedence over the generic content attribute setting in the domain lookup options (see Domain Lookup on page 246). If you enable this option but leave the attribute field blank, the content profile in the matched recipient-based policy will be used.

Domain Lookup

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

When configuring domain settings in gateway and transparent mode, if you set the *Relay type* to *LDAP Domain Mail Host*, FortiMail will query the LDAP server to look up the domain and apply the antispam, antivirus, and content profiles assigned to this domain.

If the LDAP server does not find a user matching the domain, the user is considered as unknown, and the mail will be rejected unless it has a specific access list entry.

For this option to work, your LDAP directory should contain a single generic user for each domain such as `generic@example.com` because the FortiMail unit will only look at the domain portion of the generic user's mail address, such as `example.com`.

When an SMTP session is processed, the FortiMail unit will query the LDAP server for the domain portion retrieved from the recipient email address. If the LDAP server finds a user entry, it will reply with the domain objects defined in the LDAP directory, including parent domain attribute, generic mail host attribute, generic antispam attribute, and generic antivirus attribute. The FortiMail unit will remember the mapping domain, mail routing, and antispam and antivirus profiles information to avoid querying the LDAP server again for the same domain portion retrieved from a recipient email address in the future.

If there are no antispam and antivirus profiles for the user, the FortiMail unit will use the antispam and antivirus profiles from the matching IP-based policy.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+* to expand the *Domain Lookup* section.
4. Configure the following:

GUI item	Description
Domain Lookup Query	Enter an LDAP query filter that selects a set of domain objects, whichever object class contains the attribute you configured for this option, from the LDAP directory. Since each domain needs a generic user in the LDAP directory, you can specify the query filter as: `mail=generic@$d` where the value of `$d` is the domain name.
Parent domain attribute	Enter the name of the attribute, such as `parentDomain`, whose value is the name of the parent domain from which a domain inherits the specific `RCPT TO:` check settings and quarantine report settings. The name of this attribute may vary by the schema of your LDAP directory.
Mail host attribute	Enter the name of the attribute, such as `mailHost`, whose value is the IP address of the backend mail server hosting the mailboxes of the domain. The name of this attribute may vary by the schema of your LDAP directory.
AntiSpam attribute	Enter the name of the attribute, such as `genericAntispam`, whose value is the name of the antispam profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute (that is, leave this field blank), the antispam profile in the matched recipient-based policy will be used.
AntiVirus attribute	Enter the name of the attribute, such as `genericAntivirus`, whose value is the name of the antivirus profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory.

GUI item	Description
	If you do not specify this attribute (that is, leave this field blank), the antivirus profile in the matched recipient-based policy will be used.
Content attribute	Enter the name of the attribute, such as `genericContent`, whose value is the name of the content profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute (that is, leave this field blank), the content profile in the matched recipient-based policy will be used.

Hostname/IP Lookup

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

Features such as Reverse DNS and Source can use this query to search the LDAP directory for an FQDN or IP address.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the *+* to expand the *Hostname/IP Lookup* section.
4. Configure the following:

GUI item	Description
Hostname/IP query	Enter an LDAP query filter that selects a set of mail server objects from the LDAP directory, such as: `(cn=$h)` where $h is an FQDN, IP address, or IP address in reverse DNS order (depending on which FortiMail feature will use the object). The name of this attribute may vary by the schema of your LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all mail server objects but also exclude other objects. Alternatively, you can restrict the query by configuring Base DN.

Remote Access Override

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

When you add a FortiMail administrator (see Configuring administrator accounts on page 69), you must specify an access profile (the access privileges) for the administrator. You must also specify a domain (either system or a protected domain) that the administrator is allowed to access.

If you are adding an LDAP account, you can override the access profile and domain setting with the values of the attributes returned from the LDAP server.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the +to expand the *Remote Access Override* section.
4. Configure the following:

GUI item	Description
Enable remote access override	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing access profile. If there is no match, the specified access profile will still be used. Also specify the access profile attribute.
Enable remote domain override	Enable to override the domain you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing protected domain. If there is no match, the specified domain will still be used. Also specify the domain name attribute.

LDAP Profile Chain

If you use different attributes for similar or same values on different LDAP servers, you may want to query all of the LDAP servers in sequential order (a chain query).

You can do this by grouping several LDAP profiles into one LDAP profile. The order of the profiles determines the sequential order of the queries.

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the + to expand the *LDAP Profile Chain* section.
4. From *LDAP profile*, select the profile you want to add to the chain and click the plus sign.
5. Repeat the above step to add more profiles.

Advanced

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 234.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Enable and click the + to expand the *Advanced* section.
4. Configure the following:

GUI item	Description
Timeout	Enter the maximum amount of time in seconds that the FortiMail unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server.
Referrals chase	Enable to use the LDAP server's function of referral chasing, that is, instead of returning a result, it will return a referal to another LDAP server, which may contain further information.
Enable cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiMail unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of `0` effectively disables caching.
Clear Cache	Select to empty the FortiMail unit's LDAP query cache. This can be useful if you have updated the LDAP directory, and want the FortiMail unit to refresh its LDAP query cache now with the new information. Otherwise you can wait for TTL to elapse.
TTL	Enter the amount of time, in minutes, that the FortiMail unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail unit to query the LDAP server, refreshing the cache. The default TTL value is `1440` minutes (one day). The maximum value is `10080` minutes (one week). Entering a value of `0` effectively disables caching. This option is applicable only if Enable cache is enabled.
Enable webmail password change	Enable if you want to allow FortiMail webmail users to change their password. This option does not appear for FortiMail units operating in gateway or transparent mode. If *Password schema* is *Active Directory*, this option can be used only if Use secure connection is *SSL*.
Password schema	Select your LDAP server's user schema style, either *Openldap* or *Active Directory*.
Bypass user verification if server is unavailable	If you have selected using LDAP server to verify recipient or sender address and your LDAP server is not accessible, then you can enable this option to bypass the address verification process. **Note:** This option only takes effect in gateway and transparent mode. For more information about recipient address verification, see Configuring recipient address verification on page 97.

Preparing your LDAP schema for FortiMail LDAP profiles

FortiMail units can be configured to consult an LDAP server for many things that you might otherwise normally have to configure on the FortiMail unit itself, such as user authentication, group membership, mail routing, and other features. Especially if you have a large amount of users and groups already defined on an LDAP directory,

you may find it more convenient to query those existing definitions than to recreate the definition of those same users locally on the FortiMail unit. To accomplish this, you would configure an LDAP profile, then select that LDAP profile in other areas of the configuration that should use its LDAP queries.

LDAP profiles require compatible LDAP server directory schema and contents. Your LDAP server configuration may already be compatible. However, if your LDAP server configuration does **not** contain required information in a schema acceptable to LDAP profile queries, you may be required to modify either or both your LDAP profile and LDAP directory schema.

Verify your LDAP server's configuration for each query type that you enable and configure. For example, if you enable mail routing queries, verify connectivity and that each user object in the LDAP directory includes the attributes and values required by mail routing. Failure to verify enabled queries can result in unexpected mail processing behavior.

Using common schema styles

Your LDAP server schema may require no modification if:

- your LDAP server already contains all information required by the LDAP profile queries you want to enable
- your LDAP server uses a common schema style, and a matching predefined LDAP query configuration exists for that schema style

If both of those conditions are true, your LDAP profile configuration may also be very minimal. Some queries in LDAP profiles contain schema options that automatically configure the query to match common schema styles such as IBM Lotus Domino, Microsoft ActiveDirectory (AD), and OpenLDAP. If you will only enable those queries that have schema options, it may be sufficient to select your schema style for each query.

For example, your LDAP server might use an OpenLDAP-style schema, where two types of user object classes exist, but both already have `mail` and `userPassword` attributes. Your FortiMail unit is in gateway mode, and you want to use LDAP queries to use users' email addresses to query for authentication. In this scenario, it may be sufficient to:

1. In the LDAP profile, enter the domain name or IP address of the LDAP server.
2. Configure the LDAP profile queries:
   - In *User Query*, select from *Schema* which OpenLDAP schema your user objects follow: either *InetOrgPerson* or *InetLocalMailRecipient*. Also enter the *Base DN*, *Base DN*, and *Bind password* to authenticate queries by the FortiMail unit and to specify which part of the directory tree to search.
   - In *User Authentication Option*, enable the query with the option to *Search user and try bind DN*.
3. Configure mail domains and policies to use the LDAP profile to authenticate users and perform recipient verification.

Using other schema styles

If your LDAP server's schema is **not** one of the predefined common schema styles, or if you want to enable queries that require information that does not currently exist in your directory, you may need to adapt either or both your LDAP server and LDAP profile query configuration.

Before modifying your LDAP directory, verify that changes will be compatible with other applications using the directory. You may prefer to modify the LDAP profile query and/or add new attributes than to modify existing structures that are used by other applications, in order to reduce the likelihood of disruption to other applications. For instructions on modifying schema or setting attribute values, consult the documentation for your specific LDAP server.

The primary goal when modifying your LDAP directory is to provide, in some way that can be retrieved by LDAP profile queries, the information required by FortiMail features which can use LDAP profiles. Depending on the LDAP profile queries that you enable, you may need to add to your LDAP directory:

- user objects
- user group objects
- email alias objects

Keep in mind that for some schema styles, such as that of Microsoft ActiveDirectory, user group objects may also play a double role as both user group objects and email alias objects. For the purpose of FortiMail LDAP queries, email alias objects can be any object that can be used to expand email aliases into deliverable email addresses, which are sometimes called distribution lists.

For each of those object types, you may also need to add required attributes in a syntax compatible with the FortiMail features that uses those attributes.

At a minimum, your LDAP directory must have user objects that each contain an email address attribute, and the value of that email address attribute must use full email address syntax (for example, `mail: user@example.com`). This attribute is required by *User Query*, a query which is required in every LDAP profile.

Many other aspects of LDAP profiles are flexible enough to query for the required information in more than one way. It may be sufficient to modify the query strings and other fields in the LDAP profile to match your individual LDAP directory.

For example, the purpose of the *User Query* is to find the distinguished name (DN) of user objects by their email addresses, represented by the FortiMail variable `$m`. Often user objects can be distinguished by the fact that they are the only records that contain the attribute-value pair `objectClass: User`. If the class of user name objects in your LDAP directory is not `objectClass: User` but instead `objectClass: inetOrgPerson`, you could either modify:

- the LDAP profile's user query to request user objects as they are denoted on your particular server, using `objectClass=inetOrgPerson`; for example, you might modify the user query from:

  `(&(objectClass=User)(mail=$m))`

  to be:

  `(&(objectClass=inetOrgPerson)(mail=$m))`

- the LDAP server's schema to match the queries' expected structure, where user objects are defined by `objectClass=User`

Alternatively, perhaps there are too many user objects, and you prefer to instead retrieve only those user objects belonging to a specific group number. In this case, you might modify the query string from:

`(&(objectClass=User)(mail=$m))`

to be:

`(&(objectClass=User)(gidNumber=102)(mail=$m))`

You can use any attribute-value pairs to filter the query result set, as long as they are unique and common to all objects in your intended result set.

For example, most directories do not contain an antivirus processing switch attribute for each user. However, FortiMail units can perform antivirus processing, which can be switched off or on depending on the results from an LDAP query. The FortiMail unit expects the query to return a value that may use Boolean syntax (`TRUE` or `FALSE`) that reflects whether or not, respectively, to perform antivirus processing. In this case, you would add to user objects in your LDAP directory an antivirus attribute whose value is a Boolean value.

The following table indicates expected object types, attribute names, and value syntax, as well as query results, for each LDAP profile query. Attributes listed should be present, but their names may vary by schema. Attributes that do not have a default name require that you configure them in both your LDAP profile and your LDAP directory's schema.

LDAP directory requirements for each FortiMail LDAP profile query

Object type	Attribute	Value	Query result
User Query			
User object classes such as `inetOrgPerson`, `inetLocalMailRecipient`, `User`, `dominoPerson`.	`mail`	A user's email address.	Query compares the email address to the value of this attribute to find the matching user, and retrieve that user's distinguished name (DN), which is the basis for most other LDAP profile queries.
Group Query			
(Objects from *User Query*.)	`gidNumber` or `memberOf`	Varies by schema. Typically is either a group number or the distinguished name (DN) of the group.	Query retrieves the group name for any user defined by *User Query*.
(Objects from *User Query*.)	`mail`	A user's email address.	Query uses the DN retrieved from `groupOwner` to retrieve the email address of the user specified by that DN.
User group object classes such as `group` or `groupOfNames`.	`groupOwner`	A user object's DN.	Query retrieves the DN of a user object from the group defined in `gidNumber` or `memberOf`.
User Authentication			
(Objects from *User Query*.)	`userPassword`	Any.	Query verifies user identity by binding with the user password for any user defined by *User Query*.
User Alias			

Object type	Attribute	Value	Query result
Email alias object classes such as `nisMailAlias`, or user objects from *User Query*, depending on whether your schema resolves email aliases directly or indirectly, respectively. For details, see Base DN on page 236.	`rfc822MailMember` (for alias objects) or `mail` (for user objects)	Either the user name portion of an email address (e.g. `user`; for alias objects), or the entire email address (e.g. `user@example.com`; for user objects).	Query expands an alias to one or more user email addresses. If the alias is resolved **directly**, this query retrieves the email addresses from the alias object itself. If the alias is resolved **indirectly**, this query first queries the alias object for `member` attributes, then uses the DN of each `member` in a second query to retrieve the email addresses of those user objects. For details, see Base DN on page 236.
User group object classes such as `group` or `groupOfNames`. User groups are not inherently associated with email aliases, but for some schemas, such as Microsoft Active Directory, group objects play the role of email alias objects, and are used to indirectly resolve email aliases. For details, see Base DN on page 236.	`member`	A user object's DN, or the DN of another alias object.	Query retrieves the DN of a user object that is a member of the group. This attribute is required only if aliases resolve to user email addresses indirectly. For details, see Base DN on page 236.
Mail Routing			
(Objects from *User Query*.)	`mailHost`	A fully qualified domain name (FQDN) or IP address.	Query retrieves the fully qualified domain name (FQDN) or IP address of the mail server — sometimes also called the mail host — that stores email for any user defined by *User Query*.
	`mailRoutingAddress`	A user's email address for a user account whose email is physically stored on `mailHost`.	Query retrieves the email address for a real account physically stored on `mailHost` for any user defined by *User Query*.
Address Mapping			

Object type	Attribute	Value	Query result
(Objects from *User Query*.)	No default attribute name.	A user's **internal** email address.	Query retrieves the user's **internal** email address
	No default attribute name.	A user's **external** email address.	Query retrieves the user's **external** email address.
Scan Override			
(Objects from *User Query*.)	No default attribute name.	Varies by schema. May be: • `TRUE`, `YES`, `1`, `ENABLE` or `ENABLED` (on) • `FALSE`, `NO`, `0`, `DISABLE`, or `DISABLED`, or any other value not associated with "on" (off) • the name of an antivirus profile	Query retrieves whether or not to perform **antivirus** processing, or which profile to use, for any user defined by *User Query*.
	No default attribute name.	Varies by schema. May be: • `TRUE`, `YES`, `1`, `ENABLE` or `ENABLED` (on) • `FALSE`, `NO`, `0`, `DISABLE`, or `DISABLED`, or any other value not associated with "on" (off) • the name of an antivirus profile	Query retrieves whether or not to perform **antispam** processing, or which profile to use, for any user defined by *User Query*.
Hostname/IP Lookup			
(Objects from *Base DN*.)	`cn`	A fully qualified domain name (FQDN) or IP address, or (for reverse DNS lookups) the IP address in opposite order (e.g. 5.0.168.192 instead of 192.168.0.5.)	Query retrieves the fully qualified domain name (FQDN) or IP address of the mail server — sometimes also called the mail host — that stores email for any user defined by *User Query*.
Remote Access Override			

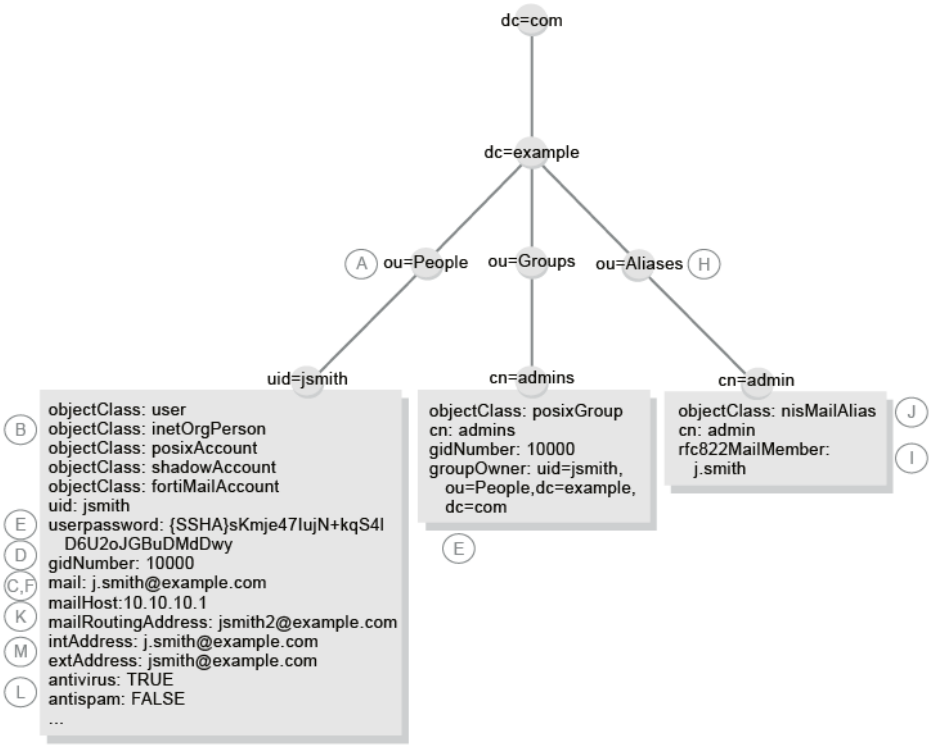
Object type	Attribute	Value	Query result
(Objects from *User Query*.)	No default attribute name.	An administrator profile name.	Query retrieves the permissions for any user defined by *User Query*.
	No default attribute name.	A domain name.	Query retrieves the protected domain for any user defined by *User Query*.
Advanced			
(Objects from *User Query*.)	`userPassword`	Any.	Query, upon successful bind using the existing password, changes the webmail password for any user defined by *User Query*.

Each LDAP profile query filter string may indicate which data types the FortiMail unit expects for each variable in the query filter string:

- `$b`: a bind DN
- `$h`: a FQDN, an IP address, or an IP address in opposite order (reverse DNS)
- `$d`: a domain name
- `$f`: a sender domain name
- `$s`: a sender email address
- `$m`: a recipient email address
- `$u`: a user name

The following example illustrates a matching LDAP directory and LDAP profile. Labels indicate the part of the LDAP profile that is configured to match the directory schema.

Example: Compatible LDAP directory and LDAP profile



Testing LDAP profile queries

After you have created an LDAP profile, you should test each enabled query in the LDAP profile to verify that the FortiMail unit can connect to the LDAP server, that the LDAP directory contains the required attributes and values, and that the query configuration is correct.

When testing a query in an LDAP profile, you may encounter error messages that indicate failure of the query and how to fix the problem.

LDAP Query Failure Message	Meaning and Solution
LDAP profile state disabled	The query is disabled in the LDAP profile. Tests cannot be performed until you enable the query.
Empty input	The query cannot be performed until you provide the information required by the query.
Connection Failed	The FortiMail unit could not connect to the LDAP server. The LDAP server may be unreachable, or the LDAP profile may be configured with an incorrect IP address, port number, or secure connection setting.

LDAP Query Failure Message	Meaning and Solution
Failed to bind with bind DN and password	The FortiMail unit successfully connected to the LDAP server, but could not authenticate in order to perform the query. If the server permits anonymous queries, the Bind DN and Bind password you specified in *User Query* should be blank. Otherwise, you must enter a valid bind DN and its password.
Unable to found user DN that matches mail address	The FortiMail unit successfully connected to the LDAP server, and, if configured, bound, but could not find a user whose email address attribute matched that value. The user may not exist on the LDAP server in the Base DN and using the query filter you specified in *User Query*, or the value of the user's email address attribute does not match the value that you supplied in *Mail address*.
Unable to find LDAP group for user	The FortiMail unit successfully located a user with that email address, but their group membership attribute did not match your supplied value. The group membership attribute you specified in *Group Query Option* may not exist, or the value of the group membership attribute may not match the value that you supplied in Group base DN. If the value does not match, verify that you have supplied the Group base DN according to the syntax expected by both your LDAP server and your configuration of *Group Query Option*.
Group owner query failure	The FortiMail unit successfully connected to the LDAP server, but could not find a group whose distinguished name matched that value. The group may not exist on the LDAP server, or the value of the group's distinguished name attribute does not match the value that you entered in Group base DN.
Authentication failure	
Failed to bind	The FortiMail unit successfully located a user with that email address, but the user's bind failed and the FortiMail unit was unable to authenticate the user. Binding may fail if the value of the user's password attribute does not match the value that you supplied in *Old password*. If this error message appears when testing Enable webmail password change, it also implies that the query failed to change the password.
Unable to find mail alias	The FortiMail unit was unable to find the email alias. The email address alias may not exist on the LDAP server in the Base DN and using the query filter you specified in *User Alias*, or the value of the alias' email address attribute does not match the value that you supplied in *Mail address*.
Error for LDAP user profile ID	The FortiMail unit failed to change the email user's password. Verify that you have entered the correct existing password in *Old password*.

To verify a user query

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *User Query* query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *User*.
5. In *Mail address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Click *Test*.

The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record.

To verify a group query

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Group Query* query you want to test.
3. Click *Test LDAP Query*.

   A pop-up window appears allowing you to test the query. Fields displayed in the window vary by whether or not *Use group name with base DN as group DN* is enabled in *Group Query*.
4. From *Select query type*, select *Group*.
5. In *Email address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Either the *Group DN* or *Group Name* field appears. If *Group DN* appears, enter the value of the user's group membership attribute. If *Group Name* appears, enter only the group name portion of the value of the user's group membership attribute.

   For example, a *Group DN* entry with valid syntax could be either:
   - `10000`
   - `admins`
   - `cn=admins,ou=People,dc=example,dc=com`

   but a *Group Name* entry with valid syntax would be `admins`.

   Valid syntax varies by your LDAP server's schema and by whether *Use group name with base DN as group DN* is enabled, but is identical to what you should enter when using this LDAP profile and entering the group name elsewhere in the FortiMail configuration, such as for a recipient-based policy.
7. Click *Test*.

   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record and find the group to which the user belongs.

To verify a group query for the group owner

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Group Query* group owner query you want to test.
3. Click *Test LDAP Query*.

   A pop-up window appears allowing you to test the query. Fields displayed in the window vary by whether or not *Use group name with base DN as group DN* is enabled in *Group Query*.
4. From *Select query type*, select *Group Owner*.
5. Either the *Group DN* or *Group Name* field appears. If *Group DN* appears, enter the distinguished name of the group object. If *Group Name* appears, enter only the group name portion of the distinguished name of the group object.

   For example, a *Group DN* entry with valid syntax would be `cn=admins,ou=People,dc=example,dc=com`, but a *Group Name* entry with valid syntax would be `admins`.

   Valid syntax varies by your LDAP server's schema and by whether *Use group name with base DN as group DN* is enabled, but is identical to what you should enter when using this LDAP profile and entering the group name elsewhere in the FortiMail configuration, such as for a recipient-based policy.
6. Click *Test*.

   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the group record and find the group owner and their email address.

To verify user authentication

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Authentication*.
5. In *Mail address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. In *Password*, enter the current password for that user.
7. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record, or binding to authenticate the user.

To verify a user alias query

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose user query options you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Alias*.
5. In *Email address*, enter the email address alias of a user on the LDAP server, such as `test-alias@example.com`.
6. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the alias record, or binding to authenticate the user.

To verify an address mapping query

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Address Mapping Option* query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Address Mapping*.
5. In *Email address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record and find the internal and external email addresses for that user.

To verify a scan override query

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Scan Override Option* (antispam, antivirus, and content profile preference) query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Scan Override*.
5. In *Email address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record and find the antispam and antivirus processing preferences for

that user.

To verify a mail routing query

1. Go to *Profile > LDAP > LDAP*.
2. Double-click the LDAP profile whose *Mail Routing* query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Mail Routing*.
5. In *Mail address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record and find the mail host and mail routing address for that user.

To verify a hostname/IP lookup query

1. Go to *Profile > LDAP > LDAP*.
2. Double-click the LDAP profile whose *Hostname/IP Lookup* query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Hostname/IP Lookup* .
5. In *Hostname/IP*, enter a mail server's FQDN and then IP address (forward and reverse DNS formats) on the LDAP server, such as `mail.example.com`, `192.169.1.5`, or `5.1.168.192`. (Format varies by the feature that uses the query, such as Reverse DNS or Source.)
6. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record and find the mail host and mail routing address for that user.

To verify the webmail password change query

1. Go to *Profile > LDAP > LDAP*.
2. Double-click the LDAP profile whose webmail password change query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Change Password*.
5. In *Email address*, enter the email address of a user on the LDAP server, such as `test@example.com`.

Only use an email account whose password it is acceptable to change, and make note of the new password. Verifying the query configuration performs a real password change, and does not restore the previous password after the query has been verified.

6. In *Password*, enter the current password for that user.
7. In *New Password*, enter the new password for that user.
8. Click *Test*.
   The FortiMail unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record, binding to authenticate the password change, and the password change operation itself.

Clearing the LDAP profile cache

You can clear the FortiMail unit's cache of query results for any LDAP profile.

This may be useful after, for example, you have updated parts of your LDAP directory that are used by that LDAP profile, and you want the FortiMail unit to discard outdated cached query results and reflect changes to the LDAP directory. After the cache is emptied, any subsequent request for information from that LDAP profile causes the FortiMail unit to query the updated LDAP server, refreshing the cache.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose query cache you want to clear.
3. Click *Test LDAP Query*.
4. From *Select query type*, select *Clear Cache*.
   A warning appears at the bottom of the window, notifying you that the cache for this LDAP profile will be cleared if you proceed. All queries will therefore be new again, resulting in decreased performance until the query results are again cached.
5. Click *OK*.
   The FortiMail unit empties cached LDAP query responses associated with that LDAP profile.

Configuring dictionary profiles

The Profiles tab lets you configure dictionary profiles.

Unlike banned words, dictionary terms are UTF-8 encoded, and may include characters other than US-ASCII characters, such as é or ñ.

Dictionary profiles can be grouped or used individually by antispam or content profiles to detect spam, banned content, or content that requires encryption to be applied. For more information on content profiles and antispam profiles, see Configuring antispam profiles and actions on page 187 and Configuring content profiles and content action profiles on page 215.

A dictionary can contain predefined and/or user-defined patterns.

The FortiMail unit comes with the following six predefined patterns. You can edit a predefined pattern and edit or delete a user-defined pattern by selecting it and then clicking the *Edit* or *Delete* icon.

If a pattern is enabled, the FortiMail unit will look for the template/format defined in a pattern. For example, if you enable the Canadian SIN predefined pattern, the FortiMail unit looks for the three groups of three digits defined in this pattern. This is useful when you want to use IBE to encrypt an email based on its content. In such cases, the dictionary profile can be used in a content profile which is included in a policy to apply to the email. For more information about IBE, see Configuring IBE encryption on page 324.

Predefined patterns

Canadian SIN	Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666.

US SSN	United States Social Security number. The format is a nine digit number, such as 078051111.
Credit Card	Major credit card number formats.
ABA Routing	A routing transit number (RTN) is a nine digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which it was drawn.
CUSIP	CUSIP typically refers to both the Committee on Uniform Security Identification Procedures and the 9-character alphanumeric security identifiers that they distribute for all North American securities for the purposes of facilitating clearing and settlement of trades.
ISIN	An International Securities Identification Number (ISIN) uniquely identifies a security. Securities for which ISINs are issued include bonds, commercial paper, equities and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at trading and settlement.

To view the list of dictionary profiles

1. Go to *Profile* > *Dictionary* > *Dictionary*.

GUI item	Description
Export (button)	Select one dictionary check box and click Export. Follow the prompts to save the dictionary file. Note that you can only export one dictionary at a time.
Import (button)	Select one dictionary check box and then click the import button to import dictionary entries into the existing dictionary. In the dialog, click Browse to locate a dictionary in text format. Click OK to upload the file. Note that you can only select one dictionary at a time and you can only import dictionary entries into an existing dictionary.
Name	Displays the dictionary name.

2. Click New to create a new profile or double-click a profile to modify it.
   A two-part page appears.
3. For a new profile, type its name. The profile name is editable later.
4. To enable or edit a predefined pattern:
   - Double-click a pattern in Smart Identifiers.
   - A dialog appears.
   - Select Enable to add the pattern to the dictionary profile.
   - To edit a predefined pattern, do the same as for a user-defined pattern in Step 5
   - Click OK.
5. To add or edit a user-defined pattern:
   - Click *New* under Dictionary Entries to add an entry or double click an entry to modify it.
   - A dialog appears.
6. Configure a custom entry.

GUI item	Description
Enable	Select to enable a pattern.
Pattern	Type a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression. Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. Regular expressions do not require slash (`/`) boundaries. For example, enter: `v[i1]agr?a` Matches are not case sensitive and can occur over multiple lines as if the word were on a single line (that is, Perl-style match modifier options `i` and `s` are in effect). The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, **not** the originally encoded string. For example, if the original encoded string is: `=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=` then the pattern must match: `Se trata del spam.` Entering the pattern `*iso-8859-1*` would **not** match. This option is not editable for predefined patterns.
Pattern type	For a new dictionary entry, select either: • *Wildcard*: *Pattern* is verbatim or uses only simple wild cards (`?` or `*`). • *Regex*: *Pattern* is a Perl-style regular expression. See also Syntax on page 381. This option is not editable for predefined patterns.
Comments	Enter any descriptions for the pattern.
Pattern weight	Enter a number by which an email's dictionary match score will be incremented for each word or phrase it contains that matches this pattern. The dictionary match score may be used by content monitor profiles and antispam profiles to determine whether or not to apply the content action. See also Dictionary section on page 198 and Configuring content monitor and filtering on page 221.
Pattern max weight	Enter the maximum by which matches of this pattern can contribute to an email's dictionary match score. This option applies only if *Enable pattern max weight limit* is enabled.
Enable pattern max weight limit	Enable if the pattern must not increase an email's dictionary match score more than the amount configured in *Pattern max weight*.
Search header	Enable to match occurrences of the pattern when it is located in an email's message headers, including the subject line. The FortiMail unit uses the full header string, including the header name and value, to match the pattern. Therefore, when you define the pattern, you can specify both the header name and value. For example, such a pattern entry as `from: .*@example.com.*` will block all email messages with the `From:` header as `xxx@example.com`.
Search body	Enable to match occurrences of the pattern when it is located in an email's message body.

To apply a dictionary, in an antispam profile or content profile, either select it individually or select a dictionary group that contains it. For more information, see Configuring dictionary groups on page 265, Configuring antispam profiles on page 187, and Configuring content profiles on page 216.

Configuring dictionary groups

The Group tab lets you create groups of dictionary profiles.

Dictionary groups can be useful when you want to use multiple dictionary profiles during the same scan.

For example, you might have several dictionaries of prohibited words — one for each language — that you want to use to enforce your network usage policy. Rather than combining the dictionaries or creating multiple policies and multiple content profiles to apply each dictionary profile separately, you could simply group the dictionaries, then select that group in the content monitor profile.

Before you can create a dictionary group, you must first create one or more dictionary profiles. For more information about dictionary profiles, see Configuring dictionary profiles on page 262.

To view and configure a dictionary group

1. Go to *Profile* > *Dictionary* > *Group*.

GUI item	Description
Create New	Select the name of a protected domain from Select Domain, then click Create New to add a dictionary for that protected domain. **Note:** If you have not yet configured a protected domain, new dictionary groups will by default be assigned to the system domain. For more information on protected domains, see “Configuring protected domains” on page 229.
Select Domain	Select the name of a protected domain to display dictionary groups belonging to that protected domain, or select system to display system-wide dictionary groups. This option is not available if you have not yet configured a protected domain. For more information on protected domains, see “Configuring protected domains” on page 229.
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Group Name	Displays the name of the dictionary group or dictionary group item.
Domain	The entire FortiMail unit (System) or name of a protected domain to which the profile is assigned. Which dictionary groups are visible and modifiable by the administrator varies by whether a FortiMail administrator account is assigned to specific protected domain. For more information, see “About administrator account permissions and domains” on page 143.
Description	The description of the dictionary group.

2. Either click New to add a profile or double-click a profile to modify it.
3. For a new group, enter the name of the dictionary group in Group name.

4. In the Available dictionaries area, select one or more dictionaries that you want to include in the dictionary group, then click ->.
   The dictionaries move to the Members area.
5. Click Create or OK.

To apply a dictionary group, select it instead of a dictionary profile when configuring an antispam profile or content profile. For details, see Configuring antispam profiles on page 187 and Configuring content profiles on page 216.

Configuring security profiles

Go to *Profile* > *Security* to create transport layer security (TLS) profiles and encryption profiles.

Configuring TLS security profiles

The *TLS* tab lets you create TLS profiles, which contain settings for TLS-secured connections.

TLS profiles, unlike other types of profiles, are applied through access control rules and message delivery rules, not policies. For more information, see Controlling SMTP access and delivery on page 148.

To view the list of TLS profiles, go to *Profile* > *Security* > *TLS*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone*. A single-field dialog appears. Enter a name for the new profile. Click *OK*.
Profile Name	Displays the name of the profile.
TLS Level	Displays the security level of the TLS connection. • *None*: Disables TLS. Requests for a TLS connection will be ignored. • *Preferred*: This is the default behavior. Whether TLS is used depends on the other party of the session. • *Secure*: Requires a certificate-authenticated TLS connection. CA certificates must be installed on the FortiMail unit before they can be used for secure TLS connections. For information on installing CA certificates, see Managing certificate authority certificates.
Action On Failure	Indicates the action the FortiMail unit takes when a TLS connection cannot be established, either: • *Temporarily Fail*: Reply to the SMTP client with a code indicating temporary failure. • *Fail*: Reject the email and reply to the SMTP client with SMTP reply code 550.  Optionally, you can choose to select the *IBE on TLS failure* option when configuring an encryption profile. For more information, see Configuring encryption profiles on page 268.

GUI item	Description
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

To configure a TLS profile

1. Go to *Profile* > *Security* > *TLS*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new profile, enter the *Profile name*.
4. From *TLS option*, select the security level of the TLS profile.
5. Configure the following, as applicable:
   The availability of the following options varies by your selection in *TLS option*.

GUI item	Description
Check TLS version	Enable to select a *Minimum TLS version* to apply for the TLS profile.  The connection will be refused if the *Minimum TLS version* is not met, regardless of whether *TLS option* is set to *Preferred* or *Secure*. • SSL 3.0 • TLS 1.0 • TLS 1.1 • TLS 1.2 • TLS 1.3
DANE	Assign a DNS-based Authentication of Named Entities (DANE) support level: • *None* • *Opportunistic* • *Mandatory* (only available when *TLS option* is set to *Secure*) For more information, see RFC 7929.
MTA-STS	Assign an MTA Strict Transport Security (MTA-STS) domain checking level.  The MTA-STS feature may only take effect when enabled on *System* > *Mail Setting* > *Mail Server Settings*. See Configuring SMTP service on page 1.
Action on failure	Select whether to fail or temporarily fail if a TLS connection with the parameters described in the TLS profile cannot be established.
Check encryption strength	Enable to require a minimum level of encryption strength. Also configure *Minimum encryption strength*. This option appears only if *TLS option* is *Secure*.
Minimum encryption strength	Enter the bit size of the encryption key. Greater key size results in stronger encryption, but requires more processing resources.

GUI item	Description
Check CA issuer	Enable and enter a string on the `CA Issuer` field. The FortiMail unit will compare the string in the *CA issuer* field with the field with that same name in the installed CA certificates. This option appears only if *TLS level* is *Secure*.
CA issuer	Select the type of match required when the FortiMail unit compares the string in the `CA Issuer` field and the same field in the installed CA certificates. For more information on CA certificates, see Managing certificate authority certificates. *Check CA issuer* must be enabled for *CA issuer* to have any effect.  The CA issuer string format must use **no spaces**, and must use forward slashes to separate the certificate components. For example: `/CN=Fortinet/O=Fortinet Ltd.` If this field is left blank, then any trusted or installed CA certificate on FortiMail can be used to check against the peer certificate signer. This option appears only if TLS level is *Secure*.
Lookup CA	To populate the *CA Issuer* field with text from a CA certificate's `CA Issuer`, select the name of a CA certificate that you have uploaded to the FortiMail unit.
Check certificate subject	Enable and enter a string in the *Certificate subject* field. The FortiMail unit will compare the string in the *Certificate subject* field with the field with that same name in the installed CA certificates.  The certificate subject string format must use **no spaces**, and must use forward slashes to separate the certificate components. For example: `/CN=Fortinet/O=Fortinet Ltd.` This option appears only if *TLS level* is *Secure*.
Certificate subject	Select the type of match required when the FortiMail unit compares the string in the *Certificate subject* and the same field in the installed CA certificates. *Check certificate subject* must be enabled for *Certificate subject* to have any effect. This option appears only if *TLS level* is *Secure*.

Configuring encryption profiles

The Encryption tab lets you create encryption profiles, which contain encryption settings for secure MIME (S/MIME), identity-based encryption (IBE), and fallback to IBE if TLS delivery fails.

The ability to fallback automatically to IBE if TLS encryption fails ensures that all email is sent encrypted, even in instances where encryption keywords are used.

Encryption profiles are applied through either message delivery rules or content action profiles used in content profiles which are included in policies. For more information, see Configuring delivery rules on page 156 and Configuring content action profiles on page 224.

Before S/MIME encryption will work, you must also create at least one internal address certificate binding. For details, see Configuring certificate bindings on page 328.

For more information about using S/MIME encryption, see Using S/MIME encryption on page 271.

For more information about using IBE, see Configuring IBE encryption on page 324.

To view or configure encryption profiles

1. Go to *Profile* > *Security* > *Encryption*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Profile Name	Displays the name of the profile.
Protocol	Displays the protocol used for this profile, S/MIME, IBE, or IBE on TLS failure.
TLS profile	Select the TLS profile for FortiMail to use first before falling back to the IBE profile, when necessary.
Encryption algorithm	Displays the encryption algorithm that will be used to encrypt the email (AES 128, AES 192, AES 256, CAST5 128, or Triple DES).
Action	For S/MIME, the actions are Encrypt, Sign, or Encrypt and Sign. For IBE, the action will be Encrypt only.
Action on failure	Indicates the action the FortiMail unit takes when S/MIME or IBE cannot be used: • Drop and send DSN: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable. • Send plain message: Deliver the email without encryption. • Enforce TLS: If the message delivery rule has no TLS profile or the TLS level in its profile is Preferred, the FortiMail unit will enforce the TLS Secure level. If the TLS level in its profile is None, then the email will temp fail because it contradicts with Enforce TLS.For more information, see Configuring delivery rules on page 156 and Configuring TLS security profiles on page 266.
Access method	Displays the action used by the mail recipients to retrieve IBE messages. • Push: A notification and a secure mail is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit does not store the message. • Pull: A notification is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit stores the message.
Maximum size (KB) for Push method	Displays the settings of the maximum message size (KB) of the secure mail delivered (or pushed) to the recipient. If the message exceeds the size limit, it will be delivered with the Pull method.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new profile, enter the name of the profile in *Profile name*.
4. In *Protocol*, select *S/MIME* or *IBE*.
5. The availability of the following options varies by your selection in *Protocol*.
6. Select the *Action method* (*Push* or *Pull*) for the mail recipients.

   For *Push*, specify the maximum message size (KB) for the *Push* method (messages exceeding the size limit will be delivered with the *Pull* method).
7. If you select S/MIME as the protocol, select an action: *Encrypt*, *Sign*, or *Encrypt and Sign*. To use S/MIME encryption, you must also configure certificate binding. For details, see Using S/MIME encryption on page

271 and Configuring certificate bindings on page 328.

8. From *Encryption algorithm*, select the encryption algorithm that will be used to encrypt email (AES 128, AES 192, AES 256, CAST5 128, or Triple DES).
9. From *Action on failure*, select the action the FortiMail unit takes when encryption cannot be used.
   - *Drop and send DSN*: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable.
   - *Send plain message*: Deliver the email without encryption.
   - *Enforce TLS*: If the TLS level in the TLS profile selected in the message delivery rule is *Encrypt* or *Secure*, the FortiMail unit will not do anything. If the message delivery rule has no TLS profile or the TLS level in its profile is *None* or *Preferred*, the FortiMail unit will enforce the *Encrypt* level.
10. Click *Create* or *OK*.

Using S/MIME encryption

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. The FortiMail unit supports S/MIME encryption.

You can encrypt email messages with S/MIME between two FortiMail units. For example, if you want to encrypt and send an email from FortiMail unit A to FortiMail unit B, you need to do the following:

1. On FortiMail unit A:
   - Import the CA certificate. For details, see Managing certificates.
   - Create a certificate binding for the outgoing email to obtain FortiMail unit B's public key in the certificate to encrypt the email. For details, see Configuring certificate bindings on page 328.
   - Create an S/MIME encryption profile. For details, see Configuring encryption profiles on page 268.
   - Apply the S/MIME encryption profile in a policy to trigger the S/MIME encryption by either creating a message delivery rule to use the S/MIME encryption profile (see Configuring delivery rules on page 156), or creating a policy to include a content profile containing a content action profile with an S/MIME encryption profile (see Controlling email based on sender and recipient addresses on page 163, Controlling email based on IP addresses on page 159, Configuring content action profiles on page 224, and Configuring content profiles on page 216).

   If the email to be encrypted is matched both by the message delivery rule and the policy, the email will be encrypted based on the content profile in the policy.

2. On FortiMail unit B:
   - Import the CA certificate. For details, see Managing certificates.
   - Create a certificate binding for the incoming email and import both FortiMail unit B's private key and certificate to decrypt the email encrypted by FortiMail unit A using FortiMail unit B's public key.

Configuring email, IP and GeoIP groups

The *Profile* > *Group* tab displays the list of email and IP group and override profiles.

Configuring email groups

Email groups are groups of email addresses that you can use to define recipients and senders that will use the same policies.

To configure email groups

1. Go to *Profile* > *Group* > *Email Group*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. In *Comment*, optionally enter a comment or description.
4. If you are creating a new group, from *Domain*, select whether this group will be available system-wide or in a specific protected domain.
5. In *Name*, enter a unique name.
   The name must contain only alphanumeric characters. Spaces are not allowed.
6. Click *New* to add email addresses.
   You can also use wildcards to enter partial patterns that can match multiple email addresses. An asterisk (*) represents one or more characters and the question mark (?) represents any single character.
   For example, the pattern `??@*.com` will match any email user with a two letter email user name from any ".com" domain name.
7. Click *Create* or *OK*.
8. To apply an email group, select it in an access control rule or recipient-based policy. See Configuring access control receiving policies on page 148 and Controlling email based on sender and recipient addresses on page 163.

Configuring IP groups

IP groups are groups of IP addresses that will use the same policies or be in the same reports.

If you need to match IP addresses in a specific geographic region, instead of manually maintaining an IP group, see Configuring GeoIP groups on page 273.

If the IP addresses are dynamic (for example, mobile devices or some home networks), then consider endpoint reputation instead (see Configuring endpoint reputation on page 1).

To configure an IP group

1. Go to *Profile* > *Group* > *IP Group*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. In *Name*, enter a unique name.
   The name must contain only alphanumeric characters. Spaces are not allowed.
4. In *Comment*, optionally enter a comment or description.
5. Under *IP Groups*, click *New*.
   A field appears under *IP/Netmask or IP Range*.
6. Enter the IP address and netmask of the group, or the IP range. Use the netmask, the portion after the slash (/), to specify the matching subnet.

For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as `10.10.10.0/24` in the access control rule table, with the `0` indicating that any value is matched in that position of the address.

Similarly, `10.10.10.10/32` will appear as 10.10.10.10/32 and match only the 10.10.10.10 address.

7. Click *Create* or *OK*.
8. To apply an IP group, select it in access control rules, IP-based policies, and reports. See Controlling SMTP access and delivery on page 148, Controlling email based on IP addresses on page 159, and Configuring report profiles and generating reports on page 346.

Configuring GeoIP groups

FortiMail can use the GeoIP database to map geographic locations to IP addresses. You can use GeoIP groups for geo-targeting of countries that require different policies, or regions that are only sources of misuse, spam, and viruses. The GeoIP database saves time instead of manually defining and updating a list of global public IP addresses.

You can also override geolocation mappings that may not be correct in the GeoIP database. See Configuring GeoIP override on page 273.

To configure a GeoIP override

1. Go to *Profile* > *Group* > *GeoIP Group*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. In *Name*, enter a unique name.

   The name must contain only alphanumeric characters. Spaces are not allowed.
4. In *Comment*, optionally enter a comment or description.
5. Enable *All countries/regions* if you want to create a group to include all countries and regions. Otherwise, disable this setting and then in the text areas that appear, select the countries, regions, or GeoIP override groups from the *Available* text area and then click the >> button to move them to *Member*.

   You can have a maximum of 30 countries and regions in each group.
6. Click *Create* or *OK*.
7. To apply a GeoIP group, select it in either an IP-based policy or access control rule. See Controlling SMTP access and delivery on page 148 and Controlling email based on IP addresses on page 159.

For better performance, use GeoIP groups in IP-based policies instead of access control rules. This blocks unwanted connections earlier, **before** authentication.

(Access control rules block unwanted connections **after** authentication. This wastes time and system resources. If there are back-end servers for authentication, recipient verification, etc., then the unwanted connections also will continue to effect those servers.)

Configuring GeoIP override

GeoIP features look up IP addresses associated with geographic locations in the GeoIP database. However, in some cases, the lookup might not be accurate, such as when geographic borders change, IP address ownership

changes, or clients use a proxy or VPN. You can override the GeoIP lookup result by manually specifying the geographic locations of some IP addresses and ranges.

To configure a GeoIP override

1. Go to *Profile* > *Group* > *GeoIP Override*.
2. Click *New*.
3. In *Name*, enter a unique name.
4. In *Comment*, optionally enter a comment or description.
5. Click *New* and enter the IPv4 address range or subnet that you want to include in the override.

Only IPv4 addresses are supported for GeoIP overrides.

6. Click *Create* or *OK*.
   To test the effect of your override, click *IP Geography Query*.
7. To apply the GeoIP override, select it in a GeoIP group. See Configuring GeoIP groups on page 273.

Configuring notification profiles

When FortiMail takes actions against email messages, you may want to inform email senders, recipients, or any other users of the actions, that is, what happened to the email.

To achieve this purpose, you need to create such kind of notification profiles and then use them in antispam, antivirus, and content action profiles. For details, see Configuring antispam action profiles on page 206, Configuring antivirus action profiles on page 213, and Configuring content action profiles on page 224.

To create a notification profile

1. Go to *Profile* > *Notification* > *Notification*. If you have created some notification profiles, you can view, clone, edit, or delete them there.
2. Click *New* to create a profile.
3. For *Name*, enter a profile name. The profile name is editable later.
4. From *Type*, select:
   - *Generic*: this type of notification profile can be used in the antispam, antivirus and content profiles to notify the sender, recipient, or other email accounts.
   - *Sender Address Rate Control*: When you configure sender address rate control notification in domain settings (see Other on page 107), you can also choose a notification profile. In this case, you only need to notify the senders, not the recipients. You do not need to include the original message as attachment either. Therefore, these two options are greyed out.
   - *Attachment Filtering*: this type of notification profile most probably be used in the content profiles where attachment filtering is implemented.
5. Choose whom you want to send notification to: sender, recipient, or other users. If you choose *Others*, you can manage the email list by using the *Add* and *Remove* buttons.

6. Select an email template to use. You can also click New to create a new template or click Edit to modify an existing template. For details about email templates, see Customizing email templates on page 79.
7. Optionally select *Include original message as attachment*.
8. Click *OK*.

Configuring security settings

The *Security* menu lets you configure antispam settings that are system-wide or otherwise not configured individually for each antispam profile.

Several antispam features require that you first configure system-wide, per-domain, or per-user settings in the *Security* menu **before** you can use the feature in an antispam profile. For more information on antispam profiles, see Configuring antispam profiles and actions on page 187.

Configuring URL filter profiles

URL filter profiles select which rating categories you want to scan, rewrite, or block in email message bodies.

You can configure how FortiMail detects URLs. See About URL types on page 278.

To configure a URL rating category profile

1. Go to *Security* > *URL Filter* > *Profile*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Profile Name	Enter a unique name.
Comment	Optional. Enter a description or comment.
FortiGuard Category	Select from the predefined categories of URLs that are defined by the FortiGuard service, such as *Bandwidth Consuming*.
Custom Category	Select from your custom URL categories. They are organized based on whether the custom category's Source is *Local* or *Remote*. See Configuring custom URL rating categories on page 276.

4. Click *Create*.
5. To apply the URL rating category profile, you can select it in:
   - antispam profiles (see FortiGuard section on page 189)
   - click protection (see Configuring CDR URL click protection and removal options on page 282)
   - FortiSandbox scanning (see Using FortiSandbox antivirus inspection on page 83)

Configuring custom URL rating categories

In addition to the predefined categories from FortiGuard, you can configure your own custom URL rating categories.

Some IDs are reserved for use by predefined categories and threat feeds. See Types and file formats of threat feeds on page 280.

For exemptions, you can use the predefined category *local-exempt*.

1. Go to *Security* > *URL Filter* > *Custom Category*.
2. Click *New*.
3. Configure the following settings:

GUI item	Description
Name	Enter a unique name.
Source	Select where the URL category is defined, either: • *Local* — On the FortiMail unit. • *Remote* — In a threat feed on an external server. Also configure Threat feed.
Threat feed	Select the threat feed. See also Configuring a threat feed on page 279.
Comment	Optional. Enter a description or comment.

4. Click *Create*.
5. To apply the custom category, select it in a URL filter profile. See Configuring URL filter profiles on page 276.

Configuring URL rating overrides

You can override and assign a different rating category to URLs. This can be useful if, for example:

- A shared web server hosts multiple different apps, and one of the URLs must be filtered differently.
- A FortiGuard URL rating is temporarily incorrect and you want to create an exemption.

You usually don't need to create a custom category for exemptions. You can use the predefined category instead. For example, to exempt a URL from features such as:
- FortiGuard URL category filtering
- URL click protection
- FortiSandbox scanning

you could create an override where you set Group to *Local* and Category to *local-exempt*.

1. Go to *Security* > *URL Filter* > *Override Rating*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Status	Enable or disable the override.
URL pattern	Enter a pattern that matches only the URLs that you want to override.

GUI item	Description
	Syntax varies by Pattern type.
Pattern type	Select the type of URL pattern, either: • *Wildcard* — Simple wild cards (`?` or `*`) if you need to match multiple characters. See Special characters with regular expressions and wildcards on page 380. • *Regular Expression* — Flexible and full-featured pattern matching. See Syntax on page 381. **Tip:** To test that a regular expression matches as expected (and does not accidentally match other text), click *Validate*.
Comment	Optional. Enter a description or comment.
Override To	
Group	Select which group of categories to filter the list in Category, either: • a predefined category group from FortiGuard, such as *Bandwidth Consuming* • *Local* or *Remote* (depending on the custom category's Source)
Category	Select which category to assign to the URLs that match URL pattern, either: • a predefined category from FortiGuard, such as *Streaming Media and Download* • a predefined category from the firmware, such as *local* or *local-exempt* • a custom category (see Configuring custom URL rating categories on page 276)

4. Click *Create*.
   The override is applied to features that use URL filter profiles. See also Configuring URL filter profiles on page 276.

About URL types

Types of URLs that URL filtering can scan include:

- **Absolute URLs** — URL syntax with scheme name (protocol), such as `http`, `https`, and `ftp`. They often only include a domain name. Example: `http://www.example.com`
- **Reference URLs** — No scheme name. Example: `example.com`

URLs in email can also be written in plain text instead of as clickable HTML links. While not technically a URL, the domain name of the sender can also be inspected.

By default, FortiMail scans for absolute URLs only. If you need to improve the spam catch rate or reduce false positives, you can change this. Use the CLI command:

```
config antispam settings
   set url-checking {aggressive | extreme | strict}
end
```

For details, see the FortiMail CLI Reference.

Configuring a threat feed

Threat feeds are plain text files that contain a list of security threats. Threat feeds can be hosted on FortiClient EMS, third party servers, or your own HTTP/HTTPS web server. In this way, FortiMail units can utilize security information from many vendors, security communities, and specialist teams in your own organization. Once FortiMail is connected to threat feeds, you can select them when you configure security features such as antivirus file signatures and antispam IP reputation and URL filters.

FortiMail periodically synchronizes with threat feeds and automatically imports changes.

A large volume of threat feeds requires more processing resources. To use this feature, FortiMail platforms with higher capacities are recommended.

If the threat feed's web server becomes unreachable and there is a connection status error, then the FortiMail continues to use its existing local cache of the threat feed, regardless of reboot. To get threat feed updates, you must re-establish network connectivity.

The maximum number of threat feeds varies by model. See Appendix B: Maximum Values on page 1.

To configure a threat feed

1. Go to *Security* > *Threat Feed* > *Threat Feed*.
2. Either click New to add a threat feed or double-click an existing one to modify it.
3. Configure the following settings and then click *Create*.

GUI item	Description
Status	Enable or disable the threat feed.
Name	Enter a unique name.
Comment	Optional. Enter a description or comment.
Resource URL	Enter the URI of the threat feed. FortiMail also supports OASIS STIX/TAXII format. To use the TAXII protocol, use the `stix://` prefix instead of `https://`.
Resource type	Select either: • *URL Category* • *IP Address* • *Malware Hash* For details, see Types and file formats of threat feeds on page 280.
Category ID	The automatically assigned identifier number for threats that match this FortiGuard URL filter category. The ID cannot be changed. The field appears only when you edit an existing threat feed, and its *Resource type* is *URL Category*.
Username	If the server requires authentication, enter the username that FortiMail will use to

GUI item	Description
	connect.
Password	If the server requires authentication, enter the password that FortiMail will use to connect.
Server identity check	Select the level of server certificate validation strictness, either: • *None* — No certificate validation. • *Basic* — Validate the server certificate. It must not be revoked or expired, and must be signed by a trusted CA. See also Managing certificate authority certificates on page 1. • *Full* — In addition to validation requirements in *Basic*, the domain name in Resource URL must match the common name (CN) field in the server certificate.  To harden security, select *Full*.
Update interval	Enter the frequency in minutes of synchronization with the threat feed. Default value is 30 minutes. Valid range is from 1 to 43200 minutes (30 days).

4. To apply the threat feed, select it in an antivirus file signature, custom URL category or override, or antispam profile. See Configuring file signatures on page 211, Configuring custom URL rating categories on page 276, and FortiGuard section on page 189.

Types and file formats of threat feeds

Each threat feed is a list of threats of one type only. File formats vary by type. Types of threat feed include:

- **URL filter (FortiGuard category)** — One URI per line in the file. For example:
  ```
  https://192.168.1.10/url
  https://example.com/url
  http://example.com:8080/url
  *.example.com/url
  ```
  Both IDN and UTF-8 encoding is supported. Wildcards (*) at the start or end are supported. IPv6 URLs must be in [ ] format.

  Domain name and URI lists from threat feeds share the rating category number range 192 to 221 (a total of 30 categories). See also Configuring custom URL rating categories on page 276.
- **IP address** — One IPv4 or IPv6 address, IP address range, or subnet per line in the file. For example:
  ```
  192.168.1.100
  172.16.1.2/24
  172.16.1.1-172.16.1.100
  2001:0db8::eade:27ff:fe04:9a01/120
  ```
- **Malware hash** — One hash per line in the file. Each line has the format:
  ```
  <hash> [optional description]
  ```
  For example:
  ```
  24cda42b9d3f723b65cb5e38d7ad17cd871132fa
  a57983cb39e25ab80d7d3dc05695dd0ee0e49766 Trojan-Ransom.Win32.Virus-Sample.abfl
  ```

For best performance, do not mix different types of hexadecimal hashes together in the list. Use either MD5, SHA1, or SHA256. Alternatively, see Configuring file signatures on page 211.

Comments are supported. For example:

```
# Comment about the URI below.
https://example.com/maliciousurl
```

File size is limited to 10 MB or 131072 entries, whichever limit is reached first. If the number of entries exceeds the limit, FortiMail displays a warning and does not load entries after the limit.

FortiMail does not detect duplicate entries (both in the same file and in different files), but you can use tools such as the `uniq` command on Linux to remove them.

Configuring content disarming and reconstruction

System-wide attachment and URL sanitization settings that are used by all content profiles are configured in *Security > Disarm & Reconstruction*.

About content disarming and reconstruction (CDR)

In an email and attachments, there may be risky URLs and HTML tags such as hyperlinks and JavaScript. Similarly, Microsoft Office and PDF attachments may have macros, links, and other active content that also can be used by spyware or malware. Zero-day or spear phishing attacks that have been specially crafted initially do not have matching virus signatures or URL ratings yet. Some email clients automatically display HTML and attachments, increasing the risk.

Content disarming and reconstruction (CDR) in content profiles (see Configuring content disarm and reconstruction (CDR) on page 218) allows you to remove or mitigate risky content and then reconstruct and still deliver the sanitized email, without affecting the integrity of the text in the email.

For example, HTML email, you could select an action in the content action profile to warn email users by tagging email that contains potentially dangerous HTML content. Alternatively, if you select to remove the HTML tags, then users can safely read the email to decide whether or not it is legitimate.

Configuring CDR attachment settings

For each CDR that content profiles can perform on attached files, configure how FortiMail should disarm or remove the files.

1. Go to *Security* > *Disarm & Reconstruction* > *Attachment*.
2. Configuring the following:

GUI item	Description
Attachment handling for deferred email	Configure the following: • *Send notification:* Enable for the recipient to receive a notification if an email attachment is subjected to deferred scanning. • *Remove all*: Send the notification with all the attachments removed. • *Disarm Office/PDF and remove others*: Send notification with the disarmed Microsoft Office or PDF attachments. Remove all other attachments that are not supported by CDR. • *Verdict threshold to disarm on delivery*: Enter the threshold at which attachments will be disarmed. For example, if set to *Medium*, the attachments with *Medium*, *High*, and *Malicious* verdicts will all be disarmed.
Attachment scan by FortiSandbox	By default, if content disarmament succeeds, then the FortiSandbox scan is bypassed. Enable *Continue FortiSandbox scan on successful content disarm* if you want to allow FortiSandbox to scan the attachment even after successful CDR.

3. Click *Apply*.
4. To use these settings as actions, select it in a content profile. See Configuring content disarm and reconstruction (CDR) on page 218.

Configuring CDR URL click protection and removal options

If you do not configure CDR in the content profile to remove URLs, then users can click them. To protect users from malicious or spam URLs, such as phishing or advertising web sites, you can configure FortiMail to use the FortiGuard URL filter service and FortiSandbox to scan the URLs when users click them. Depending on the results from FortiGuard and FortiSandbox, you can decide if you want to allow users to go to the URLs or block them.

You can also integrate with FortiIsolator to isolate threats. FortiIsolator is a browser isolation solution, which protects users against zero day malware and phishing threats that are delivered over the web and email. These threats may result in data loss, compromise, or ransomware. To protect users, FortiIsolator creates a virtual air gap between users' browsers and websites. Web content is executed in a remote disposable container and displayed to users visually, without running code from the website on their computer.

Newsletters often do not embed images in email in order to keep the email file size small so that email can be sent to many people quickly. Instead, the image files are stored at a URL on a web server or CDN. Email clients download and display the image later, when each person reads their email.

Normal HTML email newsletters often include a plain text version or a link to a web page to fall back if the images cannot be displayed in the email. Spammers and malware, however, can abuse requests to the image URLs in order to detect which recipient email addresses are valid, even when SMTP recipient verification is disabled, and to bypass email antispam and antivirus scans by transmitting the content over HTTPS instead of SMTP.

For this reason, like hyperlink URLs, image URLs also have click protection options.

For each CDR action that content profiles can perform on URLs, configure how FortiMail should change or remove the URLs.

To configure URL click protection options

1. Go to *Security* > *Disarm & Reconstruction* > *URL*.
2. Configure the following:

GUI item	Description
URL Click Protection Option	
URL Rewrite	
Category	Select which URL rating category a URL must match in order to be rewritten. See also Configuring URL filter profiles on page 276.
Base URL	Enter the prefix `https://` and then the FQDN or IP address of FortiMail. When users click a hyperlink, they will be directed to the rewritten URL on FortiMail first. **Note:** The `https://` protocol prefix is required. **Tip:** The URL is rewritten in the format: `https://example.com/fmlurlsvc/?fewReq/baseValue&url=originalUrlEscaped` where `originalUrlEscaped` is the original URL in URL-encoded format. If you want to convert it back to see the original URL, you can use a text editor or online service such as: https://www.urldecoder.org
Include image source attribute	Enable to rewrite the URLs of images that are stored on remote web serversl. **Note:** When you update FortiMail firmware from a previous version, default values are applied to any new settings. If this setting is new, the default results in a change in behavior. If you prefer the previous behavior, then enable this setting.
URL Click Handling	
Category	Select which URL rating category a URL must match in order to receive click handling. See also Configuring URL filter profiles on page 276.
Action	Select how the link will behave when click handling applies, and a user clicks a link: either *Block* or *Allow with Confirmation*.
FortiSandbox Scan	For all other URL categories not selected in *Category*, enable this setting if you want to send them to FortiSandbox for scanning (see Using FortiSandbox antivirus inspection on page 83). • *Enable*: Enable or disable the FortiSandbox scan. • *Action*: Select how the link will behave when a link is clicked during a FortiSandbox scan, either: • *Allow with Confirmation* : Allow access with warning. • *Block*: Block access. • *Submit only*: Allow access while sending the URLs for scanning. • *Timeout*: When the URLs are sent to FortiSandbox for scanning, it can take some time to get the results. Enter how long (in seconds) to wait for FortiSandbox scan results. If FortiMail does not get a reply in

GUI item	Description
	this time, then click handling instead uses the action in *Timeout action*. • *Timeout action*: Select how the link will behave when a user clicks a link after a FortiSandbox scan timeout, either: • *Allow* • *Allow with Confirmation* • *Block*
Include image source attribute	Enable to use click handling with the URLs of images that are stored on remote web servers.
FortiIsolator Integration	
Category	Select which URL rating category a URL must match in order to be reached through FortiIsolator. See Configuring URL filter profiles on page 276.
Base URL	Enter the prefix `https://` and then the FQDN or IP address of FortiIsolator. **Note:** The `https://` protocol prefix is required.
Include image source attribute	Enable to use FortiIsolator with the URLs of images that are stored on remote web servers for HTML email.
URL Removal	
Category	Select which URL rating category a URL must match in order to be removed. See Configuring URL filter profiles on page 276.
Include image source attribute	Enable to remove the URLs of images that are stored on remote web servers.
URL Neutralization	
Category	Select which URL rating category a URL must match in order to be neutralized. See Configuring URL filter profiles on page 276.
Include image source attribute	Enable to neutralize the URLs of images that are stored on remote web servers.

3. Click *Apply*.
4. To use these settings as actions, select it in a content profile. See Configuring content disarm and reconstruction (CDR) on page 218.

Configuring email quarantines and quarantine reports

The *Quarantine* submenu lets you configure quarantine settings, and to configure system-wide settings for quarantine reports.

Using the email quarantine feature involves the following steps:

- First, enable email quarantine when you configure antispam action profiles (see Configuring antispam action profiles on page 206) and content action profiles (see Configuring content action profiles on page 224).
- Configure the system quarantine administrator account who can manage the system quarantine. See Configuring the system quarantine setting on page 292.
- Configure the quarantine control accounts, so that email users can send email to the accounts to release or delete email quarantines. See Configuring the quarantine control options on page 293.
- Configure system-wide quarantine report settings, so that the FortiMail unit can send reports to inform email users of the mail quarantines. Then the users can decide if they want to release or delete the quarantined emails. See Configuring global quarantine report settings on page 285.
- Configure domain-wide quarantine report settings for specific domains. See Quarantine Report Setting on page 100.
- View and manage personal quarantines and system quarantines. See Managing the quarantines on page 42.
- As the FortiMail administrator, you may also need to instruct end users about how to access their email quarantines. See Accessing the personal quarantine and webmail on page 367.

Configuring global quarantine report settings

The *Quarantine Report* tab lets you configure various system-wide aspects of the quarantine report, including scheduling when the FortiMail unit will send reports.

For the quarantine report schedule to take effect, you must enable the quarantine action in the antispam and/or content action profile first. For details, see Configuring antispam action profiles on page 206 and Configuring content action profiles on page 224. For general steps about how to use email quarantine, see Configuring email quarantines and quarantine reports on page 285.

FortiMail units send quarantine reports to notify email users when email is quarantined to their per-recipient quarantine. If no email messages have been quarantined to the per-recipient quarantine folder in the period since the previous quarantine report, the FortiMail unit does not send a quarantine report.

In addition to the system-wide quarantine report settings, you can configure some quarantine report settings individually for each protected domain, including whether the FortiMail unit will send either or both plain text and HTML format quarantine reports. For more information about domain-wide quarantine report settings, see Quarantine Report Setting on page 100.

Starting from v4.1, domain-wide quarantine report settings are independent from the system-wide quarantine report settings.

For information on the contents of the plain text and HTML format quarantine report, see About the plain text formatted quarantine report on page 287 and About the HTML formatted quarantine report on page 289.

To configure the global quarantine report settings

1. Go to *Security* > *Quarantine* > *Quarantine Report*.
2. Configure the following:

GUI item		Description
Schedule		
	These hours	Select the hours of the day during which you want the FortiMail unit to generate quarantine reports.
	These days	Select the days of the week during which you want the FortiMail unit to generate quarantine reports.
Template		
	Quarantine report template	Select a template from the dropdown list or click *Edit* to customize it. For details about email template customization, see Customizing email templates on page 79.
Webmail Access Setting		
	Time limited access without authentication	Enable to allow user access without authentication for the following period of time.
	Expiry period	Specify the time limit for the above setting. Enter 0 to disable the above access.
	Web release host name/IP	Enter a host name for the FortiMail unit that will be used for web release links in quarantine reports (but not email release links). If this field is left blank: • If the FortiMail unit is operating in gateway mode or server mode, web release and delete links in the quarantine report will use the fully qualified domain name (FQDN) of the FortiMail unit. • If the FortiMail unit is operating in transparent mode, web release and delete links in the quarantine report will use the FortiMail unit's management IP address. For more information, see About the management IP. Configuring an alternate host name for web release and delete links can be useful if the local domain name or management IP of the FortiMail unit is not resolvable from everywhere that email users will use their quarantine reports. In that case, you can override the web release link to use a globally resolvable host name or IP address.

3. In the *Quarantine Report Recipient Setting* section, double-click a domain name to modify its related settings.
   A dialog appears.
4. Configure the following and click *OK*.

Quarantine report recipient settings

GUI item		Description
Domain name		Displays the name of a protected domain. For more information on protected domains, see Configuring protected domains on page 92.
	Send to original recipient	Select to send quarantine reports to each recipient address in the protected domain.
	Send to other recipient	Select to send quarantine reports to an email address other than the recipients or group owners, then enter the email address.
	Send to LDAP group owner based on LDAP profile	Select to send quarantine reports to the email addresses of group owners, then select the name of an LDAP profile in which you have enabled and configured in Group Query on page 238. Also configure the following two options for more granular control: • Only when original recipient is group • When group owner is found, do not send to original recipient.

About the plain text formatted quarantine report

Plain text quarantine reports:

- notify email users about email messages that have been quarantined to their per-recipient quarantine
- explain how to delete one or all quarantined email messages
- explain how to release individual email messages

For plain text quarantine reports, you can only release email from the per-recipient quarantine by using the email release method. For more information on how to release email from the per-recipient quarantine, see Releasing and deleting email via quarantine reports on page 290.

Release instructions in a plain text quarantine report may use either the management IP address or local domain name.

The contents of quarantine reports are customizable. For more information, see Customizing custom messages, and email templates on page 71.

Sample plain text quarantine report

Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00]
From: release-ctrl@example.com
Date: 12:00 PM
To: user1@example.com

Date: Thu, 04 Sep 2008 11:52:51
Subject: [SPAM] information leak
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzU3MS43NDJfNTk5ODcuRm9ydGlNYWlsLTQwMCwjRiNTIzYzMyNFLFU4OjIsUw==

Date: Thu, 04 Sep 2008 11:51:10
Subject: [SPAM] curious?
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsI0YjUyM2MjUjRSxVNzoyLA==

Date: Thu, 04 Sep 2008 11:48:50
Subject: [SPAM] Buy now!!!! lowest prices
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsI0YjUyM2NDIjRSxVNToyLA==

Actions:

o) Release a message: Send an email to <release-ctrl@example.com> with subject line set to "user1@example.com:Message-Id".
o) Delete a message: Send an email to <delete-ctrl@example.com> with subject line set to "user1@example.com:Message-Id".
o) Delete all messages: Send an email to <delete-ctrl@example.com> with subject line set to "delete_all:user1@example.com:e4d46814:ac146004:05737c7c111d68d0111d68d0111d68d0".

Sample plain text quarantine report

	Report content
Message header of quarantine report	Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00] From: release-ctrl@example.com Date: Thu, 04 Sep 2008 12:00:00 To: user1@example.com
Quarantined email #1	Date: Thu, 04 Sep 2008 11:52:51 Subject: [SPAM] information leak From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzU3MS43NDJfNTk5ODcuRm9ydGlNYWlsLTQwMCwjRiNTIzYzMyNFLFU4OjIsUw==
Quarantined email #2	Date: Thu, 04 Sep 2008 11:51:10 Subject: [SPAM] curious? From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsI0YjUyM2MjUjRSxVNzoyLA==
Quarantined email #3	Date: Thu, 04 Sep 2008 11:48:50 Subject: [SPAM] Buy now!!!! lowest prices From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsI0YjUyM2NDIjRSxVNToyLA==
Instructions for deleting or releasing quarantined email	Actions: o) Release a message: Send an email to <release-ctrl@example.com> with subject line set to "user1@example.com:Message-Id". o) Delete a message: Send an email to <delete-ctrl@example.com> with subject line set to "user1@example.com:Message-Id". o) Delete all messages: Send an email to <delete-ctrl@example.com> with subject line set to "delete_ all:user1@example.com:e4d46814:ac146004:05737c7c111d68d0111d68d0111d68d0".

About the HTML formatted quarantine report

HTML quarantine reports:

- notify email users about email messages that have been quarantined to their per-recipient quarantine
- contain links to delete one or all quarantined email messages (see Sample HTML quarantine report on page 289)
- contain links to release individual email messages (see Sample HTML quarantine report on page 289)

From an HTML format quarantine report, you can release or delete messages by using either web or email release methods. For more information on how to release email from the per-recipient quarantine, see Releasing and deleting email via quarantine reports on page 290.

Web release and delete links in an HTML formatted quarantine report may link to either the management IP address, local domain name, or an alternative host name for the FortiMail unit. For more information, see Web release host name/IP on page 286.

The contents of quarantine reports are customizable. For more information, see Customizing custom messages, and email templates on page 71.

If option to auto add to personal safe list when releasing spam is enabled, default HTML report now seems to include notification of that setting. From replacement message:

```
<**SPAM_CONFIG_NOTE**><b>Note: %%SPAM_SAFE_LIST%%.</b>
<**/SPAM_CONFIG_NOTE**>
```

Sample HTML quarantine report

Sample HTML quarantine report

Report content

Message header of quarantine report	`Subject: Quarantine Summary: [ 3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00 ]` `From: release-ctrl@example.com` `Date: Thu, 04 Sep 2008 12:00:00` `To: user1@example.com`
Quarantined email #1	**Date**: Thu, 04 Sep 2008 11:52:51 **From**: User 1 <user1@example.com> **Subject**: [SPAM] information leak **Web Actions**: Release Delete **Email Actions**: Release Delete
Quarantined email #2	**Date**: Thu, 04 Sep 2008 11:51:10 **From**: User 1 <user1@example.com> **Subject**: [SPAM] curious? **Web Actions**: Release Delete **Email Actions**: Release Delete
Quarantined email #3	**Date**: Thu, 04 Sep 2008 11:48:50 **From**: User 1 <user1@example.com> **Subject**: [SPAM] Buy now!!!! lowest prices **Web Actions**: Release Delete **Email Actions**: Release Delete
Instructions for deleting or releasing quarantined email	`Web Actions:` ` Click on Release link to send a http(s) request to have the message sent to your inbox.` ` Click on Delete link to send a http(s) request to delete the message from your quarantine.` ` Click Here to send a http(s) request to Delete all messages from your quarantine.` `Email Actions:` ` Click on Release link to send an email to have the message sent to your inbox.` ` Click on Delete link to send an email to delete the message from your quarantine.` ` Click here to send an email to Delete all messages from your quarantine.` `Other:` ` To view your entire quarantine inbox or manage your preferences, Click Here`

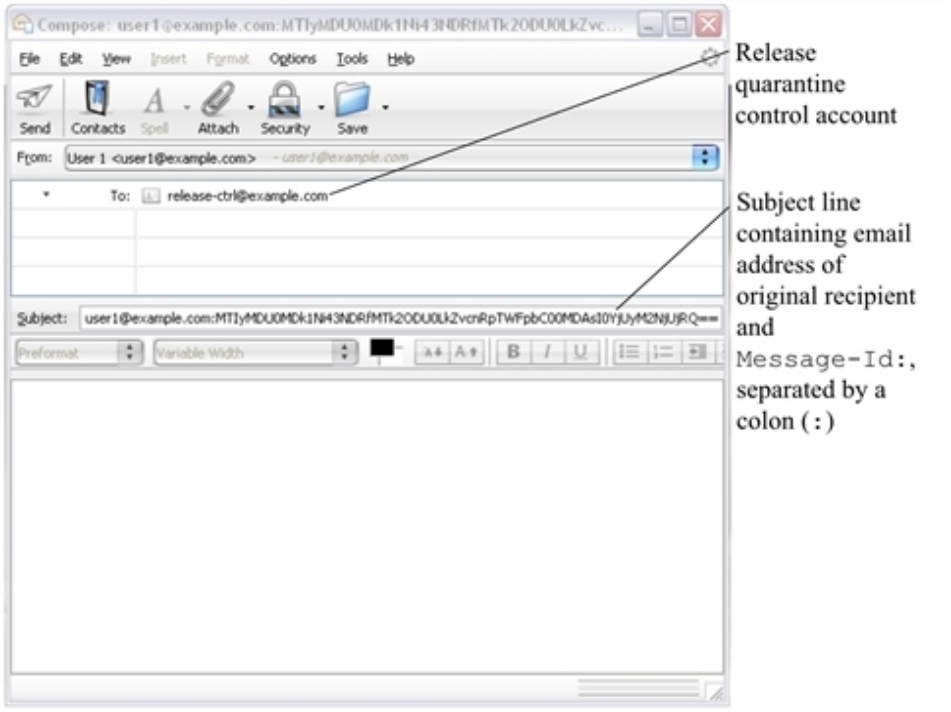
Releasing and deleting email via quarantine reports

Quarantine reports enable recipients to remotely monitor and delete or release email messages in the per-recipient quarantine folders.

Depending on whether the quarantine report is sent and viewed in plain text or HTML format, a quarantine report recipient may use either or both web release and email release methods to release or delete email from a per-recipient quarantine.

- *Web release*: To release or delete an email from the per-recipient quarantine, the recipient must click the *Release* or *Delete* web action link which sends an HTTP or HTTPS request to the FortiMail unit. Available for HTML format quarantine reports only.
- *Email release*: To release or delete an email from the per-recipient quarantine, the recipient must either:
  - Click the *Release* or *Delete* email action link which creates a new email message containing all required information, then send it to the quarantine control account of the FortiMail unit. Available for HTML format quarantine reports only.
  - Manually send an email message to the quarantine control account of the FortiMail unit. The `To:` address must be the quarantine control email address, such as `release-ctrl@example.com` or `delete-ctrl@example.com`. The subject line must contain both the recipient email address and `Message-Id:` of the quarantined email, separated by a colon (`:`), such as: `user1@example.com:MTIyMDU0MDk1Ni43NDRfMTk2ODU0LkZvcnRpTWFpbC00MDAsI0YjUyM2NjUjRQ==`

Releasing an email from the per-recipient quarantine using email release



Quarantine control email addresses are configurable. For information, see Configuring the quarantine control options on page 293.

Web release links may be configured to expire after a period of time, and may or may not require the recipient to log in to the FortiMail unit. For more information, see Configuring global quarantine report settings on page 285.

For more information on the differences between plain text and HTML format quarantine reports, see About the plain text formatted quarantine report on page 287 and About the HTML formatted quarantine report on page 289.

See also

Configuring global quarantine report settings

Managing the personal quarantines

About the plain text formatted quarantine report

About the HTML formatted quarantine report

Configuring the system quarantine setting

Go to *Security* > *Quarantine* > *System Quarantine Setting* to configure the system quarantine account, quarantine folder, and other system quarantine settings.

The system quarantine can be accessed through either:

- IMAP -- use an IMAP email client to access the FortiMail unit with the system quarantine account name (without any domain name) and password.
- Administrative GUI -- create an administrator account with the quarantine access privilege in the access profile and access the GUI using this administrator account.

The system quarantine cannot be accessed through POP3 or webmail.

To configure the system quarantine account and quarantine folders

1. Go to *Security* > *Quarantine* > *System Quarantine Setting*.
2. Configure the following:

GUI item	Description
Account Setting	
Account	Enter the user name of the system quarantine account. You can use this account to view the system quarantine via an IMAP email client.
Password	Enter the password for the system quarantine account.
Forward to	Enter an email address to which the FortiMail unit will forward a copy of each email that is quarantined to the system quarantine.
Quarantine Folders	
Enable folder rotation	Enable to rotate the folders according to the interval settings below.
Rotation interval (days)	Enter the maximum amount of time that the current system quarantine mailbox (Inbox) will be used. When the mailbox reaches this time, the FortiMail unit renames the current mailbox based on its creation date and rename date, and creates a new Inbox mailbox.
New	Click to create a new folder. When creating a folder, also specify the retention time (in days) and the administrators who are allowed to access the quarantine folder. The retention time determines how long the quarantined email will saved in the folder before it get deleted.

See also

Managing the system quarantine

Configuring the quarantine control options

Go to *Security* > *Quarantine* > *Quarantine Control* to configure quarantine release and delete control accounts. You can also specify whether to re-scan the quarantined email for virus infections before they are released. This can be useful if the email messages are quarantined due to antispam reasons, or if the antivirus signatures are updated later.

For email messages in the Virus folder of the system quarantine, they will not be rescanned when they are released. Otherwise, you may never be able to release them. For email messages in other quarantine folders, they will be rescanned when they are released for the first time. In case they are quarantined again and you still want to release them, they will be released without rescan.

Email users can remotely release or delete email messages in their per-recipient quarantine by sending email to quarantine control email addresses.

For example, if the Release account is `release-ctrl` and the local domain name of the FortiMail unit is `example.com` and `example.com` is not a protected domain, an email user could release an email message from their per-recipient quarantine by sending an email to `release-ctrl@example.com`. If the FortiMail unit's local domain name happens to be a protected domain name, the Release account address would be `release-ctrl@hostname.example.com`.

For more information on releasing and deleting quarantined items through email, see Releasing and deleting email via quarantine reports on page 290.

To configure the quarantine control settings

1. Go to Security > Quarantine > Quarantine Control.
2. Under *Quarantine Release Re-scan Setting*, specify whether to re-scan the quarantined email with the FortiMail AV engine and/or FortiSandbox before the email is released. Also specify whether to scan the personal quarantine and/or system quarantine.
3. For Release account, enter the user name portion (also known as the local-part) of the email address on the FortiMail unit that will receive quarantine release commands; for example: such as `release-ctrl`.
4. For Delete account, enter the user name portion (also known as the local-part) of the email address on the FortiMail unit that will receive quarantine delete commands; such as `delete-ctrl`.
5. Click Apply.

See also

Managing the personal quarantines

Configuring global quarantine report settings

Configuring the block lists and safe lists

You can use safe lists and block lists as a simple way to reject, discard, or allow email messages based on email addresses, domain names, and SMTP client IP addresses.

Use safe lists and block lists with caution. They can increase incorrect results.

For example, a system-level safe list entry for `*.edu` email addresses allows email from all `.edu` top level domains. Sender email addresses in the SMTP envelope (`MAIL FROM:`) and message header (`From:`) can be fake, too. The result is that all spam from any `.edu` email address — real or fake — would **bypass later antispam scans**.

Better approaches are to either:

- use access control policies with a *Safe* action with client IP addresses (which are harder to fake)
- use DKIM or SPF sender authentication (which is stronger and usually supported by email servers)

Do not safelist protected domain names. Sender email addresses can be faked, so they may not really belong to the protected domain. This could allow spammers to bypass antispam scans.

Order of execution is configurable for safe lists and block lists. See the FortiMail CLI Reference. Default order is shown in Order of execution for antispam scans on page 22.

By default, safe lists cause sender authentication (DKIM, SPF, DMARC) to be skipped, even though sender email addresses could be fake. This is configurable. See the FortiMail CLI Reference.

Multiple scopes of block lists and safe lists exist. Locations vary.

- **System-wide or per-domain**: Go to *Security* > *Block/Safe List*. For details, see Managing the global block and safe list on page 296, Managing the per-domain block lists and safe lists on page 297.
- **Per-user**: Go to either *Security* > *Block/Safe List*, *Domain & User* > *User* > *User Preference*, or let FortiMail webmail users go to their *Preferences* tab to configure their own list. For details, see Managing the personal block lists and safe lists on page 298 and Configuring user preferences on page 115.
- **Per-session**: Go to *Profile* > *Session* > *Session*. For details, see Configuring session profiles on page 171.

See also

Order of execution for antispam scans

About block list and safe list address formats

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Configuring block list settings

About block list and safe list address formats

Block lists and safe lists support these formats:

1. **Email:** Matches email addresses. Wild cards (* to match multiple characters, or ? to match any one character) are supported.

   If you upgrade from a version before FortiMail 7.0.0, domain names are converted to an entry with a wild card username (for example, `example.com` to `*@.example.com`).
2. **IP/Netmask:** Matches IP addresses or subnets. CIDR format is supported.

   If you upgrade from a version before FortiMail 7.0.0, IP addresses with no netmask are converted to a single host (for example, `10.0.0.5` to `10.0.0.5/32`).
3. **Reverse DNS:** Matches a hostname/FQDN from reverse DNS lookup (`PTR` record) results.

Valid formats may vary by the type of the block or safe list.

Avoid wild cards and large subnets if possible. They can accidentally match too much, increasing incorrect results.

Examples of valid block/safe list entries

Type	Example	Description
Email	**spammer@example.com**	Email from the sender spammer@example.com.
	?ser1@example.com	Email from any sender with any character preceding and including “ser1” at example.com.
	***@example.com**	Email from any sender at example.com.
	***@*.example.com**	Email from any sender at any subdomain of example.com.
	hostname.example.com	Email from client MTA IP which has PTR record resolving to hostname.example.com.
	user1@ex?mple.com	Email from the sender user1 in domains such as example.com, exemple.com, or exumple.com.
	user1@*.com	Email from the sender user1 at any .com domain.
IP/Netmask	**172.16.1.0/24**	Email from the IP subnet 172.16.1.0/24.
	172.16.1.1/32	Email from client IP matching 172.16.1.1.
Reverse DNS	**hostname.example.com**	Hostname/FQDN matching reverse DNS lookup results for connecting client MTA IP addresses.

The following formats are **not** valid:

- 172.168.1
- example.com
- @spam. example.com

See also

Order of execution for antispam scans

Configuring the block lists and safe lists

Managing the global block and safe list

You can configure system-wide block and safe lists to block or allow email by sender. You can also back up and restore the system-wide block and safe lists.

System-wide block lists and safe lists can also be tracked in terms of when they were created, when they last had a match or hit, and hit count. See also Configuring block list settings on page 299.

Alternatively, you can back up all system-wide, per-domain, and per-user block and safe lists together. For details, see Backup and restore on page 1.

Domain administrators can access the global block list and global safe list, and therefore could affect domains other than their own. If you do not want to permit this, do **not** provide *Read-Write* permission to the *Block/Safe List* category in domain administrators' access profile.

To configure the system-wide block list or safe list

1. Go to *Security* > *Block/Safe List* > *System*.
2. Either:
   - To block email by sender, select *Block* from the *List* dropdown.
   - To allow email by sender, select *Safe* from the *List* dropdown.
3. Click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 295.
4. Click *Create*.
5. From the safe/block lists, you can also select *Backup* to back up the list or *Restore* to restore a backup list.

- Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.
- Only CSV files with "pattern" and "comment" in the first line can be restored.

See also

Configuring the block lists and safe lists

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution for antispam scans

About block list and safe list address formats

Backup and restore

Managing the per-domain block lists and safe lists

You can configure block and safe lists that are specific to a protected domain in order to block or allow email by sender.

Alternatively, you can back up all system-wide, per-domain, and per-user block and safe lists together. For details, see Backup and restore on page 1.

To configure the per-domain block lists or safe lists

1. Go to *Security* > *Block/Safe List* > *Domain*.

GUI item	Description
Show domain association	Enable to filter by domain association in the domain block/safe list.
Domain	Displays the name of the protected domain to which the block list and safe list belong. For more information on protected domains, see Configuring protected domains on page 92.
Block List	Click the *List* icon to display, modify, back up, or restore the block list for the protected domain.
Safe List	Click the *List* icon to display, modify, back up, or restore the safe list for the protected domain.

2. Click the *Block List* or *Safe List* icon.
3. Click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 295.

Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution for antispam scans

About block list and safe list address formats

Backup and restore

Managing the personal block lists and safe lists

You can modify email users' personal block or safe lists in order to block or allow email by sender.

Alternatively, email users can also configure their own per-user block list and safe list: in FortiMail webmail, go to the *Preferences* tab. For more information, see the online help for FortiMail webmail.

You can also back up and restore the per-user block lists and safe lists.

Alternatively, you can back up all system-wide, per-domain, and per-user block and safe lists together. For details, see Backup and restore on page 1.

To configure the per-user block lists or safe lists

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. Users in the selected domain will be displayed. In the *Search* field, type the user name of the email user whose per-user block list or safe list you want to modify, and click *Enter*.
3. Select a use and click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 295.

   If you add the user's email address to the same user's personal safe list, the FortiMail unit will ignore this entry. This prevents spammers from using that email address as a disguise to send spam.

4. Click *Backup* to back up the list or *Restore* to restore a backup list.

   Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Configuring block list settings

Order of execution for antispam scans

About block list and safe list address formats

Backup and restore

Configuring block list settings

The *Setting* tab lets you configure the action to take if an email message arrives from a blocklisted domain name, email address, or IP address. You may also enable or disable block/safe list tracking.

The FortiMail unit will apply this action to email matching system-wide, per-domain, and per-session profile block lists.

Domain administrators can configure the block list action, and therefore could affect domains other than their own. If you do not want to permit this, do **not** provide *Read-Write* permission to the *Block/Safe List* category in domain administrators' access profile.

To configure block list settings

1. Go to *Security* > *Block/Safe List* > *Setting*.
2. Select the action, either:
   - *Reject*: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (`Relaying denied`).
   - *Discard*: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client.
   - *Use AntiSpam profile settings*: Use the actions configured in the antispam profile that you selected in the policy that matches the email message. See also Configuring antispam profiles and actions on page 187.
3. Enable *Block/Safe list tracking* to track various blocklist and safelist statistics, including creation time, last hit time, and hit count. These statistics are tracked under *Security* > *Block/Safe List* > *System* and *Security* > *Block/Safe List* > *Domain*.
4. Enable *Status* under *Auto Aging Of List Entries* to apply automatic purging of system and domain block and safe lists that are listed for a defined *Retention period* (up to a maximum of 365 days).

   Once *Auto Aging Of List Entries* is enabled and a *Retention period* is applied, you may manually remove any expired entries on-demand by using the *Cleanup* option from the system and domain block/safe lists.

5. Click *Apply*.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Order of execution for antispam scans

Configuring greylisting

Go to *Security* > *Greylist* to configure greylisting and to view greylist-exempt senders.

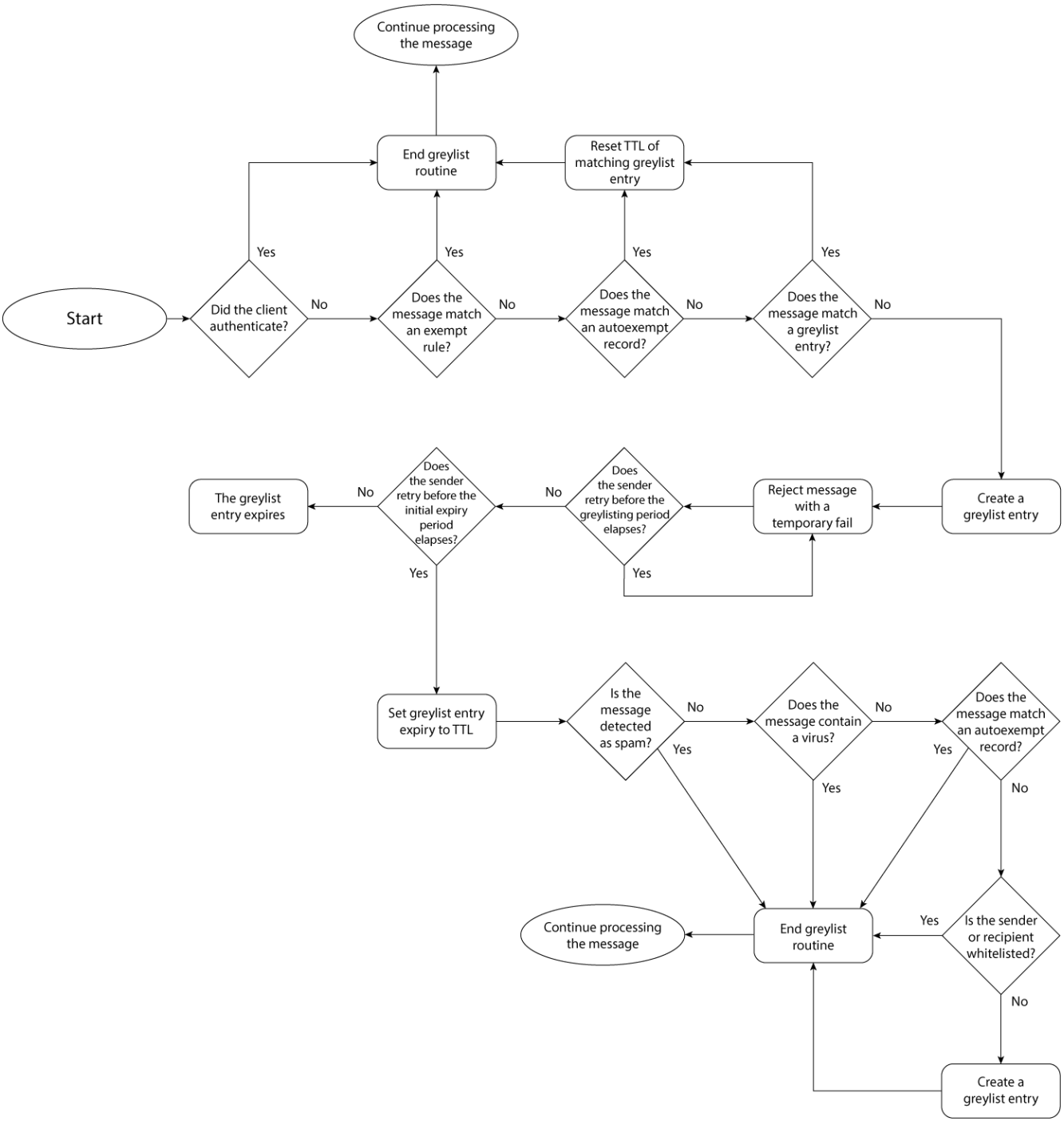
About greylisting

Greylist scanning blocks spam based on the behavior of the sending server, rather than the content of the messages. When receiving an email from an unknown server, the FortiMail unit will temporarily reject the message. If the mail is legitimate, the originating server will try to send it again later (RFC 2821), at which time the FortiMail unit will accept it. Spammers will typically abandon further delivery attempts in order to maximize spam throughput.

Advantages of greylisting include:

- Greylisting is low-maintenance, and does not require you to manually maintain IP address lists, block lists or safe lists, or word lists. The FortiMail unit automatically obtains and maintains the required information.
- Spam blocked by greylisting never undergoes other antispam scans. This can save significant amounts of processing and storage resources. For this reason, enabling greylisting can improve FortiMail performance.
- Even if a spammer adapts to greylisting by retrying to send spam, the greylist delay period can allow time for FortiGuard Antispam and DNSBL servers to discover and blocklist the spam source. By the time that the spammer finally succeeds in sending the email, other antispam scans are more likely to recognize it as spam.

Workflow of greylist scanning



Greylisting is omitted if the matching access control rule's Action is RELAY. For more information on antispam features' order of execution, see Order of execution for antispam scans on page 22.

When an SMTP client first attempts to deliver an email message through the FortiMail unit, the greylist scanner examines the email message's combination of:

- sender email address in the message envelope (`MAIL FROM:`)
- recipient email address in the message envelope (`RCPT TO:`)
- IP address of the SMTP client

The greylist scanner then compares the combination of those attributes to manual and automatic greylist entries. The greylist scanner evaluates the email for matches in the following order:

1. manual greylist entries, also known as exemptions (see Manual greylist entries on page 304)
2. consolidated automatic greylist entries, also known as autoexempt entries (see Automatic greylist entries on page 303)
3. individual automatic greylist entries, also known as greylist entries

For more information on the types of greylist entries, see Automatic greylist entries on page 303 and Automatic greylist entries on page 303.

According to the match results, the greylist scanner performs one of the following:

- If a matching entry exists, the FortiMail unit continues with other configured antispam scans, and will accept the email if no other antispam scan determines that the email is spam. For automatic greylist entry matches, each accepted subsequent email also extends the expiry date of the automatic greylist entry according to the configured time to live (TTL) (automatic greylist entries are discarded if no additional matching email messages are received by the expiry date).
- If no matching entry exists, the FortiMail unit creates a pending individual automatic greylist entry (see Viewing the pending and individual automatic greylist entries on page 57) to note that combination of sender, recipient, and client addresses, then replies to the SMTP client with a temporary failure code. During the greylist delay period after the initial delivery attempt, the FortiMail unit continues to reply to delivery attempts with a temporarily failure code. To confirm the pending automatic greylist entry and successfully send the email message, the SMTP client must retry delivery during the greylist window: after the delay period, but before the expiry of the pending entry.

Subsequent email messages matching a greylist entry are accepted by the greylist scanner without being subject to the greylisting delay.

For information on how the greylist scanner matches email messages, see Matching automatic greylist entries on page 302. For information on configuring the greylisting delay, window, and entry expiry/TTL, see Configuring the greylist TTL and initial delay on page 304.

Matching automatic greylist entries

While the email addresses in the message envelope must match exactly, the IP address of the SMTP client is a less specific match: any IP address on the /24 network will match.

For example, if an email server at 192.168.1.99 is known to the greylist scanner, its greylist entry contains the IP address `192.168.1.0` where `0` indicates that any value will match the last octet, and that any IP address starting with `192.168.1` will match that entry.

This greylist IP address matching mechanism restricts the number of IP addresses which can match the greylist entry while also minimizing potential issues with email server farms. Some large organizations use many email

servers with IP addresses in the same class C subnet. If the first attempt to deliver email receives a temporary failure response, the second attempt may come from an email server with a different IP address. If an exact match were required, the greylist scanner would treat the second delivery attempt as a new delivery attempt unrelated to the first. Depending on the configuration of the email servers, the email message might never be delivered properly. Approximate IP address matching often prevents this problem.

For very large email server farms that require greater than a /24 subnet, you can manually create greylist exemptions. For more information, see Manual greylist entries on page 304.

Automatic greylist entries

The automatic greylisting process automatically creates, confirms pending entries, and expires automatic greylist entries, reducing the need for manual greylist entries. The automatic greylisting process can create three types of automatic greylist entries:

- pending (see Viewing the pending and individual automatic greylist entries on page 57)
- individual (see Viewing the pending and individual automatic greylist entries on page 57)
- consolidated (see Viewing the consolidated automatic greylist exemptions on page 59)

Pending entries are created on the initial delivery attempt, and track the email messages whose delivery attempts are currently experiencing the greylist delay period. They are converted to confirmed individual entries if a delivery attempt occurs after the greylist delay period, during the greylist window.

The automatic greylisting process can reduce the number of individual automatic greylist entries by consolidating similar entries after they have been confirmed during the greylisting window. Consolidation improves performance and greatly reduces the possibility of overflowing the maximum number of greylist entries.

Consolidated automatic greylist entries include only:

- the domain name portion of the sender email address
- the IP address of the SMTP client

They do not include the recipient email address, or the user name portion of the sender email address. By containing only the domain name portion and not the entire sender email address, a consolidated entry can match all senders from a single domain, rather than each sender having and matching their own individual automatic greylist entry. Similarly, by not containing the recipient email address, any recipient can share the same greylist entry. Because consolidated entries have broader match sets, they less likely to reach the time to live (TTL) than an individual automatic greylist entry.

For example, example.com and example.org each have 100 employees. The two organizations work together and employees of each company exchange email with many of their counterparts in the other company. If each example.com employee corresponds with 20 people from example.org, the FortiMail unit used by example.com will have 2000 greylist entries for the email received from example.org alone. By consolidating, these 2000 greylist entries are replaced by a single entry.

Not all individual automatic greylist entries can be consolidated. Because consolidated entries have fewer message attributes, more email messages may match each entry, some of which could contain different recipient email addresses and sender user names than those of the originally greylisted email messages. To prevent spam from taking advantage of the broader match sets, requirements for creation of consolidated entries are more strict than those of individual automatic greylist entries. FortiMail units will create a consolidated (autoexempt) entry only if the email:

- does not match any manual greylist entry (exemption)
- passes the automatic greylisting process
- passes all configured antispam scans
- passes all configured antivirus scans
- passes all configured content scans
- does not match any safe lists

If an email message fails to meet the above requirements, the FortiMail unit instead maintains the individual automatic greylist entry.

If an email message matches a manual greylist entry, it is not subject to automatic greylisting and the FortiMail unit will not create an entry in the individual or consolidated automatic greylist or autoexempt list.

After an individual automatic greylist entry is consolidated, both the consolidated autoexempt entry and the original greylist entry will coexist for the length of the greylist TTL. Because email messages are compared to the autoexempt list before the greylist, subsequent matching email will reset only the expiry date of the autoexempt list entry, but not the expiry date of the original greylist entry. Eventually, the original greylist entry expires, leaving the automatic greylist entry.

Manual greylist entries

In some cases, you may want to manually configure some greylist entries. Manual greylist entries are exempt from the automatic greylisting process, and are therefore not subject to the greylist delay period and confirmation.

For example, a manual greylist entry can be useful when email messages are sent from an email server farm whose network is larger than /24. For very large email server farms, if a different email server attempts the delivery retry each time, the greylist scanner could perceive each retry as a first attempt, and automatic greylist entries could expire before the same email server retries delivery of the same email. To prevent this problem, you can manually create an exemption using common elements of the host names of the email servers.

For more information on creating manual greylist entries, see Manually exempting senders from greylisting on page 305.

Configuring the greylist TTL and initial delay

The Setting tab lets you configure time intervals used during the automatic greylisting process.

For more information on the automatic greylisting process, see About greylisting on page 300.

To configure greylisting intervals

1. Go to *Security* > *Greylist* > *Setting*.
2. Configure the following:

GUI item	Description
TTL	Enter the time to live (TTL) that determines the maximum amount of time that unused automatic greylist entries will be retained. Expiration dates of automatic greylist entries are determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings`. The default initial expiry time is 4 hours. If the initial expiry time elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. • TTL: Between the entry's PASSTHROUGH time and initial expiry time, if the entry is hit again (the sender retries to send the message again), the entry's expiry time will be reset by adding the TTL value (time to live) to the message's "Received" time. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. For more information on automatic greylist entries, see Viewing the greylist statuses on page 56.
Greylisting period	Enter the length of the greylist delay period. For the initial delivery attempt, if no manual greylist entry (exemption) matches the email message, the FortiMail unit creates a pending automatic greylist entry, and replies with a temporary failure code. During the greylist delay period after this initial delivery attempt, the FortiMail unit continues to reply to additional delivery attempts with a temporary failure code. After the greylist delay period elapses and before the pending entry expires (during the greylist window), any additional delivery attempts will confirm the entry and convert it to an individual automatic greylist entry. The greylist scanner will then allow delivery of subsequent matching email messages. For more information on pending and individual automatic greylist entries, see Viewing the pending and individual automatic greylist entries on page 57.

You can use the CLI to change the default 4 hour greylist window. For more information, see the CLI command `set greylist-init-expiry-period` under `config antispam settings` in the FortiMail CLI Reference.

Manually exempting senders from greylisting

The Exempt tab displays manual greylist entries, which exempt email messages from the automatic greylisting process and its associated greylist delay period.

Greylisting is omitted if the matching access control rule's Action is RELAY. For more information on antispam features' order of execution, see Order of execution for antispam scans on page 22.

For more information on the automatic greylisting process, see About greylisting on page 300. For more information on manual greylist entries, see Manual greylist entries on page 304.

To view and configure manual greylist entries

1. Go to *Security* > *Greylist* > *Exempt*.

GUI item	Description
Sender Pattern	Displays the pattern that defines a matching sender address in the message envelope (`MAIL FROM:`). The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 381. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).
Recipient Pattern	Displays the pattern that defines a matching recipient address in the message envelope (`RCPT TO:`). The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 381. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).
Sender IP/Netmask	Displays the IP address and netmask that defines SMTP clients (the last hop address) that match this entry. `0.0.0.0/0` matches all SMTP client IP addresses.
Reverse DNS Pattern	Displays the pattern that defines a matching result when the FortiMail unit performs the reverse DNS lookup of the IP address of the SMTP client. The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 381. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).

2. Click New to add an entry or double-click an entry to modify it.
   A dialog appears.
3. Configure the following:

GUI item	Description
Sender pattern	Enter the pattern that defines a matching sender email address in the message envelope (`MAIL FROM:`). To match any sender email address, enter either `*`, or, if Regular expression is enabled, `.*`. You can create a pattern that matches multiple addresses either by: • including wild card characters (`*` or `?`). An asterisk (`*`) matches one or more characters; a question mark (`?`) matches any single character. • using regular expressions. You must also enable the Regular expression option.
Regular expression	For any of the pattern options, select the accompanying Regular expression check box if you entered a pattern using regular expression syntax. See also Syntax on page 381.

GUI item	Description
Recipient pattern	Enter the pattern that defines a matching recipient address in the message envelope (`RCPT TO:`). To match any recipient email address, enter either `*`, or, if Regular expression is enabled, `.*`. See also Syntax on page 381.
Sender IP/Netmask	Enter the IP address and netmask that defines SMTP clients that match this entry. To match any SMTP client IP address, enter `0.0.0.0/0`. You can create a pattern that matches multiple addresses by entering any bit mask other than `/32`. For example, entering `10.10.10.10/24` would match the 24-bit subnet of IP addresses starting with 10.10.10, and would appear in the list of manual greylist entries as `10.10.10.0/24`.
Reverse DNS pattern	Enter the pattern that defines valid host names for the IP address of the SMTP client (the last hop address). Since the SMTP client can use a fake self-reported host name in its SMTP greeting (`EHLO/HELO`), you can use a reverse DNS lookup of the SMTP client's IP address to get the real host name of the SMTP client. Then the FortiMail greylist scanner can compare the host name resulting from the reverse DNS query with the pattern that you specify. If the query result matches the specified pattern, the greylist exempt rule will apply, Otherwise, the rule will not apply. You can create a pattern that matches multiple addresses either by: • including wild card characters (`*` or `?`). An asterisk (`*`) matches one or more characters; a question mark (`?`) matches any single character. • using regular expressions. You must also enable the Regular expression option. See also Syntax on page 381.

No pattern can be left blank in a greylist exempt rule. To have the FortiMail unit ignore a pattern, enter an asterisk (*) in the pattern field. For example, if you enter an asterisk in the Recipient Pattern field and do not enable Regular Expression, the asterisk matches all recipient addresses. This eliminates the recipient pattern as an item used to determine if the rule matches an email message.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Example: Manual greylist entries (exemptions)

Example Corporation uses a FortiMail unit that is operating in gateway mode, and uses greylisting to reduce the quantity of spam they receive at their protected domain, example.com.

Example Corporation wants to exempt some email from the initial greylist delay period by creating manual greylist entries (exemptions to the automatic greylisting process) that match trusted combinations of SMTP client IP addresses and recipient email addresses.

Rule 1

Example Corporation has a number of foreign offices. Email from these offices does not need to be greylisted.The IP addresses of email servers in the foreign offices vary, though their host names all begin with “mail” and end with “example.com”.

Rule 1 uses the recipient pattern and the reverse DNS pattern to exempt from the automatic greylisting process all email messages that are sent to recipients at example.com, and are being delivered by an email server with a host name beginning with “mail” and ending with “example.com”.

Rule 2

Example Corporation works closely with a partner organization, Example Org, whose email domain is example.org. Email from the example.org email servers does not need to be greylisted. The IP addresses of email servers for example.org are within the 172.20.120.0/24 subnet, and have a host name of mail.example.org.

Rule 2 uses the recipient pattern, sender IP/ netmask, and reverse DNS pattern to exempt from the automatic greylisting process all email messages that are sent to recipients at example.com by any email server whose IP address is between 172.20.120.1 and 172.20.120.255 and whose host name is mail.example.org.

Configuring bounce verification and tagging

The *Bounce Verification* submenu lets you configure bounce address tagging and verification.

Spammers sometimes fraudulently use others’ email addresses as the sender email address in the message envelope (`MAIL FROM:`) when delivering spam. When an email cannot be delivered, email servers often return a delivery status notification (DSN) message, sometimes also known as a bounce message, to the sender email address located in the message envelope.

While DSNs are normally useful in notifying email users when an email could not be delivered, in this case, it could result in delivery of a DSN to an email user who never actually sent the original message. Because the invalid bounce message is from a valid email server, it can be difficult to detect as invalid.

You can combat this problem with bounce address tagging and verification. If the FortiMail unit tags outgoing email, it can verify the tags of incoming bounce messages to guarantee that the bounce message is truly in reply to a previous outgoing email.

For a FortiMail unit to perform bounce address tagging:

- bounce verification must be enabled
- a bounce address key must exist and be activated
- in the protected domain to which the sender belongs, the Bypass bounce verification option must be disabled
- the recipient domain must not be in the tagging exempt list

The FortiMail unit will use the currently activated key to generate bounce address tags for all outgoing email. You can create multiple keys, but only one can be activated at any time.

The activated private key is used, together with randomizing data, to generate the tag that is applied to the sender email address in the message envelope, also known as the bounce address, of all outgoing messages. The format of tagged sender email addresses is:

`prvs=1234567890=user1@example.com`

where the sender email address is `user1@example.com` and the prefix is the bounce address tag. The tag is different for every email message, and uniquely identifies the email message.

Bounce address tagging is applied to the sender email address in the message envelope only; it is not applied to the sender email address in the message header.

If the email server for the recipient email domain cannot deliver the email, it will send a bounce message whose recipient is the tagged email address. When the bounce message arrives at the FortiMail unit, it will use the private keys to verify the bounce address tag. Incoming email is subject to bounce verification if all the following is true:

- bounce verification is enabled
- at least one bounce address key exists
- in the protected domain to which the recipient belongs, the Bypass Bounce Verification option is disabled (see Configuring protected domains on page 92)
- in the session profile, the Bypass Bounce Verification check option is disabled (see Configuring session profiles on page 171)
- the sender email address (`MAIL FROM:`) in the message envelope is empty
- the DSN sender is not in the bounce verification exempt list

The sender email address is typically empty for bounce messages. The sender email address may also be empty for some types of spam that are not bounce messages. Because the sender email addresses of those types of spam will not have a proper tag, similar to bounce message spam, these spam will fail the bounce verification process. Email sent from email clients or webmail will not have an empty sender email address, and therefore will not be subject to the bounce verification process.

If the tag is successfully verified, the bounce verification scan removes the tag, restoring the recipient email address to one known by the protected domain, and allows the bounce message.

If the tag is **not** successfully verified, the bounce verification scan will perform the action that you have configured for invalid bounce messages.

To configure bounce verification settings

1. Go to *Security* > *Bounce Verification* > *Setting*.
2. Configure the following:

GUI item	Description
Status	Enable verification of bounce address tags for all incoming email. If you want to make exceptions for email that does not require bounce address tag verification, you can bypass bounce verification in protected domains and session profiles. For more information, see Configuring protected domains on page 92 and Configuring session profiles on page 171.
Tag expiry (days)	Enter the number of days after creation when bounce message keys will expire and their resulting tags will fail verification.

GUI item	Description
Key auto-removal	Specify when the unused and deactivated keys will be deleted. The activated key will not be automatically removed.
Action	Select which action that a FortiMail unit will perform when an incoming email fails bounce address tagging verification, either: • *Reject*: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (`Relaying denied`). • *Discard*: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client. • *Use antispam profile setting*: Use the default action configured in the antispam profile that you selected in the policy that matches the email message. For more information on actions, see Configuring antispam action profiles on page 206.
Bounce Verification Key	Use this area to manage the keys.
New, Edit, Delete (buttons)	Create, edit or delete a key. **Note:** If you delete a key, any email with a tag generated when that key was active will fail bounce verification. After activating a new key, keep the previously active key until any tags generated with the old key expire. *Delete* is unavailable if the *Status* of the key is *Active*.
Key name	Enter the string of text that will be used together with randomizing data in order to generate each bounce address tag. Keys must not be identical. This field cannot be modified after a key is created. Instead, you must create a new key. If you are certain that no email has used a key, and therefore no bounce messages can exist which would require tag verification, you can safely delete that key.
Status	Select the activation status of the key. • *Active*: The key will be activated, and used to generate bounce address tags for outgoing messages. If any other key is currently activated, it will be deactivated when this new key is saved and activated. • *Inactive*: The key will be deactivated. You can activate the key at a later time. Only one of the keys may be activated at any given time.The activated key is the one that will be used to generate tags for outgoing messages. Both activated and deactivated keys will be used for bounce address tag verification of incoming email.

Excluding recipient domains from bounce verification tagging

If you do not want to tag the email sent to certain recipients, you can do so by adding the recipient domain to the exempt list.

To configure the tagging exempt list

1. Go to *Security* > *Bounce Verification* > *Tagging Exempt List*.
2. Click *New*.
3. Add the recipient domain name.
4. Click *Create*.

Excluding senders from bounce verification

If you do not want to verify bounce verification tags from certain senders, you can do so by adding the sender host names to the exempt list.

To configure the verification exempt list

1. Go to *Security* > *Bounce Verification* > *Verification Exempt List*.
2. Click *New*.
3. Add the host name. FortiMail will use reverse DNS to resolve the client's IP address into host name. You can use wildcard to include all hosts within a domain. For example, you could enter:
   `*.example.com`
4. Click *Create*.

Configuring sender rewriting scheme

Go to *Security* > *Sender Rewriting Scheme* to configure sender rewriting scheme (SRS) settings, and maintain a domain name exempt list.

SRS is used to rewrite the envelope sender of an email address (`MAIL FROM`), so that the email may be forwarded by an MTA if necessary without being rejected by the receiving server which may have a strict SPF policy in place.

In FortiMail gateway mode, SRS rewriting will be implemented under the following conditions:

- The original sender is from a non-protected domain.
- The email is incoming (destined to a protected domain) before alias expansion or address mapping.
- After the alias expansion or address mapping, the recipient is on a non-protected domain.

For example, user1@protected-domain.com receives an email from user2@unprotected-domain-A.com, and user1@protected-domain.com is mapped to user3@unprotected-domain-B.com, then SRS will rewrite user2@unproteced-domain-A.com to user2@protected-domain.com.

In FortiMail server mode, if webmail users configure auto forward, SRS rewriting will be implemented under the following conditions:

- The original sender is from a non-protected domain.
- The forwarded address is also on a non-protected domain.

To configure SRS settings

1. Go to *Security* > *Sender Rewriting Scheme* > *Setting*.
2. Configure the following as required:

GUI item	Description
Domain for rewrite	Select which domains to rewrite for external senders sending emails. • None: No domains are rewritten. • Protected Domains: Only protected domains are rewritten. • All Domains: All domains are rewritten.
Rewritten address handling	Select which action to take for rewritten addresses. • None: Deny any recipient that is previously rewritten. • Reverse: Reverse the recipient address and send the email to the original sender, for those recipients that are previously rewritten senders.

- If *Default domain for authentication* (under *System > Mail Setting > Mail Server Setting*) is not enabled, SRS rewrite will not work.
- If there are multiple domains, the default domain will be used for SRS rewrite.

Excluding domains from SRS

If you want to exempt certain domain names from SRS, you can do so by adding the recipient domain name to the exempt list.

To configure the domain name exempt list

1. Go to *Security > Sender Rewriting Scheme > Exempt List*.
2. Click *New*.
3. Add the recipient domain name.
4. Click *Create*.

Configuring preferences

Go to *Security > Option > Preference* to configure some global settings for action profile, mail scan, and antispam preferences.

GUI item	Description
Action Profile	In action profiles (see Configuring antispam action profiles on page 206, Configuring antivirus action profiles on page 213, and Configuring content action profiles on page 224), you can select an action: • *System quarantine* • *Personal quarantine*

GUI item	Description
	• *Disclaimer insertion* • *Subject tag location* • *Replacement message location* For delivery and quarantine actions, you can select which form of the email to use: • *Modified copy* — Modify the email according to the action. • *Unmodified copy* — Original email header and body.  If the email is in its original form, the recipient in the SMTP envelope (`RCPT TO:`) still might be rewritten by the action. For example, when the HTML content is converted to text, if you choose to deliver the unmodified copy, then the HTML version will be delivered; if you choose to deliver the modified copy, then the plain text version will be delivered. For *Disclaimer insertion*, select when to insert the disclaimer: • *Selected messages* — Only new email in threads. Thread replies do not receive a disclaimer. This avoids repeatedly inserting disclaimers that recipients have already seen.  Threads are detected when the same domain is in both the `Message-ID:` and `In-Reply-To:/References:` message headers. In RFC 2822, those message headers are optional. If an email client doesn't support them, then this setting has no effect. • *All messages* — Both new and reply email in threads. For *Subject tag location*, you can choose to insert the tag at the beginning or end of the subject line. For *Replacement message location*, you can choose to append the replacement message to the beginning or end of the email.
Execute attachment scan on spam email under personal quarantine	For spam that is sent to personal quarantine, select whether to continue or stop later scans of the email's attachments.
Mail Scan	Specify the following: • *Maximum level to decompress archive file* — Enter how many levels to decompress the archived files for antivirus and content scan. Valid range is 1 to 36. Default value is 12. • *Maximum archive file size to decompress (MB)* — Enter the maximum file size to scan after the archived files are decompressed. This applies to every single file after decompression. Bigger files will not be scanned. Default value is 10MB. • *Maximum compression ratio for archive bomb* — Enter the maximum compression ratio for FortiMail to decompress. Valid range is 1 to 1000. Default value is 200.

GUI item	Description
AntiSpam	
DMARC Report Generation	Select either: • *Enable* — Collect DMARC check data. Each day, for each sender domain that matched a policy where DMARC checks are enabled, send a report to that domain's authorized DMARC report recipient. Also configure Sender address local part. **Note:** If a sender does not have a valid DMARC RUA/RUF configured in the domain's DNS `TXT` record, then even if you enable DMARC reports, FortiMail cannot send them to that domain because there is no report recipient email address. **Tip:** If you have the DMARC report analysis feature license, then you can instead use charts with statistics about DMARC reports.You can also generate DMARC reports on demand, and send them to other recipients. See Viewing DMARC report statistics on page 55 and On-demand DMARC reports on page 90. • *Disable* — Do not collect DMARC check data. Do not generate a report. • *Monitor Only* — Collect DMARC check data, but do not generate a report. This system-wide setting can be overridden by a per-domain setting. For details, see DMARC Report Setting on page 104.
Sender address local part	Enter the local part (username) that the FortiMail unit will use as its sender email address (`From:`) when it sends DMARC report email. Default is `noreply`. Change it if, for example, an administrator wants replies about DMARC reports. Also configure DMARC Report Generation.
Analysis	Indicates whether the DMARC report analysis feature licence is valid. See also DMARC report analysis on page 1.
Impersonation analysis	Email impersonation is one of the email spoofing attacks. It forges the email header to deceive the recipient because the message appears to be from a different source than the actual address. To fight against email impersonation, you can map display names with email addresses and check email for the mapping. You can choose whether the impersonation analysis uses manual mapping entries or dynamic entries. You can also use both types of entries. • *Manual* — Use the entries you manually entered under *Profile* > *AntiSpam* > *Impersonation*. • *Dynamic* — Use the entries automatically learned by the FortiMail mail statistics service. To enable this service, enable `mailstat-service` under `config system global`. The default setting is *Manual*.
QR code URL scan	Select which locations to scan for QR code images that contain known spam URLs. • *Inline image* — Embedded inline, in the email body. • *Attachment image* — Email attachments. If PDF attachment scan is also enabled in the antispam profile (see Configuring antispam profiles and actions on page 187), QR code images in the PDF attachment will also be scanned.

Training and maintaining the Bayesian databases

Bayesian scanning uses databases to determine if an email is spam. For Bayesian scanning to be effective, the databases must be trained with known-spam and known-good email messages so the scanner can learn the differences between the two types of email. To maintain its effectiveness, false positives and false negatives must be sent to the FortiMail unit so the Bayesian scanner can learn from its mistakes.

Be aware that, without ongoing training, Bayesian scanning will become significantly less effective over time and thus Fortinet does not recommend enabling the Bayesian scanning feature.

The *Security* > *Option* > *Bayesian* submenu lets you manage the databases used to store statistical information for Bayesian antispam processing, and to configure the email addresses used for remote control and training of the Bayesian databases.

To use a Bayesian database, you must enable the Bayesian scan in the antispam profile. For more information, see Configuring antispam profiles on page 187.

Types of Bayesian databases

FortiMail units have two types of Bayesian databases:

- Global
- Group

All types contain Bayesian statistical data that can be used by Bayesian scans to detect spam, and should be trained in order to be most accurate for detecting spam within their respective scopes. For more information on training each type of Bayesian database, see Training the Bayesian databases on page 316.

Only one Bayesian database is used by any individual Bayesian scan; which type will be used depends on the directionality of the email and your configuration of the FortiMail unit's protected domains and antispam profiles. For information, see Use global Bayesian database on page 109.

Global

The global Bayesian database is a single database that contains Bayesian statistics that can be used to detect spam for any email user.

Outgoing antispam profiles can use only the global Bayesian database. Incoming antispam profiles can use global or domain Bayesian databases.

If all spam sent to all protected domains has similar characteristics and you do not require your Bayesian scans to be tailored specifically to the email of a protected domain, using the global database for all Bayesian scanning may be an ideal choice, because there is only one database to train and maintain.

For email that does not require use of the global database, if you want to use the global database, you must disable use of the per-domain Bayesian databases. For information on configuring protected domains to use the global Bayesian database, see Use global Bayesian database on page 109.

Group

Group Bayesian databases, also known as per-domain Bayesian databases, contain Bayesian statistics that can be used to detect spam for email users in a specific protected domain. FortiMail units can have multiple group Bayesian databases: one for each protected domain.

If you require Bayesian scans to be tailored specifically to the email received by each protected domain, using per-domain Bayesian databases may provide greater accuracy and fewer false positives.

For example, medical terms are a common characteristic of many spam messages. However, those terms may be a poor indicator of spam if the protected domain belongs to a hospital. In this case, you may want to train a separate, per-domain Bayesian database in which medical terms are not statistically likely to indicate spam.

If you want to use a per-domain database, you must disable use of the global Bayesian databases. For information on disabling use of the global Bayesian database for a protected domain, see Use global Bayesian database on page 109.

Training the Bayesian databases

Bayesian scans analyze the words (or "tokens") in an message header and message body of an email to determine the probability that it is spam. For every token, the FortiMail unit calculates the probability that the email is spam based on the percentage of times that the word has previously been associated with spam or non-spam email. If a Bayesian database has not yet been trained, the Bayesian scan does not yet know the spam or non-spam association of many tokens, and does not have enough information to determine the statistical likelihood of an email being spam. By training a Bayesian database to recognize words that are and are not likely to be associated with spam, Bayesian scans become increasingly accurate.

However, spammers are constantly trying to invent new ways to defeat antispam filters. In one technique commonly used in attempt to avoid antispam filters, spammers alter words commonly identified as characteristic of spam, inserting symbols such as periods (**.**), or using nonstandard but human-readable spellings, such as substituting Â, Ç, Ë, or Í for A, C, E or I. These altered words are technically different tokens to a Bayesian database, so mature Bayesian databases may require some ongoing training to recognize new spam tokens.

You generally will not want to enable Bayesian scans until you have performed initial training of your Bayesian databases, as using untrained Bayesian databases can increase your rate of spam false positives and false negatives.

To initially train the Bayesian databases

1. Train the global database by uploading mailbox (.mbox) files. For details, see Backing up, batch training, and monitoring the Bayesian databases on page 319.
   By uploading mailbox files, you can provide initial training more rapidly than through the Bayesian control email addresses. Training the global database ensures that outgoing antispam profiles in which you have enabled Bayesian scanning, and incoming antispam profiles for protected domains that you have configured to use the global database, can recognize spam.

   If you have configured the FortiMail unit for email archiving, you can make mailbox files from archived email and spam. For details, see Managing archived email.

You can leave the global database untrained if both these conditions are true:

- no outgoing antispam profile has Bayesian scanning enabled
- no protected domain is configured to use the global Bayesian database

2. Train the per-domain databases by uploading mailbox (.mbox) files. For details, see Backing up, batch training, and monitoring the Bayesian databases on page 319.
   By uploading mailbox files, you can provide initial training more rapidly than through the Bayesian control email addresses. Training per-domain databases ensures that incoming antispam profiles for protected domains that you have configured to use the per-domain database can recognize spam.
   You can leave a per-domain database untrained if either of these conditions are true:
   - the protected domain is configured to use the global Bayesian database
   - no incoming antispam profiles exist for the protected domain
3. If you have enabled incoming antispam profiles to train Bayesian databases when the FortiMail unit receives training messages, and have selected those antispam profiles in recipient-based policies that match training messages, instruct FortiMail administrators and email users to forward sample spam and non-spam email to the Bayesian control email addresses. For more information, see Configuring the Bayesian training control accounts on page 322, Accept training messages from user on page 199, and Training Bayesian databases on page 366.

Before instructing email users to train the Bayesian databases, verify that you have enabled the FortiMail unit to accept training messages. If you have not enabled the “Accept training messages from users” option in the antispam profile for policies which match training messages, the training messages will be discarded without notification to the sender, and no training will occur.

FortiMail units apply training messages to either the global or per-domain Bayesian database, whichever is enabled for the sender’s protected domain.

Example: Bayesian training

In this example, Company X has set up a FortiMail unit to protect its email server. With over 1,000 email users, Company X plans to enable Bayesian scanning for incoming email. You, the system administrator, have been asked to configure Bayesian scanning, perform initial training of the Bayesian databases, and configure Bayesian control email addresses for ongoing training.

The local domain name of the FortiMail unit itself is example.com.

Company X has email users in two existing protected domains:

- example.net
- example.org

Each protected domains receives email with slightly different terminology, which could be considered spam to the other protected domain, and so will use separate per-domain Bayesian databases.

To facilitate initial training of each per-domain Bayesian database, you have used your email client software to collect samples of spam and non-spam email from each protected domain, and exported them into mailbox files:

- example-net-spam.mbox
- example-net-not-spam.mbox
- example-org-spam.mbox

- example-org-not-spam.mbox

After initial training, email users will use the default Bayesian control email addresses to perform any required ongoing training for each of their per-domain Bayesian databases.

To enable use of per-domain Bayesian databases

1. Go to *Domain & User > Domain > Domain*.
2. Select the row corresponding to example.net and click Edit.
3. Click the arrow to expand Advanced Setting and click Other.
4. Disable *Use global bayesian database*.
5. Click OK.
   Repeat the above steps for the protected domain example.org.

To initially train each per-domain Bayesian database using mailbox files

1. Go to *Security > Option > Bayesian*.
2. Under Database Training, from Select a domain, select a domain.
   This example uses example.net and example.org.
3. In the Operations area, click Train group Bayesian database with email samples.
   A dialog appears.
4. In Clean emails, click Browse and locate example-net-not-spam.mbox.
5. In Spam emails, click Browse and locate example-net-spam.mbox.
6. Click OK.
   Repeat the above steps for the protected domain example.org and its sample Bayesian database files.

To enable Bayesian scanning

1. Go to *Profile > AntiSpam > AntiSpam*.
2. In the row corresponding to an antispam profile that is selected in a policy that matches recipients in the protected domain example.net, click Edit.
3. Enable Bayesian.
4. Click the arrow to expand Bayesian.
5. Enable the option Accept training messages from user.
6. Click OK.
   Repeat the above steps for all incoming antispam profiles that are selected in policies that match recipients in the protected domain example.org.

To perform ongoing training of each per-domain Bayesian database

1. Notify email users that they can train the Bayesian database for their protected domain by sending them an email similar to the following:

This procedure assumes the default Bayesian control email addresses. To configure the Bayesian control email addresses, go to *Security > Bayesian > Control Account*.

```
All employees,
We have enabled a new email system feature that can be trained to recognize the differences
      between spam and legitimate email. You can help to train this feature. This message
      describes how to train our email system.
If you have old email messages and spam...
```

- Forward the old spam to learn-is-spam@example.com from your company email account.
- Forward any old email messages that are not spam to learn-is-not-spam@example.com from your company email account.

If you receive any new spam, or if a legitimate email is mistakenly classified as spam...

- Forward spam that was not recognized to is-spam@example.com from your company email account.
- Forward legitimate email that was incorrectly classified as spam to is-not-spam@example.com from your company email account.

2. Notify other FortiMail administrators that they can train the per-domain Bayesian databases for those protected domains by forwarding email to the Bayesian control accounts, described in the previous step. To do so, they must configure their email client software with the following sender addresses:
   - default-grp@example.net
   - default-grp@example.org

   For example, when forwarding a training message from the sender (`From:`) email address `default-grp@example.net`, the FortiMail unit will apply the training message to the per-domain Bayesian database of example.net.

See also

Training the Bayesian databases

Types of Bayesian databases

Backing up, batch training, and monitoring the Bayesian databases

Configuring the Bayesian training control accounts

Configuring global quarantine report settings

Backing up, batch training, and monitoring the Bayesian databases

You can train, back up, restore, and reset the global and per-domain Bayesian databases. You can also view a summary of the number of email messages that have been used to train each Bayesian database.

You can alternatively train Bayesian databases by forwarding spam and non-spam email to Bayesian control email addresses. For more information, see Training the Bayesian databases on page 316.

You can alternatively back up, restore, and reset all Bayesian databases at once. For more information, see Backup and restore.

Domain administrators cannot access the global Bayesian settings.

For details, see About administrator account permissions on page 67.

To individually train, view and manage Bayesian databases

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database:
   - For the global Bayesian database, from Select a domain, select System. For more information, see Use global Bayesian database on page 109.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.

   The Summary area displays the total number of email messages that the Bayesian database has learned as spam or not spam.
3. For any level of Bayesian database, select an operation:
   - To train a Bayesian database using mailbox files on page 320
   - To back up a Bayesian database on page 321
   - To restore a Bayesian database on page 321
   - To reset a Bayesian database on page 321

To train a Bayesian database using mailbox files

Uploading mailbox files trains a Bayesian database with many email messages at once, which is especially useful for initial training of the Bayesian database until it reaches maturity. Because this method appends to the Bayesian database rather than overwriting, you may also perform this procedure periodically with new samples of spam and non-spam email for batch maintenance training.

If you have configured the FortiMail unit for email archiving, you can make mailbox files from archived email and spam. For details, see Managing archived email.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Train global Bayesian database with mbox files
   - Train group Bayesian database with mbox files

   A pop-up window appears enabling you to specify which mailbox files to upload.
4. In the Innocent mailbox field, click Browse, then select a mailbox file containing email that is not spam.
5. In the Spam mailbox field, click Browse, then select a mailbox file containing email that is spam.
   For best results, the mailbox file should contain a representative sample of spam for the specific FortiMail unit, protected domain, or email user.
6. Click OK.
   Your management computer uploads the file to the FortiMail unit to train the database, and the pop-up window closes. Time required varies by the size of the file and the speed of your network connection. To update the training summary display in the Summary area with the new number of learned spam and non-spam messages, refresh the page by selecting the tab.

To back up a Bayesian database

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Backup global Bayesian database
   - Backup group Bayesian database

   A pop-up window appears enabling you to download the database backup file.
4. Select a location in which to save the database backup file and save it.
   The Bayesian database backup file is downloaded to your management computer. Time required varies by the size of the file and the speed of your network connection.

To restore a Bayesian database

Back up the Bayesian database before beginning this procedure. Restoring a Bayesian database replaces all training data stored in the database. For more information on backing up Bayesian database files, see To back up a Bayesian database on page 321 or Backup and restore.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Restore global Bayesian database
   - Restore group Bayesian database

   A pop-up window appears enabling you to upload a database backup file.
4. Click Browse to locate and select the Bayesian database backup file, then click OK.
5. Click OK.
   The Bayesian database backup file is uploaded from your management computer, and a success message appears. Time required varies by the size of the file and the speed of your network connection.

   If a database operation error message appears, you can attempt to repair database errors. For more information, see Backup and restore.

To reset a Bayesian database

Back up the Bayesian database before beginning this procedure. Resetting a Bayesian database deletes all training data stored in the database. For more information on backing up Bayesian database files, see To back up a Bayesian database on page 321 or Backup and restore.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Reset global Bayesian database
   - Reset group Bayesian database

   A pop-up window appears asking for confirmation.
4. Click Yes.
   A status message notifies you that the FortiMail unit has emptied the contents of the Bayesian database.

See also

Training the Bayesian databases

Types of Bayesian databases

Configuring the Bayesian training control accounts

Backup and restore

Configuring the Bayesian training control accounts

The Control Account tab lets you configure the email addresses used for remote training of the Bayesian databases.

To train the Bayesian databases through email, email users and FortiMail administrators forward spam and non-spam email (also called training messages) to the appropriate Bayesian control email address. Bayesian control email addresses consist of the user name portion (also known as the local-part) of the email address configured on this tab and the local domain name of the FortiMail unit. For example, if the local domain name of the FortiMail unit is example.com, you might forward spam to `learn-is-spam@example.com`.

If the FortiMail unit is configured to accept training messages, it will use the email to train one or more Bayesian databases. To accept a training message:

- The training message must match a recipient-based policy.
- The matching recipient-based policy must specify use of an antispam profile in which *Accept training messages from user* is enabled.

If either of these conditions is not met, the FortiMail unit will silently discard the training message without using them for training.

If these conditions are both met, the FortiMail unit accepts the training message and examines the user name portion and domain name portion of the sender address.

Depending on whether the sender's protected domain is configured to use the global or per-domain Bayesian database (the option *Use global Bayesian database*), the FortiMail unit trains that Bayesian database.

To configure the Bayesian control email addresses, go to *Security* > *Option* > *Bayesian*.

GUI item	Description
"is really spam" user name	Enter the user name portion of the email address, such as `is-spam`, to which email users will forward spam false negatives. Forwarding false negatives corrects the Bayesian database when it inaccurately classifies spam as being legitimate email.
"is not really spam" user name	Enter the user name portion of the email address, such as `is-not-spam`, to which email users will forward spam false positives. Forwarding false positives corrects the Bayesian database when it inaccurately classifies legitimate email as being spam.
"learn is spam" user name	Enter the user name portion of the email address, such as `learn-is-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
"learn is not spam" user name	Enter the user name portion of the email address, such as `learn-is-not-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
training group	Enter the user name portion of the email address, such as `default-grp`, that FortiMail administrators can use as their sender email address when forwarding email to the “learn is spam” email address or “learn is not spam” email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain).

See also

Training the Bayesian databases

Types of Bayesian databases

Backing up, batch training, and monitoring the Bayesian databases

Configuring file signatures

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring encryption settings

Use the *Encryption* menu to configure IBE encryption settings and certificate binding for S/MIME encryption.

Configuring IBE encryption

The *Encryption > IBE > IBE Encryption* submenu lets you configure the Identity Based Encryption (IBE) service. With IBE, you can send secured email through the FortiMail unit.

IBE is a type of public-key encryption. IBE uses identities (such as email addresses) to calculate encryption keys that can be used for encrypting and decrypting electronic messages. Compared with traditional public-key cryptography, IBE greatly simplifies the encryption process for both users and administrators. Another advantage is that a message recipient does not need any certificate, key pre-enrollment, or specialized software to access the email.

About FortiMail IBE

The FortiMail unit encrypts an email message using the public key generated with the recipient's email address. The email recipient does not need to install any software or generate a pair of keys in order to access the email.

When an email reaches the FortiMail unit, the FortiMail unit applies its IP-based policies and recipient-based policies containing IBE-related content profiles as well as the message delivery rules to the email. If a policy or rule match is found, the FortiMail unit encrypts the email using the public key before sending a notification to the recipient. Sample secure message notification on page 325 shows a sample notification.

The notification email contains an HTML attachment, which contains instructions and links telling the recipient how to access the encrypted email.

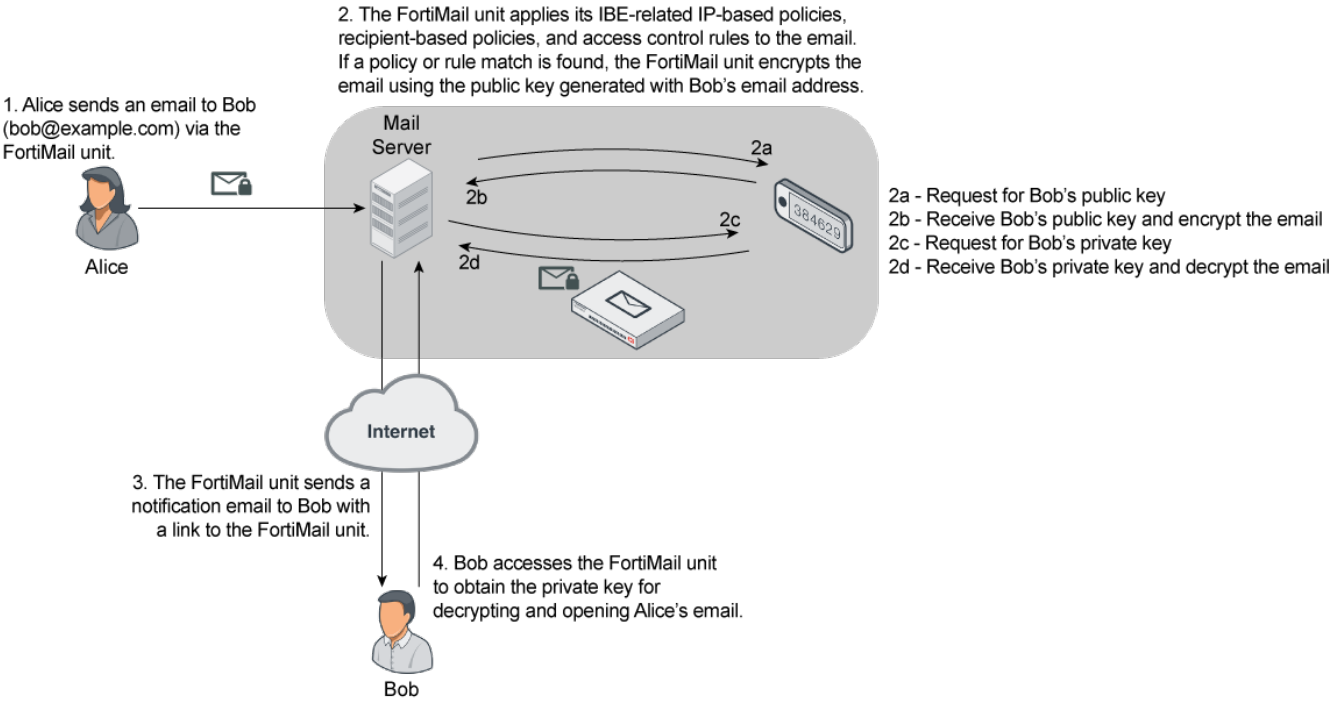
If this is the first time the recipient receives such a notification, the recipient must follow the instructions and links to register on the FortiMail unit before reading email.

If this is not the first time the recipient receives such a notification and the recipient has already registered on the FortiMail unit, the recipient only needs to log in to the FortiMail unit to read email.

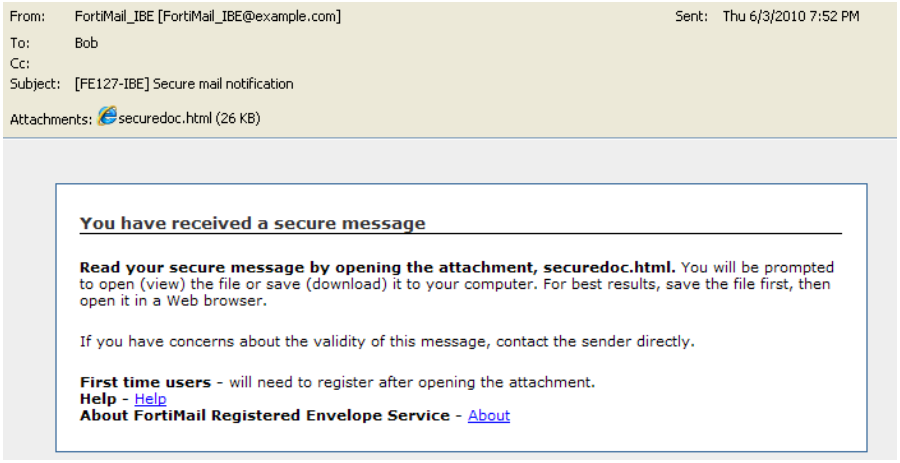
When the recipient opens the mail on the FortiMail unit, the email is decrypted automatically.

Due to more confining security restrictions imposed on Apple iOS devices, email attachments included in IBE push (for details about IBE push and pull methods, see Configuring encryption profiles on page 268) notification messages can no longer be opened properly on iOS 10 and later. Therefore, users cannot view the encrypted email messages on these iOS devices. Users should download and open the attachments on their computers as a workaround.

How FortiMail works with IBE



Sample secure message notification



External IBE users can only access their secure messages via the link in the IBE notification email, while internal users (protected domain users) can also access their secure messages via webmail login.

FortiMail IBE configuration workflow

Follow the general steps below to use the FortiMail IBE function:

- Configure and enable the IBE service. See Configuring IBE services on page 326.
- Manage IBE users. See Configuring IBE users on page 125.
- Configure an IBE encryption profile. See Configuring encryption profiles on page 268.

If you want to encrypt email based on the email contents:

- Add the IBE encryption profile to the content action profile. See Configuring content action profiles on page 224.
- Add the content action profile to the content profile and configure the scan criteria in the content profile, such as attachment filtering, file type filtering, and content monitor and filtering including the dictionary and action profiles. See Configuring content profiles on page 216.
- Add the content profile to the IP-based and recipient-based policies to determine email that needs to be encrypted with IBE. See Controlling email based on sender and recipient addresses on page 163, and Controlling email based on IP addresses on page 159.
  For example, on the FortiMail unit, you have:
  - configured a dictionary profile that contains a pattern called “Confidential”, and enabled *Search header* (see Configuring dictionary profiles on page 262)
  - added the dictionary profile to a content profile which also includes a content action profile that has an encryption profile in it
  - included the content profile to IP and recipient policies

  You then notify your email users on how to mark the email subject line and header if they want to send encrypted email.

  For example, Alice wants to send an encrypted email to Bob through the FortiMail unit. She can add “Confidential” in the email subject line, or “Confidential” in the header (in Microsoft Outlook, when compiling a new mail, go to *Options* > *Message settings* > *Sensitivity*, and select *Confidential* in the list). The FortiMail unit will apply the policies you configured to the email by checking the email’s subject line and header. If one of them matches the patterns defined in the dictionary profile, the email will be encrypted.
- Configure IBE email storage.
- Configure log settings for IBE encryption. See Configuring logging on page 343.
- View logs of IBE encryption. See Viewing log messages on page 35.

If you want to encrypt email using message delivery rules:

- Configure message delivery rules using encryption profiles to determine email that need to be encrypted with IBE. See Configuring delivery rules on page 156.
- Configure IBE email storage.
- Configure log settings for IBE encryption. See Configuring logging on page 343.
- View logs of IBE encryption. See Viewing log messages on page 35.

For full configuration and procedural details, depending on your environment's requirements, see Encrypting confidential emails in FortiMail and How to encrypt emails sent from a designated source in FortiMail.

Configuring IBE services

You can configure, enable, or disable IBE services which control how secured mail recipients use the FortiMail IBE function. For details about how to use IBE service, see FortiMail IBE configuration workflow on page 325.

To configure IBE service

1. Go to *Encryption > IBE > IBE Encryption*.
2. Configure the following:

GUI item	Description
Enable IBE service	Enable or disable IBE secure mail service.
IBE service name	Enter the name for the IBE service. This is the name the secure mail recipients will see once they access the FortiMail unit to view the secure mail.
Activation is required for account registration	When enabled, IBE users receive a validation email that contains an activation link to complete the account registration. When disabled, IBE users are redirected to the IBE account after registration. **Note:** If the IBE user registered by clicking the registration link inside the reset notification email, they will not be redirected, and will need to login to their account.
Account registration expiry time (days)	Enter the number of days that the secure mail recipient has to register on the FortiMail unit to view the mail before the registration expires. The starting date is the date when the FortiMail unit sends out the first notification to a mail recipient.
Account inactivity expiry time (days)	Enter the number of days the secure mail recipient can access the FortiMail unit without registration. For example, if you set the value to 30 days and if the mail recipient did not access the FortiMail unit for 30 days after the user registers on the unit, the recipient will need to register again if another secure mail is sent to the user. If the recipient accessed the FortiMail unit on the 15th days, the 30-day limit will be recalculated from the 15th day onwards.
Account password reset expiry time (hours)	Enter the password reset expiry time in hours. This is for the recipients who have forgotten their login passwords and request for new ones. The secured mail recipient must reset the password within this time limit to access the FortiMail unit.
Encrypted email retention period (days)	Enter the number of days that the secured mail will be saved on the FortiMail unit.
Allow secure replying	Select to allow the secure mail recipient to reply the email with encryption.
Allow secure forwarding	Select to allow the secure mail recipient to forward the email with encryption.
Allow secure composing	Select to allow the secure mail recipient to compose an email. The FortiMail unit will use policies and mail delivery rules to determine if this mail needs to be encrypted. For encrypted email, the domain of the composed mail's recipient must be a protected one, otherwise an error message will appear and the mail will not be delivered.
"Help" content URL	If you want to create a custom help file on how to access the IBE secure email, enter the URL for your file. The mail recipient can click the "Help" link from the secure mail notification to view your file.

GUI item	Description
	If you leave this setting empty, a link to the default help file will be added to the secure mail notification.
"About" content URL	If you want to create a custom file about IBE secure mail, enter the URL for the file. The mail recipient can click the "About" link in the secure mail notification to view your file. If you leave this setting empty, a link to the default file about FortiMail IBE secure mail will be added to the secure mail notification.
Allow custom user control	If your organization has its own user authentication tools, enable this setting. Then configure: **"Custom user control" URL**: URL where you can determine if an IBE user exists. **"Custom forgot password" URL**: URL where IBE users authenticate.
Authentication Setting	In *Authentication mode*, select either two-factor authentication, one-time password (OTP) tokens, or password only. Then also configure *Max. number of attempts* for the maximum number of tries a user is allowed for authentication. Two-factor authentication tokens can be delivered via either SMS or email. To configure OTP or multi-factor authentication, see the FortiMail CLI Reference. See also the User registration process with two-factor authentication on page 128.
Notification Setting	Under *Account Status Notification*,select which notifications will be sent to users. For *Expiration*, also define when the expiration notification should be sent. Under *Email Status Notification*, you can choose to send a notification to the sender or recipient when the secure email is read or remains unread for a specified period of time. Click the *Edit* link to modify the email template. For details, see Customizing email templates on page 79. Depending on the IBE email access method (either push or pull) you defined in Configuring encryption profiles on page 268, the notification settings behave differently. • If the IBE message is stored on FortiMail (pull access method), the "read" notification will only be sent the first time the message is read. • If the IBE message is not stored on FortiMail (push access method), the "read" notification will be sent every time the message is read, that is, after the user pushes the message to FortiMail and FortiMail decrypts the message. • There is no "unread" notification for IBE push messages.

Configuring certificate bindings

Go to *Encryption > S/MIME > Certificate Binding* to create certificate binding profiles, which establish the relationship between an email address and the certificate that:

- proves an individual's identity
- provides their keys for use with encryption profiles

Use this relationship and that information for secure MIME (S/MIME) according to RFC 2634.

If an incoming email message is encrypted, FortiMail compares the recipient's identity with the list of certificate bindings to determine if it has a key that can decrypt the email. If there is a matching **private key**, FortiMail will decrypt the email before delivering it. If there is **not**, then FortiMail forwards the still-encrypted email to the recipient.

If you have selected an encryption profile (see Configuring encryption profiles on page 268) with an encryption action in the message delivery rule that applies to the session, then FortiMail compares the recipient's identity with the list of certificate bindings to determine if it has a certificate and **public key**. If there is a matching public key, then FortiMail will encrypt the email using the algorithm specified in the encryption profile. If there is **not**, then FortiMail performs the failure action indicated in the encryption profile.

If an incoming email message is digitally signed, FortiMail will **not** verify the signature. Instead, it will deliver the message unmodified. Email clients usually do the verification.

If you have selected an encryption profile with signing action in the message delivery rule that applies to the session, then FortiMail compares the sender's identity with the list of certificate bindings to determine if it has a certificate and **private key**. If there is a matching private key, it will add a digital signature using the algorithm specified in the encryption profile. If there is **not**, then FortiMail performs the failure action indicated in the encryption profile.

FortiMail does **not** check if an outgoing email is already encrypted. Email clients optionally can apply their own additional layer of S/MIME encryption (such as if they require non-repudiation) before they submit email for delivery through FortiMail.

The destination of an S/MIME email can be another FortiMail, for gateway-to-gateway S/MIME, but it could alternatively be any email gateway or server, as long as one of the following supports S/MIME and possesses the sender's certificate and public key, either the:

- destination's mail relay or mail server
- recipient's email client

This is necessary to decrypt the email; otherwise, the recipient cannot read the email.

Before any personal certificate that you upload will be valid for use, you must upload the certificate of its signing certificate authority (CA). For details, see Managing certificate authority certificates.

To view and configure certificate binding

1. Go to *Encryption* > *S/MIME* > *Certificate Binding*.

GUI item	Description
Profile ID	Displays the name of the profile.
Address Pattern	Displays the email address or domain associated with the identity represented by the personal or server certificate.
Key Usage	Displays if the key is for encryption, signing, or encryption and signing.
Identity	Displays the identity, often a first and last name, included in the common name (CN) field of the Subject line of the personal or server certificate.
Private Key	Displays the private key associated with the identity, used to decrypt and sign email from that identity.
Valid From	Displays the beginning date of the period of time during which the certificate and its keys are valid for use by signing and encryption.
Valid To	Displays the end date of the certificate's period of validity. After this date and time, the certificate expires, although the keys may be retained for the purpose of decrypting and reading email that was signed and encrypted previously.
Status	Indicates whether the certificate is currently not yet valid, valid, or expired, depending on the current system time and the certificate's validity period.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click a profile to modify it.
3. In *Address Pattern*, enter the email address or email domain that you want to use the certificate in this binding.

   For example, you might bind a personal certificate for `User1` to the email address, `user1@example.com`.
4. From Key type, select what kind of keys you want to upload. If you only have a public key, you can only use it to encrypt email. If you have a public key and private key pair, you can use them to encrypt email (with a public key), decrypt email (with a private key), or digitally sign email (with a private key).
5. Select one of the following ways to either import and bind a personal certificate, or to bind an existing server certificate:
   - *Import PKCS12 file*: Upload and bind a personal certificate-and-key file that uses the public key cryptography standard #12 (PKCS #12), stored in a password-protected file format (.p12).
   - *Import PEM files*: Upload and bind a pair of personal certificates and public and private keys that use privacy-enhanced email (PEM), a password-protected file format (.pem).
   - *Choose from local certificate list*: Bind a certificate that you have previously uploaded to the FortiMail unit. For details, see Managing local certificates on page 1.
6. Depending on your selection in *Import key from*, either upload the personal certificate files and enter their password, or select the name of a local certificate from *Select local certificate*list.

   If a certificate import does not succeed and event logging is enabled, to determine the cause of the failure, you can examine the event log messages. Log messages may indicate errors such as an unsupported password-based encryption (PBE) algorithm:

```
PKCS12 Import: err=0x6074079: digital envelope routines / EVP_PBE_CipherInit / unknown pbe
      algorithm
```

For best results, use 3DES with SHA1. RC2 is not supported.

7. Click *Create*.
   Certificate bindings will be used automatically as needed for matching message delivery rules in which you have selected an encryption profile. For details, see Using S/MIME encryption on page 271, Configuring encryption profiles on page 268, and Configuring delivery rules on page 156. It will also be used in the content profile and then in the policies which use the content profile.

See also

Configuring encryption profiles

Configuring data loss prevention

The FortiMail data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. After you define sensitive data patterns, you can take actions against the email containing data matching these patterns. You configure the DLP system by creating individual rules based on document fingerprint, file filters or sensitive information in a DLP profile and assign the profile to a policy.

This section describes how to configure the DLP settings.

DLP configuration workflow

DLP is designed for high-end platforms.

To use the DLP feature

1. Define the sensitive data. See Defining the sensitive data on page 332.
2. Define the DLP scan rules which specify the information to be checked in the email traffic. See Configuring DLP rules on page 334.
3. Define DLP profiles, which use one or more rules. See Configuring DLP profiles on page 334. You also specify the actions for the matched rules. These are the same action profiles you use in the content profiles. See Configuring content action profiles on page 224.
4. Apply the DLP profiles to the IP or recipient based policies. See Controlling email based on sender and recipient addresses on page 163 and Controlling email based on IP addresses on page 159.

Defining the sensitive data

Sensitive data can be any of the following types:

- **User-defined**: You specify what information should be checked, such as a word, a phrase, or a regular expression. See also Syntax on page 381.
- **Predefined**: For your convenience, FortiMail comes with a list of predefined information types, such as credit card numbers and SIN numbers. To view the predefined sensitive data, go to *Data Loss Prevention > Sensitive Data > Standard Compliance*.
- **Document fingerprints**: see DLP document fingerprinting on page 333.
- **File filters**: Also used in the content profiles. See Configuring file filters on page 222.

DLP document fingerprinting

One of the DLP techniques to detect sensitive data is fingerprinting (also called document fingerprinting). Most DLP techniques rely on you providing a characteristic of the file you want to detect, whether it's the file type, the file name, or part of the file contents. Fingerprinting is different in that you provide the file itself. The FortiMail unit then generates a checksum fingerprint and stores it. The FortiMail unit generates a fingerprint for all email attachments, and compares it to all of the fingerprints stored in its fingerprint database. If a match is found, the configured action is taken.

Currently, Microsoft Office, Open Office, PDF and text files can be detected by DLP fingerprinting and fingerprints can be saved for each revision of your files as they are updated.

The FortiMail unit must have access to the documents for which it generates fingerprints. There are two methods to generate fingerprints:

- One method is to manually upload documents to be fingerprinted directly to the FortiMail unit.
- (**Not available for FortiMail Cloud**) The other is to allow the FortiMail unit to access a network share that contains the documents to be fingerprinted.

If only a few documents are to be fingerprinted, a manual upload may be the easiest solution. If many documents require fingerprinting, or if the fingerprinted documents are frequently revised, using a network share makes user access easier to manage.

When you generate document fingerprints, only Microsoft Office, Open Office, PDF and text files with a minimum of 50 characters are supported.

To configure manual document fingerprints

1. Go to *Data Loss Prevention* > *Sensitive Data* > *Fingerprint*.
2. Click *New* and configure the following:

GUI item	Description
Name	Enter a descriptive name for the fingerprint.
Description	Optionally enter a description.
File list	Click *New* to browse to the file and generate a fingerprint for it. In the Fingerprint Status column, one of the following status will be displayed: • To be generated - The status when you've uploaded the file to the Fingerprint list before clicking the Create button. • Being generated: The status when the fingerprint generating process is executing. • Generated - The fingerprint has been generated. • Not generated - No fingerprint has been generated for the file because there is not enough text or the fingerprint is being generated • File type not supported - The file type is not supported to generated fingerprint.

See also

Configuring DLP rules

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring DLP rules

DLP scan rules specify what to look for in what part of the email. For example, you can specify to scan for some sensitive data in email bodies and attachments.

To configure DLP rules

1. Go to *Data Loss Prevention* > *Rule & Profile* > *Rule*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Name	Enter a descriptive name for the rule.
Description	Optionally enter a description.
Conditions	Select either Match all conditions or Match any condition. Click *New* to add conditions. Depending on what email part you select, you can specify different conditions.
Exceptions	Click *New* to add exceptions. Email matching the exceptions will not be scanned.

Configuring DLP profiles

After you configure the scan rules or conditions, you add them to the DLP profiles. In the profiles, you also specify what actions to take (for details about action profiles, see Configuring content action profiles on page 224). Then you apply the DLP profiles to the IP or recipient based policies.

To configure a DLP profile

1. Go to *Data Loss Prevention* > *Rule & Profile* > *Profile*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Name	Enter a name for the profile.
Action	Select a default action to use when the specified scan rules match the email. Click *New* to create a new action profile. See Configuring content action profiles on page 224.
Comment	Optional. Enter a comment.
Content Scan Setting	Click *New* to configure the following settings: • Enabled: check this box to enable the settings. • Scan rule: select a scan rule from the dropdown list. Or click *New* to create a new rule. • Action: select an action profile from the dropdown list. Or click New to create a new profile. If no action profile is selected, the default one will be used.

Logs, reports, and alerts

FortiMail units provide extensive logging capabilities for virus incidents, spam incidents and system events. Detailed log information and reports provide analysis of network activity to help you identify security issues and reduce network misuse and abuse.

Logs are useful when diagnosing problems or when you want to track actions the FortiMail unit performs as it receives and processes traffic.

This section includes:

About FortiMail logging

FortiMail units can log many different email activities and traffic including:

- system-related events, such as system restarts and HA activity
- virus detections
- spam filtering results
- POP3, SMTP, IMAP and webmail events

You can select which severity level an activity or event must meet in order to be recorded in the logs. For more information, see Log message severity levels on page 339.

A FortiMail unit can save log messages to its hard disk or a remote location, such as a Syslog server or a Fortinet FortiAnalyzer unit. For more information, see Configuring logging on page 343. It can also use log messages as the basis for reports. For more information, see Configuring report profiles and generating reports on page 346.

Accessing FortiMail log messages

There are several ways you can access FortiMail log messages:

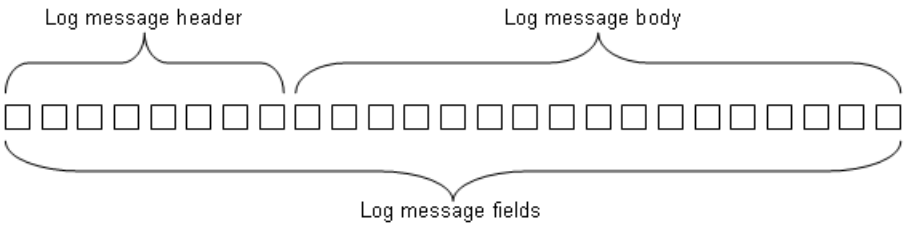
- On the FortiMail GUI, you can view log messages by going to *Monitor* > *Log*. From here you can download log messages to your computer by clicking *Export* and view them later.
- Go to *Log & Report* > *Log Setting* > *Remote* and add a FortiAnalyzer unit as a remote host in order to send log messages to FortiAnalyzer. You can send log messages to any Syslog server from here.

Log message syntax

All FortiMail log messages are comprised of a log header and a log body.

- **Header** — Contains the time and date the log originated, a log identifier, the type of log, the severity level (priority) and where the log message originated.
- **Body** — Describes the reason why the log was created, plus any actions that the FortiMail appliance took to respond to it. **These fields may vary by log type.**

Log message header and body



For example, in the following event log, the bold section is the header and the italic section is the body.

```
date=2012-08-17 time=12:26:41 device_id=FE100C3909600504 log_id=0001001623 type=kevent subtype=admin
      pri=information user=admin ui=GUI(172.20.120.26) action=login status=success reason=none
      msg="User admin login successfully from GUI(172.20.120.26)"
```

Device ID field

Depending on where you view log messages, log formats may vary slightly. For example, if you view logs on the FortiMail GUI or download them to your computer, the log messages do not contain the device ID field. If you send the logs to FortiAnalyzer or other Syslog servers, the device ID field will be added.

Policy ID and domain fields

FortiMail 5.0 added two new fields -- policy ID and domain -- to history logs.

The policy ID is in the format of x:y:z, where:

- x is the ID of the global access control policy.
- y is the ID of the IP-based policy.
- z is the ID of the recipient-based policy.

If the value of x, y, and z is 0, it means that no policy is matched.

If the matched recipient-based policy is incoming, the protected domain will be logged in the domain field.

If the matched recipient-based policy is outgoing, the domain field will be empty.

Endpoint field

FortiMail 4.0 MR3 added a field called `endpoint` to the history and antispam logs. This field displays the endpoint's subscriber ID, MSISDN, login ID, or other identifiers. This field is empty if the sender IP is not matched to any endpoint identifier or if the endpoint reputation is not enabled in the session profiles.

Log_part field

In FortiMail 3.0 MR3 and newer, the log header of some log messages may include an extra field, `log_part`, which provides numbered identification (such as 00, 01, and 02) when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length was reduced.

Hex numbers in history logs

If you view the log messages on the FortiMail GUI or send the logs to a Syslog server, the dispositions and classifiers are described. However, if you download log files from FortiMail GUI to your computer and open them, the dispositions and classifiers are displayed in hex numbers. For explanation of these numbers, see the Classifiers and dispositions in history logs on page 340.

See also

FortiMail log types

Configuring logging

Log message severity levels

Viewing log messages

Viewing reports

FortiMail log types

FortiMail units can record the following types of log messages. Event logs also include several subtypes. You can view and download these logs from the Log submenu of the Monitor tab.

Log types

Log Types	Default File Name	Description
History (statistics)	alog	Records all email traffic going through the FortiMail unit (SMTP relay or proxy).
System Event (kevent)	klog	Records system management activities, including changes to the system configuration as well as administrator and user log in and log outs.
Mail Event (event)	elog	Records webmail, SMTP, POP3, and IMAP events.
Antispam (spam)	slog	Records spam detection events.
Antivirus (virus)	vlog	Records virus detection events.
Encryption (encrypt)	nlog	Records detection of IBE-related events. See also.Configuring encryption profiles on page 268.

Email related logs contain a session identification (ID) number, which is located in the session ID field of the log message. The session ID corresponds to all the relevant log types so that the administrator can get all the information about the event or activity that occurred on their network.

For more information about these specific log types, see the FortiMail Log Reference.

Avoid recording highly frequent log types to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

See also

Log message severity levels

Viewing log messages

Configuring logging

About FortiMail logging

Subtypes

FortiMail logs are grouped into categories by log type and subtype as shown in the table below:

Log Type	Subtype
kevent	admin config config-user dns ha system update
event	imap pop3 smtp webmail
virus	infected malware-outbreak file-signature
spam	default admin user
statistics	(no subtype)
encrypt	(no subtype)

Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `pri=warning`.

Log severity levels

Levels (0 is highest)	Name	Description
0	Emergency	The system has become unstable
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notice	Information about normal events.
6	Information	General information about system operation.

For each location where the FortiMail unit can store log files, you can define the severity threshold of the log messages to be stored there.

Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

The FortiMail system stores all log messages equal to or exceeding the severity level you select. However, the relevant information level logs are always stored for any other level log selection. For example, if you select Error, the FortiMail system stores log messages whose severity level is Error, Critical, Alert, or Emergency. And the relevant information level logs are also stored.

Classifiers and dispositions in history logs

Each history log contains one field called Classifier and another called Disposition.

The Classifier field displays which FortiMail scanner applies to the email message. For example, “Banned Word” means the email messages was detected by the FortiMail banned word scanner. The Disposition field specifies the action taken by the FortiMail unit.

If you view the log messages on the FortiMail GUI or send the logs to a Syslog server, the dispositions and classifiers are displayed in English terms. However, if you download log files from FortiMail GUI to your computer and open them, the dispositions and classifiers are displayed in hex numbers.

The following tables map the hex numbers for classifiers with their description.

Classifiers

Hex Number	Classifier	Hex Number	Classifier
0x00	Undefined	0x2A	Message Cryptography
0x01	User Safe	0x2B	Delivery Control
0x02	User Discard	0x2C	Encrypted Content
0x03	System Safe	0x2D	SPF Failure as Spam
0x04	System Discard	0x2E	Fragmented Email
0x05	RBL	0x2F	Email Contains Image
0x06	SURBL	0x30	Content Requires Encryption
0x07	FortiGuard AntiSpam	0x31	FortiGuard AntiSpam Block IP
0x08	FortiGuard AntiSpam-Safe	0x32	Session Remote
0x09	Bayesian	0x33	FortiGuard Phishing
0x0A	Heuristic	0x34	AntiVirus
0x0B	Dictionary Scanner	0x35	Sender Address Rate Control
0x0C	Banned Word	0x36	SMTP Auth Failure
0x0D	Deep Header	0x37	Access Control List Reject
0x0E	Forged IP (before v5.2 release)	0x38	Access Control List Discard
0x0F	Quarantine Control	0x39	Access Control List Bypass
0x10	Tagged virus (before v4.3 release)	0x3A	FortiGuard Antispam Webfilter
0x11	Attachment Filter (see note above)	0x3B	Newsletter Suspicious
0x12	Grey List	0x3C	TLS Streaming
0x13	Bypass Scan On Auth	0x3D	Policy Match
0x14	Disclaimer	0x3E	Dynamic Safe List
0x15	Defer Delivery	0x3F	Sender Verification
0x16	Session Domain	0x40	Behavior Analysis
0x17	Session Limits	0x41	FortiGuard Spam Outbreak
0x18	Session Safe	0x42	Newsletter
0x19	Session Block	0x43	DMARC
0x1A	Content Monitor and Filter	0x44	File Signature
0x1B	Content Monitor as Spam	0x45	Sandbox
0x1C	Attachment as Spam	0x46	Malware Outbreak
0x1D	Image Spam	0x47	DLP Filter
0x1E	Sender Reputation	0x48	DLP Treated as Spam

Hex Number	Classifier	Hex Number	Classifier
0x1F	Access Control List Relay Denied	0x49	DLP Requires Encryption
0x20	Safelist Word	0x4A	Access Control List Safe
0x21	Domain Safe	0x4B	Virus Outbreak
0x22	Domain Block	0x4C	FortiGuard Antispam Webfilter
0x23	SPF (not in use)	0x4D	Impersonation Analysis
0x24	Domain Key (not in use)	0x4E	Session Action
0x25	DKIM (not in use)	0x4F	SPF Sender Alignment
0x26	Recipient Verification	0x50	SPF Check
0x27	Bounce Verification	0x51	Sandbox URL
0x28	Endpoint Reputation	0x52	Sandbox No Result
0x29	SSL Profile Check	0x53	Content Modification
		0x54	DKIM Failure

When the classifier is “Attachment Filter”, a new field “atype” (attachment type) is also displayed. This field is for debug purpose only.

Dispositions

Hex number	Disposition	Hex Number	Disposition
0x00	Undefined	0x10000	Encryption
0x01	Accept the message	0x20000	Decryption
0x02	Move to a specified folder	0x40000	Deliver the message to an alternate host
0x04	Send a reject to the SMTP client	0x80000	Deliver the message to a set of recipients
0x08	Add a header to the message	0x100000	Archive the message
0x10	Modify the subject line	0x200000	Encase the original message with customizable text
0x20	Quarantine the message	0x400000	Wrap the original message
0x40	Insert disclaimer content	0x800000	Notification
0x80	Block the message	0x1000000	Sign the message using SMIME/CMS
0x100	Replace banned attachments	0x2000000	Defer the message disposition
0x200	Delay and greylist the message	0x4000000	Convert HTML attachment to text

Hex number	Disposition	Hex Number	Disposition
0x400	Forward the message to a review account	0x8000000	Remove active HTML content
0x800	Added a disclaimer to the body	0x10000000	Remove URLs from processed HTML attachments
0x1000	Added a disclaimer to the headers	0x20000000	Deliver to original host
0x2000	Defer message delivery	0x40000000	Content Disarm and Reconstruction
0x4000	Quarantine for review	0x80000000	URL Click Protection
0x8000	Treat as spam	0x100000000	Domain quarantine

The disposition field in a log message may contain one or more dispositions or actions. For example, “Accept” and “Defer” dispositions may appear in the same message. Defer disposition is added when an email message is deferred for either of the following two reasons: FortiGuard antispam outbreak and FortiSandbox scan.

The "Accept" disposition is logged when any other actions are not taken.

See also

FortiMail log types

Viewing log messages

Configuring logging

About FortiMail logging

Configuring logging

The *Log Setting* sub menu allows you to:

- Set the severity level
- Configure which types of log messages to record
- Specify where to store the logs

You can configure the FortiMail Cloud to store log messages to the FortiAnalyzer Cloud (license required).

If you need remote logging, please contact Fortinet Support.

Logging to FortiAnalyzer Cloud

If you have the FortiAnalyzer Cloud Storage Subscription license, you can log to the cloud service. In addition to the following procedures, you must configure FortiAnalyzer Cloud to accept FortiMail logs. For information about how to configure FortiAnalyzer Cloud, see the FortiAnalyzer Cloud Deployment Guide.

Logs stored remotely cannot be viewed from the GUI of the FortiMail unit. If you require the ability to view logs from the GUI, also enable local storage. For details, see Configuring logging on page 343.

Before you can log to a remote location, you must first enable logging. For logging accuracy, you should also verify that the FortiMail unit's system time is accurate. For details, see Configuring system time on page 71.

To configure logging to FortiAnalyzer Cloud

1. Go to to *Dashboard* > *Status*.
2. Under *License Information*, for FortiCloud, click *Activate*.
3. Enter your FortiCare license information.
4. Go to *Log & Report* > *Log Setting* > *FortiAnalyzer Cloud*.
5. Enable the status and click *Apply*. If FortiMail has the correct license registered with FortiCare, then a connection is established with FortiAnalyzer Cloud. You can also use the *Test connection* button to test and troubleshoot network connections.
6. From *Log level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.

   For information about severity levels, see Log message severity levels on page 339.
7. In *Logging Policy Configuration*, enable the types of logs you want to record to this storage location.
8. Click *Apply*.

See also

Log message severity levels

Configuring logging

Configuring logging

Downloading log files

You can download log files to your management computer. Downloading log files can be useful if you want to view log messages on your management computer, or if you want to download a backup copy of log files to another location before deleting them from the FortiMail unit's hard disk.

To download a log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as *History*.
3. Select the row(s) corresponding to the log file(s) that you want to download and click *Export* > *Export Selected*. You can select multiple non-contiguous rows by holding Ctrl while selecting the log files.

The log file downloads in comma-separated value (CSV) format with a file extension of `.csv`. You can view this format in a spreadsheet application such as Microsoft Excel.

4. If your web browser prompts you for the location to save the file, browse to select or enter the name of the folder.

To download all log files

1. Go to *Monitor* > *Log*.
2. Click a log type tab.
3. Click *Export* > *Export All*.
   The log file downloads in comma-separated value (CSV) format with a file extension of `.csv`.
4. If your web browser prompts you for the location to save the file, browse to select or enter the name of the folder.

See also

Configuring logging

Viewing log messages

Deleting rotated log files

You can delete rotated (also called "rolled") log files. This can be useful if you want to free disk space used by old log files to make disk space available for newer log files.

Back up the current log file before deleting a log file. When deleting a log file, log messages are permanently removed, and cannot be recovered. For instructions on how to download a backup copy of a log file, see Downloading log files on page 344.

To delete a rolled log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as *History*.
3. In the *Action* column, in the row corresponding to the log file that you want to delete, click *Delete*.
   A confirmation dialog appears.
4. Click *Delete*.

To delete multiple rolled log files

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as *History*.
3. If you want to delete selected log files, mark the checkbox in each row corresponding to a log file that you want to delete.
4. If you want to delete all rolled log files, mark the checkbox in the column heading for the column that contains checkboxes. This automatically marks all other checkboxes.
5. Click *Delete Selected Items*.
   A dialog appears.
6. Click *OK*.

See also

Configuring report profiles and generating reports

A report profile is a group of settings with the report name, subject, schedule, and other information that the FortiMail unit uses when it generates reports. The reports show the information in tabular and graphical format.

Statistics in the reports are generated from log data. Log retention must allow enough time for the report to be generated before the log file is deleted. See Configuring logging on page 343.

Configuring domain-level mail statistics reports

If you have the feature license for it, you can generate reports that focus on email processing for each protected domain.

To configure the report profile

1. Purchase the feature license and enable the feature. See Domain mail statistics on page 1.
   By default, its corresponding areas of the GUI are hidden and disabled.
2. Go to *Log & Report* > *Report Setting* > *Domain Mail Statistics*.
3. To enable the report, select *Generate report*.
4. If the report should include statistics about all protected domains, enable *All domains*.
   Otherwise disable it. Text areas appear. In *Available domains*, select the names of protected domains, and then click >> to move it to *Selected domains*.
5. In *Schedule*, select the how frequently the FortiMail unit will generate the report. Also configure *At hour* with the time of day when the report will be generated, and, if you selected a weekly report, which days of the week.
   Time periods included in the report are everything in the schedule interval.

   Generating reports can be resource intensive. To avoid slower email processing, you may want to schedule reports to generate them during times with low traffic volume, such as at night.

6. Click *Apply*.
7. If you want to generate a report immediately (on demand; the report is also generated later, according to the schedule), click *Generate Now*. (This button is not available if *Generate report* is disabled.)
   Otherwise you can wait for the schedule to trigger the report, and then view it. See Viewing reports on page 65.

Configuring system-level mail statistics reports

To configure the report profile

1. Go to *Log & Report* > *Report Setting* > *Mail Statistics*.

GUI item	Description
Generate (button)	Select a report profile and then click this button to generate a report immediately, on demand. See Viewing reports on page 65.
Report Name	Displays the name of the report profile.
Recipient Domain	Displays the name of the recipient domain.
Sender Domain	Displays the name of the sender domain.
Schedule	Displays the frequency with which the FortiMail unit generates a scheduled report. If the report is generated on demand, *Not Scheduled* appears in this column.

2. Click *New* to add a profile, or double-click a profile to modify it.
3. Configure the following settings:

GUI item	Description
Report name	Enter a name for the report. Do not include spaces.
Comment	Optional. Enter a description or comment.
Time period	Select the time range of log messages from which to generate the report.

4. Expand and configure the following sections:
   - Query Selection on page 347.
   - Schedule on page 348.
   - Recipient Domain and Sender Domain on page 349.
   - Conditions on page 349.
   - Email Notification on page 349
5. Click *Create* or *OK*.

Query Selection

When configuring a report profile, you can select one or more queries or query groups that define the subject matter of the report.

Each query group contains multiple individual queries, each of which correspond to a chart that will appear in the generated report. You can select all queries within the group by marking the check box of the query group, or you can expand the query group and individually select each query to include.

For example:

- If you want the report to include charts about spam, select both the *Spam by Sender* and *Spam by Recipient* query groups.
- If you want the report to specifically include only a chart about top virus senders by date, expand the query group *Virus by Sender* and select only the individual query *Top Virus Sender By Date*.

GUI item	Description
Mail Filtering Statistics	Select to include high-level categories, such as mail, spam, non-spam, and virus.
Mail High Level	Select to include all top level and summary information for all queries, such as *Top Client IP By Date*.
Mail Statistics	Select to include information on daily, hourly or weekly email message statistics, such as *Mail Stat Messages By Day*.
Mail by Recipient	Select to include information on email messages by each recipient, such as *Top Recipient By Date*.
Mail by Sender	Select to include information on email messages by each sender, such as *Top Sender By Date*.
Spam by Recipient	Select to include information on spam by each recipient, such as *Top Spam Recipient By Date*.
Spam by Sender	Select to include information on spam by each sender, such as *Top Spam Sender By Date*.
Statistics	Select to include information on generalized email message statistics (less granular than *Mail Statistics*).
Total Summary	Select to include summary information, such as *Total Sent And Received*.
Virus by Sender	Select to include information on infected email messages by each sender, such as *Top Virus Sender By Date*.
Virus by Recipient	Select to include information on infected email messages by each recipient, such as *Top Virus Recipient By Date*.

Schedule

When configuring a report profile, you can select when the report will generate. Alternatively, you can leave it unscheduled.

Generating reports can be resource intensive. To avoid slower email processing, you may want to schedule reports to generate them during times with low traffic volume, such as at night. Alternatively, you can generate them on demand, only when necessary.

Expand the *Schedule* section, then in the *Schedule* dropdown, select either:

GUI item	Description
Not Scheduled	Select if you do **not** want the FortiMail unit to generate the report automatically according to a schedule. The report is only generated when you manually click Generate to generate it on demand.
Daily	Select to generate the report each day. Also configure *At hour*.

GUI item	Description
These days	Select to generate the report on specific days of each week, then select those days. Also configure *At hour*.
These dates	Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. For example, to generate a report on the 1st and 30th day of every month, enter `1,30`. Also configure *At hour*.

Recipient Domain and Sender Domain

When configuring a report profile, you must specify at least one protected domain that is in recipient and/or sender email addresses. The log messages that match those protected domains are used when generating the report.

1. Expand the *Recipient Domain* and/or *Sender Domain* sections.
2. Disable *All domains*.
   Options appear to select specific protected domains.
3. In the *Available domains* area, select one or more protected domains that you want to include in the report, and then click *>>* to move them to the *Selected domains* area.
   Optionally, in *External domain*, you can also enter a domain name that is **not** a protected domain, and then click *>>* to move it to *Selected domains*.
   To remove a domain from a report, select it in the *Selected domains* area, and then click *<<*.

Conditions

When configuring a report profile, you can choose to report only on logged email messages that match adirectionality: incoming, outgoing, or both.

1. Expand the *Conditions* section.
2. In *Direction*, select the direction of email relative to protected domains: either *Incoming*, *Outgoing*, or *All*.
3. In *Destination*, select how you want to define the destination address of the email: either *User Defined* or *IP Group*. Then select the name of an IP group, or enter the IP address and network mask.

Email Notification

When configuring a report profile, you can have the FortiMail unit email an attached copy of the generated report, in either HTML or PDF file format, to designated recipients.

1. Expand the *Email Notification* section.
2. In *Report format*, select the file format of the attachment for the generated report, either *html* or *pdf*.
3. In the *Email address* field, enter an email address that will receive the report, and then click *>>* to add it to the list of recipients in *All notification Email address*.
   To remove a recipient address, select it and click *<<*.

Configuring mailbox statistics reports

The FortiMail unit can generate reports on the total number of active mailboxes during a particular time period, as specified in the report profile creation. Mailbox statistic reports can be configured based on schedule, domain, and email address notification. After configuration, to view historical active mailbox counts over the last 30 days and 12 months, go to *FortiView* > *Mail Statistics* > *Active Mailbox*.

Alternatively, you can use the dashboard to get the current number of active mailboxes and a list of their usernames. See Active mailbox user list on page 30.

To configure the report profile

1. Purchase the feature license and enable the feature. See Mailbox accounting service on page 1. (If you have FortiMail Cloud, this feature is already included and enabled.)

   By default, the corresponding areas of the GUI are hidden and disabled.
2. Go to *Log & Report* > *Report Setting* > *Mailbox Statistics*.

GUI item	Description
Generate (button)	Select a report profile, and then click this button to generate a report immediately, on demand. See Viewing reports on page 65.
Report Name	Displays the name of the report profiles.
Domain	Displays the protected domain name(s).
Schedule	Displays the frequency with which the FortiMail unit generates a scheduled report. If the report is designed for manual generation, *Not Scheduled* appears in this column.

3. Click *New* to add a profile or double-click a profile to modify it.
4. Configure the following settings:

GUI item	Description
Report name	Enter a name for the report. Do not include spaces.
Time period	Select the time range of log messages from which to generate the report.
Include mailbox list	Enable this option to include information about the active mailboxes for each protected domain and the last time that email was delivered to them.

5. Expand and configure the following sections:
   - Schedule on page 350
   - Domain on page 351
   - Email Notification on page 351
6. Click *Create* or *OK*.

Schedule

When configuring a report profile, you can select when the report will generate. Alternatively, you can leave it unscheduled.

Generating reports can be resource intensive. To avoid slower email processing, you may want to schedule reports to generate them during times with low traffic volume, such as at night. Alternatively, you can generate them on demand, only when necessary.

Expand the *Schedule* section, then in the *Schedule* dropdown, select either:

GUI item	Description
Not Scheduled	Select if you do **not** want the FortiMail unit to generate the report automatically according to a schedule. The report is only generated when you manually click Generate to generate it on demand.
Daily	Select to generate the report each day. Also configure *At hour*.
Weekly	Select to generate the report on specific days of each week, then select those days. Also configure *At hour*.
Monthly	Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. For example, to generate a report on the 1st and 30th day of every month, enter `1,30`. Also configure *At hour*.

Domain

When configuring a report profile, you must specify at least one protected domain whose log messages are used when generating the report.

1. Expand the *Domain* section.
2. Disable *All domains*.
   Options appear to select specific protected domains.
3. In the *Available domains* area, select one or more protected domains that you want to include in the report, and then click >> to move them to the *Selected domains* area.
   To remove a domain from a report, select it in the *Selected domains* area, and then click <<.

Email Notification

When configuring a report profile, you can have the FortiMail unit email an attached copy of the generated report to designated recipients.

1. Expand the *Email Notification* section.
2. In the *Email address* field, enter an email address that will receive the report, and then click >> to add it to the list of recipients in *All notification Email address*.
   To remove a recipient address, select it and click <<.

Microsoft 365, Exchange and Google Workspace threat remediation

Microsoft 365, Exchange (EWS) and Google Workspace email messages can now be scanned in real-time, whereby email is scanned immediately after the email arrives in the user's mailbox.

You can also conduct on-demand search and scan of email messages already delivered to the user's inbox. Once scanned, you can decide what to do with the infected or spam email. You can also manually apply actions directly to the email messages you specify.

Microsoft 365, Exchange, and Google Workspace protection features are license based. If you have not purchased the required licenses, this feature does not display on the GUI.

The real-time scan feature requires the following:

- FortiMail must have a valid CA-signed certificate; and the Common Name (CN) or Subject Alternative Name (SAN) of the certificate must match your FortiMail hostname.
- FortiMail must be reachable by hostname (not IP address).
- Set the base URL to receive notification to your FortiMail hostname and ensure that the hostname is resolvable to your FortiMail's public IP address via public DNS servers so that Microsoft 365/Exchange/Google Workspace can reach your FortiMail for Webhook notifications. For details, see Configuring scanning policies on page 356.

Microsoft Exchange 2013 or above is required for full EWS API support.

You can switch to Microsoft 365 and Google API View in the FortiMail Cloud portal. For details, see FortiMail Cloud Portal Guide.

Microsoft 365, Exchange, and Google Workspace protection workflow

To use this feature, do the following:

1. Connect to Microsoft 365/Exchange or Google Workspace by creating an account on FortiMail with the Microsoft 365/Exchange or Google Workspace domain administrator's credentials. See Configuring

accounts on page 353.

2. Create antivirus, antispam, content, DLP, and action profiles to be used to scan the email. See Configuring profiles on page 359.
3. Conduct real-time scans or scheduled scans and searches for email according to your criteria. See Configuring scanning policies on page 356.
4. View the history, antivirus, and antispam logs. See Monitoring log messages on page 360.
5. View and generate mail statistic reports in FortiView, based on mail count, size, scan and transfer speed, and notification delay and by received notifications. See Microsoft 365 and Google Workspace notification statistics.

See also

Configuring accounts on page 353

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring accounts

Before you can scan email in Microsoft 365/Exchange or Google Workspace mailboxes, you must connect to a respective server.

- Adding a Microsoft 365 account in FortiMail requires your Tenant ID, Application ID, and Application Secret.
- Adding a Microsoft Exchange account in FortiMail requires your service URL, service account and password.
- Adding a Google Workspace account in FortiMail requires an email address designated for the administrator, and the account's JSON content.

To create a Microsoft 365 account

On the MS365 side:

When acquiring the Tenant ID and Application ID from Microsoft 365, you must also grant consent permissions for the admin.

Add the following permissions for the administrator in Microsoft 365:

- User.Read.All
- Mail.ReadWrite
- Mail.Send
- Directory.Read.All

By default, *User.Read* is added.

On the FortiMail side:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *System* > *Account* > *Account*.
3. Click *New*.

4. Leave *Status* enabled.
5. Set *Type* to *Microsoft 365*.
6. Enter the *Tenant ID*, *Application ID*, and the *Application Secret*. You receive log on credentials when you create the custom application on Microsoft Azure. For details, see the Azure documentation.
7. Select a regional *Service Endpoint* appropriate to your geographical location.
8. Enable *Real-time Scan* if you wish to conduct real-time scanning of emails that match certain criteria specified in a real-time scan policy. For more information, see Enabling and configuring real-time scanning on page 357.
9. Optionally, click *New* under *User Filter Setting* to configure user filter settings. Enable *Status*, select the appropriate user *Type*, and specify additional options depending upon the filter type selected, then click *Create*.

FortiMail supports the importation of Azure AD user group memberships, which can subsequently be applied to domain level recipient policies.

To use this feature, select *Azure AD Group* from the *Type* dropdown when configuring *User Filter Settings*.

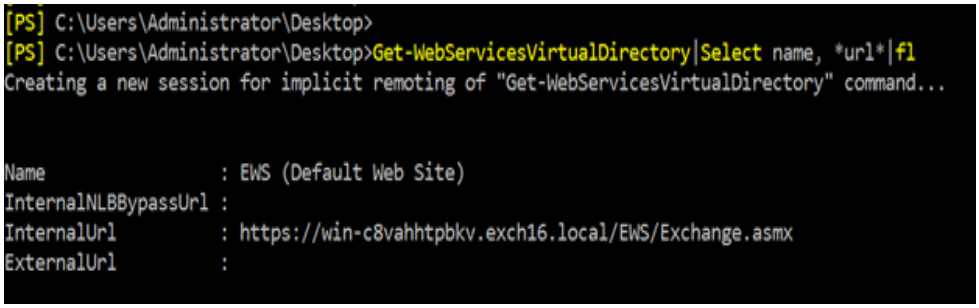
This feature is currently only available when configuring Microsoft 365 accounts.

10. When finished configuring the account, click *Create*.

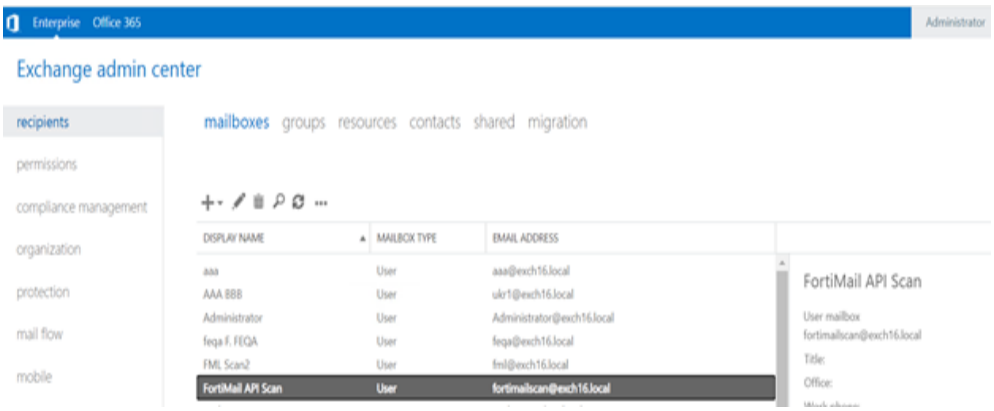
To create a Microsoft Exchange account

On the Microsoft Exchange Server side:

1. Go to the Exchange management shell and run the following command:
   `Get-WebServicesVirtualDirectory|Select name, *url*|fl`



2. Take note of the internal URL. You'll need to enter it on the FortiMail side. And make sure the URL is reachable by FortiMail via HTTPs.
3. Go to Exchange admin center > recipients > mailboxes, click "+" and create a new mailbox as the service account.



4. Go to the Exchange management shell and enter the following command to set the “Application Impersonation” role for the service account:
   `New-ManagementRoleAssignment -Name:FortiMailScan -Role:ApplicationImpersonation -User:service@domain`
   Where “service@domain” is the service account mailbox created in the previous step.
5. Go to Exchange admin center > permissions > admin roles, and edit “Discovery Management”. Add “Mailbox Search” to its roles and add the service account to its members.
6. Go to the Exchange management shell, and run the following command:
   `Get-GlobalAddressList|fl name,guid`
7. Take note of the default global address list (Guid). You’ll need to enter it on the FortiMail side.

On the FortiMail side:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *System* > *Account* > *Account*.
3. Click *New*.
4. Set *Type* to *Microsoft Exchange*.
5. Enter the Exchange Server's service URL, service account, password and global address list.
6. Enable *Real-time Scan* if you wish to conduct real-time scanning of emails that match certain criteria specified in a real-time scan policy. For more information, see Enabling and configuring real-time scanning on page 357.
7. Optionally, click *New* under *User Filter Setting* to configure user filter settings. Enable *Status*, select the appropriate user *Type*, and specify additional options depending upon the filter type selected, then click *Create*.

To create a Google Workspace account

On the Google Cloud side:

1. Log in to the Google Cloud console as the Workspace admin.
2. From the *Project* dropdown list, click *New Project*. Enter a new project name, then switch to the new project.
3. Go to *APIs & Services*.
4. Click *Enable APIs and Services*, search and enable *Admin SDK API*, *Gmail API*, and *Cloud Pub/Sub API*.
5. Go to *APIs & Services* > *OAuth Consent*, select *Internal* and then select *Create*. Enter the name and contact email. Save and continue.
6. Add the following scopes, then save and continue:

```
https://mail.google.com
https://www.googleapis.com/auth/admin.directory.user.readonly
https://www.googleapis.com/auth/admin.directory.domain.readonly
https://www.googleapis.com/auth/pubsub
```

7. Go to *APIs & Services* > *Credentials*. Click *Create Credentials*. Select *Service Account*, and enter the name, click *Create and Continue*, and then *Done*.
8. Go to *IAM & Admin* > *Service Accounts*. Click on the default account in the list. Go to *Keys*tab. Click *Add Key*, *Create New Key*, *JSON*, and *Create*. Store the JSON file securely.
9. Go to *Details* of the new account, and expand *Advanced Settings*. Copy the client ID.
10. Click *View Google Workspace Admin Console*, and log in as super admin.
11. Go to *Security* > *Access and Data Control* > *API Controls*. *Click Manage Domain Wide Delegation*, and then *Add New*. Enter the copied client ID and the above scopes.
12. Click *Authorize*.

On the FortiMail side:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *System* > *Account* > *Account*.
3. Click *New*.
4. Leave *Status* enabled.
5. Set *Type* to *Google Workspace*.
6. Enter the *Admin email* and the *JSON content*. You receive JSON credentials when you create the custom application on Google Workspace. For details, see the Google documentation.
7. Enable *Real-time Scan* if you wish to conduct real-time scanning of emails that match certain criteria specified in a real-time scan policy. For more information, see Enabling and configuring real-time scanning on page 357.
8. Optionally, click *New* under *User Filter Setting* to configure user filter settings. Enable *Status*, select the appropriate user *Type*, and specify additional options depending upon the filter type selected, then click *Create*.
9. When finished configuring the account, click *Create*. If successful, your account will appear in the account list, showing FortiMail connected to Microsoft 365/Exchange or Google Workspace.
10. Click *View User List* to view the following email user information under the selected account:
    - *Status*: Displays whether the user is subscribed or not.
    - *Email*: User names of the email users on the Microsoft 365/Exchange or Google Workspace account.
    - *Expiry Date*: Subscription expiry date and time to notifications of the user's real-time email.

Configuring scanning policies

After you connect to Microsoft 365/Exchange or Google Workspace and create profiles, you can scan certain email according to the criteria you specify. These can be real-time scans, or on-demand scheduled scans and searches.

Enabling and configuring real-time scanning

Real-time scanning allows you to apply security profiles and their actions to only those emails that match certain criteria specified in a real-time scan policy. These criteria are based on source, sender, and recipient information.

Before you can configure real-time scan policies, you must first enable the feature, and define the base URL for the FortiMail unit to receive notifications from Microsoft 365/Exchange or Google Workspace. For prerequisites of the FortiMail base URL and host name, see Microsoft 365, Exchange and Google Workspace threat remediation on page 352.

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *Policy* > *Real-time Scan* > *Setting*.
3. Select *Enable*.
4. Verify the *Base URL to receive notification* field, which is based on the local host and domain name of the FortiMail unit. To define this URL:
   a. Go to *View* > *Advanced View*.
   b. Go to *System* > *Mail Setting* > *Mail Server Settings*.
   c. Under *Local Host*, enter the *Host name* and *Local domain name* of the FortiMail system, and click *Apply*.
5. Select an appropriate Service endpoint from the dropdown menu, depending on your geographic location.
6. Determine whether you want to *Log* all email, or only those emails that match a policy.

To configure a real-time scan policy:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *Policy* > *Real-time Scan* > *Policy*.
3. Click *New* and configure the following:

GUI item	Description
Status	Select or clear to enable or disable the policy.
Comment	Enter a comment if necessary.
Account	Select a Microsoft 365/Exchange or Google Workspace account.
Source	Select either **IP/Netmask**, **IP Group**, or **GeoIP Group**, and enter the appropriate source information.
Sender	Define the sender type, and enter the type's settings as required.
Recipient	Define the recipient type, and enter the type's settings as required.
Profiles	Select profile(s) to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profiles.

Hide email on arrival (Microsoft 365 only)

With real-time scanning, there is still a small risk that users may open dangerous emails in Microsoft 365 before the FortiMail unit can finish scanning the email, especially if the email contains large attachments. To mitigate this risk, you can enable a feature that automatically moves email to a hidden folder on arrival for it to be

subjected to real-time scanning. After the email is scanned and deemed safe, it is then removed from the hidden folder and put into the user's mailbox.

This feature (disabled by default) can only be enabled using the *CLI Console*.

To enable this feature, open the *CLI Console* and enter the following:

```
config cloud-api setting
   set hide-email-on-arrival enable
end
```

Release system quarantine email (Microsoft 365 only)

You can enable a feature that automatically stores FortiMail system quarantined email, both original and modified copies, in Microsoft 365. All the tenant, user, and message GUIDs are stored in the FortiMail system quarantine. After the email is scanned and deemed safe, it is then released and redelivered to the user.

This feature (enabled by default) can only be enabled using the *CLI Console*.

To enable this feature, open the *CLI Console* and enter the following:

```
config cloud-api setting
   set system-quarantine-release-original enable
end
```

Configuring scheduled scan

In addition to automatic scanning, you can also search for specific email on Microsoft 365 or Google Workspace and manual apply actions.

To scan email on demand for Microsoft 365/Exchange or Google Workspace:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *Policy* > *Scheduled Scan & Search* > *Scan*.
3. Click *New* and configure the following:

GUI item	Description
Description	Enter a descriptive name.
Account	Select to scan **All** accounts, or specify specific accounts to scan.
Sender	Select the sender type, and enter the type's settings as required.
Recipient	Select the recipient type, and enter the type's settings as required.

GUI item	Description
Schedule	Specify a scheduled time and email start and end time range.
Profiles	Select profile(s) to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profiles.
Condition	Specify the search criteria.

4. If *Schedule* is set to *Now*, click *Scan*. If *Schedule* is set to *Later*, *Daily*, or *Weekly*, click *OK*.
5. The scanning status of all the scan tasks will be displayed: either Running, Done, Scheduled, or Stopped.
6. After the scan process is done, you can double click on the scan task to view the details.

Configuring scheduled search

To search for email and take manual actions:

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *Policy* > *Scheduled Scan & Search* > *Search*.
3. Click *New* and configure the following:

GUI item	Description
Description	Enter a descriptive name.
Account	Select to search **All** accounts, or specify specific accounts to search.
Sender	Select the sender type, and enter the type's settings as required.
Recipient	Select the recipient type, and enter the type's settings as required.
Schedule	Specify a scheduled time and email start and end time range.
Search Action	Select an action profile to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profile.
Condition	Specify the search criteria.

4. If *Schedule* is set to *Now*, click *Scan*. If *Schedule* is set to *Later*, *Daily*, or *Weekly*, click *OK*.
5. The search status of all the search tasks will be displayed: either Running, Done, Scheduled, or Stopped.
6. After the search process is done, you can double click on the search task to view the details.
7. To take any action towards a specific email (if the search task has not already applied an action), from the search result list, select the email and select the action from the *Apply Action* dropdown list. For action definitions, see Configuring action profiles on page 360.

Configuring profiles

Before you can scan the email on Microsoft 365/Exchange or Google Workspace, you must configure the antivirus, antispam, content, DLP, and action profiles to use.

The antivirus, antispam, content, and DLP profile configurations are almost identical to the regular profile configurations, except for some settings that do not apply to this situation. For details about these profiles, see:

- Configuring antivirus profiles
- Configuring antispam profiles
- Configuring content profiles
- Configuring DLP profiles

Configuring action profiles

When you scan email on Microsoft 365/Exchange or Google Workspace, you can apply action profiles towards the infected email. Note that since you are applying actions on Microsoft 365/Exchange or Google Workspace, the action definitions are different from the actions performed on FortiMail itself.

To configure an action profile

1. Go to *View* > *Microsoft & Google API View*.
2. Go to *Profile* > *Action* > *Action*.
3. Click *New* and configure the following:

GUI item	Description
Profile name	Enter a name for the action profile.
Replace attachment with message	Select to replace the email attachment that triggers a scanner (such as the content and antivirus attachment filters) with a custom message. For more information about custom replacement message, see Configuring custom messages on page 71.
Notify with profile	Select to send out notifications to the recipients specified in the notification profile. For more information about notification profiles, see Configuring notification profiles on page 274.
Action	Specify one of the following final actions: • ***None***: No action will be taken. • ***Discard***: Delete the email message from the user's inbox on Microsoft 365/Exchange or Google Workspace. • ***Personal quarantine***: Move the email message from the user's inbox to the junk folder on Microsoft 365/Exchange, or to the spam folder on Google Workspace. • ***System quarantine***:Move the email message to FortiMail system quarantine. If desired, the user needs to contact the FortiMail system administrator to release the quarantined email. • ***Move to folder***: Move the email message from the user's inbox to a specified folder on Microsoft 365/Exchange, or Google Workspace.

Monitoring log messages

The *Monitor* > *Log* submenu includes the following tabs, one for each log type:

- *History*: Where you can view the log of scanned and searched email messages.
- *Mail Event*: Where you can view the log of all and/or SMTP mail events.
- *AntiVirus*: Where you can view the log of email messages detected as infected by a virus.
- *AntiSpam*: Where you can view the log of email messages detected as spam.
- Log Search Task: Where you can create and view a log of search tasks.

The log lists are sorted by the time range of the log messages contained in the log file, with the most recent log files appearing near the top of the list.

For example, the current log file would appear at the top of the list, above a rolled log file whose time might range from `2008-05-08 11:59:36 Thu` to `2008-05-29 10:44:02 Thu`.

For more information about how to use FortiMail logs, see Viewing log messages on page 35.

Troubleshooting

This section provides guidelines to help you determine why your FortiMail unit is behaving unexpectedly. It includes general troubleshooting methods and specific troubleshooting tips using both the command line interface (CLI) and the GUI. Each troubleshooting item describes both the problem and the solution.

Some CLI commands provide troubleshooting information not available through the GUI. The GUI is better suited for viewing large amounts of information on screen, reading logs and archives, and viewing status through the dashboard.

For additional information, see Best practices and fine tuning.

Troubleshoot antispam issues

Problem

The spam detection rate is low.

Solution

- Confirm that no SMTP traffic is bypassing the FortiMail unit due to an incorrect routing policy. Configure routers and firewalls to direct all SMTP traffic to or through the FortiMail unit to be scanned. If the FortiMail unit is operating in gateway mode, for each protected domain, modify public DNS records to keep only a single MX record entry that points to the FortiMail unit.
- **Use safe lists and block lists with caution.** They can increase incorrect results.

  For example, a system-level safe list entry for `*.edu` email addresses allows email from all `.edu` top level domains. Sender email addresses in the SMTP envelope (`MAIL FROM:`) and message header (`From:`) can be fake, too. The result is that all spam from any `.edu` email address — real or fake — would bypass antispam scans.

  Better approaches are to either use client IP addresses (which are harder to fake) in access control policies or to use DKIM or SPF sender authentication (which is stronger and widely supported).

  Do not safelist protected domain names. Sender email addresses can be faked, so they may not really belong to the protected domain. This could allow spammers to bypass antispam scans.
- Verify that all protected domains have matching policies and proper protection profiles.
- Consider enabling adaptive antispam features such as greylisting and sender reputation.

Enable additional antispam features gradually, and do not enable additional antispam features after you have achieved a satisfactory spam detection rate. Excessive antispam scans can unnecessarily decrease the performance of the FortiMail unit.

Problem

Email users are spammed by DSN for email they did not actually send.

Solution

Spammers may sometimes use the delivery status notification (DSN) mechanism to bypass antispam measures. In this attack, sometimes called “backscatter”, the spammer spoofs the email address of a legitimate sender and intentionally sends spam to an undeliverable recipient, expecting that the recipient’s email server will send a DSN back to the sender to notify him/her of the delivery failure. Because this attack utilizes innocent email servers and a standard notification mechanism, many antispam mechanisms may be unable to detect the difference between legitimate and spoofed DSN.

To detect backscatter

1. Enable bounce address tagging and configure an active key (see Configuring bounce verification and tagging on page 308).
2. Next, disable both the *Bypass bounce verification* option (see Configuring protected domains on page 92) and the *Bypass bounce verification check* option (see Configuring session profiles on page 171).
3. In addition, verify that all outgoing and incoming email passes through the FortiMail unit. The FortiMail unit cannot tag email, or recognize legitimate DSN for previously sent email, if all email does not pass through it. For details, see Configuring bounce verification and tagging on page 308.

Problem

Email users cannot release and delete quarantined messages by email.

Solution

Two common reasons are:

- The domain name portion of the recipient email address (for example, fortimail.example.com in release-ctrl@fortimail.example.com) could not be resolved by the DNS server into the FortiMail unit's IP address.
- The sender’s email address in the release message was not the same as the intended recipient of the email that was quarantined. If you have configured your mail client to handle multiple email accounts, verify that the release/delete message is being sent by the email address corresponding to that per-recipient quarantine. For example, if an email for user@example.com is quarantined, to release that email, you must send a release message from user@example.com.

Problem

Attachments less than the 10 MB configured limit are not deliverable

Solution

The message limit is a total maximum for the entire transmitted email: the message body, message headers, all attachments, and encoding, which in some cases can expand the size of the email. For example, depending on the encoding and the content of the email, an email with an 8 MB attachment could easily exceed the transmitted message size limit of 10 MB.

Therefore, attachments should be significantly smaller than the configured limit.

Problem

The exported email archive is an empty file.

Solution

Make sure you select the check boxes of archived email (see Configuring email archiving accounts on page 1) that you want to export. Only email whose *Status* column contains a check mark will be exported.

Problem

Event log messages show DNSBL query errors.

Solution

Log messages such as:

```
RblServer::check 20.4.90.202.zen.spamhaus.org error=2 : 'Host name lookup failure'
```

could mean that the query is being refused because it exceeds pre-defined service limitations by the DNSBL service provider. If you have very high volumes of email traffic, consider providing a DNSBL server on your local network by synchronizing the DNSBL database to it. For details, consult your service provider.

Problem

Antispam quarantine reports are delayed.

Solution

In most cases, this is caused by an excessive number of quarantine accounts.

When an email is accepted for a recipient and identified as spam, a quarantine account is automatically created in FortiMail.

Check that these quarantine accounts are valid, as netbots and spam harvest scans can cause the creation of a large number of false accounts.

There are options to manage quarantine accounts in FortiMail. These options are available under *Domain & User > Domain > Domain* (not in server mode).

- Enable *Recipient Address Verification* to stop invalid account creation with SMTP or LDAP authentication (Note that LDAP cache should be enabled).
- Remove invalid accounts by enabling *Automatic Removal of Invalid Quarantine Accounts*.

Recipient validation is a clean solution with a performance cost on SMTP or LDAP services. Its another disadvantage is that it also results in informing the outside whether the accounts are valid or not.

The automatic clearance of accounts is started once per day at 4:00 AM by default, but can be modified by the following CLI command:

```
config antispam settings
   set backend-verify <hh:mm:ss>
end
```

where `hh` is the hour according to a 24-hour clock, `mm` is the minute, and `ss` is the second.

Contact Fortinet customer support for assistance

After you define your problem, researched a solution, created a plan, and executed that plan, and if you have not solved the problem, it is time to contact Fortinet customer support for assistance.

To receive technical support and service updates, your Fortinet product must be registered. Registration, support programs, assistance, and regional phone contacts are available at the following URL:

https://support.fortinet.com/

When you are registered and ready to contact support:

1. Prepare the following information first:
   - your contact information
   - the configuration file
   - access to recent log files
   - a network topology diagram and IP addresses
   - a list of troubleshooting steps performed so far and the results
2. Document the problem and the steps you took to define the problem.
3. Open a support ticket.

Setup for email users

This section contains information that you may need to inform or assist your email users so that they can use FortiMail features.

This information is **not** the same as what is included in the help for FortiMail webmail. It is included in the Administration Guide because:

- Email users may require some setup **before** they can access the help for FortiMail webmail.
- Some information may be too technical for some email users.
- Email users may not be aware that their email has been scanned by a FortiMail unit, much less where to get documentation for it.
- Email users may not know which operation mode you have configured.
- Email users may be confused if they try to access a feature, but you have not enabled it (such as Bayesian scanning or their personal quarantine).
- You may need to tailor some information to your network or email users.

Training Bayesian databases

Bayesian scanning can be used by antispam profiles to filter email for spam. In order to be accurate, the Bayesian databases that are at the core of this scan must be trained. This is especially important when the databases are empty.

Be aware that, without ongoing training, Bayesian scanning will become significantly less effective over time and thus Fortinet does not recommend enabling the Bayesian scanning feature.

Administrators can provide initial training. For details, see Training the Bayesian databases on page 316. If you have enabled it (see Configuring the Bayesian training control accounts on page 322 and Accept training messages from user on page 199),email users can also contribute to training the Bayesian databases.

To help to improve the accuracy of the database, email users selectively forward email to the FortiMail unit. These email are used as models of what is or is not spam. When it has seen enough examples to become more accurate at catching spam, a Bayesian database is said to be well-trained.

For example, if the local domain is example.com, and the Bayesian control email addresses are the default ones, an administrator might provide the following instructions to his or her email users.

To train your Bayesian filters

1. Initially, forward a sample set of spam and non-spam messages.
   - If you have collected **spam**, such as in a junk mail folder, and want to train your personal antispam filters, forward them to `learn-is-spam@example.com` from your email account. Similar email will be recognized as spam.
   - If you have collected **non-spam** email, such as your inbox or archives, and want to train your personal spam filters, forward them to `learn-is-not-spam@example.com` from your email account. Similar email will be recognized as legitimate email.

2. On an ongoing basis, to fine-tune your antispam filters, forward any corrections — spam that was mistaken for legitimate email, or email that was mistaken for spam.
   - Forward undetected spam to `is-spam@example.com` from your email account.
   - Forward legitimate email that was mistaken for spam to `is-not-spam@example.com` from your email account.
   - If you belong to an alias and receive spam that was sent to the alias address, forward it to `is-spam@example.com` to train the alias's database. Remember to enter the alias, instead of your own email address, in the `From:` field.

   This helps your antispam filters to properly distinguish similar email/spam in the future.

Managing tagged spam

Instead of detaining an email in the system or personal quarantine, the administrator can configure the FortiMail unit to tag the subject line or header of an email that is detected as spam. For details, see Configuring antispam profiles and actions on page 187.

Once spam is tagged, the administrator notifies email users of the text that comprises the tag. Email users can then set up a rule-based folder in their email clients to automatically collect the spam based on tags.

For example, if spam subject lines are tagged with "SPAM", email users can make a spam folder in their email client, then make filter rules in their email clients to redirect all email with this tag from their inbox into the spam folder.

Methods to create mailbox folders and filter rules vary by email client. For instructions, see your email client's documentation.

Accessing the personal quarantine and webmail

Each email user has a personal quarantine, also known as the *Bulk* mailbox folder. If you selected that action in the antispam action profiles, spam for an email user is redirected to their personal quarantine.

Email users should monitor their personal quarantines to ensure that legitimate email is not accidentally quarantined. To do this, you can enable quarantine reports (see Configuring global quarantine report settings on page 285, Configuring protected domains on page 92, and Using quarantine reports on page 369). You can also enable email users to view their *Bulk* folder through FortiMail webmail.

In addition to personal quarantine access, in server mode, FortiMail webmail also provides access to the *Inbox*, address book, and other features.

Available access methods vary by the operation mode of the FortiMail unit:

- Accessing personal quarantines through FortiMail webmail (gateway and transparent mode)
- Accessing FortiMail webmail (server mode)
- Accessing mailboxes through POP3 or IMAPv4 (server mode)

Email users cannot access their personal quarantines through POP3 or IMAP.

Accessing personal quarantines through FortiMail webmail (gateway and transparent mode)

To allow email users to access *Bulk* folders through FortiMail webmail, the administrator must:

- create an authentication profile that allows users to authenticate
- configure an incoming recipient-based policy that matches the email user's address, where webmail access to the quarantine is enabled, and the authentication profile is selected

For details, see Controlling email based on sender and recipient addresses on page 163 and Configuring authentication profiles on page 231.

Once this is configured, the administrator informs email users of the FortiMail webmail URL. When they log in, email users will immediately see their *Bulk* folders (unlike server mode, in gateway mode or transparent mode, this is the only mailbox folder).

For additional instructions related to their personal quarantine, email users can click the *Help* button in FortiMail webmail.

Accessing FortiMail webmail (server mode)

Unlike gateway mode and transparent mode, server mode does not require that the administrator create an authentication profile. However, he or she must still configure an incoming recipient-based policy that matches the email user's address, where webmail access to the quarantine is enabled through a resource profile.

Once this is configured, the administrator informs email users of the FortiMail webmail URL. When they log in, email users will immediately see their mailbox folders, including their *Inbox*, in addition to their *Bulk* folder.

For additional instructions related to their personal quarantine, email users can click the *Help* button in FortiMail webmail.

Accessing mailboxes through POP3 or IMAPv4 (server mode)

To allow email users to access their *Inbox*, *Bulk*, and other folders through an email client, the administrator must configure an incoming recipient-based policy that matches the email user's address, where POP3/IMAPv4 access to the quarantine is enabled.

Once this is configured, the administrator tells email users about the IP address and POP3/IMAPv4 port number of the FortiMail unit (see also Appendix: Port Numbers on page 375), which they will use when configuring their

email client to connect. After their email client is connected, email users will see their mailbox folders, including their *Inbox* and *Bulk*.

If tagged spam (see Configuring antispam profiles and actions on page 187) appears in their *Inbox*, email users can use their email client's filtering rules to redirect spam email to their *Bulk* folder or other folder.

Methods vary by the email client. For details, see the email client's documentation.

Using quarantine reports

If an administrator has enabled:

- quarantine reports to email users (see Configuring global quarantine report settings on page 285)
- the quarantine control email addresses (see Configuring the quarantine control options on page 293)

When email is added to their personal quarantine, email users will periodically receive an email similar to one of the samples below.

Email users can follow the instructions in the quarantine report to release or delete email from their personal quarantine. Quarantine reports can be used from with FortiMail webmail, or from an email client with POP3 access.

Example: Quarantine report (HTML)

The following sample report in HTML format informs the email user about how many messages are in quarantine, and explains how to delete one or all quarantined messages, and how to release an individual email. Email users can make decisions to release or delete an email based on a message's subject and sender information contained in the body of the report.

Sample quarantine report in HTML format

Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00]
From: release-ctrl@example.com
Date: 12:00 PM
To: user1@example.com

Date:	From:	Subject:	Web Actions:	Email Actions:
Thu, 04 Sep 2008 11:52:51	User 1 <user1@example.com>	[SPAM] information leak	Release Delete	Release Delete
Thu, 04 Sep 2008 11:51:10	User 1 <user1@example.com>	[SPAM] curious?	Release Delete	Release Delete
Thu, 04 Sep 2008 11:48:50	User 1 <user1@example.com>	[SPAM] Buy now!!!! lowest prices	Release Delete	Release Delete

Web Actions:
Click on **Release** link to send a http(s) request to have the message sent to your inbox.
Click on **Delete** link to send a http(s) request to delete the message from your quarantine.
Click Here to send a http(s) request to **Delete all messages** from your quarantine.

Email Actions:
Click on **Release** link to send an email to have the message sent to your inbox.
Click on **Delete** link to send an email to delete the message from your qurantine.
Click here to send an email to **Delete all messages** from your quarantine.

Other:
To view your entire quarantine inbox or manage your preferences, Click Here

Example: Quarantine report (plain text)

The following sample report in plain text format informs email users about how many messages are in quarantine, and explains how to delete one or all quarantined messages, and how to release an individual email. Email users can make decisions to release or delete an email based on a message's subject and sender information contained in the body of the report.

Note that email users cannot access their personal quarantines through POP3 or IMAP.

Sample quarantine report in plain text format

```
To: user1@example.com
      From: release-ctrl@fm3.example.com
      Subject: Quarantine Summary: [3 message(s) quarantined from Wed, 11 Jul 2007 11:00:01 to Wed,
      11 Jul 2007 12:00:01]
      Date: Wed, 11 Jul 2007 12:00:01 -0400
Date: Wed, 11 Jul 2007 11:11:25
      Subject: Sign up for FREE offers!!!
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166681.l6BFAj510009380000@fm3.example.com
Date: Wed, 11 Jul 2007 11:14:16
      Subject: Buy cheap stuff!
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166854.l6BFDchG0009440000@fm3.example.com
Date: Wed, 11 Jul 2007 11:15:46
      Subject: Why pay more?
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166944.l6BFF7HI0009460000@fm3.example.com
Actions:
o) Release a message:
      Send an email to <release-ctrl@fm3.example.com> with subject line set to
      "user1@example.com:Message-Id".
o) Delete a message:
      Send an email to <delete-ctrl@fm3.example.com> with subject line set to
      "user1@example.com:Message-Id".
o) Delete all messages:
      Send an email to <delete-ctrl@fm3.example.com> with subject line set to "delete_
      all:user1@example.com:ea809095:ac146004:05737c7c111d68d0111d68d0111d68d0".
```

Sending email from an email client (gateway and transparent mode)

To enable email users to send email through the FortiMail unit using an email client, the administrator must:

- Create an access control rule that permits valid email clients to connect. For details, see Configuring access control receiving policies on page 148.
- Create an authentication profile to authenticate the users. For details, see Configuring authentication profiles on page 231.
- Enable SMTP authentication in the incoming recipient-based policy. For details, see Controlling email based on sender and recipient addresses on page 163.

The email user must configure their email client with:

- outgoing SMTP email server that is either the FortiMail unit (gateway mode) or the protected SMTP server (transparent mode)
- enabled SMTP authentication
- user name and password (provided by the administrator; these credentials must mast the ones retrieved by the authentication profile)
- authentication that includes the domain name, such as `user1@example.com` instead of `user1`

Appendix: Supported RFCs

SMTP RFCs

- **RFC 1213 (Obsoletes: 1158)** (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)
- **RFC 1918 (Obsoletes: 1627, 1597)** (Address Allocation for Private Internets)
- **RFC 1985** (SMTP Service Extension for Remote Message Queue Starting)
- **RFC 2034** (SMTP Service Extension for Returning Enhanced Error Codes)
- **RFC 2045 (Obsoletes: 1590, 1522, 1521, 1342, 1341)** (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)
- **RFC 2505** (Anti-Spam Recommendations for SMTP MTAs)
- **RFC 2634** (Enhanced Security Services for S/MIME)
- **RFC 2920 (Obsoletes: 2197, 1854)** (SMTP Service Extension for Command Pipelining)
- **RFC 3207 (Obsoletes: 2487)** (SMTP Service Extension for Secure SMTP over TLS)
- **RFC 3461 (Obsoletes: 1891)** (SMTP Service Extension for Delivery Status Notifications (DSNs))
- **RFC 3463 (Obsoletes: 1893)** (Enhanced Mail System Status Codes)
- **RFC 3464 (Obsoletes: 1894)** (Extensible Message Format for Delivery Status Notifications)
- **RFC 3635 (Obsoletes: 2665, 2358, 1650)** (Definitions of Managed Objects for the Ethernet-like Interface Types)
- **RFC 4954 (Obsoletes: 2554)** (SMTP Service Extension for Authentication)
- **RFC 5321 (Obsoletes: 2821, 1869, 1651, 1425, 974, 821)** (SMTP)
- **RFC 5322 (Obsoletes: 2822, 822)** (Internet Message Format)
- **RFC 5751 (Obsoletes: 3851** (Secure/Multipurpose Internet Mail Extension (S/MIME) Version 3.2)
- **RFC 6376 (Obsoletes: 5672, 4871, 4870)** (DomainKeys Identified Mail (DKIM) Signatures)
- **RFC 6522 (Obsoletes: 3462, 1892)** (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages)
- **RFC 6409 (Obsoletes: 4409, 2476)** (Message Submission)
- **RFC 7208 (Obsoletes: 4408)** (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail)

This RFC is partially supported. Macros and EXISTS modifiers are currently treated as neutral.

IMAP RFCs

- **RFC 2088** (IMAP4 Non-synchronizing Literals)
- **RFC 2177** (IMAP4 Idle Command)
- **RFC 2221** (Login Referrals)
- **RFC 2342** (IMAP4 Namespace)
- **RFC 2683** (IMAP4 Implementation Recommendations)
- **RFC 2971** (IMAP4 ID Extension)
- **RFC 3348** (IMAP4 Child Mailbox Extension)
- **RFC 3501 (Obsoletes: 2060, 1730)** (IMAP4 rev1)
- **RFC 3502** (IMAP Multiappend Extension)
- **RFC 3516** (IMAP4 Binary Content Extension)
- **RFC 3691** (Unselect Command)
- **RFC 4315 (Obsoletes: 2359)** (UIDPLUS Extension)
- **RFC 4469** (Catenate Extension)
- **RFC 4731** (Extension to SEARCH Command for Controlling What Kind of Information Is Returned)
- **RFC 4959** (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response)
- **RFC 5032** (WITHIN Search Extension)
- **RFC 5161** (Enable Extension)
- **RFC 5182** (Extension for Referencing the Last SEARCH Result)
- **RFC 5255** (IMAP Internationalization)
- **RFC 5256** (Sort and Thread Extensions)
- **RFC 5258 (Obsoletes: 3348)** (List Command Extensions)
- **RFC 5267** (Contexts for IMAP4)
- **RFC 5819** (Extension for Returning STATUS Information in Extended LIST)
- **RFC 6154** (LIST Extension for Special-Use Mailboxes)
- **RFC 6851** (MOVE extension)
- **RFC 7162 (Obsoletes: 5162, 4551)** (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC))

POP3 RFCs

- **RFC 1939 (Obsoletes: 1725, 1460, 1225, 1081)** (POP3)
- **RFC 2449** (POP3 Extension Mechanism)

Other RFCs

- **RFC 1155 (Obsoletes: 1065)** (Structure and Identification of Management Information for TCP/IP-based Interface)
- **RFC 1157 (Obsoletes: 1098, 1067)** (SNMP v1)
- **RFC 1213 (Obsoletes: 1158)** (MIB 2)
- **RFC 2047** (MIME (Multipurpose Internet Mail Extensions) Part Three:Message Header Extensions for Non-ASCII Text)
- **RFC 2578 (Obsoletes: 1902, 1442)** (Structure of Management Information Version 2)
- **RFC 2579 (Obsoletes: 1903, 1443)** (Textual Conventions for SMIv2)
- **RFC 2595** (Using TLS with IMAP, POP3 and ACAP)
- **RFC 3410 (Obsoletes: 2570)** (SNMP v3)
- **RFC 3416 (Obsoletes: 1905, 1448)** (SNMP v2)

Appendix: Port Numbers

Firewalls (if any) between FortiMail and other devices may need to open the following inbound (listening) and outbound ports in order to communicate with other devices. Required port numbers vary by which features you enable.

Default port numbers are listed. Many are configurable. See the links in each row of:

- Incoming (listening) port numbers on page 375
- Outgoing port numbers on page 377

In its factory default configuration, FortiMail does not accept packets on any port except port1 and port2 network interfaces, which only accept:

- ICMP ping
- HTTPS connections on TCP/443 to the administrative GUI
- SSH connections on TCP/22 to the CLI

Incoming (listening) port numbers

FortiMail features listen for communications from other devices on these ports.

If port forwarding is enabled, then the FortiMail unit listens on more port numbers that are not associated with FortiMail features, but instead are forwarded to other devices on the network. See Configuring port forwarding on page 1. If traffic capture is enabled, then the FortiMail unit listens on port numbers that are specified by the filter. See Traffic capture on page 89.

Default Port Number	IP Protocol	Source IP address	Purpose
80	TCP	• Administrators • Email users	• Administrative GUI (HTTP) • Quarantine access • Webmail (server mode only)
443	TCP		• Administrative GUI (HTTPS) • REST API • Quarantine access • Webmail (server mode only)
22	TCP	• Administrators • FortiManager	• Administrative CLI (SSH) • Configuration and firmware push
23	TCP	• Administrators	• Administrative CLI (Telnet)

Default Port Number	IP Protocol	Source IP address	Purpose
161	UDP	• FortiManager	SNMPquery
25	TCP	• Email servers, relays • Email users	• Email relay/proxy/server (SMTP) • Spam sample submission by email users
465	TCP		• Email relay/proxy/server (SMTPS) • Spam sample submission by email users
587	TCP	• Email users	Email sending (SMTP for email users to send email separately from relays/servers)
143	TCP		• Email (IMAP; server mode only) • Email archive access
993	TCP		• Email (IMAPS; server mode only) • Email archive access
110	TCP		• Email (POP3; server mode only) • Quarantine access
995	TCP		Email (POP3S; server mode only)
443	TCP	• FortiMail **Note:** All HA ports must be open between heartbeat interfaces: • primary to secondary units • secondary to secondary units	HA centralized monitoring
6688	TCP		HA centralized monitoring
20000	UDP and TCP		HA heartbeat signal (base port)
20001	UDP and TCP		HA synchronization control
20002	TCP		HA file synchronization
20003	TCP		HA data synchronization
20004	TCP		HA checksum synchronization
20005	UDP and TCP		HA cluster join request
20010-20014	UDP and TCP		HA group mode
25	TCP		HA service monitoring (SMTP)
80	TCP		HA service monitoring (HTTP)
110	TCP		HA service monitoring (POP3)
143	TCP		HA service monitoring (IMAP)
443	TCP	• FortiGate	Security Fabric (HTTPS management)

Outgoing port numbers

FortiMail communicates to these port numbers on other servers and devices.

Default Port Number	IP Protocol	Destination IP Address	Purpose
443	TCP	• Directory server	Authentication (HTTPS SAML SSO)
389	TCP and UDP		Authentication (LDAP)
636	TCP		Authentication (LDAPS)
1812	TCP		Authentication (RADIUS)
143	TCP	• Email server	Authentication (IMAP)
993	TCP		Authentication (IMAPS)
110	TCP		Authentication (POP3)
995	TCP		Authentication (POP3S)
25	TCP		• Authentication (SMTP) • Email delivery to protected domains (SMTP) • Recipient address verification • Delivery failure notifications (DSN) • Alert email
465	TCP		• Authentication (SMTPS) • Email delivery to protected domains (SMTPS) • Recipient address verification • Delivery failure notifications (DSN) • Alert email
21	TCP	• Network attached storage or file share server	Backup of configuration (FTP)
22	TCP		Backup of configuration (SFTP/SSH)
22	TCP		Backup of mailboxes (SFTP/SSH)
445	TCP and UDP		Backup of mailboxes (SMB/CIFS)
3260	TCP		Backup of mailboxes (iSCSI)
2049	TCP and UDP		Backup of mailboxes (NFS)
2049	TCP and UDP		External storage for mailboxes and quarantine (NFS)
3260	TCP		External storage for mailboxes and quarantine (iSCSI)
443 or 8890	TCP	• Fortinet	• FortiGuard Antivirus engine and virus signature updates (see also Required URLs for FortiGuard services on page 379)

Default Port Number	IP Protocol	Destination IP Address	Purpose
			• License validation
53 or 8888	UDP or TCP		FortiGuard Antispam rating query
53	UDP	• DNSBL server	Third-party DNSBL/RBL spam rating query
53	UDP	• SURBL server	Third-party SURBL URL rating query
53	UDP	• DNS server	• Domain name resolution (DNS) • Record queries such as MX and DKIM
123	UDP	• Fortinet • Time server	Time synchronization (NTP)
443	TCP	• FortiMail **Note:** All HA ports must be open between heartbeat interfaces: • primary to secondary units • secondary to secondary units	HA centralized monitoring
6688	TCP		HA centralized monitoring
20000	UDP and TCP		HA heartbeat signal (base port)
20001	UDP and TCP		HA synchronization control
20002	TCP		HA file synchronization
20003	TCP		HA data synchronization
20004	TCP		HA checksum synchronization
2005	UDP and TCP		HA cluster join request
20010-20014	UDP and TCP		HA group mode
25	TCP		HA service monitoring (SMTP)
80	TCP		HA service monitoring (HTTP)
110	TCP		HA service monitoring (POP3)
143	TCP		HA service monitoring (IMAP)
514	TCP		Centralized quarantine (clear text)
6514	TCP		Centralized quarantine (secure)
8013	TCP	• FortiGate	• Security Fabric (HTTPS to upstream) • FortiView
443	TCP	• FortiNDR	File scan
514	TCP	• FortiSandbox	• File scan (OFTPS) • URL scan (HTTPS) **Note:** Proxies are not currently supported.
443	TCP	• FortiManager	Registration, configuration backup/pull, and firmware pull
162	UDP		Event traps (SNMP)

Default Port Number	IP Protocol	Destination IP Address	Purpose
514	UDP and TCP	• FortiAnalyzer • Syslog	Logging
80 or 443	TCP	• Dynamic DNS servers	Dynamic DNS (HTTP or HTTPS)
80 and 443	TCP	• Web servers	Resolution of URL redirects (for example, tiny URLs) into the target URL
80, or port number in OCSP certificate	TCP	• Directory or PKI servers	Certificate revokation query

Required URLs for FortiGuard services

Firewalls and web filters between the FortiMail unit and the Internet must allow requests to the following URLS, which are used by FortiMail features that connect to Fortinet's FortiGuard services:

- update.fortiguard.net
- securewf.fortiguard.net (global) or ussecurewf.fortiguard.net (United States only)
- service.fortiguard.net (global) or usservice.fortiguard.net (United States only)

Appendix: Wildcards and regular expressions

Some FortiMail features support the use of wildcard characters (* or ?) or Perl-style regular expressions in order to create patterns that match multiple IP addresses, email addresses, or other data.

For detailed information on using regular expressions, see:

http://perldoc.perl.org/perlretut.html

Special characters with regular expressions and wildcards

Wildcard patterns are written slightly differently than regular expressions.

A wildcard character is a special character that matches one or more other characters. Wildcard patterns use an:

- asterisk (*), which matches zero or more of any characters
- question mark (?), which matches any one character

In regular expressions, instead of ?, use a period (.).

For example, the regular expression `example.com` matches `example.com`, but also `exampleacom`, `examplebcom`, `examplecom`, etc.

In regular expressions, instead of *, use `.*`. An asterisk (*) matches only the **exact** character before it 0 or more times, not 0 or more times of **any** character. Therefore to achieve the same match as the wildcard pattern, you must use `.*`.

For example, the regular expression `example*.com` matches `exampleeeeee.com`, but does **not** match `example.com`. This is different from a simple wildcard pattern, which would match both. To fix this so that the regular expression matches the same text as a wildcard pattern, the regular expression should be `exampl.*\.com`.

Special characters are usually interpreted as a pattern, but you can also match them literally. To match `.` or *, prefix it with the escape character, backslash (`\`) . For example, to match `example.com`, use the regular expression `example\.com`. For a list of other special characters, see Syntax on page 381.

Case sensitivity

By default, regular expression pattern matching in FortiMail is ***not case sensitive***. For example, `bad language` matches `bad language`, `Bad LAnguaGe`, etc.Therefore, the regular expression `/i`, which is used to make a word or phrase case insensitive in other products, should not be used in the FortiMail configuration.

If you need to enable case sensitive matching, then prefix the regular expression with `(?-i)`.

For example, `(?-i)abc` will match string `abc` with case sensitivity so that `ABC` or `Abc` will not match it.

Modifiers

FortiMail supports the following match operator modifiers (also called options or flags). Options are put after the delimiter. For details, see Syntax on page 381.

Regular Expression Option	Description
`m`	Treat the string as multiple lines in the format `/<string>/m`.
`s`	Treat the string as a single line.
`x`	Ignore the white spaces in the expression in the format `/a b c/x` so that it matches `abc`.

Word boundary

In Perl-style regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression `test` matches the whole word `test` but also any word that contains those characters, such as `attest`, `mytest`, `testimony`, `atestb`, etc.

Use the notation `\b` to specify where a word must start or end. To match exactly and only the whole word `test`, for example, the regular expression should be `\btest\b`. See also Syntax on page 381.

Syntax

Regular expressions on FortiMail units use Perl-style syntax. The following table lists some example regular expression syntax, and describes strings that match and do not match.

Regular Expression	Matches and Non-Matches
`abc`	`abc` anywhere in the string.
`^abc`	`abc` at the beginning of the string.
`abc$`	`abc` at the end of the string.
`a|b`	Either `a` or `b`.
`^abc|abc$`	`abc` at either the beginning or the end of the string, but **not** in the middle.
`ab{2,4}c`	`a` followed by two, three, or four `b` and then `c`.
`ab{2,}c`	`a` followed by at least two `b` and then `c`.
`a.*c`	`a` followed by zero or more characters of any type, and then `c`.
`ab+c`	`a` followed by one or more `b` and then `c`.
`ab?c`	`a` followed by an optional `b` and then `c`. That is, either `abc` or `ac`.
`a.c`	`a` followed by any one character (but **not** newline) and then `c`.
`a\.c`	`a.c`  Backslash is an escape character.You can use it to match any character such as `*` or `.` literally, not interpret it as a wildcard operator in pattern syntax.
`[abc]`	Either `a`, `b`, or `c`.
`(?-i)Abc`	`Abc` but **not** `abc`. (Case insensitivity is disabled.)
`[a-z]`	Any single uppercase or lowercase letter in the English language alphabet, but **not** numbers or special characters.
`[abc]+`	Any combination of one or more `a`, `b`, and/or `c` characters, such as `a`, `abba`, or `acbabcacaa`.
`[^abc]+`	Any combination of one or more characters that does **not** contain an `a`, `b`, and/or `c`, such as `defg`.
`\d\d`	Any two decimal digits, such as `42`. Same as `\d{2}`.
`[[:alnum:]]*`	Alphanumeric characters, zero or more, in any combination.
`\w+`	A word (a non-empty sequence of alphanumeric characters and underscores), such as `foo`, `bar8`, or `baz_1`.
`100\s*mk`	`100` and `mk` separated by zero or more white space characters (spaces, tabs, newlines).
`abc\b`	`abc` followed by a word boundary, such as `abc!` but **not** `abcd`.
`start\B`	`start` when **not** followed by a word boundary, such as `starting` but **not** `start time`.
`\x{2709}`	The character or emoji `2709` (an envelope icon), defined by its Unicode hexadecimal character number.
`/a b c/x`	`abc` anywhere in the string.

Regular Expression	Matches and Non-Matches
	 Delimiters can be used to add regular expressions within other text. Delimiters surround the regular expression. The first character (in this example, `/`) is used as the delimiter. Between the first and second delimiter is the regular expression pattern. Leading and trailing space, if any, is treated as part of the regular expression. If the second `/` is missing, an error occurs. Anything after the second `/` are options. In this example, the option `x` ignores white space between the letters in the pattern `a b c`.

Example regular expressions

Depending on where you want to match in an email or SMTP session, you may need to add syntax to the following patterns in order to match a whole line, or only at the start and/or end of text. For example, to compare the pattern to an entire line: `^pattern$`

Email addresses

Email address user names are often a mix of letters, numbers, and possibly periods (`.`).

```
[[:alnum:].]*@example\.com
```

Alternative words in a phrase

```
/word1|word2|word3/
```

Purposefully misspelled words

Spammers often insert other characters between the letters of a word to avoid detection by antispam software, or replace characters with similar-looking numbers, punctuation, or characters in another language.

```
.*v.*i.*a.*g.*r.*
```

```
cr[eéèêë3]*dit [sS§5]c[oO0]re
```

Common spam phrases

Number of spaces, characters, and punctuation may vary.

```
try it for fr[e]+
```

```
student[ _-]*loans
```

```
you[’`"']re already approved
```

```
special[ _;!%~#§£€@°()\+\-\*\.]*offer
```

www.fortinet.com