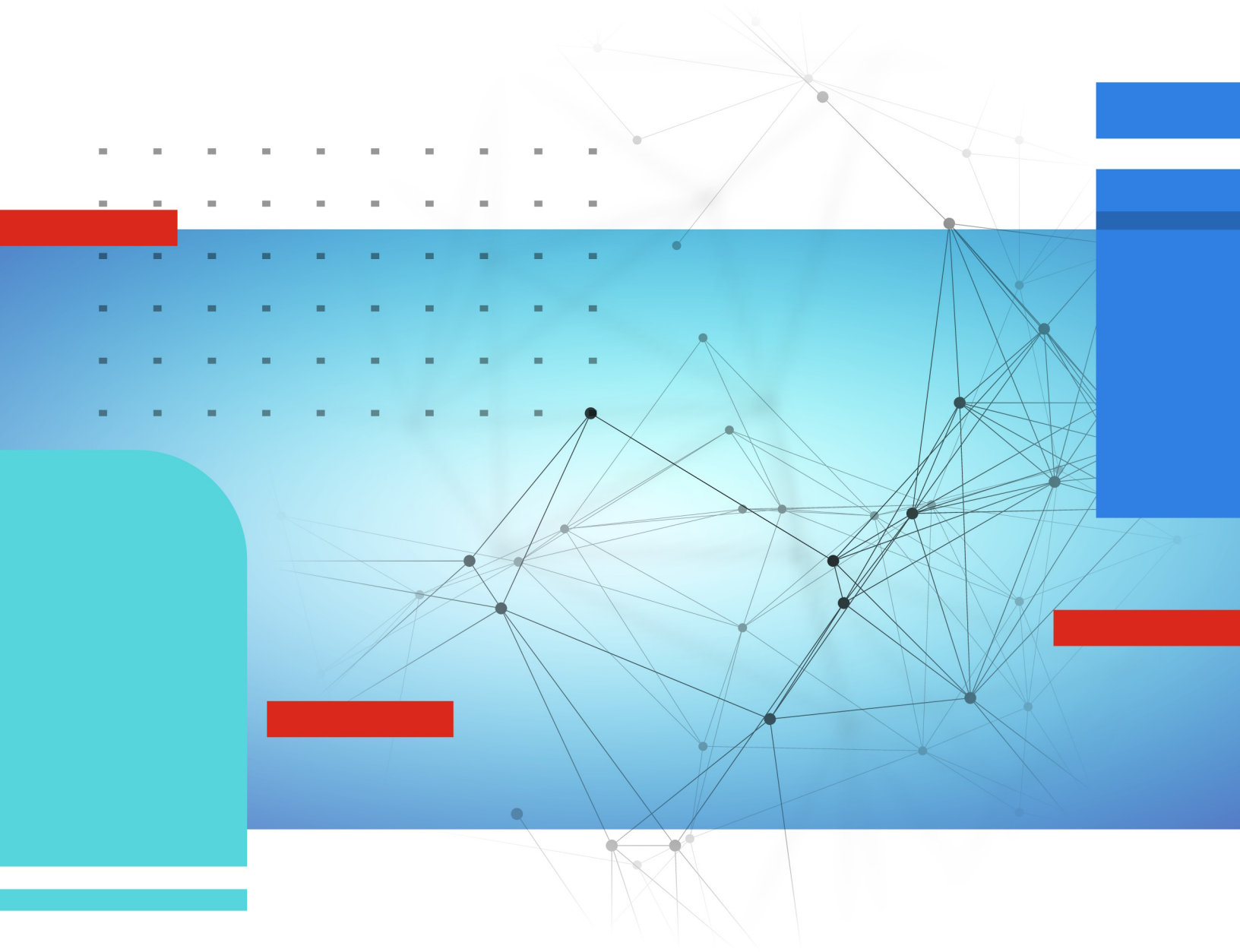
Administration Guide

FortiMail 7.6.1



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

FORTINET VIDEO GUIDE
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 CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 25, 2024
FortiMail 7.6.1 Administration Guide
06-761-000000-20240925

TABLE OF CONTENTS

Change log

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

Date	Change Description
2024-04-29	Initial release of FortiMail 7.6.1 Administration Guide.

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 C: Port Numbers on page 611.

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 17.

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 19.

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.

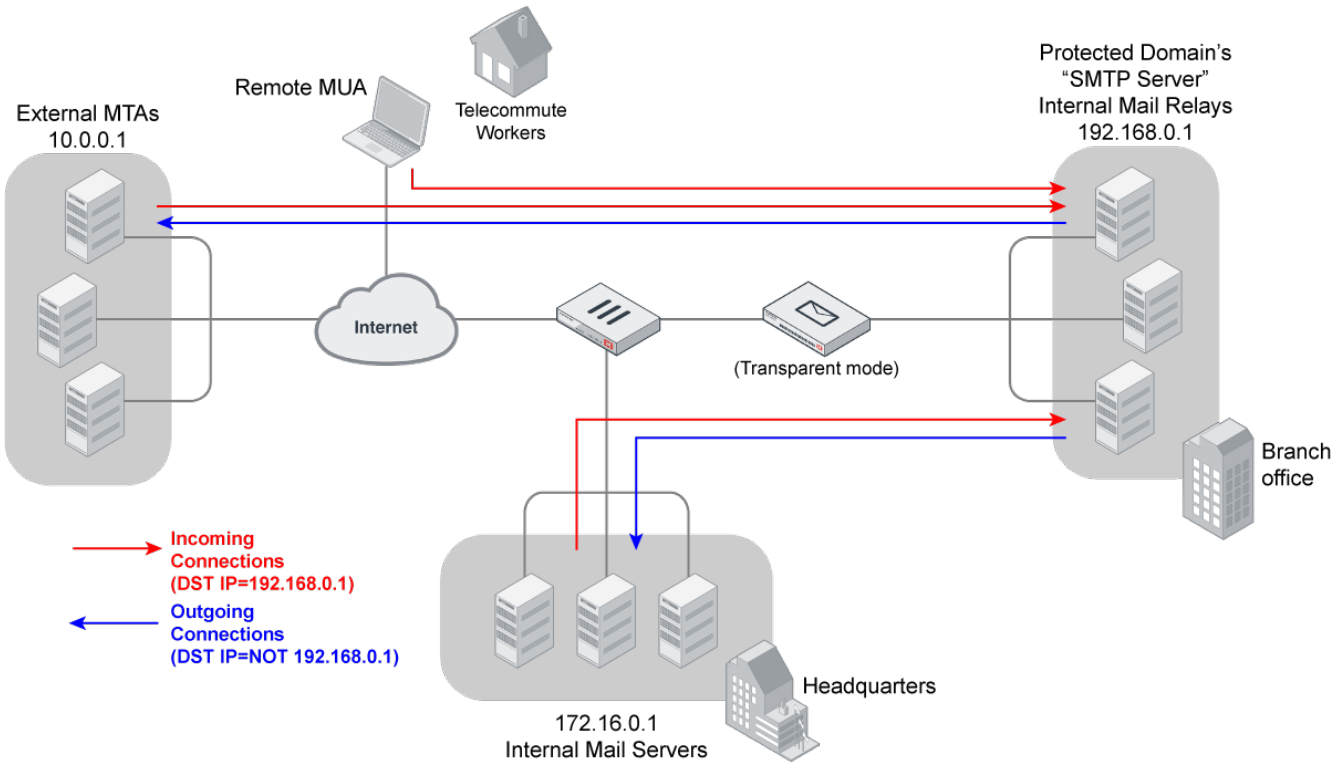
Connection directionality versus email directionality

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, "Hide the transparent box" 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 on page 34.

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 333. For information about profiles, see Configuring profiles on page 361.

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

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 280.

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 280.

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 337.

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 280.

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 204.

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 the GUI appearance on page 212.

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 361 and Configuring security settings on page 463.

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 on page 26.

FortiMail antispam technique highlights

Greylist scanning	See Configuring greylisting on page 488.
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 386.
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 385.
Bayesian scanning	See Training the Bayesian databases on page 508.
Heuristic scanning	See Heuristic section on page 385.
Image spam scanning	See Image spam section on page 388.
PDF scanning	See Scan PDF attachment on page 378.
Block/safe lists	• For information on global block/safe lists, see Managing the global block and safe list on page 484. • For information on domain-wide block/safe lists, see Managing the per-domain block lists and safe lists on page 485. • For information on personal block/safe lists, see Managing the personal block lists and safe lists on page 487. • For information on session block/safe lists, see Configuring sender reputation options on page 362.
Banned word scanning	See Banned word section on page 386.

Safe list word scanning	See Safelist word section on page 387.
Sender reputation	See Viewing sender reputation statuses on page 137.

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

FortiMail units perform each of the antispam scanning and other actions listed in the sequence presented in the following table. Disabled scans are skipped. This is a general sequence only. Aactions are based on the results of many factors.

This table does not include everything the FortiMail unit does when a client connects to deliver email. **Only the antispam techniques**, and other functions having an effect on the antispam techniques, are included. Other functions that are not antispam related may be running in parallel to the ones in the table.

FortiMail actions can be categorized as following:

- **Final actions**: Reject, discard, rewrite, personal quarantine, and system quarantine. If these actions are taken, no more further scanning will be processed.
- **Non-final actions**: Tag, add header, replace, archive, notify, BCC, and encrypt. If one or more of these actions

have been taken, FortiMail will keeping process the email with other scanners.

- **Delivery actions**: Original Host, Alternate Host, BCC

Exceptions:

- If antivirus scanning is matched, antispam scanning will be skipped.
- If antivirus and antispam scanning is matched with non-final actions, attachment scanning will still be done but content monitor will not.
- If Sandbox scanning is matched, content monitor will still be done.
- If FortiGuard antispam and IP reputation checking detects spam, no further antispam checking will be performed, even though the actions are non-final.

The PDF file type scan is not listed in the following table. When enabled, the PDF file type converts the first page of any PDF attachments into to a format that the heuristic, banned word, and image spam scanners can scan. If any of these scanners are enabled, they will scan the first page of the PDF at the same time they examine the message body, according to the sequence in the table.

Execution sequence of antispam techniques

Check	Check Involves	Action If Positive	Action If Negative
Client initiates communication with the FortiMail unit			
Sender reputation	Client IP address	If the client IP is in the sender reputation database, check the score and enable any appropriate restrictions, if any.	Add the IP address to the sender reputation database and keep a reputation score based on the email received. Proceed to the next check.
FortiGuard block IP check	Client IP address	If “Check FortiGuard Block IP at connection phase” is enabled in a session profile, FortiMail will check the client IP address against the FortiGuard block IP list. If positive, FortiMail rejects the email.	Proceed to the next check.
Endpoint reputation	Client endpoint ID	If the client endpoint ID is in the sender reputation database, check the score and enable any appropriate restrictions, if any.	Add the IP address to the endpoint reputation database and keep a reputation score based on the email received. Proceed to the next check.
Sender rate control per connection	Client IP address	Apply any connection limitations specified in the session profile. Proceed to the next check.	In there are no connection limitations, or if no session profile applies, proceed to the next check.
HELO/EHLO received from SMTP client			

Check	Check Involves	Action If Positive	Action If Negative
HELO/EHLO	Domain of the `HELO`/`EHLO` command	If invalid characters appear in the domain, reject the `HELO`/`EHLO` command. Session will not continue until a proper `HELO`/`EHLO` command is received.	Proceed to the next check.
MAIL FROM: and RCPT TO: commands received from SMTP client			
Sender rate control per message	Client IP address	Apply any connection limitations specified in the session profile. Proceed to the next check.	In there are no connection limitations, or if no session profile applies, proceed to the next check.
Sender domain check	Domain of envelope sender (`MAIL FROM:`)	If any of the domain checks (the `Check sender domain` and Reject empty domains checks listed in Unauthenticated Session Settings in the session profile) fail, an error is returned to the SMTP client. The error depends on which particular check failed.	Proceed to the next check.
Recipient verification	Envelope recipient (`RCPT TO:`)	If the recipient is unknown, reject the message.	Proceed to the next check.
System safe list (Phase I)	Client IP address and email address/domain of the envelope sender (`MAIL FROM:`)	If the client IP or email address/domain of the sender appear in the system safe list, deliver the email and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
Greylist	Envelope sender (`MAIL FROM:`), envelope recipient (`RCPT TO:`), and client IP subnet address	If the sender is in the greylist database or if the client IP subnet appears in the greylist exempt list, the message is passed to the next check. **Note:** This check is omitted if the access control rule's action is RELAY.	If the sender is not in the greylist database, a temporary failure code is returned to the SMTP client.
System block list (Phase I)	Client IP address and email address/domain of the envelope sender (`MAIL FROM:`)	If the client IP or email address/domain of the sender appear in the system block list, invoke the block list action for the email.	Proceed to the next check.
Session sender safe list (Phase I)	Client IP address and email address/domain of the envelope sender (`MAIL FROM:`)	If the client IP or email address/domain of the sender appear in the session safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.

Check	Check Involves	Action If Positive	Action If Negative
Session sender block list (Phase I)	Client IP address and email address/domain of the envelope sender (`MAIL FROM:`)	If the client IP or email address/domain of the sender appear in the session block list, invoke the block list action for the message.	Proceed to the next check.
Authentication difference check	Envelope sender (`MAIL FROM:`)	Checks to see if the sender email address in the SMTP envelope matches the authenticated user name. If not allowed in the IP-based policy, the email will be rejected.	Proceed to the next check.
Bounce Verification	Envelope recipient (`RCPT TO:`)	Apply actions specified in the bounce verification settings.	Proceed to the next check.
Access control rules	Client IP address, envelope sender and recipient (`MAIL FROM: and RCPT TO:`)	If the combination of client IP, the email address/domain of the sender, and the email address/domain of the recipient matches an access control rule (Policy > Access Control > Receiving), the FortiMail unit performs the action selected in the access control rule (or TLS profile, if selected). For details, see Configuring access control receiving policies on page 337.	If a matching access control rule does not exist: • If recipient is a member of a protected domain, the default action is Relay. • Otherwise, the default action is Reject. For more information, see Configuring access control receiving policies on page 337.
Recipient domain check	Domain of envelope recipient (`RCPT TO:`)	If any of the domain checks (the Check recipient domain and Reject if recipient and `HELO/EHLO` domain match but sender domain is different checks listed in Unauthenticated Session Settings in the session profile) fail, an error is returned to the SMTP client. The error depends on which check failed.	Proceed to the next check.
Session recipient safe list	Envelope recipient (`RCPT TO:`)	If the recipient appears in the session recipient safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
Session recipient block list	Envelope recipient (`RCPT TO:`)	If the recipient appears in the session recipient block list, reject the message.	Proceed to the next check.
DATA command received from SMTP client			

Check	Check Involves	Action If Positive	Action If Negative
System safe list (Phase II)	Message header sender (`From:`)	If the email address/domain of the sender appears in the system safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
System block list (Phase II)	Message header sender (`From:`)	If the email address/domain of the sender appears in the system block list, invoke the block list action for the message.	Proceed to the next check.
Domain safe list	Client IP, envelope sender (`MAIL FROM:`) and message header sender (`From:`)	If the client IP, email address/domain of the sender appears in the domain safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
Domain block list	Client IP, envelope sender (`MAIL FROM:`) and message header sender (`From:`)	If the client IP, email address/domain of the sender appears in the domain block list, invoke the block list action for the message.	Proceed to the next check.
Session sender safe list (Phase II)	Message header sender (`From:`)	If the email address/domain of the sender appears in the session sender safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
Session sender block list (Phase II)	Message header sender (`From:`)	If the email address/domain of the sender appears in the session sender block list, the block list action is invoked.	Proceed to the next check.
Personal safe list	Client IP, envelope sender (`MAIL FROM:`) and message header sender (`From:`)	If the client IP, email address/domain of the sender appears in the personal safe list, deliver the message and cancel remaining antispam checks (but not the antivirus and content checks).	Proceed to the next check.
Personal block list	Client IP, envelope sender (`MAIL FROM:`) and message header sender (`From:`)	If the client IP, email address/domain of the sender appears in the personal block list, the message is discarded.	Proceed to the next check.
End of message (EOM) command received from SMTP client			

Check	Check Involves	Action If Positive	Action If Negative
Antivirus	Message body and attachments	If an infected message is detected, and the antispam profile is configured to treat viruses as spam, the default spam action will be invoked on the infected message.	Proceed to the next check.
Safe List Word	Message subject and/or body	If the safelisted word scanner determines that the message is not spam, deliver the message and cancel remaining antispam checks.	Proceed to the next check.
FortiGuard Antispam	Message header and body	If the FortiGuard scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used. No further antispam checking will be performed.	Proceed to the next check.
DMARC	Client IP address	DMARC performs email authentication with SPF and DKIM checking. If failed, treat the email as spam.	Proceed to the next check.
SPF check	Client IP address	This option compares the client IP address to the IP addresses of authorized senders in the DNS record (RFC 4408). If failed, treat the email as spam.	Proceed to the next check.
DKIM check	Message header and body	If a DKIM signature is present (RFC 6376), decrypt and verify the DKIM signature using the sender domain's public key in the DNS TXT record. If failed, treat the email as spam.	Proceed to the next check.
ARC	Message header	In the event DKIM and SPF fails to successfully pass messages to intermediaries (such as mailing lists or email account forwarding), Authenticated Received Chain (ARC) can permit intermediate servers to sign the original message's validation results. Therefore, ARC validation should only apply when the receiver has established trust with the ARC signers.	Proceed to the next check.
Spam outbreak protection	Message header and body	If the FortiGuard scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.

Check	Check Involves	Action If Positive	Action If Negative
Behavior analysis	Message body	If the scanner determines the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Impersonation checks	Message header	If the scanner determines the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Banned Word	Message subject and/or body	If the banned word scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Dictionary	Message body	If the dictionary scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
DNSBL	Client IP address	If the DNSBL scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
SURBL	Every URL in the message body	If the SURBL scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Heuristic	Message body	If the heuristic antispam scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Image Spam	Embedded images If Aggressive scan is enabled, attached images are also examined.	If the image spam scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.

Check	Check Involves	Action If Positive	Action If Negative
Header analysis	Message header	If the header analysis scan determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Bayesian	Message body	If the Bayesian scanner determines that the message is spam, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Suspicious Newsletter	Message header and body	If the newsletter scan determines that the message is a newsletter, the configured individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
Content	Message header, body, and attachment	If the content scanner determines that the message is spam or prohibited, the action configured in the content profile individual action is invoked. If the individual action is set to default, then the antispam profile default action is used.	Proceed to the next check.
DLP	Message header, body, and attachment	Apply the action configured in the DLP profile.	Deliver the message.

FortiMail operation modes

FortiMail units can run in one of three operation modes: gateway mode, transparent mode, and server mode.

Gateway mode

- The FortiMail unit acts as a mail transfer agent (MTA), or email gateway, relaying email to and from the email servers that it protects.
- Simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning.
- FortiMail does not locally store email unless queued, quarantined, or archived.

Transparent mode

- The FortiMail unit transparently proxies or relays email traffic to and from the email servers that it protects.
- Eliminates the need to change existing mail server network configuration.
- FortiMail does not locally store email unless queued, quarantined, or archived.

Server mode

- The FortiMail unit operates as a standalone, full-featured email server and MTA.
- The FortiMail unit locally stores email for delivery to its email users. Email users can access their email using FortiMail webmail, POP3, or IMAP.

All operation modes can scan email traffic for viruses and spam, and can quarantine suspicious email and attachments.

Comparison of gateway, transparent, and server mode of operation

	Gateway	Transparent	Server
SMTP role	MTA/relay	Transparent proxy/relay	Server
FortiMail unit is hidden	No	Yes, if enabled	No
Email user accounts	Preferences and per-recipient quarantine only	Preferences and per-recipient quarantine only	Yes
Requires DNS record change	Yes	No, if hidden with no per-recipient quarantines or Bayesian scan	Yes
May require changes to SMTP client configurations or other infrastructure	Yes	No	Yes
Requires FortiMail unit located between external MTAs and protected email servers	No	Yes	N/A (FortiMail unit acts as email server)
Protected email servers	Separate	Separate	Integrated (FortiMail unit acts as email server)

In addition, some FortiMail features are specific to the operation mode. As a result, changing the operation mode may reset your FortiMail configuration.

FortiMail high availability

FortiMail units can be configured to operate in high availability (HA) clusters. See About HA modes on page 223.

FortiMail management methods

After you install the FortiMail unit, you can configure and manage the unit via either:

- GUI
- command line interface (CLI)

The CLI is only available to administrator accounts whose Domain is System. It is **not** available to domain (tiered) administrator accounts. For more information on domain administrators, see About administrator account permissions and domains on page 165.

Depending on the FortiMail unit's model number, you may also be able to reset the configuration and to configure basic settings such as operation mode and IP addresses using the buttons and LCD on the front panel. For details, see Configuring system options on page 172.

This Administration Guide describes the GUI. For equivalent documentation of the CLI, see the FortiMail CLI Reference.

Basic mode versus advanced mode

The GUI enables you to configure the FortiMail unit by connecting to the FortiMail unit through a web browser. The GUI has two modes: standard mode and advanced mode.

- Standard mode
  Provides easy navigation using a simplified set of menu options that allow for many, but not all, typical FortiMail unit configurations. Less frequently used options are hidden, and some configurations are simplified by providing you with predefined configuration sets.
- Advanced mode
  Provides the full set of menu options which allows you to achieve more complex configurations.

You can switch between the basic mode and advanced mode of the GUI at any time with no configuration loss. If, for example, you prefer standard mode but need to configure an item available only in advanced mode, you can switch to advanced mode, configure the item, then switch back to standard mode. To switch between the two modes, select either *Standard Mode* or *Advanced Mode* from the dropdown list on the top right corner of the GUI.

Setting up the FortiMail system

This chapter includes details about completing FortiMail initial setup. After this initial setup, you can customize the configuration and use all the features as required.

FortiMail initial setup involves the following steps:

1. Connecting to the GUI or CLI
2. Choosing the operation mode
3. Running the Quick Start Wizard
4. Connecting to FortiGuard services
5. Gateway mode deployment
6. Transparent mode deployment
7. Server mode deployment
8. Testing the installation
9. Backing up the configuration

Connecting to the GUI or CLI

To configure and maintain the FortiMail unit, you can connect to it using either the:

- GUI, a graphical user interface (GUI), from within a current web browser (see Connecting to the FortiMail GUI for the first time on page 36)
- command line interface (CLI), a command line interface similar to DOS or UNIX commands, from a Secure Shell (SSH) or Telnet terminal (see Connecting to the FortiMail CLI for the first time on page 38)
- front panel's LCD display and control buttons available on some models (see Using the front panel's control buttons and LCD display on page 43).

Connecting to the FortiMail GUI for the first time

To use the GUI for the initial setup, you must have:

- a computer with an Ethernet port
- a supported web browser. For information about supported browser versions, see the release notes for your release.
- a crossover Ethernet cable

Default settings for connecting to the GUI

Network Interface	port1
URL	https://192.168.1.99/admin
Administrator Account	admin
Password	(none)

To connect to the GUI

1. Configure the management computer to be on the same subnet as the port1 interface of the FortiMail unit.

   For example, in Microsoft Windows 10, from the Windows Start menu, go to *Settings* > *Network & Internet* > *Change adapter options* > *Local Area Connection Properties* > *Internet Protocol Version 4 (TCP/IPv4) Properties* and change the management computer IP address to 192.168.1.2 and the netmask to 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiMail unit's port1.
3. Start your web browser and enter the URL:

   https://192.168.1.99/admin

   (Remember to include the "s" in `https://`, and `/admin` at the end of the URL.)

   If you are connecting to FortiMail-VM with a trial license or to a LENC version of FortiMail, you may not be able to see the logon page due to an SSL/TLS cipher error during the connection. In this case, you must configure your web browser to accept low encryption. For example, in Mozilla Firefox, if you receive this error message:

   `ssl_error_no_cypher_overlap`

   then you may need to enter:

   `about:config`

   in the URL bar, and then set `security.ssl3.rsa.rc4_40_md5` to `true`.

   To support HTTPS authentication, the FortiMail unit ships with a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiMail unit. When you connect, depending on your web browser and prior access of the FortiMail unit, your browser might display two security warnings related to this certificate:

   - The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate
   - The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

   Both warnings are normal for the default certificate.
4. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.

   For details on accepting the certificate, see the documentation for your web browser.

   The login dialog appears.
5. In the *Name* field, type `admin`, then select Login (in its default state, there is no password for this account).

   Login credentials entered are encrypted before they are sent to the FortiMail unit. If your login is successful, the GUI appears.

Choosing a GUI view

FortiMail administrative GUI has multiple views:

- **Simple View**: Default view for the first time login. Displays only the most commonly used menu options.
- **Advanced View**: Displays all the menu options.
- **Microsoft 365 & Google Workspace View**: Available if you have the Microsoft 365 and Google Workspace API feature license.

To change to a different view, from the eye icon dropdown list on the upper right corner, select a different view. Your view setting will be saved.

Connecting to the FortiMail CLI for the first time

For the initial configuration, you can access the CLI from your management computer either:

- **Locally** — Connect your computer directly to the FortiMail unit's console port.
- **Through the network**— Connect your computer through any network attached to one of the FortiMail unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect using the *CLI Console* widget in the GUI.

Local access is required in some cases.

- If you are installing your FortiMail unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection.
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process has completed, and therefore local CLI access is the only viable option.

Local console connection and initial configuration

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiMail unit, using its DB-9 or RJ-45 console port.

Requirements

- a computer with an available serial communications (COM) port
- an RJ-45-to-DB-9 (null modem) console cable
- a terminal emulation software such as PuTTY

The following procedure describes connection using PuTTY software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the console cable, connect the FortiMail unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start PuTTY.
3. In the *Category* tree on the left, go to *Connection* > *Serial* and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1

Parity	None
Flow control	None

4. In the *Category* tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
5. Click *Open*.
6. Press the Enter key to initiate a connection.
   The login prompt appears.
7. Type a valid administrator account name (such as `admin`) and press Enter.
8. Type the password for that administrator account then press Enter (in its default state, there is no password for the `admin` account).
   The CLI displays a command line prompt.

Initial system configuration with the CLI

Once you've connected to the FortiMail CLI, you can configure FortiMail system settings.

The following are only the CLI commands for basic system settings that are required to deploy the FortiMail unit to its intended location on your network. For information on other CLI commands, see the FortiMail CLI Reference.

To change an administrator password:

```
config system admin
   edit <administrator_name>
      set password <new-password_str>
end
```

To change the operation mode:

```
config system global
   set operation_mode {gateway | server | transparent}
end
```

To configure the IP address of port1 etc.:

```
config system interface
   edit <interface_name>
      set ip <address_ipv4>
      set ipv6 <address_ipv6>
end
```

To configure the default route/gateway:

```
config system route
   edit <route_int>
      set destination <destination_ipv4mask>
      set gateway <router_ipv4>
      set interface <interface_name>
end
```

To configure the DNS servers:

```
config system dns
   set primary <dns_ipv4>
   set secondary <dns_ipv4>
end
```

To configure NTP time synchronization:

```
config system time ntp
   set ntpserver {<address_ipv4> | <host_fqdn>}
   set ntpsync {enable | disable}
   set syncinterval <interval_int>
end
```

To log out:

```
exit
```

Enabling access to the CLI through the network (SSH or Telnet)

SSH, Telnet, or CLI Console widget (via the GUI) SSH or Telnet access to the CLI requires connecting your computer to the FortiMail unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

If you do not want to use an SSH/Telnet client and you have access to the GUI, you can alternatively access the CLI through the network using the *CLI Console* widget in the GUI. For details, see the FortiMail CLI Reference.

If you do not want to use an SSH/Telnet client and you have access to the GUI, you can alternatively access the CLI through the network using the *CLI Console* widget in the GUI.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is **not** connected directly or through a switch, you must also configure the FortiMail unit with a static route to a router that can forward packets from the FortiMail unit to your computer.

Telnet is not a secure access method. Use SSH to access the CLI from the Internet or any other untrusted network.

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as PuTTY
- the console cable included in your FortiMail package
- a crossover or straight-through network cable
- prior configuration of the operating mode, network interface, and static route (see Initial system configuration with the CLI on page 39)

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiMail unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiMail unit.
2. Note the number of the physical network port on the FortiMail unit.
3. Using a local console connection, connect and log into the CLI. For details, see Local console connection and initial configuration on page 38.

4. Enter the following commands:

```
config system interface
  edit <interface_name>
    set allowaccess {http https ping snmp ssh telnet}
end
```

where:

- `<interface_name>` is the name of the network interface associated with the physical network port, such as `port1`
- `{http https ping ssh telnet}` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`; omit protocols that you do not want to permit

For example, to exclude HTTP, SNMP, ICMP `ECHO` (ping), and Telnet, and allow only secure HTTPS and SSH administrative access on `port1`:

```
config system interface
  edit "port1"
    set allowaccess ping https ssh
  next
end
```

5. To confirm the configuration, enter the command to view the access settings for the interface.

```
show system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the interface.

To connect to the CLI through the network interface, see Connecting to the CLI using SSH on page 41 or Connecting to the CLI using Telnet on page 42.

Connecting to the CLI using SSH

Once the FortiMail unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths vary by whether you have enabled FIPS-CC mode, and whether you have enabled strong cryptography, but generally include SSH version 2 with AES-128 and SHA-256 or better.

Requirements

- a FortiMail network interface configured to accept SSH connections (see Enabling access to the CLI through the network (SSH or Telnet) on page 40)
- terminal emulation software such as PuTTY

To connect to the CLI using SSH

1. On your management computer, start PuTTY.
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.
3. In *Port*, type `22`.
4. From *Connection type*, select *SSH*.
5. Click *Open*.

   The SSH client connects to the FortiMail unit.

   The SSH client may display a warning if this is the first time you are connecting to the FortiMail unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiMail unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiMail unit with no network hosts between them, this is normal.

6. Click *Yes* to verify the fingerprint and accept the FortiMail unit's SSH key. You will not be able to log in until you have accepted the key.

   The CLI displays a login prompt.
7. Type a valid administrator account name (such as `admin`) and press Enter.
8. Type the password for this administrator account and press Enter.

If four incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The CLI displays a command line prompt (by default, its host name followed by a `#`). You can now enter CLI commands.

Connecting to the CLI using Telnet

Once the FortiMail unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Requirements

- a FortiMail network interface configured to accept Telnet connections (see Enabling access to the CLI through the network (SSH or Telnet) on page 40)
- terminal emulation software such as PuTTY

To connect to the CLI using Telnet

1. On your management computer, start PuTTY.
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled Telnet administrative access.
3. In *Port*, type `23`.
4. From *Connection type*, select *Telnet*.
5. Click *Open*.

   The CLI displays a login prompt.
6. Type a valid administrator account name (such as `admin`) and press Enter.
7. Type the password for this administrator account and press Enter.

If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The CLI displays a command line prompt (by default, its host name followed by a `#`). You can now enter CLI commands.

Logging out from the CLI console

Regardless of how you connect to the FortiMail CLI console (direct console connection, SSH, or Telnet), to log out, enter the `exit` command.

See also

Connecting to the FortiMail GUI for the first time

Using the front panel's control buttons and LCD display

On some FortiMail models, you can use the front panel's control buttons and LCD display to configure the:

- IP addresses and netmasks for each of the network interfaces
- default route/gateway
- operating mode

You can also use the front panel to reset the FortiMail unit to the default settings for its firmware version.

After using the front panel to configure these basic settings, you must still connect to the GUI to complete additional setup. To continue, see Connecting to the FortiMail GUI for the first time on page 36.

Choosing the operation mode

Once the FortiMail unit is mounted and powered on, and you have completed initial setup, you can configure the operation mode of the FortiMail unit using the CLI or GUI.

FortiMail units can run in one of three operation modes: gateway mode, transparent mode, or server mode. For details about the three modes, see FortiMail operation modes on page 33.

You will usually choose the operation mode that is appropriate for your topology and requirements and configure the operation mode only **once**, just after physical installation and initial configuration, and before using the Quick Start Wizard.

This section describes each operation mode, assisting you in choosing the mode that best suits your requirements.

This section contains the following topics:

Deployment guidelines

Generally speaking, gateway mode is suitable for most deployment environments. It is usually easier to implement and better understood. Exceptions are situations where neither DNS MX records nor IP addresses cannot be modified.

Transparent mode was developed for the purpose of implementing FortiMail in carrier environments to combat outgoing spam. It is suitable for certain environments but needs more careful routing handling and good understanding of network and application layer transparency.

Transparent mode is the best choice for combating outgoing spam in carrier environments.

You use server mode to set up a standalone email server or to replace an existing email server.

After you set the operation mode, run the Quick Start Wizard to set up a basic system. Then deploy your FortiMail unit. The details vary depending on the operation mode you chose. For instructions, consult the applicable sections:

- Gateway mode deployment
- Transparent mode deployment
- Server mode deployment

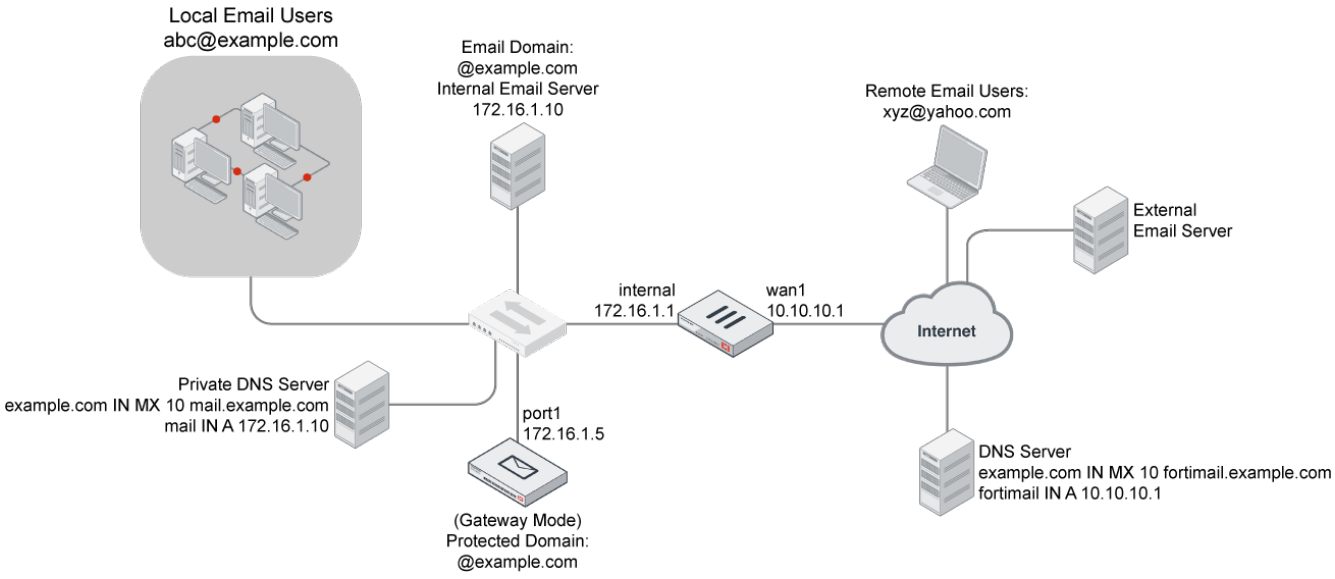
Characteristics of gateway mode

When operating in gateway mode, the FortiMail unit acts as a mail transfer agent (MTA), sometimes known as an email gateway or relay. The FortiMail unit receives email messages, scans for viruses and spam, then relays email to its destination email server for delivery. External MTAs connect to the FortiMail unit, rather than directly to the protected email server.

FortiMail units operating in gateway mode provide a web-based user interface from which email users can access personal preferences and their per-recipient quarantined email. However, FortiMail units operating in gateway mode do **not** locally host mailboxes such as each email user's inbox. Mailboxes are stored on the protected email servers.

Gateway mode requires some changes to an existing network. Requirements include MX records on public DNS servers for each protected domain, which must refer to the FortiMail unit instead of the protected email servers. You may also need to configure firewalls or routers to direct SMTP traffic to the FortiMail unit rather than your email servers.

Example gateway mode topology



For example, an Internet service provider (ISP) could deploy a FortiMail unit to protect their customers' email servers. For security reasons, customers do not want their email servers to be directly visible to external MTAs. Therefore, the

ISP installs the FortiMail unit in gateway mode, and configures its network such that all email traffic must pass through the FortiMail unit before reaching customers' email servers.

For sample deployment scenarios, see Gateway mode deployment on page 54.

Characteristics of transparent mode

When operating in transparent mode, the FortiMail acts as either an implicit relay or a proxy. The FortiMail unit intercepts email messages, scans for viruses and spam, then transmits email to its destination email server for delivery. External MTAs connect through the FortiMail unit to the protected email server.

Transparency at both the network and application layers is configurable, but not required. When hiding, the FortiMail unit preserves the IP address and domain name of the SMTP client in IP headers and the SMTP envelope and message headers, rather than replacing them with its own.

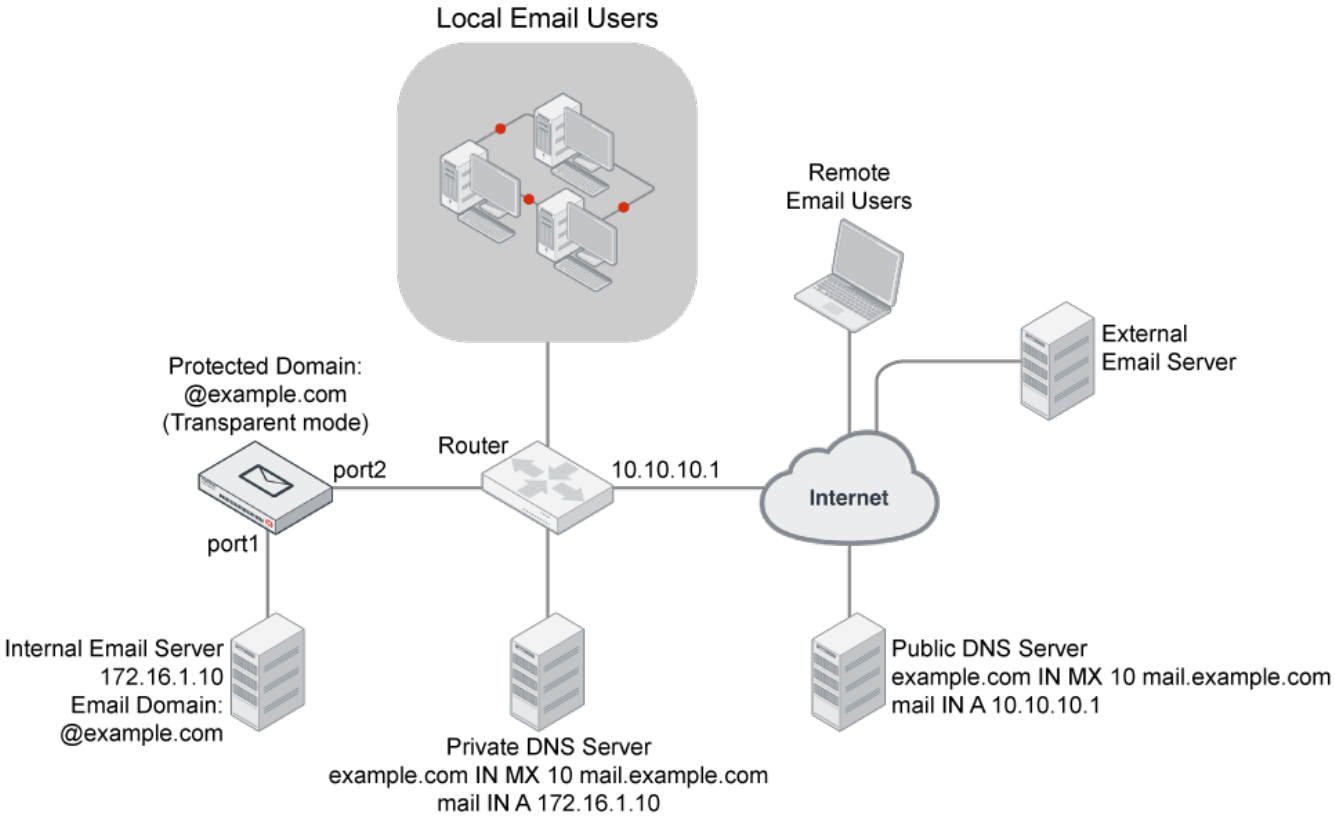
FortiMail units operating in transparent mode provide a web-based user interface from which email users can access personal preferences and email quarantined to their per-recipient quarantine. However, FortiMail units operating in transparent mode do **not** locally host mailboxes such as each email user's inbox. These mailboxes are stored on the protected email servers.

By default, FortiMail units operating in transparent mode are configured as a bridge, with all network interfaces on the same subnet. You can configure out-of-bridge network interfaces if you require them, such as if you have some protected email servers that are not located on the same subnet. If you set an interface to route mode, you must assign the interface a local IP address that belongs to a different subnet from that of the management IP.

Port 1 is the only port permanently attached to the built-in bridge and thus cannot be set in route mode.

Transparent mode usually requires no changes to an existing network. Requirements include that the FortiMail unit must be physically inline between the protected email server and all SMTP clients—unlike gateway mode. Because FortiMail units operating in transparent mode are invisible, clients cannot be configured to route email directly to the FortiMail unit; so, it must be physically placed where it can intercept the connection.

Example transparent mode topology



Do not connect two ports to the same VLAN on a switch or the same hub. Some Layer 2 switches become unstable when they detect the same media access control (MAC) address originating on more than one network interface on the switch, or from more than one VLAN.

For example, a school might want to install a FortiMail unit to protect its mail server, but does not want to make any changes to its existing DNS and SMTP client configurations or other network topology. Therefore, the school installs the FortiMail unit in transparent mode.

For sample deployment scenarios, see Transparent mode deployment on page 63.

Characteristics of server mode

When operating in server mode, the FortiMail 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.

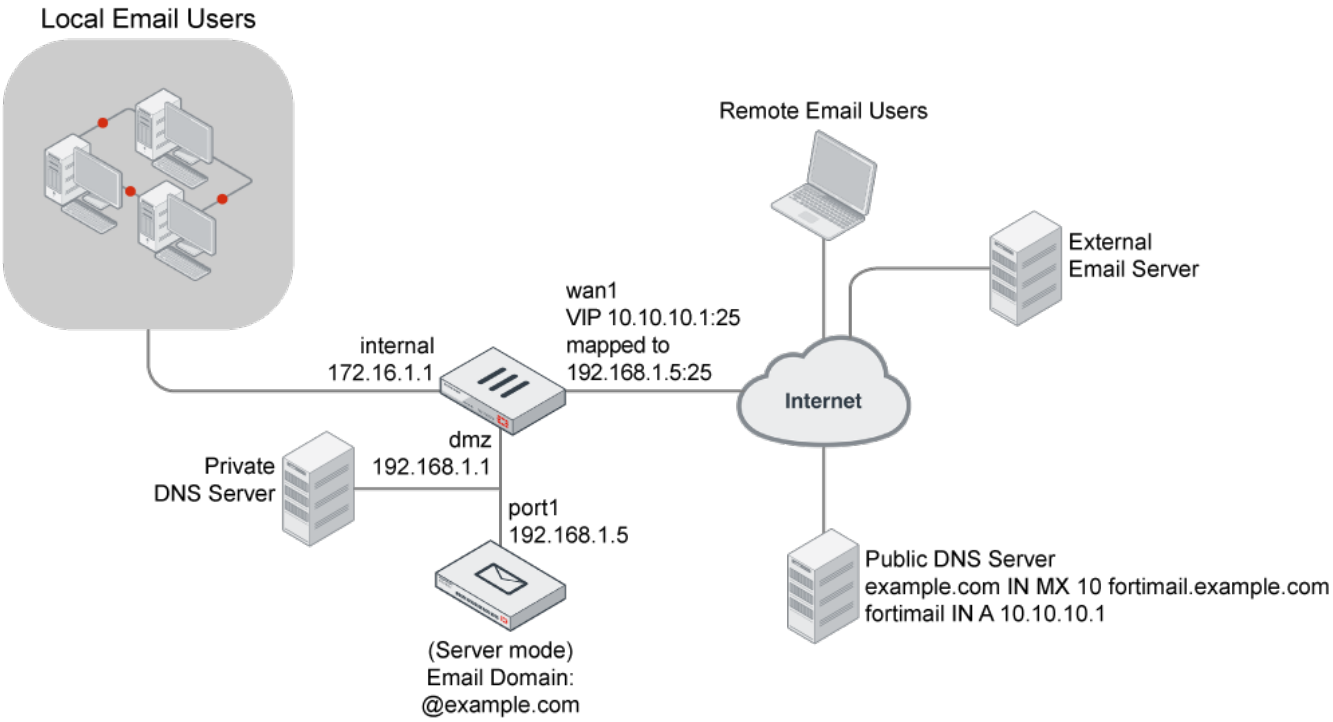
FortiMail units operating in server mode provide a web-based user interface from which email users can access:

- personal preferences
- email quarantined to their per-recipient quarantine
- their locally hosted mailboxes such as each email user's inbox.

In addition, email users can retrieve email using POP3 or IMAP.

Server mode requires some changes to an existing network. Requirements include MX records on public DNS servers for each protected domain. The records must refer to the FortiMail unit. You may also need to configure firewalls or routers to direct SMTP traffic to the FortiMail unit.

Example server mode topology



For example, a company might be creating a network, and does not have an existing email server. The company wants the convenience of managing both their email server and email security on one network device. Therefore, the company deploys the FortiMail unit in server mode.

For sample deployment scenarios, see Server mode deployment on page 85.

Changing the operation mode

By default, FortiMail units operate in gateway mode. If you do not want your FortiMail unit to operate in gateway mode, before configuring the FortiMail unit or using the Quick Start Wizard, select the operation mode.

The default mode is gateway. If that is your chosen mode, you can skip the following procedure.

To select the operation mode

1. Open the GUI (See Connecting to the FortiMail GUI for the first time on page 36).
2. In the System Information widget on the dashboard, select either Gateway, Server, or Transparent from the Operation mode dropdown list.

A confirmation dialog appears, warning you that many settings will revert to their default value for the version of your FortiMail unit's firmware.

3. Select OK.
   The FortiMail unit changes the operation mode and restarts. The Login dialog of the GUI appears.

Do not change the operation mode once you have committed resources to configuring FortiMail. Changing the operation mode resets most of the configuration to the factory defaults.

Running the Quick Start Wizard

The Quick Start Wizard leads you through required configuration steps, helping you to quickly set up your FortiMail unit.

While all settings configured by the Quick Start Wizard can also be configured through the standard and advanced modes of the GUI, the wizard presents each setting in the necessary order. The wizard also provides descriptions to assist you in configuring each setting. These descriptions are not available in the GUI.

The Quick Start Wizard allows you to set up FortiMail in server mode or gateway mode, but not in the transparent mode.

The following topics describe how to use the Quick Start Wizard:

Starting the wizard

1. Open the GUI in a browser.
2. In either standard mode or advanced mode, select Wizard from the dropdown list in the top right corner of the GUI.
3. Select OK when prompted to continue. The first page of the wizard appears in a new window over the GUI. You cannot access the GUI when the wizard is open.
   You can navigate through the wizard using the Next and Back buttons at the lower corners of the window.

None of the settings you make on the wizard take effect until you click OK on the last step.

Step 1: Time Settings

Select the time zone.

Step 2: Network Settings

Configure the following network settings.

Port1 IP	Enter the IP address of the port1 network interface, such as `192.168.1.99`. This option does not appear if the FortiMail unit is operating in transparent mode.
Primary DNS	Enter the IP address of the primary server to which the FortiMail unit will make DNS queries. **Caution:** Verify connectivity with the DNS servers. Failure to verify connectivity could result in many issues, including the inability of the FortiMail unit to process email.
Secondary DNS	Enter the IP address of the secondary server to which the FortiMail unit will make DNS queries.
Default Gateway	Enter the IP address of the default gateway router.

Step 3: Local Host Settings

You usually should configure the FortiMail unit with a local domain name that is different from that of protected email servers, such as mail.example.com for the FortiMail unit and server.mail.example.com for the protected email server. The local domain name of the FortiMail unit will be used in many features such as email quarantine, Bayesian database training, spam report, and delivery status notification (DSN) email messages. If the FortiMail local domain is the same as one of its protected domains, FortiMail will use its FQDN to send out reports, so as to distinguish itself from the protected domains or other subdomains.

The local domain name must be globally DNS-resolvable only if the FortiMail unit is used as a relay server for outgoing email.

Host name	Enter the host name of the FortiMail unit. You should use a different host name for each FortiMail unit, especially when you are managing multiple FortiMail units of the same model, or when configuring a FortiMail high availability (HA) cluster. This will enable you to distinguish between different members of the cluster. If the FortiMail unit is in HA mode: • when you connect to the GUI, your web browser will display the host name of that cluster member in its status bar. • the FortiMail unit will add the host name to the subject line of alert email messages.
Local domain name	Enter the local domain name to which the FortiMail unit belongs. The FortiMail unit's fully qualified domain name (FQDN) is in the format: `<Host Name>.<Local Domain Name>`

This option does not appear if the FortiMail unit is operating in server mode.

Note: The local domain name can be a subdomain of an internal domain if the MX record for the domain on the DNS server can direct the mail destined for the subdomain to the intended FortiMail unit.

Step 4: Edit Administrator Password

By default, it has no password. Adding a password is optional for this account, but for security reasons, you should provide a password.

Failure to configure a strong administrator password could compromise the security of your FortiMail unit.

To change the password

1. Select Change password.
2. Enter and confirm a new password.
3. Select Next to move to the next step.

Step 5: Operation Mode

Select either the gateway mode or server mode. Note that if you want to run FortiMail in transparent mode, you cannot run the wizard.

Step 6: Domain Configuration

Step 6of the Quick Start Wizard configures the protected domains.

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
- the domain name portion (the portion which follows the “@” symbol) of recipient email addresses in the envelope

Both of which the FortiMail unit compares to connections and email messages when looking for traffic that involves the protected domain.

For example, if you wanted to scan email from email addresses such as user.one@example.com that are 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`.

You must configure at least one protected domain. FortiMail units can be configured to protect one or more email domains that are hosted on one or more email servers.

Exceptions include if you will not apply recipient-based policies or authentication profiles, such as in Example 3: FortiMail unit for an ISP or carrier on page 74.

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`.
Use MX record (gateway mode only)	Select to enable the FortiMail unit to query the DNS server's MX record for the FQDN or IP address of the SMTP server for this domain name. **Note**: If enabled, 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. For details, see Configuring DNS records on page 55 (gateway mode) or Configuring DNS records on page 85 (transparent mode).
SMTP server (gateway mode only)	Enter the fully qualified domain name (FQDN) host name or IP address of the primary SMTP server for this protected domain, then also configure Port. 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.
Port (gateway mode only)	Enter the port number on which the SMTP server listens. See also Appendix C: Port Numbers on page 611.
Use SMTPS (gateway mode only)	Enable to use SMTPS for connections originating from or destined for this protected server.
Use SMTP for recipient verification (gateway mode only)	Enable it if you want to use the SMTP server to verify the recipients.

Step 7: Policy Settings

Policy settings decides how to apply the scan policies. By default, FortiMail comes with system wide IP and recipient based policies.

Inbound email scan	Enable to scan the inbound email destined to the protected domains.
Outbound email scan	Enable to scan the outbound email destined to the unprotected domains.
Email relay for protected domain (gateway mode only)	If you specify the SMTP server's IP address in the previous step, the option appears. Enable it to add the protected domain to the ACL and set the action to relay.

Step 8: Reviewing and saving the configuration

Step 8 presents a list of all settings you have made in the wizard.

- Review the configuration.
- To change a setting, click Back until you reach the applicable step.
- If all settings are correct, select OK.

Settings in the wizard do not take effect until you click OK.

The wizard and the dashboard disappear, and FortiMail prompts you to log in.

Continuing the installation

After using the Quick Start Wizard:

1. If you have multiple FortiMail units, and you want to configure them in high availability (HA) mode, configure the HA settings before physically connecting the FortiMail units to your network.
   For instructions on configuring HA, see Using high availability (HA) on page 223
2. If you have subscribed to FortiGuard Antivirus or FortiGuard Antispam services, connect the FortiMail unit to the Fortinet Distribution Network (FDN) to update related packages. For details, see Connecting to FortiGuard services on page 52.
3. You may need to configure additional features that may be specific to your operation mode and network topology, such as configuring your router or firewall, and records on your public DNS server. For instructions applicable to your operation mode, see:
   - Gateway mode deployment
   - Transparent mode deployment
   - Server mode deployment
4. Verify that email clients can connect to or through the FortiMail unit. For details, see Testing the installation on page 95.

Connecting to FortiGuard services

After the FortiMail unit is physically installed and configured to operate in your network, if you have subscribed to FortiGuard Antivirus and/or FortiGuard Antispam services, connect the FortiMail unit to the Fortinet Distribution Network (FDN).

Connecting your FortiMail unit to the FDN or override server ensures that your FortiMail unit can:

- download the most recent FortiGuard Antivirus definitions and engine packages
- query the FDN for blocklisted servers and other real-time information during FortiGuard Antispam scans, if configured

This way, you scan email using the most up-to-date protection.

The FDN is a world-wide network of Fortinet Distribution Servers (FDS). When a FortiMail unit connects to the FDN to download FortiGuard engine and definition updates, by default, it connects to the nearest FDS based on the current time zone setting. You can override the FDS to which the FortiMail unit connects.

Your FortiMail unit may be able to connect using the default settings. However, you should confirm this by verifying connectivity.

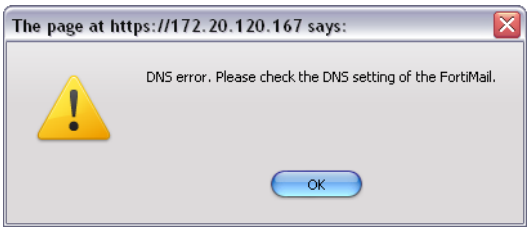
You must first register the FortiMail unit with the Fortinet Technical Support web site, https://support.fortinet.com/, to receive service from the FDN. The FortiMail unit must also have a valid Fortinet Technical Support contract which includes service subscriptions, and be able to connect to the FDN or the FDS that you will configure to override the default FDS addresses.

Before performing the next procedure, if your FortiMail unit connects to the Internet using a proxy, use the CLI command `config system fortiguard antivirus` to enable the FortiMail unit to connect to the FDN through the proxy.

To verify rating query connectivity

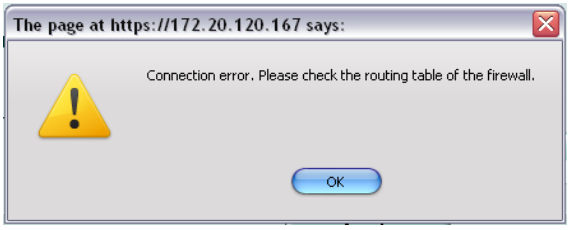
1. Go to System > FortiGuard > AntiSpam in the advanced mode of the GUI.
2. Make sure the Enable Service check box is marked. If it is not, mark it and click Apply.
   If the FortiMail unit can reach the DNS server, but cannot successfully resolve the domain name of the FDS, a message appears notifying you that a DNS error has occurred.

   DNS error when resolving the FortiGuard Antispam domain name

3. Verify that the DNS servers contain A records to resolve service.fortiguard.net and other FDN servers. You may be able to obtain additional insight into the cause of the query failure by manually performing a DNS query from the FortiMail unit using the following CLI command:
   `execute nslookup name service.fortiguard.net`
   If the FortiMail unit cannot successfully connect, or if your FortiGuard Antispam license does not exist or is expired, a message appears notifying you that a connection error has occurred.

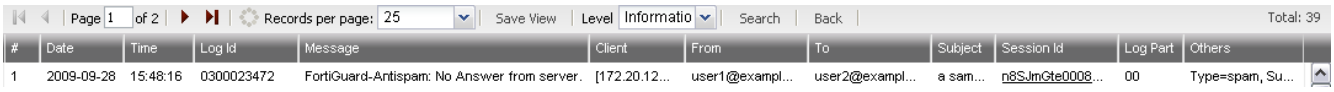
   Connection error when verifying FortiGuard Antispam rating query connectivity

4. Verify that:
   - your FortiGuard Antispam license is valid and currently active
   - the default route (located in System > Network > Routing) is correctly configured
   - the FortiMail unit can connect to the DNS servers you configured during the Quick Start Wizard (located in System > Network > DNS), and to the FDN servers
   - firewalls between the FortiMail unit and the Internet or override server allow FDN traffic (For configuration examples specific to your operation mode, see Gateway mode deployment on page 54, Transparent mode deployment on page 63, or Server mode deployment on page 85.)

5. Obtain additional insight into the point of the connection failure by tracing the connection using the following CLI command:
   `execute traceroute <address_ipv4>`
   where `<address_ipv4>` is the IP address of the DNS server or FDN server.
   When query connectivity is successful, antispam profiles can use the FortiGuard-AntiSpam scan option.
   If FortiGuard Antispam scanning is enabled, you can use the antispam log to analyze any query connectivity interruptions caused because FortiMail cannot connect to the FDN and/or its license is not valid. To enable the antispam log, go to Log & Report > Log Setting > Local in the advanced mode of the GUI. To view the antispam log, go to Monitor > Log > AntiSpam, then mark the check box of a log file and click View.
   If FortiMail cannot connect with the FDN server, the log Message field contains:
   `FortiGuard-Antispam: No Answer from server.`

Antispam log when FortiGuard Antispam query fails



Verify that the FortiGuard Antispam license is still valid, and that network connectivity has not been disrupted for UDP port 53 traffic from the FortiMail unit to the Internet.

Configuring antivirus updates

You can configure the FortiMail unit to periodically request FortiGuard Antivirus engine and definition updates from the FDN or override server.

You can manually initiate updates as alternatives or in conjunction with scheduled updates. You might schedule updates every night at 2 AM or weekly on Sunday, when email traffic volume is light.

To configure scheduled updates

Go to System > FortiGuard > AntiVirus in the advanced mode of the GUI.

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.

Gateway mode deployment

After completing the Quick Start Wizard, you may need to configure some items that are specific to your network topology or the operation mode of your FortiMail unit.

This section contains examples of how to deploy a FortiMail unit operating in gateway mode. Other sections discuss deployment in the other two modes.

This section includes the following topics:

Configuring DNS records

You must configure public DNS records for the protected domains and for the FortiMail unit itself.

If you are unfamiliar with configuring DNS and related MX and A records, first read DNS role in email delivery on page 19.

For performance reasons, and to support some configuration options, you may also want to provide a private DNS server for exclusive use by the FortiMail unit.

This section includes the following:

Configuring DNS records for the protected domains

Regardless of your private network topology, in order for external MTAs to deliver email through the FortiMail unit, you must configure the public MX record for each protected domain to indicate that the FortiMail unit is its email gateway.

For example, if the fully qualified domain name (FQDN) of the FortiMail unit is fortimail.example.com, and example.com is a protected domain, the MX record for example.com would be:

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

If your FortiMail unit will operate in gateway mode, configure the MX record to refer to the FortiMail unit, and remove other MX records. If you fail to do so, external MTAs may not be able to deliver email to or through the FortiMail unit, or may be able to bypass the FortiMail unit by using the other MX records. If you have configured secondary MX records for failover reasons, consider configuring FortiMail high availability (HA) instead. For details, see FortiMail high availability on page 34.

An A record must also exist to resolve the host name of the FortiMail unit into an IP address.

For example, if the MX record indicates that fortimail.example.com is the email gateway for a domain, you must also configure an A record in the example.com zone file to resolve fortimail.example.com into a public IP address:

```
fortimail IN A 10.10.10.1
```

where `10.10.10.1` is either the public IP address of the FortiMail unit, or a virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit.

If your FortiMail unit will relay outgoing email, you should also configure the public reverse DNS record. The public IP address of the FortiMail unit, or the virtual IP address on a firewall or router that maps to the private IP address of the

FortiMail unit, should be globally resolvable into the FortiMail unit's FQDN. If it is not, reverse DNS lookups by external SMTP servers will fail.

For example, if 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.

Configuring DNS records for the FortiMail unit itself

In addition to that of protected domains, the FortiMail unit must be able to receive web connections, and send and receive email, for its own domain name. Dependent features include:

- delivery status notification (DSN) email
- spam reports
- email users' access to their per-recipient quarantined mail
- FortiMail administrators' access to the GUI by domain name
- alert email
- report generation notification email

For this reason, you should also configure public DNS records for the FortiMail unit itself.

Appropriate records vary by whether or not *Web release host name/IP* (located in Security > Quarantine > Quarantine Report in the advanced mode of the GUI) is configured:

- Case 1: Web Release Host Name/IP is empty/default
- Case 2: Web Release Host Name/IP is configured

Case 1: Web Release Host Name/IP is empty/default

When Web release host name/IP is not configured (the default), the web release/delete links that appear in spam reports use the fully qualified domain name (FQDN) of the FortiMail unit.

For example, if the FortiMail unit's host name is `fortimail`, and its local domain name is `example.net`, resulting in the FQDN `fortimail.example.net`, a spam report's default web release link might look like (FQDN highlighted in bold):

```
https://fortimail.example.net
     /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
     TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

In the DNS configuration to support this and the other DNS-dependent features, you would configure the following three records:

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
1 IN PTR fortimail.example.net.
```

where:

- `example.net` is the local domain name to which the FortiMail unit belongs; in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI, email users' access to their per-

recipient quarantines, to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit, and to resolve to the IP address of the FortiMail unit for the purpose of the web release/delete hyperlinks in the spam report

- `10.10.10.1` is the public IP address of the FortiMail unit

Case 2: Web Release Host Name/IP is configured

You could configure Web release host name/IP to use an alternative fully qualified domain name (FQDN) such as `webrelease.example.info` instead of the configured FQDN, resulting in the following web release link (web release FQDN highlighted in bold):

```
https://webrelease.example.info
     /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
     TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

Then, in the DNS configuration to support this and the other DNS-dependent features, you would configure the following MX record, A records, and PTR record (unlike Case 1: Web Release Host Name/IP is empty/default on page 56, in this case, two A records are required; the difference is highlighted in bold):

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
webrelease IN A 10.10.10.1
1 IN PTR fortimail.example.net.
```

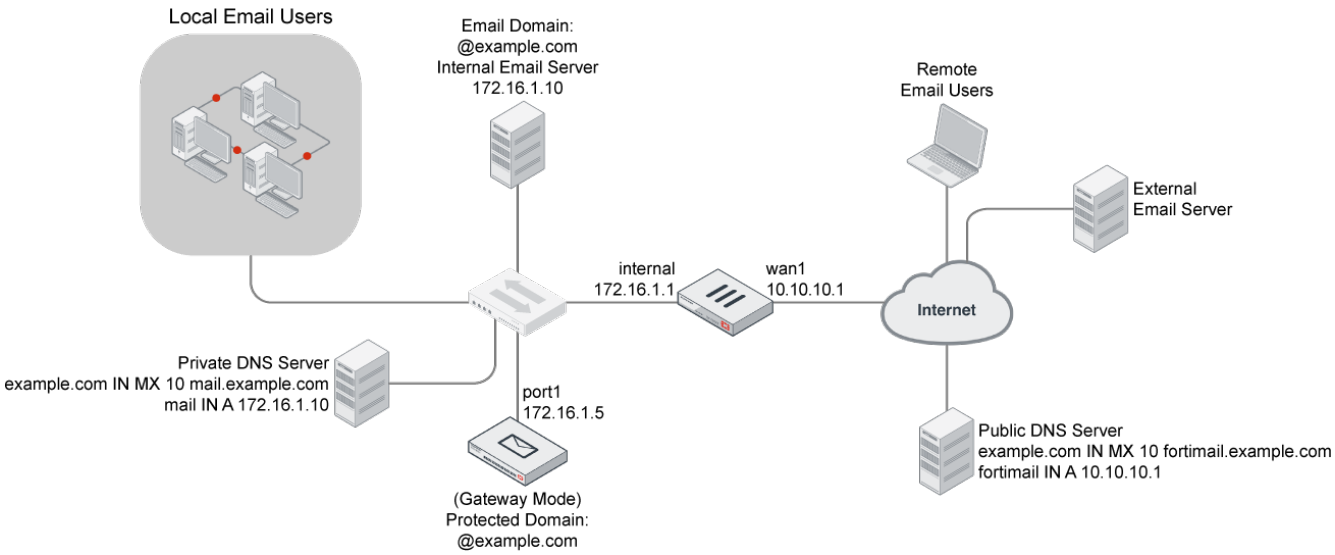
where:

- `example.net` is the local domain name to which the FortiMail unit belongs; in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI and to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit
- `webrelease` is the web release host name; in the A record of the zone file for example.info, it resolves to the IP address of the FortiMail unit for the purpose of the web release/delete hyperlinks in the spam report
- `10.10.10.1` is the public IP address of the FortiMail unit

Configuring a private DNS server

In addition to the public DNS server, consider providing a private DNS server on your local network to improve performance with features that use DNS queries.

Public and private DNS servers (gateway mode)



In some situations, a private DNS server may be required. A private DNS server is required if you enable the Use MX record option. Because gateway mode requires that public DNS servers have an MX record that routes mail to the FortiMail unit, but Use MX record requires an MX record that references the protected SMTP server, if you enable that option, you must configure the records of the private DNS server and public DNS server differently.

For example, if both a FortiMail unit (`fortimail.example.com`) operating in gateway mode and the SMTP server reside on your private network behind a router or firewall as shown in the previous diagram, and the *Use MX Record* option is enabled, then the following table shows differences between the public and private DNS servers for the authoritative DNS records of `example.com`.

Public versus private DNS records when "Use MX record" is enabled

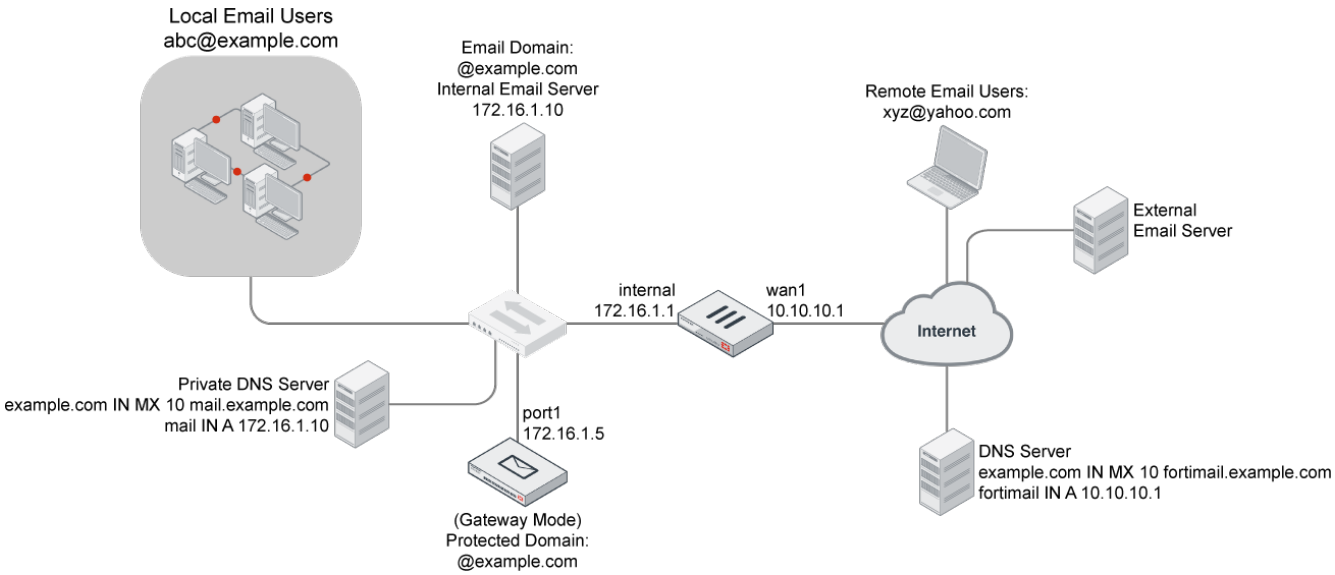
Private DNS server	Public DNS server
`example.com IN MX 10 mail.example.com`	`example.com IN MX 10 fortimail.example.com`
`mail IN A 172.16.1.10`	`fortimail IN A 10.10.10.1`
	`1 IN PTR fortimail.example.com`

If you choose to add a private DNS server, to configure the FortiMail unit to use it, go to *System* > *Network* > *DNS* in the advanced mode of the GUI.

Example 1: FortiMail unit behind a firewall

In this example, a FortiMail unit operating in gateway mode, a protected email server, a private DNS server, and email users' computers are all positioned within a private network, behind a firewall. Remote email users' computers and external email servers are located on the Internet, outside of the network protected by the firewall. The FortiMail unit protects accounts for email addresses ending in "@example.com", which are hosted on the local email server.

FortiMail unit behind a NAT device



The private DNS server is configured to locally replicate records from public DNS servers for most domains, with the exception of records for protected domains, which instead have been configured differently locally in order to support the Use MX record option.

To deploy the FortiMail unit behind a NAT device such as a firewall or router, you must complete the following:

- Configuring the firewall
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 55.

Configuring the firewall

In order to create the outgoing firewall policy that governs the IP address of the FortiMail unit, you must first define the IP address of the FortiMail unit by creating a firewall address entry.

In order to create the firewall policy that forwards email-related traffic to the FortiMail unit, you must define a static NAT mapping from a public IP address on the FortiGate unit to the private IP address of the FortiMail unit by creating a virtual IP (VIP) entry. Similarly, in order to create the firewall policy that forwards POP3/IMAP-related traffic to the protected email server, you must first define a static NAT mapping from a public IP address on the FortiGate unit to the private IP address of the protected email server by creating a virtual IP entry.

Once the firewall address and VIPs are configured, you must create firewall policies that:

- allow incoming FortiMail services that are received at the virtual IP address, then applies a static NAT when forwarding the traffic to the private network IP address of the FortiMail unit.
- allow outgoing email and other FortiMail connections from the FortiMail unit to the Internet.
- allow incoming POP3 and IMAP traffic that is received at the virtual IP address, then applies a static NAT when forwarding the traffic to the private network IP address of the protected email server.

For more information about how to configure the firewall address, virtual IPs, and firewall policies, see the FortiGate documentation.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail (SMTP) server/MTA. For local email users, this is the private network IP address of the FortiMail unit, 172.16.1.5; for remote email users, this is the virtual IP on the FortiGate unit that maps to the FortiMail unit, 10.10.10.1 or fortimail.example.com.

If you do not configure the email clients to send email through the FortiMail unit, incoming email delivered to your protected email server can be scanned, but email outgoing from your email users cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

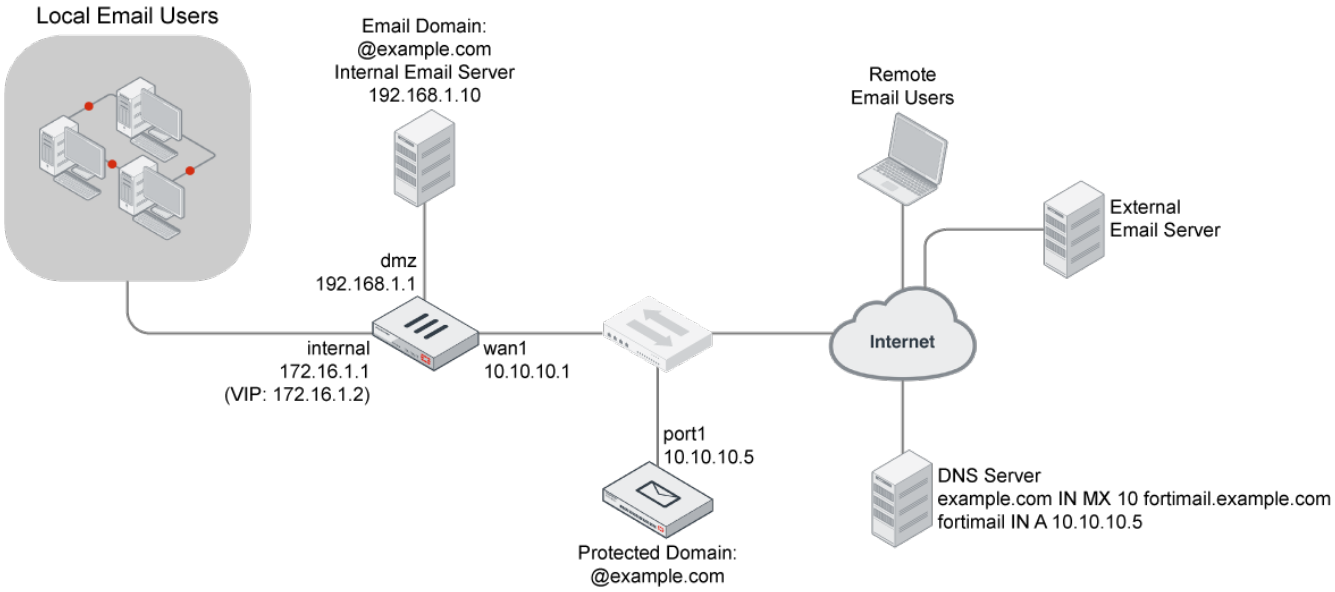
Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 2: FortiMail unit in front of a firewall

In this example, a FortiMail unit operates in gateway mode within a private network, but is separated from the protected email server and local email users' computers by a firewall. The protected email server is located on the demilitarized zone (DMZ) of the firewall. The local email users are located on the internal network of the firewall. Remote email users' computers and external email servers are located on the Internet, outside of the private network. The FortiMail unit protects accounts for email addresses ending in "@example.com," which are hosted on the local email server.

FortiMail unit in front of a NAT device



To deploy the FortiMail unit in front of a NAT device such as a firewall or router, you must complete the following:

- Configuring the firewall
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 55.

Configuring the firewall

In order to create the firewall policies that governs traffic from the IP addresses of local email users, the protected email server, and the IP address of the FortiMail unit, you must first define the IP addresses of those hosts by creating firewall address entries.

In order to create the firewall policies that forward from the FortiMail unit and local and remote email users to the protected email server, you must first define static NAT mappings from a public IP address on the FortiGate unit to the IP address of the protected email server, and from an internal IP address on the FortiGate unit to the IP address of the protected email server, by creating virtual IP entries.

With the FortiMail unit in front of a FortiGate unit, the internal network located behind the FortiGate unit, and the protected email server located on the DMZ, you must configure firewall policies to allow:

- between the internal network and the FortiMail unit
- between the internal network and protected email server
- between the protected email server and the FortiMail unit
- between the protected email server and the Internet

For more information about how to configure the firewall address, virtual IPs, and firewall policies, see the FortiGate documentation.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail (SMTP) server/MTA. For both local and remote email users, this is 10.10.10.5 or fortimail.example.com.

If you do not configure the email clients to send email through the FortiMail unit, incoming email delivered to your protected email server can be scanned, but email outgoing from your email users cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

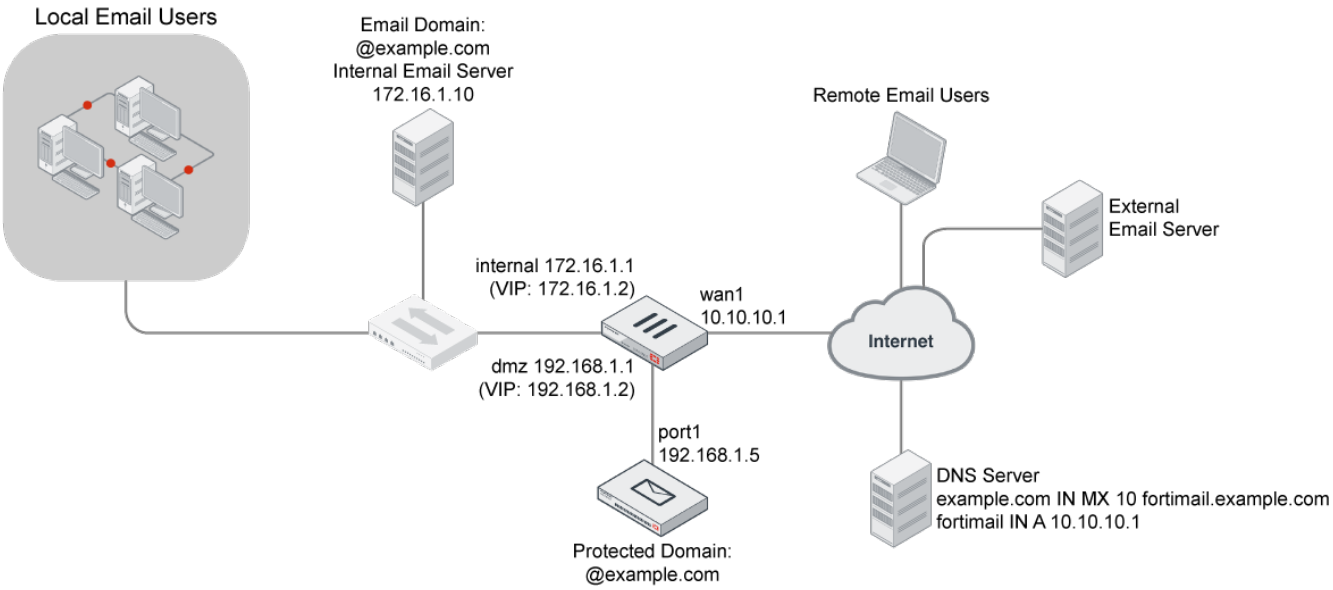
Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 3: FortiMail unit in DMZ

In this example, a FortiMail unit operating in gateway mode, a protected email server, and email users' computers are all positioned within a private network, behind a firewall. However, the FortiMail unit is located in the demilitarized zone (DMZ) of the firewall, separated from the local email users and the protected email server, which are located on the internal network of the firewall. Remote email users' computers and external email servers are located on the Internet, outside of the network protected by the firewall. The FortiMail unit protects accounts for email addresses ending in "@example.com", which are hosted on the local email server.

FortiMail unit in DMZ



To deploy the FortiMail unit in the DMZ of a firewall, you must complete the following:

- Configuring the firewall
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 55.

Configuring the firewall

In order to create the firewall policies that governs traffic from the IP addresses of local email users and the protected email server, and the IP address of the FortiMail unit, you must first define the IP addresses of those hosts by creating firewall address entries.

In order to create the firewall policy that forwards email-related traffic to the FortiMail unit, you must first define a static NAT mapping from a public IP address on the FortiGate unit to the IP address of the FortiMail unit by creating a virtual IP entry. You must also create virtual IPs to define static NAT mappings:

- from a public IP address on the FortiGate unit to the IP address of the protected email server
- from an IP address on the internal network of the FortiGate unit to the IP address of the FortiMail unit

- from an IP address on the DMZ of the FortiGate unit to the IP address of the protected email server

With the FortiMail unit in front of a FortiGate unit, and local email users and protected email server located behind the FortiGate unit on its internal network, you must configure firewall policies to allow traffic:

- between the internal network and the FortiMail unit
- between the protected email server and the Internet
- between the FortiMail unit and the Internet

For more information about how to create firewall policies, see the FortiGate documentation.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail (SMTP) server/MTA. For local email users, this is 172.16.1.2, the virtual IP on the internal network interface of the FortiGate unit that is mapped to the IP address of the FortiMail unit; for remote email users, this is 10.10.10.1 or fortimail.example.com, the virtual IP on the wan1 network interface of the FortiGate unit that is mapped to the FortiMail unit.

If you do not configure the email clients to send email through the FortiMail unit, incoming email delivered to your protected email server can be scanned, but email outgoing from your email users cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Transparent mode deployment

The following procedures and examples show you how to deploy the FortiMail unit in transparent mode.

Configuring DNS records

If the FortiMail unit is operating in transparent mode, in most cases, configuring DNS records for protected domain names is not required. Proper DNS records for your protected domain names are usually already in place. However, you must configure public DNS records for the FortiMail unit itself.

If you are unfamiliar with configuring DNS and related MX and A records, first read DNS role in email delivery on page 19.

For performance reasons, and to support some configuration options, you may also want to provide a private DNS server for exclusive use by the FortiMail unit.

This section includes the following:

- Configuring DNS records for the FortiMail unit itself
- Configuring a private DNS server

Configuring DNS records for the FortiMail unit itself

In addition to that of protected domains, the FortiMail unit must be able to receive web connections, and send and receive email, for its own domain name. Dependent features include:

- delivery status notification (DSN) email
- spam reports
- email users' access to their per-recipient quarantined mail
- FortiMail administrators' access to the GUI by domain name
- alert email
- report generation notification email

For this reason, you should also configure public DNS records for the FortiMail unit itself.

Appropriate records vary by whether or not *Web release host name/IP* (located in Security > Quarantine > Quarantine Report in the advanced mode of the GUI) is configured:

- Case 1: Web Release Host Name/IP is empty/default
- Case 2: Web Release Host Name/IP is configured

Unless you have enabled both Hide the transparent box in each protected domain and Hide this box from the mail server in each session profile, the FortiMail unit is **not** fully transparent in SMTP sessions: the domain name and IP address of the FortiMail unit may be visible to SMTP servers, and they might perform reverse lookups. For this reason, public DNS records for the FortiMail unit usually should include reverse DNS (RDNS) records.

Case 1: Web release host name/IP is empty/default

When *Web release host name/IP* is not configured (the default), the web release/delete links that appear in spam reports use the fully qualified domain name (FQDN) of the FortiMail unit.

For example, if the FortiMail unit's host name is `fortimail`, and its local domain name is `example.net`, resulting in the FQDN `fortimail.example.net`, a spam report's default web release link might look like (FQDN highlighted in bold):

```
https://fortimail.example.net
     /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
     TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

In the DNS configuration to support this and the other DNS-dependent features, you would configure the following three records:

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
```

```
1 IN PTR fortimail.example.net.
```

where:

- `example.net` is the local domain name to which the FortiMail unit belongs; in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI, email users' access to their per-recipient quarantines, to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit, and to resolve to the IP address of the FortiMail unit for the purpose of the web release/delete hyperlinks in the spam report
- `10.10.10.1` is the public IP address of the FortiMail unit

Case 2: Web release host name/IP is configured

You could configure *Web release host name/IP* to use an alternative fully qualified domain name (FQDN) such as `webrelease.example.info` instead of the configured FQDN, resulting in the following web release link (web release FQDN highlighted in bold):

```
https://webrelease.example.info
     /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
     TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

Then, in the DNS configuration to support this and the other DNS-dependent features, you would configure the following MX record, A records, and PTR record (unlike Case 1: Web Release Host Name/IP is empty/default on page 56, in this case, two A records are required; the difference is highlighted in bold):

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
webrelease IN A 10.10.10.1
1 IN PTR fortimail.example.net.
```

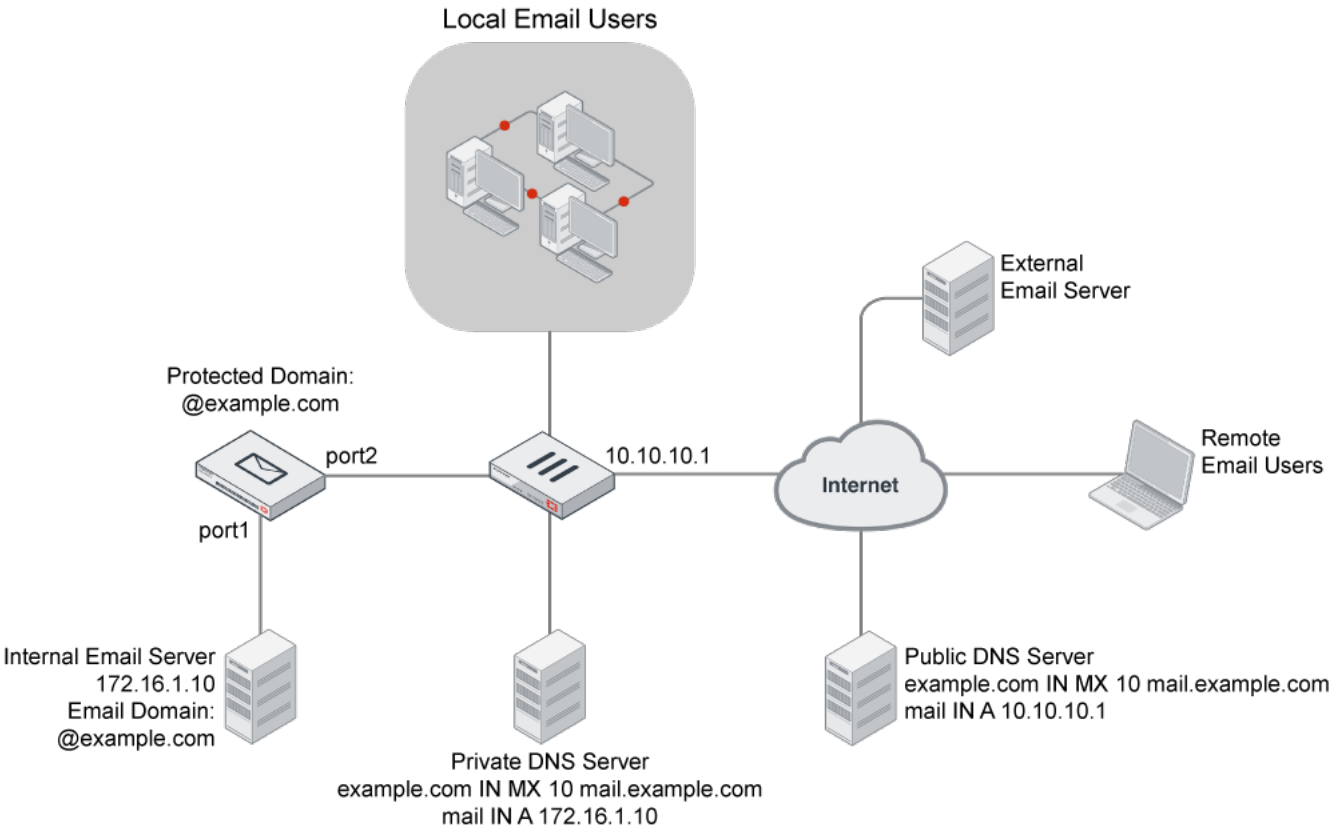
where:

- `example.net` is the local domain name to which the FortiMail unit belongs; in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI and to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit
- `webrelease` is the web release host name; in the A record of the zone file for example.info, it resolves to the IP address of the FortiMail unit for the purpose of the web release and delete hyperlinks in the spam report
- `10.10.10.1` is the public IP address of the FortiMail unit

Configuring a private DNS server

Consider providing a private DNS server on your local network to improve performance with features that use DNS queries.

Public and private DNS servers (transparent mode)



A private DNS server may be required if the following conditions are met:

- You configure the FortiMail unit to use a private DNS server.
- Both the FortiMail unit and the protected SMTP server reside on the internal network, with private network IP addresses.
- You enable the Use MX record option.

Configure the A records on the private DNS server and public DNS server differently: the private DNS server must resolve to the domain names of the SMTP servers into private IP addresses, while the public DNS server must resolve them into public IP addresses.

For example, if both a FortiMail unit (fortimail.example.com) operating in transparent mode and the SMTP server reside on your private network behind a router or firewall as illustrated in Public and private DNS servers (gateway mode) on page 57, and the *Use MX record* option is enabled, the following table illustrates differences between the public and private DNS servers for the authoritative DNS records of `example.com`.

Public versus private DNS records when *Use MX Record* is enabled

Private DNS server	Public DNS server
`example.com IN MX 10 mail.example.com`	`example.com IN MX 10 mail.example.com`
`mail IN A 172.16.1.10`	`mail IN A 10.10.10.1`
`10 IN PTR fortimail.example.com`	`1 IN PTR fortimail.example.com`

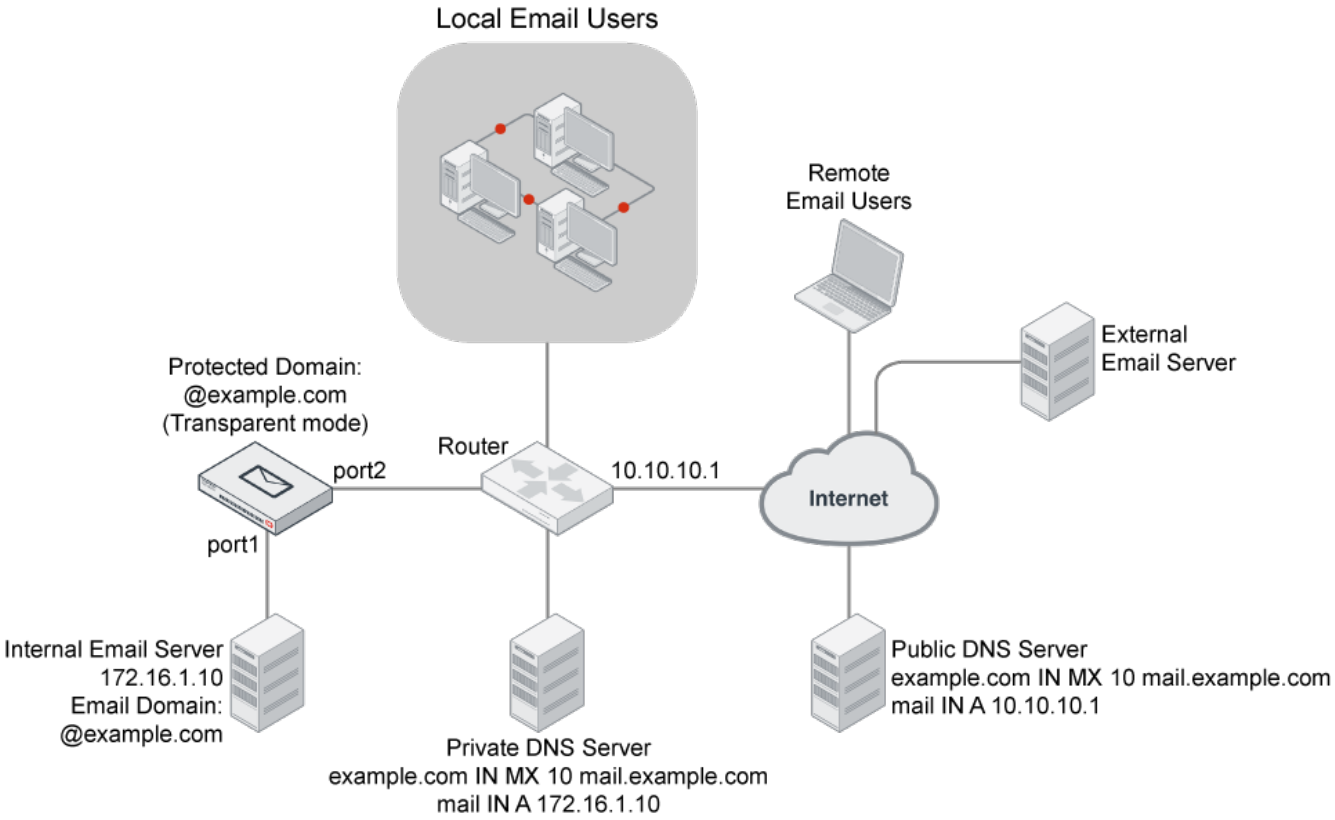
If you choose to add a private DNS server, to configure the FortiMail unit to use it, go to *System* > *Network* > *DNS* in the advanced mode of the GUI.

Example 1: FortiMail unit in front of an email server

In this example, a FortiMail unit operating in transparent mode is in front of one email server.

This example assumes that the FortiMail unit is protecting one email server. If your FortiMail unit is protecting multiple email servers and they are not on the same subnet, you must first remove some network interfaces from the bridge and configure static routes. For an example of configuring out-of-bridge network interfaces, see Removing the network interfaces from the bridge on page 79.

Transparent mode deployment to protect an email server



To deploy the FortiMail unit in front of an email server, you must complete the following:

- Configuring the protected domains and session profiles
- Configuring the proxies and implicit relay
- Testing the installation

This example assumes you have already completed the Quick Start Wizard. For details, see Running the Quick Start Wizard on page 48.

Configuring the protected domains and session profiles

When configuring the protected domain and session profiles, you can select transparent mode options to hide the existence of the FortiMail unit.

To configure the transparent mode options of the protected domain

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the domain and then click *Edit*.
3. Configure the following:

Transparent Mode Options	Description
This server is on (transparent mode only)	Select the network interface (port) to which the protected SMTP server is connected. **Note:** Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface.

Hide the transparent box (transparent mode only)	Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in:
	• the SMTP greeting (`HELO`/`EHLO`) in the envelope and in the `Received:` message headers of email messages
	• the IP addresses in the IP header
	This masks the existence of the FortiMail unit to the protected SMTP server.
	Disable to replace the SMTP client's IP address or domain name with that of the FortiMail unit.
	For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in bold):
	`Received: from 192.168.1.1 (`**`EHLO 172.16.1.1`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`[172.16.1.1]`**` with SMTP id kAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT`
	But if the option is disabled, the message headers would contain:
	`Received: from 192.168.1.1 (`**`EHLO fortimail.example.com`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`fortimail.example.com`**` with SMTP id kAOFJl4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT`
	Note: If the protected SMTP server applies rate limiting according to IP addresses, enabling this option can improve performance. The rate limit will then be separate for each client connecting to the protected SMTP server, rather than shared among all connections handled by the FortiMail unit.
	Note: Unless you have enabled Take precedence over recipient based policy match in the IP-based policy, this option has precedence over the Hide this box from the mail server option in the session profile, and may prevent it from applying to incoming email messages.

Transparent Mode Options	Description
	Note: This function does not take effect if the email is sent from protected domains to protected domains. **Note:** When this option is enabled, you cannot use IP pools for this protected domain, and you should specify an SMTP server other than the FortiMail unit for outgoing mail. For more information, see “Use client-specified SMTP server to send email” on page 285.
Use this domain’s SMTP server to deliver the mail (transparent mode only)	Enable to allow SMTP clients to send outgoing email directly through the protected SMTP server. Disable to, instead of allowing a direct connection, proxy the connection using the incoming proxy, which queues email messages that are not immediately deliverable.

4. Select OK.

To configure the transparent mode options of the session profile

1. Go to *Policy* > *IP Policy* > *IP Policy*.
2. In the *Session* column for an IP-based policy, select the name of the session profile to edit the profile.
3. Configure the following:

Connection Setting	
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 • the IP addresses in the IP header This masks the existence of the FortiMail unitto 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 have enabled Take precedence over recipient based policy match in the IP-based policy, the Hide the transparent box option in the protected domain has precedence over this option, and may prevent it from applying to incoming email messages.

4. Click *OK*.
5. Repeat the previous three steps for each IP-based policy.

Configuring the proxies and implicit relay

When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified.

Exceptions to SMTP connections that can be proxied or relayed include SMTP connections destined for the FortiMail unit itself. For those local connections, such as email messages from email users requesting deletion or release of their quarantined email, you must choose to either allow or block the connection.

You configure proxy/relay pick-up separately for incoming and outgoing connections.

For information on determining directionality, see Connection directionality versus email directionality on page 18.

In this deployment example, incoming connections arriving on port2 must be scanned before traveling to the main email server, and therefore are configured to be *Proxy* — that is, picked up by the implicit relay.

Outgoing connections arriving on port1 will contain email that has already been scanned once, during SMTP clients' relay to the main email server. Scanning outgoing connections again using either the outgoing proxy or the implicit relay would waste resources. Therefore outgoing connections will be Pass through.

To configure SMTP proxy and implicit relay pick-up

1. Go to System > Network > Interface.
2. Edit *SMTP Proxy* settings on both Port 1 and Port 2:

Port 1		
	Incoming connections	*Drop*
	Outgoing connections	*Pass through*
	Local connections	*Enable*
Port 2		
	Incoming connections	*Proxy*
	Outgoing connections	Drop
	Local connections	Disable

If *Use client-specified SMTP server to send email* is disabled under System > Mail Setting > Proxies, and an SMTP client is configured to authenticate, you must configure and apply an authentication profile. Without the profile, authentication with the built-in MTA will fail. Also, the mail server must be explicitly configured to allow relay from the built-in MTA in this case.

Testing the installation

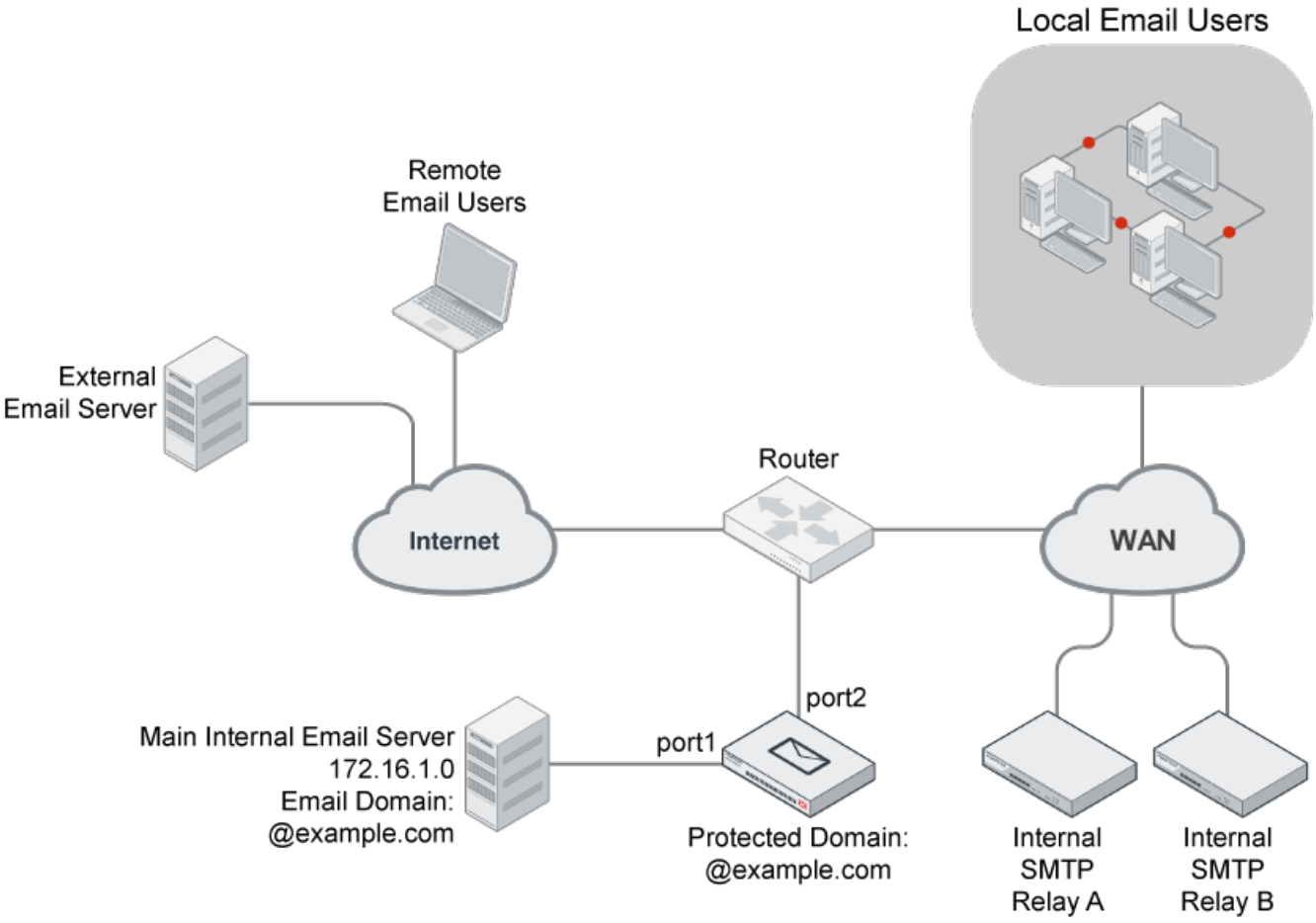
Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 2: FortiMail unit in front of an email hub

In this example, a FortiMail unit operating in transparent mode is positioned between an email gateway and other internal email servers.

When sending email with external recipients, the email servers (Relay A and Relay B) in each WAN location are required to deliver through the main email server, which encrypts outgoing SMTP connections. The firewall will only allow SMTP traffic from the main email server.

Transparent mode deployment to protect an email hub



To deploy the FortiMail unit in front of one or more email servers, you must complete the following:

- Configuring the protected domains and session profiles
- Configuring the proxies and implicit relay
- Testing the installation

This example assumes you have already completed the Quick Start Wizard. For details, see Running the Quick Start Wizard on page 48.

Configuring the protected domains and session profiles

When configuring the protected domain and session profiles, you can select transparent mode options to hide the existence of the FortiMail unit.

To configure the transparent mode options of the protected domain

1. Go to Domain & User > Domain > Domain.
2. In the row corresponding to the protected domain, select Edit.
3. Configure the following settings under *Transparent Mode Options* (transparent mode only):

GUI option	Description
This server is on (transparent mode only)	Select the network interface (port) to which the protected SMTP server is connected. **Note:** Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface.

Hide the transparent box (transparent mode only)
Note: This function does not take effect if the email is sent from protected domains to protected domains.
	Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in:
	• the SMTP greeting (`HELO`/`EHLO`) in the envelope and in the `Received:` message headers of email messages
	• the IP addresses in the IP header
	This masks the existence of the FortiMail unit to the protected SMTP server.
	Disable to replace the SMTP client's IP address or domain name with that of the FortiMail unit.
	For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in **bold**):
	`Received: from 192.168.1.1 (`**`EHLO 172.16.1.1`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`[172.16.1.1]`**` with SMTP id kAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT`
	But if the option is disabled, the message headers would contain:
	`Received: from 192.168.1.1 (`**`EHLO fortimail.example.com`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`fortimail.example.com`**` with SMTP id kAOFJl4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT`
	Note: If the protected SMTP server applies rate limiting according to IP addresses, enabling this option can improve performance. The rate limit will then be separate for each client connecting to the protected SMTP server, rather than shared among all connections handled by the FortiMail unit.

GUI option	Description
	Note: Unless you have enabled Take precedence over recipient based policy match in the IP-based policy, this option has precedence over the Hide this box from the mail server option in the session profile, and may prevent it from applying to incoming email messages. **Note:** This function does not take effect if the email is sent from protected domains to protected domains. **Note:** When this option is enabled, you cannot use IP pools for this protected domain, and you should specify an SMTP server other than the FortiMail unit for outgoing mail. For more information, see “Use client-specified SMTP server to send email” on page 285.
Use this domain’s SMTP server to deliver the mail (transparent mode only)	Enable to allow SMTP clients to send outgoing email directly through the protected SMTP server. Disable to, instead of allowing a direct connection, proxy the connection using the incoming proxy, which queues email messages that are not immediately deliverable.

4. Select OK.

To configure the transparent mode options of the session profile

1. Go to Policy > IP Policy > IP Policy.
2. In theSession column for an IP-based policy, select the name of the session profile to edit the profile.
3. Configure the following:

Connection Setting	
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 • the IP addresses in the IP header This masks the existence of the FortiMail unitto 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 have enabled Take precedence over recipient based policy match in the IP-based policy, the Hide the transparent box option in the protected domain has precedence over this option, and may prevent it from applying to incoming email messages.

4. Select OK.
5. Repeat the previous three steps for each IP-based policy.

Configuring the proxies and implicit relay

When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified.

Exceptions to SMTP connections that can be proxied or relayed include SMTP connections destined for the FortiMail unit itself. For those local connections, such as email messages from email users requesting deletion or release of their quarantined email, you must choose to either allow or block the connection.

Proxy/relay pick-up is configured separately for incoming and outgoing connections.

For information on determining directionality, see Connection directionality versus email directionality on page 18.

In this deployment example, incoming connections arriving on port2 must be scanned before traveling to the main email server, and therefore are configured to be Proxy — that is, picked up by the implicit relay.

Outgoing connections arriving on port1 will contain email that has already been scanned once, during SMTP clients' relay to the main email server. In addition, outgoing connections by the main mail server will be encrypted using TLS. Encrypted connections cannot be scanned. Therefore outgoing connections will be passed through, and neither proxied nor implicitly relayed.

To configure SMTP proxy and implicit relay pick-up

1. Go to System > Network > Interface in the advanced mode of the GUI.
2. Edit *SMTP Proxy* settings on both Port 1 and Port 2:

Port 1		
	Incoming connections	Drop
	Outgoing connections	Pass through
	Local connections	Enable
Port 2		
	Incoming connections	Proxy
	Outgoing connections	Drop
	Local connections	Disable

Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 3: FortiMail unit for an ISP or carrier

In this example, a FortiMail unit operating in transparent mode is positioned as an offshoot from the backbone or other primary traffic flow between the internal and external network. A router uses policy-based routes to redirect only SMTP

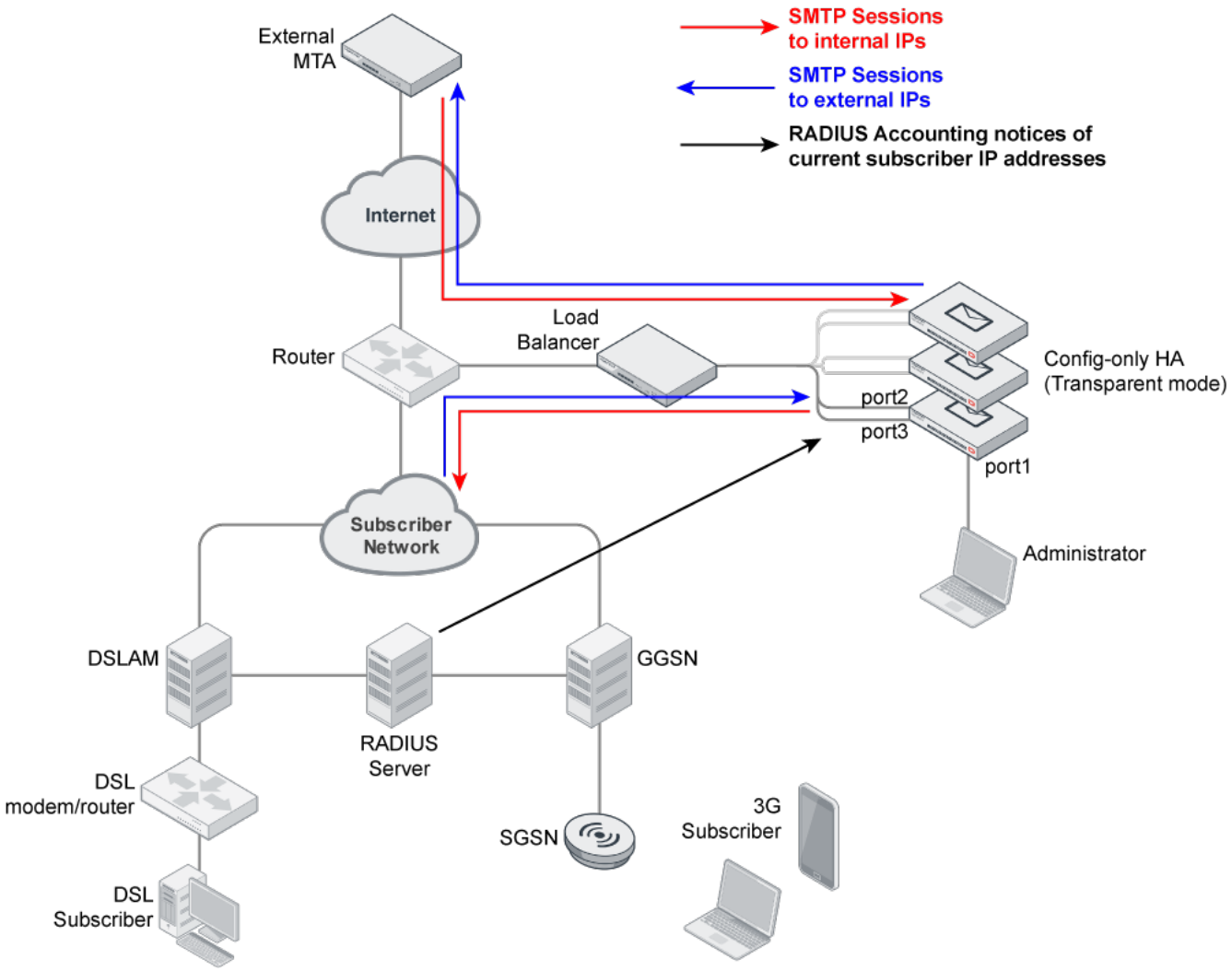
connections to the FortiMail unit, which scans the traffic before allowing legitimate connections to return the overall flow. The FortiMail unit does **not** receive non-SMTP traffic (this would result in unnecessary processing and resource usage).

For increased session-handling capacity, multiple FortiMail units could be clustered into an active-active HA group and deployed behind a load balancer that is attached to the router. Connections to the same source IP address would be handled by the same FortiMail unit to avoid sessions split among multiple units, and to maintain the accuracy of IP statistics. Otherwise, attach a single FortiMail unit to the router.

Service providers often fundamentally require transparent mode. Requiring subscribers to explicitly configure a mail relay can be problematic, and in the case of 3G mobile subscribers, impossible. Therefore gateway mode is not suitable. Transparent mode makes SMTP scanning possible without configuration by the subscriber.

A dual-arm attachment is used. This provides natural isolation of traffic before and after inspection, which can be useful if traffic requires further analysis such as packet traces by a sniffer (if you use a load balancer and it does not support the same session on two different ports, deploy the FortiMail unit using a single-arm attachment instead. For example, Foundry IronServer has been known to require single-arm attachment).

Transparent mode deployment at an ISP or carrier (with HA cluster)



Each network interface in the dual-arm attachment (port2 and port3) is removed from the Layer 2 bridge, and is configured with its own IP address. This reduces the possibility of Ethernet loops and improves compatibility with other filtering devices. Routes are configured between port2 and port3.

Because port1 cannot be removed from the bridge, and the management IP is accessible from any bridging network interface, port1 is reserved for direct connections from the administrator's computer (if the administrator's computer is not directly connected but is instead part of a management LAN, a route must also be configured for port1).

Network address translation (NAT) must **not** occur on any device between the FortiMail unit and SMTP clients, such as subscribers and external MTAs. Antispam scans involving the SMTP client's IP address, such as sender reputation, carrier endpoint reputation, session rate limits, and mail rate limits, require the ability to correctly identify each source of email by its unique IP address in order to operate correctly. NAT would interfere with this requirement.

Full transparency is configured. Popular email services such as Microsoft Hotmail may rate limit by an SMTP client's IP address in order to reduce spam. If the FortiMail unit were **not** transparent to those mail servers, all SMTP connections from your subscribers would appear to come from the FortiMail unit. The result is that external mail servers could throttle the connections of all subscribers behind the FortiMail unit. To prevent this, each individual SMTP client's IP address should be visible to external MTAs. NAT therefore would also interfere with the requirement of transparency.

Protected domains and access control rules (sometimes called access control lists or ACLs) are not configured. Instead, administrators will configure ACLs on their own internal or external MTAs.

You could configure ACLs to reject SMTP connections from specific IP addresses if required by your security policy. However, in this example, because no protected domains are configured, ACLs are not required. For connections to unprotected SMTP servers, the implicit ACL permits the connection if no other ACL is configured.

To prevent SMTP clients' access to open relays, the outgoing proxy will require all connections to be authenticated using the SMTP `AUTH` command, but will not apply authentication profiles on behalf of the SMTP servers, as no protected domains are configured. It will also not interfere with command pipelining. However, the outgoing proxy will be configured to block TLS connections, whose encryption would prevent the FortiMail unit from being able to scan the connection.

The outgoing proxy is enabled. Unlike other transparent mode deployments, because no protected domains are defined, **all** connections will be considered to be outgoing — that is, destined for an SMTP server whose IP address is not configured in the SMTP server field in a protected domain. As a result, all connections will be handled by the outgoing proxy. The built-in MTA will never be implicitly used, and the incoming proxy will never be used. If a destination SMTP server is unavailable, the outgoing proxy will refuse the connection. The FortiMail unit will not queue undeliverable mail. Instead, each SMTP client will be responsible for retrying its own delivery attempts.

Unlike other FortiMail deployments, because the ISP or carrier uses a RADIUS server to authenticate and/or track the currently assigned IP addresses of subscribers, the FortiMail unit can combat spam using the carrier endpoint reputation feature.

The FortiMail unit scans SMTP connections originating from **both** the internal and external network.

- Scanning connections from the **external** network protects subscribers from viruses and spam.
- Scanning connections from the **internal** network protects subscribers' service levels and reduces cost of operation to the ISP or carrier by preventing its public IP addresses from being added to DNS block list (DNSBL) servers.

Why should you scan email originating from the internal network?

Spammers often use a subscriber account to send spam, either by purchasing temporary Internet access or, increasingly, by infecting subscriber's computers or phones. Infected devices become part of a botnet that can be used to infect more devices, and to send spam.

Because many mail servers use DNSBL to combat spam, if a subscriber's IP address is added to a DNSBL, it can instantly cause email service interruption. If the subscriber's IP address is dynamic rather than static, when the spammer's IP address is reassigned to another subscriber, this can cause problems for an innocent subscriber. Even worse, if many subscribers on your network share a single public IP address, if that single IP address is blocklisted, all of your customers could be impacted.

Protecting the public range of IP addresses from being blocklisted is essential for service providers to be able to guarantee a service level to subscribers.

In addition to jeopardizing customer retention, spam originating from your internal network can also cost money and time. Spam consumes bandwidth and network resources. Tracking which in your block of IPs is currently blocklisted, and paying to have them de-listed, can be a significant recurring cost.

By scanning email destined for the Internet, you can thereby reduce your own costs and maximize customers' satisfaction with your service levels.

To deploy the FortiMail unit at an ISP or carrier, you must complete the following:

- Configuring the connection with the RADIUS server
- Removing the network interfaces from the bridge
- Configuring the session profiles
- Configuring the IP-based policies
- Configuring the outgoing proxy
- Testing the installation

This example assumes you have already completed the Quick Start Wizard. For details, see Running the Quick Start Wizard on page 48.

Configuring the connection with the RADIUS server

FortiMail units can use your RADIUS accounting records to combat spam and viruses. This reduces spam and viruses originating from your network, and reduces the likelihood that your public IP addresses will be blocklisted.

Unlike MTAs, computers in homes and small offices and mobile devices such as laptops and cellular phones that send email may not have a static IP address. Cellular phones' IP addresses especially may change very frequently. After a device leaves the network or changes its IP address, its dynamic IP address may be reused by another device. Because of this, a sender reputation score that is directly associated with an SMTP client's IP address may not function well. A device sending spam could start again with a clean sender reputation score simply by rejoining the network to get another IP address, and an innocent device could be accidentally blocklisted when it receives an IP address that was previously used by a spammer.

To control spam from SMTP clients with dynamic IP addresses, you may be able to use the endpoint reputation score method instead.

The endpoint reputation score method does not directly use the IP address as the SMTP client's unique identifier. Instead, it uses the subscriber ID, login ID, MSISDN, or other identifier (An MSISDN is the number associated with a mobile device, such as a SIM card on a cellular phone network). The IP address is only temporarily associated with this identifier while the device is joined to the network.

When a device joins the network of its service provider, such as a cellular phone carrier or DSL provider, it may use a protocol such as PPPoE or PPPoA which supports authentication. The network access server (NAS) queries the remote

authentication dial-in user (RADIUS) server for authentication and access authorization. If successful, the RADIUS server then creates a record which associates the device's MSISDN, subscriber ID, or other identifier with its current IP address.

The server, next acting as a RADIUS client, sends an accounting request with the mapping to the FortiMail unit (the FortiMail unit acts as an auxiliary accounting server if the endpoint reputation daemon is enabled). The FortiMail unit then stores the mappings, and uses them for the endpoint reputation feature.

When the device leaves the network or changes its IP address, the RADIUS server acting as a client requests that the FortiMail unit stop accounting (that is, remove its local record of the IP-to-MSISDN/subscriber ID mapping). The FortiMail unit keeps the reputation score associated with the MSISDN or subscriber ID, which will be re-mapped to the new IP address upon the next time that the mobile device joins the network.

The endpoint reputation feature can be used with traditional email, but it can also be used with MMS text messages.

The multimedia messaging service (MMS) protocol transmits graphics, animations, audio, and video between mobile phones. There are eight interfaces defined for the MMS standard, referred to as MM1 through MM8. MM3 uses SMTP to transmit text messages to and from mobile phones. Because it can be used to transmit content, spammers can also use MMS to send spam.

You can blocklist MSISDNs or subscriber IDs to reduce MMS and email spam.

In addition to manually blocklisting or exempting MSISDNs and subscriber IDs, you can configure automatic blocklisting based upon endpoint reputation scores. If a carrier end point sends email or text messages that the FortiMail unit detects as spam, the endpoint reputation score increases. You can configure session profiles to log or block, for a period of time, email and text messages from carrier end points whose endpoint reputation score exceeds the threshold during the automatic blocklisting window.

To configure your RADIUS server

1. On your RADIUS server, configure the FortiMail unit as an auxiliary RADIUS server, to which it will send copies when its accounting records change.
2. Specify that it should send the `Calling-Station-Id` and `Framed-IP-Address` attributes to the FortiMail unit. The data type of the value of `Calling-Station-Id` may vary. For 3G subscribers, the RADIUS server typically uses `Calling-Station-Id` to contain an MSISDN. For ADSL subscribers, the RADIUS server typically uses to contain a login ID, such as an email address.
3. Determine whether your RADIUS server sends the `Framed-IP-Address` attribute's value in network order (e.g. 192.168.1.10) or host order (e.g. 10.1.168.192).
4. Verify that routing and firewall policies permit RADIUS accounting records to reach the FortiMail unit.

To enable the FortiMail unit to receive RADIUS records

1. Connect to the CLI.
   This feature cannot be configured through the GUI. For instructions on how to connect to the CLI, see Connecting to the GUI or CLI on page 36.
2. Enter the following command to enable the FortiMail unit to receive RADIUS records by starting the endpoint reputation daemon:
```
config antispam settings
   set carrier-endpoint-status enable
end
```
3. Enter the following command to configure the RADIUS secret:
```
config antispam settings
   set carrier-endpoint-acc-secret <secret_str>
end
```

where <secret_str> is the secret configured on the RADIUS server.

4. Enter the following command to configure whether to enable or disable the FortiMail unit to validate RADIUS requests using the RADIUS secret:
```
config antispam settings
   set carrier-endpoint-acc-validate {enable | disable}
end
```
where {enable | disable} indicates your choice.
5. Enter the following command to configure whether or not the FortiMail unit will acknowledge accounting records:
```
config antispam settings
   set carrier-endpoint-acc-response {enable | disable}
end
```
where {enable | disable} indicates your choice.
6. Enter the following command to indicate that the RADIUS server will send the value of the Framed-IP-Address attribute in network order:
```
config antispam settings
   set carrier-endpoint-framed-ip-order {host-order | network-order}
end
```
where {host-order | network-order} indicates your choice (most RADIUS servers use network order).

Removing the network interfaces from the bridge

In transparent mode, by default, network interfaces are members of a Layer 2 bridge, and have no IP addresses of their own. To connect to the GUI, administrators connect to any network interface that is a member of the bridge, using the management IP.

In this deployment example, only port1 will remain a member of the bridge. Administrators will directly connect their computer to that network interface in order to access the GUI or CLI. The network interfaces through which SMTP traffic passes, port2 and port3, will have their own IP addresses, and will not act as a Layer 2 bridge. As a result, the management IP will not be accessible from port2 and port3. In addition, all administrative access protocols will be disabled on port2 and port3 to prevent unauthorized administrative access attempts from the subscriber and external networks.

Both port2 and port3 will be connected to the same router, and do not require additional static routes.

To remove port2 and port3 from the bridge

1. Go to System > Network > Interface.
2. Double-click port2 to edit it.
3. Enable Do not associate with management IP.
The network interface will be removed from the bridge, and may be configured with its own IP address.
4. In IP/Netmask, type the IP address and netmask of the network interface.
5. Under Advanced Setting, next to Access, disable **all** administrative access protocols, including HTTPS, SSH, and PING.
6. Next to Administrative status, select Up.
7. Select OK.
8. Repeat this procedure for port3.

Configuring the session profiles

When configuring the protected domain and session profiles, you can select transparency, encryption, authentication, and antispam IP-based reputation settings that will be applied by an IP-based policy.

In this deployment example, you configure two session profiles:

- a profile for connections from subscribers
- a profile for connections from SMTP clients on the external network

FortiMail applies each profile in the IP-based policy that governs connections from either the subsurface or external network.

In both profiles, TLS-encrypted connections are not allowed in order to prevent viruses from entering or leaving the subscriber network, since encrypted connections cannot be scanned. Authentication is required to prevent spammers from connecting to open relays. No protected domains are configured, and so transparency will be configured through the session profiles alone. This will hide the existence of the FortiMail unit to all SMTP clients.

Because subscribers use dynamic IP addresses, instead of sender reputation, endpoint reputation is used in the subscribers' session profile to score their trustworthiness. Endpoint reputation scans use RADIUS accounting notices from your RADIUS server to map subscriber end point identifiers or MSISDNs to their current IP address. Subscribers who have a reputation for sending spam or viruses will be blocked, thereby reducing the risk that your public IP addresses could be blocklisted by DNS block list (DNSBL) services.

Sender reputation, which functions best with static IP addresses and does not require a RADIUS server, will be used in the external networks' session profile to score SMTP clients on external networks. This will help to prevent viruses and spam from reaching your subscribers.

To configure the session profile for connections from external SMTP clients

1. Go to Profile > Session > Session in the advanced mode of the GUI.
2. Select New.
3. In Profile name, type a name for the session profile, such as `external_session_profile`.
4. Configure the following:

Connection Setting	
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 • the IP addresses in the IP header This masks the existence of the FortiMail unitto the protected SMTP server.
Sender Reputation	
Enable sender reputation	Enable to accept or reject email based upon sender reputation scores.
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. The enforced rate limit is either **Restrict number of email per hour to n** or **Restrict email to n percent of the previous hour**, whichever value is greater.

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 n percent of 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.
Reject client at	Enter a sender reputation score over which the FortiMail unit will return a permanent rejection error when the SMTP client attempts to initiate a connection.
Session Setting	
Prevent encryption of the session (transparent mode only)	Enable to block `STARTTLS`/MD5 commands so that email connections cannot be TLS-encrypted.
Unauthenticated Session Setting	
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 their domain could be blocklisted by other SMTP servers.

5. Select Create.

To configure the session profile for connections from internal SMTP clients

1. Go to Profile > Session > Session in the advanced mode of the GUI.
2. Select New.
3. In Profile name, type a name for the session profile, such as `internal_session_profile`.
4. Configure the following:

Connection Setting	
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 • the IP addresses in the IP header This masks the existence of the FortiMail unitto the protected SMTP server.
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, if enabled, the FortiGuard AntiSpam service. This option applies only if you have enabled *Use client-specified SMTP server to send email*, and only for outgoing connections.
Endpoint Reputation	

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.
Action	Select either: • **Reject**: Reject email and MMS messages from MSISDNs/subscriber IDs whose endpoint reputation scores exceed Auto blocklist score trigger value. • **Monitor**: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose endpoint reputation scores exceed Auto blocklist score trigger value. Log entries appear in the history log.
Auto blocklist score trigger value	Enter the endpoint 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.
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.
Session Setting	
Prevent encryption of the session (transparent mode only)	Enable to block STARTTLS/MD5 commands so that email connections cannot be TLS-encrypted.
Unauthenticated Session Setting	
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 their domains could be blocklisted by other SMTP servers.

Configuring the IP-based policies

Session profiles are applied to IP-based policies governing SMTP client connections.

In this deployment example, two IP-based policies are configured. The first policy governs connections from the internal subscriber network. The second policy matches all other connections that did not match the first policy, and will therefore govern connections from the external network.

To configure the IP-based policy for connections from internal SMTP clients

1. Go to Policy > IP Policy > IP Policy in the advanced mode of the GUI.
2. Select New.
3. In Source IP/Netmask, type the IP address and netmask of your subscriber network.
4. In Destination, type `0.0.0.0/0` to match all SMTP server IP addresses.
5. From Session, select internal_session_profile.
6. From AntiSpam, select the name of an antispam profile. When this profile detects spam, it will affect the subscriber's endpoint reputation score.

7. From AntiVirus, select the name of an antivirus profile. When this profile detects a virus, it will affect the subscriber's endpoint reputation score.
8. Select Create.

   The internal network policy appears at the bottom of the list of IP-based policies. Policies are evaluated in order until a policy is found that matches the connection.

   Because the default IP-based policy (`0.0.0.0/0 --> 0.0.0.0/0`) matches all connections, and because it is first in the list, in order for connections to be able to match the new policy, you must move the new policy to an index number **above** the default policy.

To move a policy

1. Select the new IP policy and click Move.
   A menu appears with four choices: Down, Up, after, Before.
2. Do one of the following:

- Select Up to move it one position in that direction and repeat the movement until the new record is in the top position.
- Select Before. A dialog appears.
  - In the field beside Move right before, enter 1.
  - Click OK.

Your new policy for internal SMTP clients should now appear above the default policy, in the row whose index number is 1.

To configure the IP-based policy for connections from external SMTP clients

1. Go to Policy > IP Policy > IP Policy in the advanced mode of the GUI.
2. Select Edit for the default policy whose Match column contains `0.0.0.0/0 --> 0.0.0.0/0`.
3. From Session, select external_session_profile.
4. From AntiSpam, select the name of an antispam profile. When this profile detects spam, it will affect the SMTP client's sender reputation score.
5. From AntiVirus, select the name of an antivirus profile. When this profile detects a virus, it will affect the SMTP client's sender reputation score.
6. Select OK.

Configuring the outgoing proxy

When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified.

Exceptions to SMTP connections that can be proxied or relayed include SMTP connections destined for the FortiMail unit itself. For those local connections, such as email messages from email users requesting deletion or release of their quarantined email, you must choose to either allow or block the connection.

Proxy pick-up is configured separately for incoming and outgoing connections.

For information on determining directionality, see Connection directionality versus email directionality on page 18.

In this deployment example, there are no protected domains; therefore, all connections are outgoing. In addition, per-domain and per-recipient Bayesian databases and per-recipient quarantines do not exist and, therefore, the FortiMail unit does not need to receive local SMTP connections in order to train databases or delete or release a domain's recipient's quarantined email.

The FortiMail unit must not expend resources to queue undeliverable email, nor reroute connections, and therefore it must not implicitly use its built-in MTA. Instead, it must always use its outgoing proxy by enabling Use client-specified SMTP server to send email under System > Mail Setting > Proxies. Because port1 is used exclusively for administration, the outgoing proxy must be configure to pick up outgoing connections only on port2 and port3.

To configure outgoing proxy pick-up

1. Go to System > Mail Setting > Proxies in the advanced mode of the GUI.
2. Enable Use client-specified SMTP server to send email.
3. Go to System > Network > Interface.
4. Edit *SMTP Proxy* settings on both port 2 and port 3:

Port 2		
	Incoming connections	Drop
	Outgoing connections	Proxy
	Local connections	Disable
Port 3		
	Incoming connections	Drop
	Outgoing connections	Proxy
	Local connections	Disable

Configuring policy-based routes on the router

After you have configured the FortiMail settings, you must create policy routes on the router to redirect the SMTP traffic (from and to the subscribers) to the FortiMail unit for scanning.

For example, on the FortiGate unit as the firewall, you can create two routes: one for the external-to-subscribers SMTP traffic and one for the subscribers-to-external SMTP traffic.

For details, see the FortiGate Handbook on https://docs.fortinet.com.

Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Unlike other deployments, this deployment requires that SMTP clients be configured to use the SMTP `AUTH` command, and not to use TLS. Before testing, you should verify that SMTP clients that will connect for themselves through the FortiMail unit meet those requirements. If some subscribers require TLS or do not use authentication, consider first making separate session profiles and IP-based policies for those subscribers.

Server mode deployment

The following procedures and examples show you how to deploy the FortiMail unit in server mode.

- Configuring DNS records
- Example 1: FortiMail unit behind a firewall
- Example 2: FortiMail unit in front of a firewall
- Example 3: FortiMail unit in DMZ

Configuring DNS records

You must configure public DNS records for the protected domains and for the FortiMail unit itself.

If you are unfamiliar with configuring DNS and related MX and A records, first read DNS role in email delivery on page 19.

For performance reasons, you may also want to provide a private DNS server for use exclusively by the FortiMail unit.

This section includes the following:

- Configuring DNS records for protected domains
- Configuring DNS records for the FortiMail unit itself
- Configuring a private DNS server

Configuring DNS records for protected domains

Regardless of your private network topology, in order for external MTAs to deliver email to the FortiMail unit, you must configure the public MX record for each protected domain to indicate that the FortiMail unit is its email server.

For example, if the fully qualified domain name (FQDN) of the FortiMail unit is fortimail.example.com, and example.com is a protected domain, the MX record for example.com would be:

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

If your FortiMail unit will operate in server mode, configure the MX record to refer to the FortiMail unit, and remove other MX records. If you fail to do so, external MTAs may not be able to deliver email to or through the FortiMail unit, or may be able to bypass the FortiMail unit by using the other MX records. If you have configured secondary MX records for failover reasons, consider configuring FortiMail high availability (HA) instead. For details, see FortiMail high availability on page 34.

An A record must also exist to resolve the host name of the FortiMail unit into an IP address.

For example, if the MX record indicates that fortimail.example.com is the email gateway for a domain, you must also configure an A record in the example.com zone file to resolve fortimail.example.com into a public IP address:

```
fortimail IN A 10.10.10.1
```

where `10.10.10.1` is either the public IP address of the FortiMail unit, or a virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit.

If your FortiMail unit will relay outgoing email, you should also configure the public reverse DNS record. The public IP address of the FortiMail unit, or the virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit, should be globally resolvable into the FortiMail unit's FQDN. If it is not, reverse DNS lookups by external SMTP servers will fail.

For example, if 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.

Configuring DNS records for the FortiMail unit itself

In addition to that of protected domains, the FortiMail unit must be able to receive web connections, and send and receive email, for its own domain name. Dependent features include:

- delivery status notification (DSN) email
- spam reports
- email users' access to their per-recipient quarantines
- FortiMail administrators' access to the GUI by domain name
- alert email
- report generation notification email

For this reason, you should also configure public DNS records for the FortiMail unit itself.

Appropriate records vary by whether or not *Web release host name/IP* (located in Security > Quarantine > Quarantine Report in the advanced mode of the GUI) is configured:

- Case 1: Web release host name/IP is empty/default on page 86
- Case 2: Web release host name/IP is configured on page 87

Case 1: Web release host name/IP is empty/default

If Web release host name/IP is not configured (the default), the web release/delete links that appear in spam reports will use the fully qualified domain name (FQDN) of the FortiMail unit.

For example, if the FortiMail unit's host name is `fortimail`, and its local domain name is `example.net`, resulting in the FQDN `fortimail.example.net`, a spam report's default web release link might look like (FQDN highlighted in bold):

```
https://fortimail.example.net
      /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
      TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

In the DNS configuration to support this and the other DNS-dependent features, you would configure the following three records:

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
1 IN PTR fortimail.example.net.
```

where:

- `example.net` is the local domain name to which the FortiMail unit belongs; in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI, email users' access to their per-recipient quarantines, to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit, and to resolve to the IP address of the FortiMail unit for the purpose of the web release/delete hyperlinks in the spam report
- `10.10.10.1` is the public IP address of the FortiMail unit

Case 2: Web release host name/IP is configured

You could configure Web release host name/IP to use an alternative fully qualified domain name (FQDN) such as `webrelease.example.info` instead of the configured FQDN, resulting in the following web release link (web release FQDN highlighted in bold):

```
https://webrelease.example.info
      /releasecontrol?release=0%3Auser2%40example.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRp
      TWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%3D%3D%3Abf3db63dab53a291ab53a291ab53a291
```

Then, in the DNS configuration to support this and the other DNS-dependent features, you would configure the following MX record, A records, and PTR record (unlike Case 1: Web Release Host Name/IP is empty/default on page 56, in this case, two A records are required; the difference is highlighted in bold):

```
example.net IN MX 10 fortimail.example.net
fortimail IN A 10.10.10.1
webrelease IN A 10.10.10.1
1 IN PTR fortimail.example.net.
```

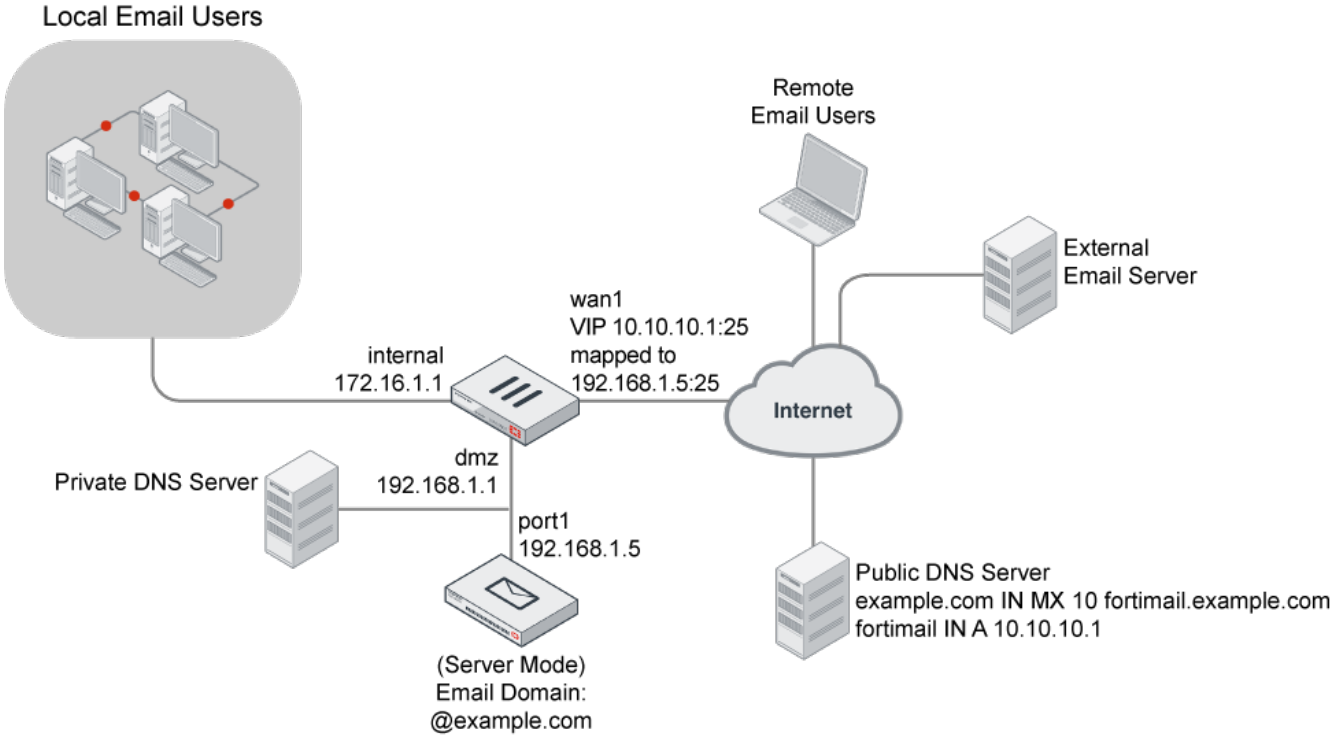
where:

- `example.net` is the local domain name to which the FortiMail unit belongs in the MX record, it is the local domain for which the FortiMail is the mail gateway
- `fortimail.example.net` is the FQDN of the FortiMail unit
- `fortimail` is the host name of the FortiMail unit; in the A record of the zone file for example.net, it resolves to the IP address of the FortiMail unit for the purpose of administrators' access to the GUI and to resolve the FQDN referenced in the MX record when email users send Bayesian and quarantine control email to the FortiMail unit
- `webrelease` is the web release host name; in the A record of the zone file for example.info, it resolves to the IP address of the FortiMail unit for the purpose of the web release/delete hyperlinks in the spam report
- `10.10.10.1` is the public IP address of the FortiMail unit

Configuring a private DNS server

In addition to the public DNS server, consider providing a private DNS server on your local network to improve performance with features that use DNS queries.

Public and private DNS servers (server mode)



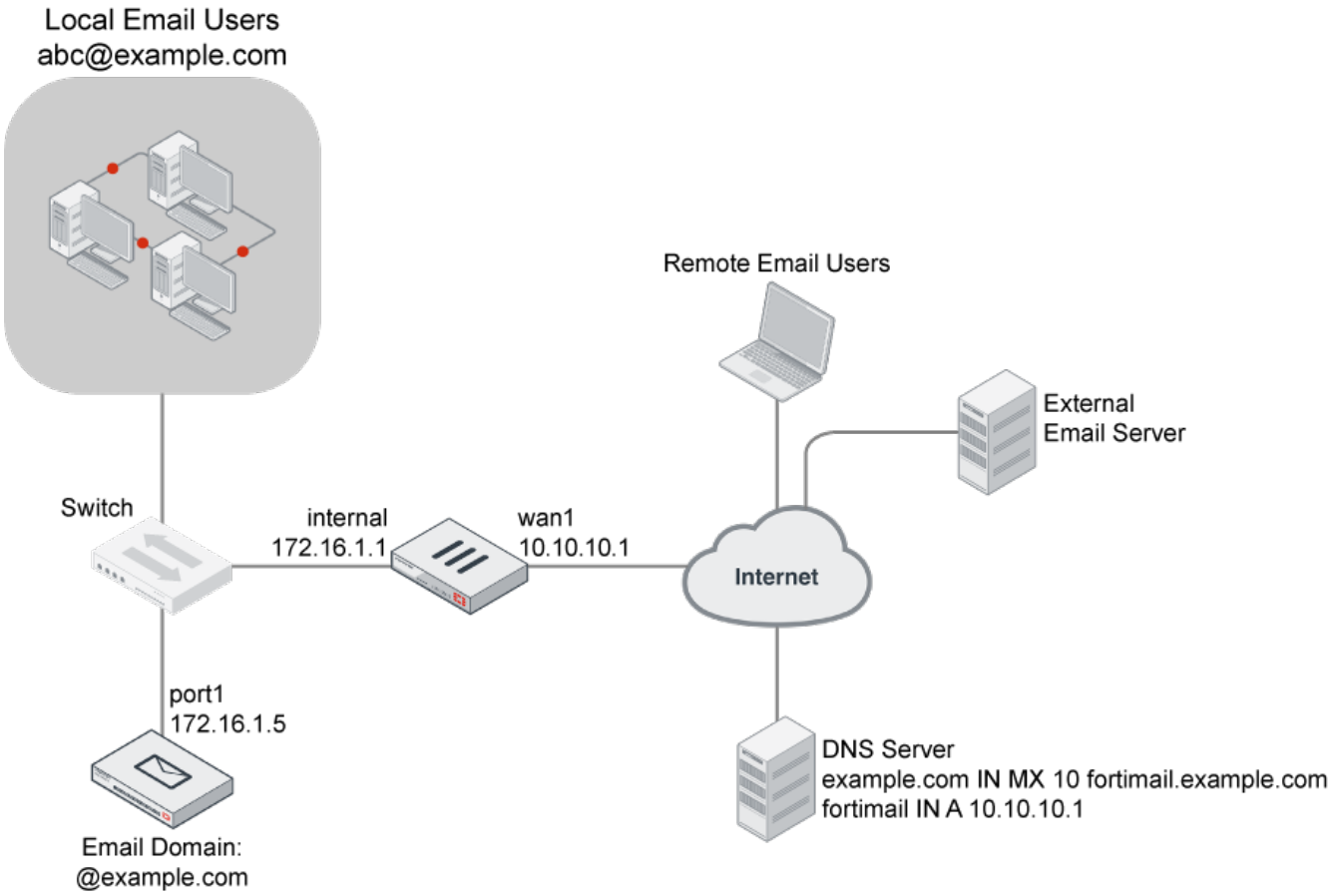
If the FortiMail unit is operating in server mode, the private DNS server should contain identical records to a public DNS server.

If you choose to add a private DNS server, to configure the FortiMail unit to use it, go to System > Network > DNS in the advanced mode of the GUI.

Example 1: FortiMail unit behind a firewall

In this example, a FortiMail unit operating in server mode and email users' computers are both positioned within a private network, behind a firewall. Remote email users' computers and external email servers are located on the Internet, outside of the network protected by the firewall. The FortiMail unit hosts and protects accounts for email addresses ending in "@example.com".

Server mode deployment behind a NAT device



To deploy the FortiMail unit behind a NAT device such as a firewall or router, you must complete the following:

- Configuring the firewall
- Configuring the email user accounts
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 85.

Configuring the firewall

In order to create the outgoing firewall policy that governs the IP address of the FortiMail unit, you must first define the IP address of the FortiMail unit by creating a firewall address entry.

In order to create the firewall policy that forwards email-related traffic to the FortiMail unit, you must first define a static NAT mapping from a public IP address on the FortiGate unit to the IP address of the FortiMail unit by creating a virtual IP entry.

Once the firewall address and VIPs are configured, you must create firewall policies that

- allow incoming email and other FortiMail services that are received at the virtual IP address, then applies a static NAT when forwarding the traffic to the private network IP address of the FortiMail unit.
- allow outgoing email and other connections from the FortiMail unit to the Internet.

For more information about how to configure the firewall address, virtual IPs, and firewall policies, see the FortiGate documentation.

Configuring the email user accounts

Create email user accounts for each protected domain on the FortiMail unit.

You may choose to create additional email user accounts later, but you should create at least one email user account for each protected domain that you can use in order to verify connectivity for the domain.

To add an email user (Server mode only)

1. Go to *Domain & User* > *User* > *User*.
2. From the Domain list, select example.com.
3. Either select New to add an email user, or double-click an email user you want to modify.
   A dialog appears.
4. In User name, enter the user name portion, such as `user1`, of the email address that will be locally deliverable on the FortiMail unit (user1@example.com).
5. Select Password, then enter the password for this email account.
6. In Display Name, enter the name of the user as it should appear in a MUA, such as `"Test User 1"`.
7. Select Create for a new user or OK for an existing user.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the private network IP address of the FortiMail unit, 172.16.1.5; for remote email users, this is the virtual IP on the FortiGate unit that maps to the FortiMail unit, 10.10.10.1 or fortimail.example.com.

If you do not configure the email clients to send email through the FortiMail unit, incoming email can be scanned, but outgoing email cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

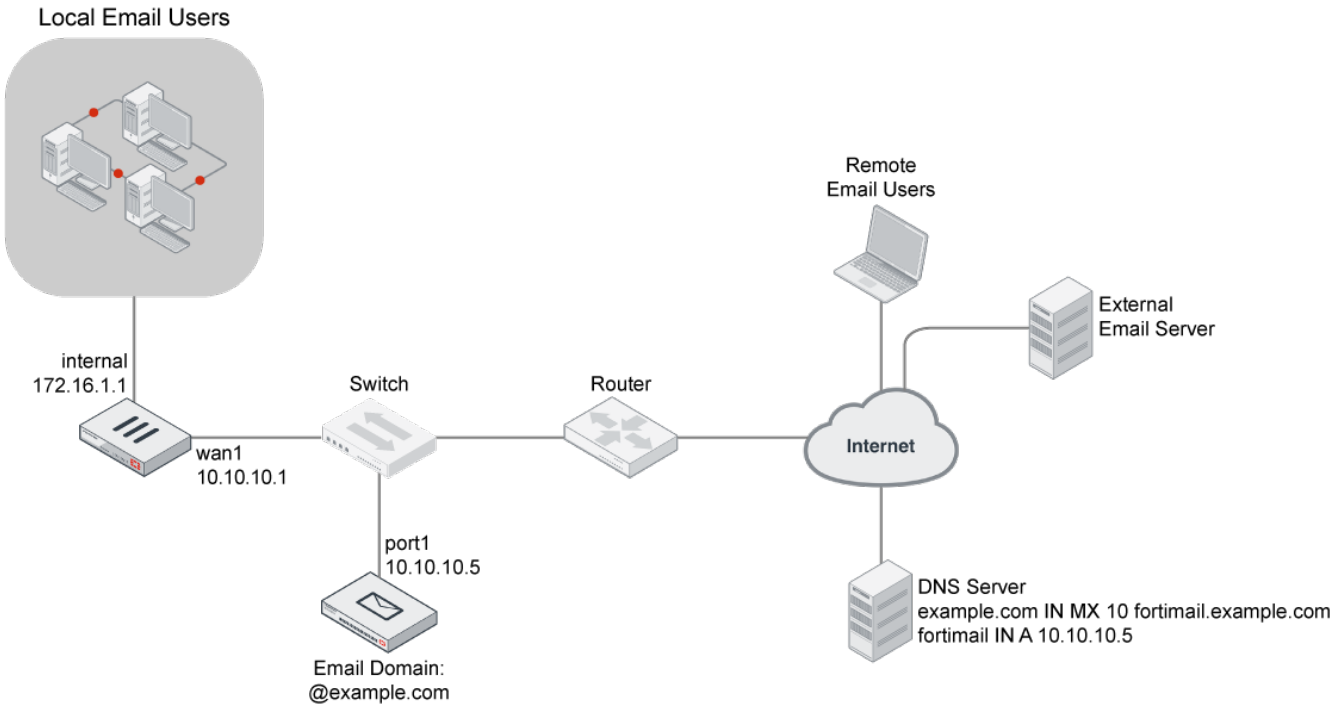
Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 2: FortiMail unit in front of a firewall

In this example, a FortiMail unit operating in server mode within a private network, but is separated from local email users' computers by a firewall. Remote email users' computers and external email servers are located on the Internet, outside of the private network. The FortiMail unit hosts and protects accounts for email addresses ending in "@example.com".

Server mode deployment in front of a NAT device



To deploy the FortiMail unit in front of a NAT device such as a firewall or router, you must complete the following:

- Configuring the firewall
- Configuring the email user accounts
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 85.

Configuring the firewall

In order to create the outgoing firewall policy that governs traffic from the IP addresses of local email users to the IP address of the FortiMail unit, you must first define the IP addresses of the local email users and the FortiMail unit by creating firewall address entries.

Once the firewall address is configured, create a firewall policy that allows outgoing email and other FortiMail connections from the local email users to the FortiMail unit.

For more information about how to configure the firewall address and firewall policies, see the FortiGate documentation.

Configuring the email user accounts

Create email user accounts for each protected domain on the FortiMail unit.

You may choose to create additional email user accounts later, but you should create at least one email user account for each protected domain in order to verify connectivity for the domain.

To add an email user (Server mode only)

1. Go to *Domain & User* > *User* > *User*.
2. From the Domain list, select example.com.
3. Either select New to add an email user, or double-click an email user you want to modify.
   A dialog appears.
4. In User Name, enter the user name portion, such as `user1`, of the email address that will be locally deliverable on the FortiMail unit (user1@example.com).
5. Select Password, then enter the password for this email account.
6. In Display Name, enter the name of the user as it should appear in a MUA, such as `"Test User 1"`.
7. Select Create for a new user or OK for an existing user.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the virtual IP address on the FortiGate unit that maps to the FortiMail unit, 172.16.1.2; for remote email users, this is the public IP address of the FortiMail unit, 10.10.10.5 or fortimail.example.com.

If you do not configure the email clients to send email through the FortiMail unit, incoming email can be scanned, but outgoing email cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

Testing the installation

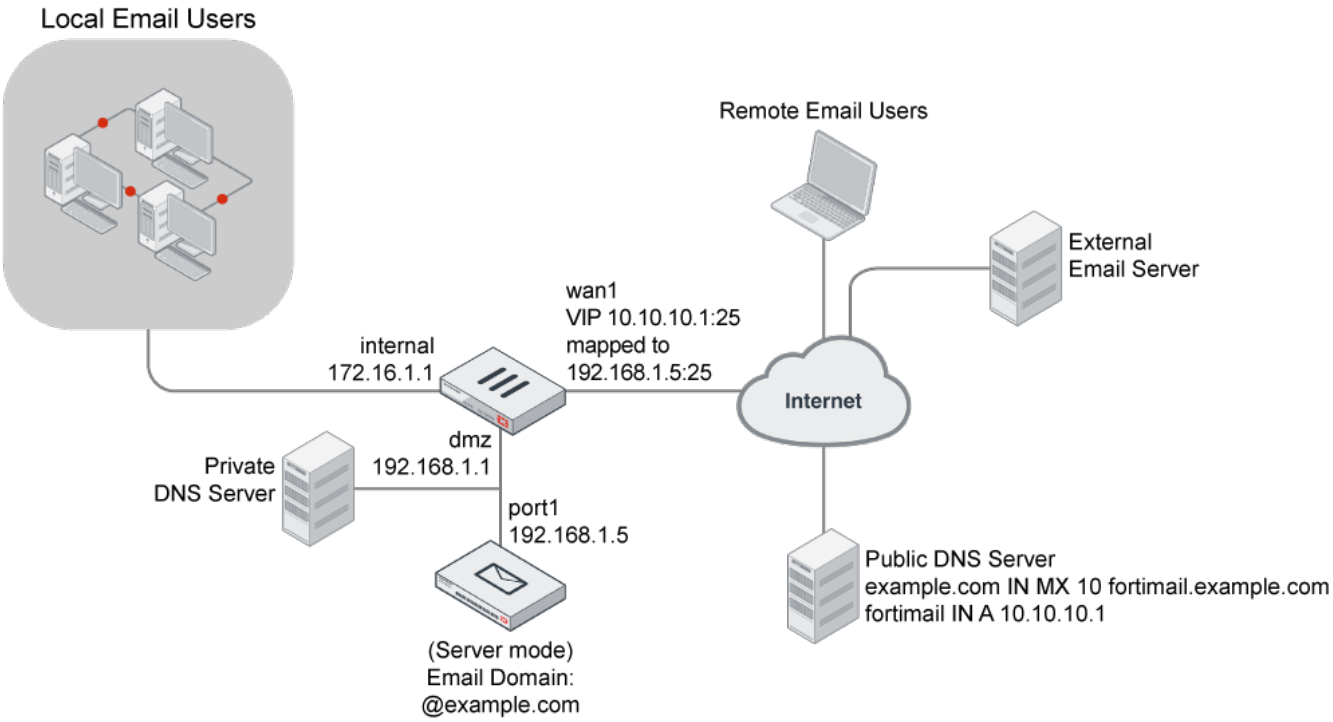
Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

Example 3: FortiMail unit in DMZ

In this example, a FortiMail unit operates in server mode within the demilitarized zone (DMZ). It is protected by a firewall but also separated from local email users' computers by it. Remote email users' computers and external email servers

are located on the Internet, outside of the private network. The FortiMail unit hosts and protects accounts for email addresses ending in “@example.com”.

Server mode deployment in a DMZ



To deploy the FortiMail unit in the DMZ of a NAT device such as a firewall or router, you must complete the following:

- Configuring the firewall
- Configuring the email user accounts
- Configuring the MUAs
- Testing the installation

This example assumes you have already completed the Quick Start Wizard and configured records on the DNS server for each protected domain. For details, see Running the Quick Start Wizard on page 48 and Configuring DNS records on page 85.

Configuring the firewall

In order to create the firewall policies that govern traffic to and from the IP addresses of local email users and the IP address of the FortiMail unit, you must first define the IP addresses of the local email users and the IP address of the FortiMail unit by creating firewall address entries.

In order to create the firewall policies that forward email-related traffic to the FortiMail unit from the internal network and from the Internet, you must first define two static NAT mappings:

- from a public IP address on the FortiGate unit to the IP address of the FortiMail unit
- from a virtual IP address on the 172.16.1.* network to the IP address of the FortiMail unit by creating a virtual IP entries

Once the firewall address and VIPs are configured, you must create firewall policies that:

- allow incoming email and other FortiMail services that are received at the virtual IP address, then applies a static NAT when forwarding the traffic to the private network IP address of the FortiMail unit.
- allow outgoing email and other FortiMail connections from the FortiMail unit to the Internet.
- allow outgoing email and other FortiMail connections from the local email users to the FortiMail unit.

For more information about how to configure the firewall address, virtual IPs, and firewall policies, see the FortiGate documentation.

Configuring the email user accounts

Create email user accounts for each protected domain on the FortiMail unit.

You may choose to create additional email user accounts later, but you should create at least one email user account for each protected domain in order to verify connectivity for the domain.

To add an email user (Server mode only)

1. Go to *Domain & User* > *User* > *User*.
2. From the Domain list, select example.com.
3. Either select New to add an email user, or double-click an email user you want to modify.
   A dialog appears.
4. In User Name, enter the user name portion, such as `user1`, of the email address that will be locally deliverable on the FortiMail unit (user1@example.com).
5. Select Password, then enter the password for this email account.
6. In Display Name, enter the name of the user as it should appear in a MUA, such as `"Test User 1"`.
7. Select Create for a new user or OK for an existing user.

Configuring the MUAs

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the FortiMail address, 192.168.1.5; for remote email users, this is the virtual IP address on the wan1 network interface of the FortiGate unit that maps to the FortiMail unit, 10.10.10.1 or fortimail.example.com.

If you do not configure the email clients to send email through the FortiMail unit, incoming email can be scanned, but outgoing email cannot.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see Testing the installation on page 95.

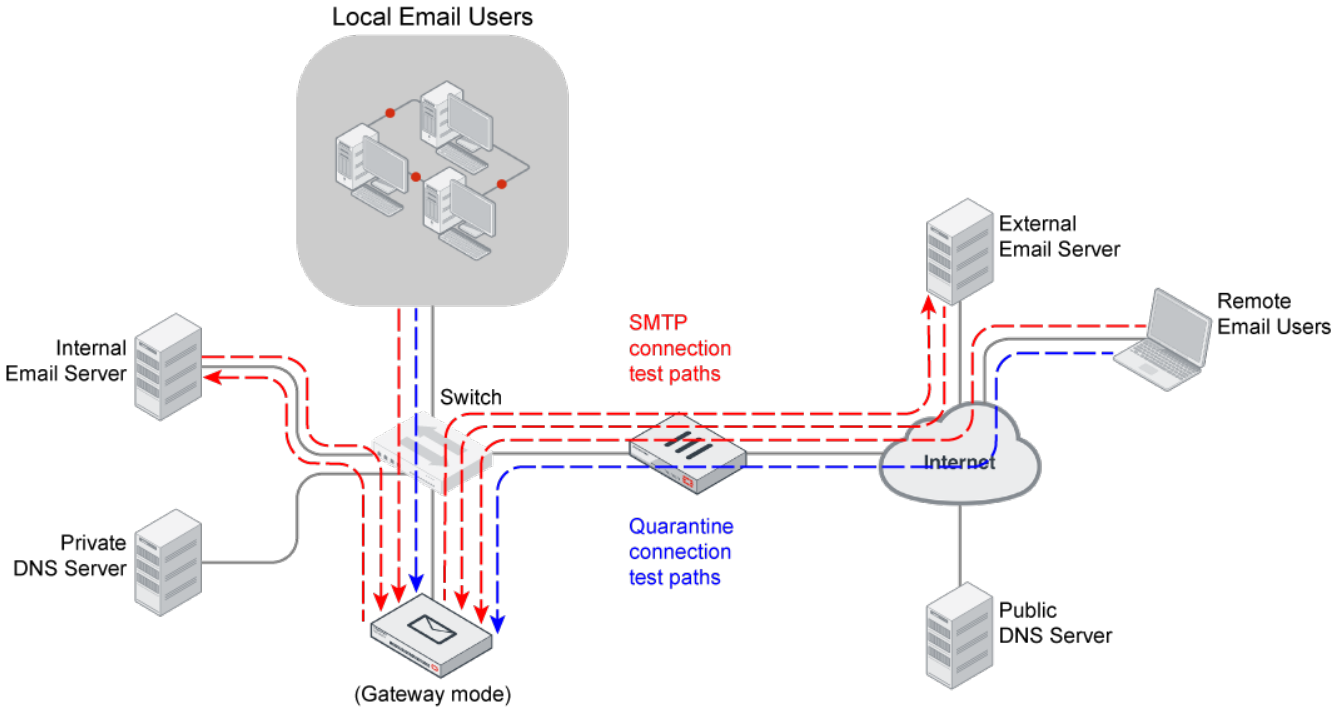
Testing the installation

After completing the installation, test it by sending email between legitimate SMTP clients and servers at various points within your network topology.

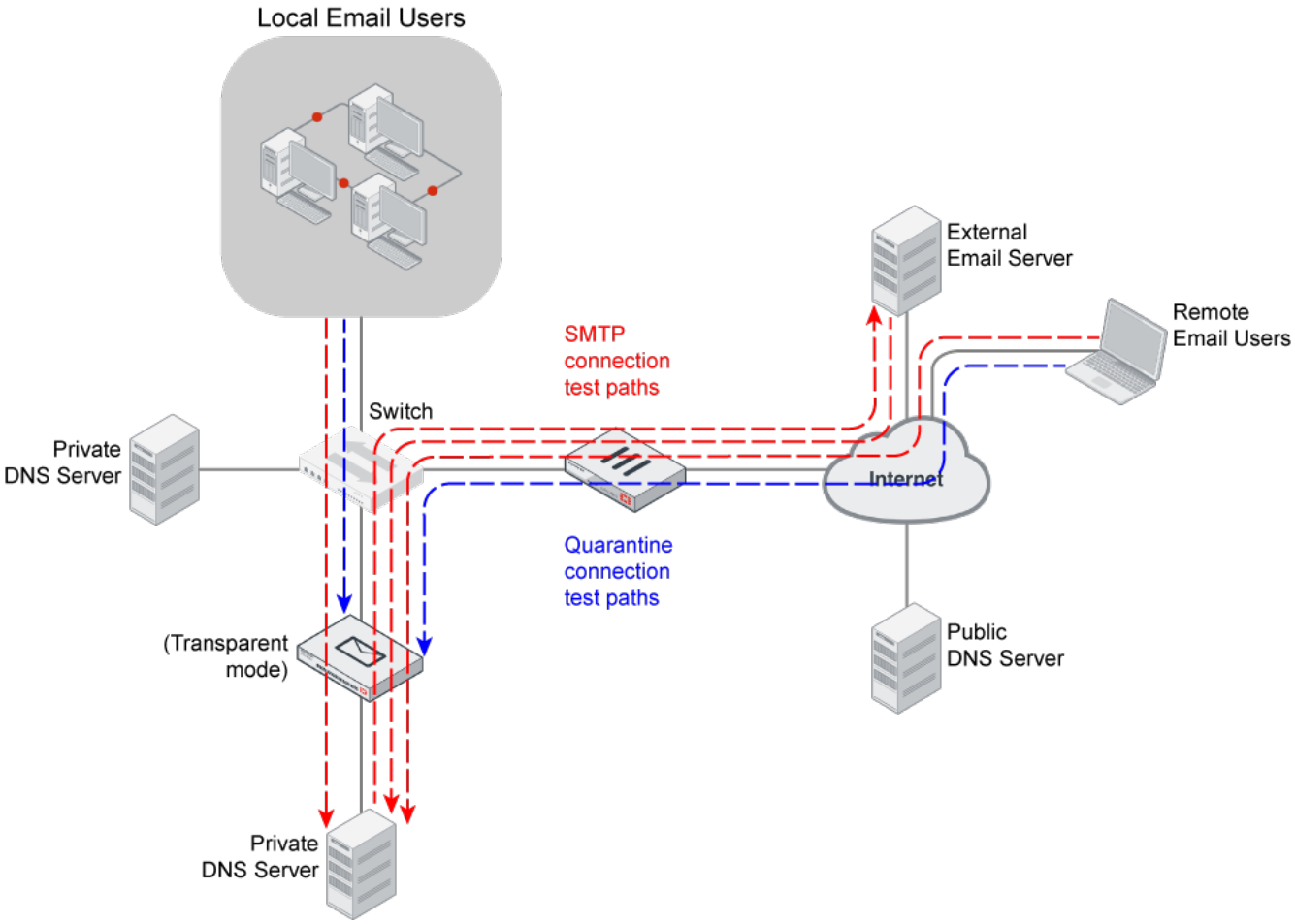
If the FortiMail unit is operating in gateway mode or transparent mode, you may also wish to test access of email users to their per-recipient quarantined email.

If the FortiMail unit is operating in server mode, you may also wish to test access to FortiMail webmail, POP3, and/or IMAP.

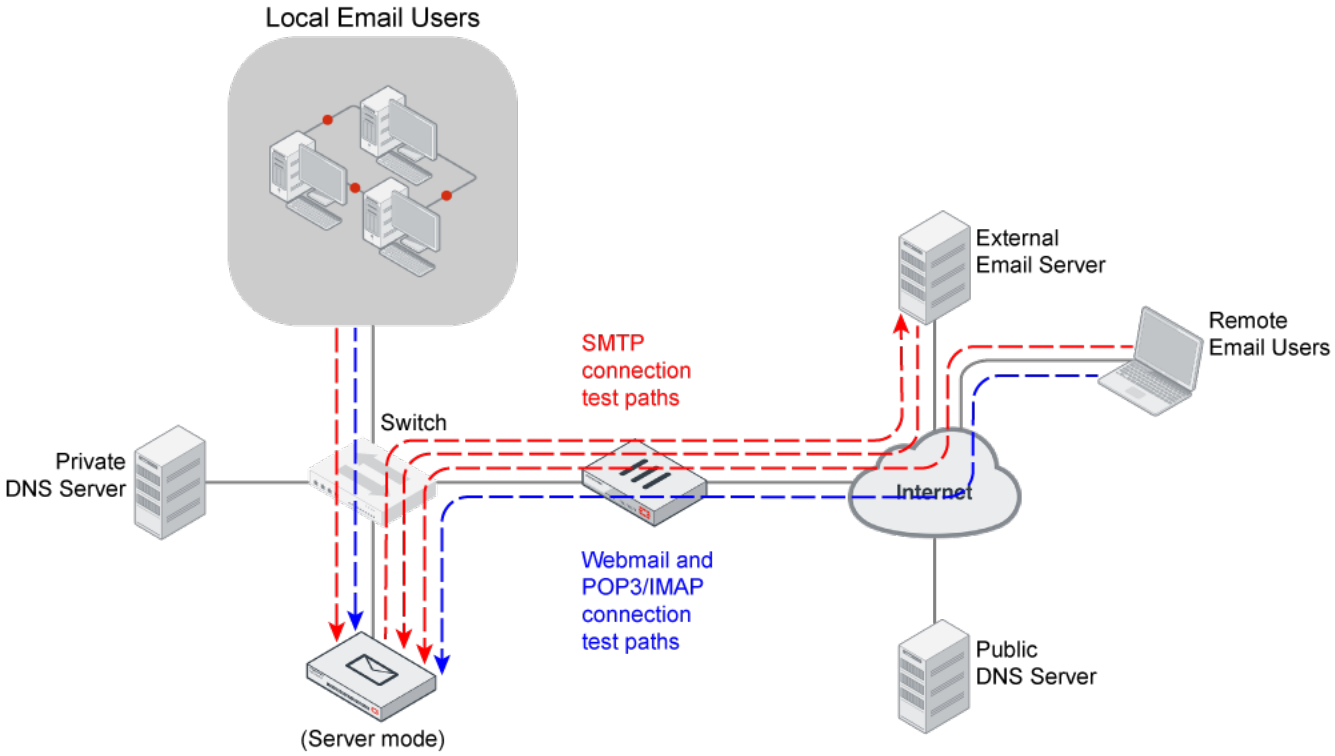
Connection test paths (gateway mode)



Connection test paths (transparent mode)



Connection test paths (server mode)



To verify all SMTP connections to and from your FortiMail unit, consider both internal and external recipient email addresses, as well as all possible internal and external SMTP clients and servers that will interact with your FortiMail unit, and send email messages that test the connections both to and from each of those clients and servers. For example:

1. Using an SMTP client on the **local** network whose MTA is the FortiMail unit or protected email server, send an email from an **internal** sender to an **internal** recipient.
2. Using an SMTP client on the **local** network whose MTA is the FortiMail unit or protected email server, send an email from an **internal** sender to an **external** recipient.
3. Send an email from an **external** sender to an **internal** recipient.
4. If you have remote SMTP clients such as mobile users or branch office SMTP servers, using an SMTP client on the **remote** network whose MTA is the FortiMail unit or protected email server, send an email from an **internal** sender to an **internal** recipient.
5. If you have remote SMTP clients such as mobile users or branch office SMTP servers, using an SMTP client on the **remote** network whose MTA is the FortiMail unit or protected email server, send an email from an **internal** sender to an **external** recipient.

If you cannot connect, receive error messages while establishing the connection, or the recipient does not receive the email message, verify your configuration, especially:

- routing and policy configuration of intermediary NAT devices such as firewalls or routers
- connectivity of the FortiMail unit with the Fortinet Distribution Network (FDN)
- external email servers' connectivity with and the configuration of the public DNS server that hosts the MX records, A records, and reverse DNS records for your domain names
- the FortiMail unit's connectivity with and the configuration of the local private DNS server (if any) that caches records for external domain names and, if the Use MX record option is enabled, hosts private MX records that refer to your protected email servers

- access control rules on your FortiMail unit
- configuration of MUAs, including the IP address/domain name of the SMTP and POP3/IMAP server, authentication, and encryption (such as SSL or TLS)

For information on tools that you can use to troubleshoot, see Troubleshooting tools on page 98.

Troubleshooting tools

To locate network errors and other issues that may prevent email from passing to or through the FortiMail unit, FortiMail units feature several troubleshooting tools. You may also be able to perform additional tests from your management computer or the computers of SMTP clients and servers.

This section includes:

- Ping and traceroute
- Nslookup
- Telnet connections to the SMTP port number
- Log messages
- Greylist and sender reputation displays
- Mail queues and quarantines
- Packet capture

Ping and traceroute

If your FortiMail unit cannot connect to other hosts, you may be able to use ICMP ping and traceroute to determine if the host is reachable or locate the node of your network at which connectivity fails, such as when static routes are incorrectly configured. You can do this from the FortiMail unit using CLI commands.

For example, you might use ICMP ping to determine that 172.16.1.10 is reachable (commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded):

```
FortiMail-400 # execute ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=64 time=2.4 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=1.4 ms

--- 172.20.120.167 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.4/2.4 ms
```

or that 192.168.1.10 is **not** reachable:

```
FortiMail-400 # execute ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 192.168.1.10 ping statistics ---
```

```
5 packets transmitted, 0 packets received, 100% packet loss
```

Both ping and traceroute require that network nodes respond to ICMP ping. If you have disabled responses to ICMP on your network, hosts may appear to be unreachable to ping and traceroute, even if connections using other protocols can succeed.

If the host is not reachable, you can use traceroute to determine the router hop or host at which the connection fails:

```
FortiMail-400 # execute traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 32 hops max, 72 byte packets
1  192.168.1.2 2 ms 0 ms 1 ms
2  * * *
```

Nslookup

It is critical that FortiMail has good access to DNS services to properly handle SMTP sessions and apply antispam scans, including FortiGuard Antispam. If DNS queries fail, they will be recorded in the event log under *Monitor* > *Log* > *System Event*.

If a DNS query fails or resolves incorrectly, you may want to manually query your DNS server to verify that the records are correctly configured. You can do this from the FortiMail unit using CLI commands.

For example, you might query for the mail gateway of the domain example.com (commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded):

```
FortiMail-400 # execute nslookup mx example.com
example.com mail exchanger = 10 mail.example.com.
```

or query to resolve mail.example.com and service.fortiguard.net (the domain name of a FortiGuard Distribution Network server) into IP addresses:

```
FortiMail-400 # execute nslookup name mail.example.com
Name: mail.example.com
Address: 192.168.1.10
FortiMail-400 # execute nslookup name service.fortiguard.net
Name: service.fortiguard.net
Address: 212.95.252.120
Name: service.fortiguard.net
Address: 72.15.145.66
Name: service.fortiguard.net
Address: 69.90.198.55
```

For more information on CLI commands, see the FortiMail CLI Reference.

Like verifying DNS connectivity and configuration from the FortiMail unit, you may also be able to verify DNS connectivity and configuration from protected and external mail servers using similar commands. This can be necessary if the devices are configured to use different DNS servers. For details, see the documentation for those mail servers.

Telnet connections to the SMTP port number

Instead of using an SMTP client to verify SMTP connections, you can manually establish SMTP connections by using a Telnet client. Especially if your SMTP client or SMTP server is unable to establish a connection, manually attempting the

connection may provide you with SMTP error codes or other insight into why the connection is failing.

Common SMTP error codes

SMTP error code number	Description
500	Syntax error, command unrecognized
501	Syntax error in parameters or arguments
502	Command not implemented (such as for ESMTP and other SMTP protocol extensions that are not enabled/installed on the SMTP server)
503	Bad sequence of commands

If extended SMTP error codes are installed and enabled on the target SMTP server, a manual Telnet connection may enable you to view additional error descriptions. For example, the enhanced error code `4.3.2 Please Try Again Later` may notify you that a temporary condition exists preventing delivery, such as greylisting or service unavailability, and that the SMTP client should try delivery again later.

How you should establish the connection depends on the origin and destination of the SMTP connection that you want to test, either:

- From the FortiMail unit to an SMTP server
- To or through the FortiMail unit

From the FortiMail unit to an SMTP server

If you are not sure if the FortiMail unit can use SMTP to reach an SMTP server, you might use the `execute telnettest <fqdn_str>:<port_int>` CLI command.

For example, to test SMTP connectivity with mail.example.com on the standard SMTP port number (see also Appendix C: Port Numbers on page 611; commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded):

```
FortiMail-400 # execute telnettest mail.example.com:25
Connecting to remote host succeeded.
```

To or through the FortiMail unit

If you are not sure if a MUA can use SMTP to reach a FortiMail unit that is operating in gateway mode or server mode, or not sure which SMTP commands the FortiMail unit was configured to accept, from the email user's computer or an external SMTP server, you might open a command prompt and use the command line Telnet client.

For example, to send a test email message (commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded):

```
$ telnet fortimail.example.com 25
Trying fortimail.example.com...
Connected to fortimail.example.com.
Escape character is '^]'.
220 fortimail.example.com ESMTP Smtpd; Mon, 6 Oct 2008 14:47:32 -0400
EHLO mail.example.com
250-fortimail.example.com Hello [172.16.1.10], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
```

```
250-8BITMIME
250-SIZE 10485760
250-DSN
250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
MAIL FROM: <user1@internal.example.com>
250 2.1.0 user1@example.com... Sender ok
RCPT TO: <user2@external.example.net>
250 2.1.5 user2@example.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Subject: TEST
This is a test email message.
.
250 2.0.0 m96IlWkF001390 Message accepted for delivery
QUIT
221 2.0.0 fortimail.example.com closing connection
Connection closed by foreign host.
$
```

where:

- `fortimail.example.com` is the fully qualified domain name (FQDN) of your FortiMail unit
- the FortiMail unit is listening for SMTP connections on the default SMTP port number, `25`; see also Appendix C: Port Numbers on page 611
- `mail.example.com` is the fully qualified domain name (FQDN) of a protected email server from which you are connecting, whose domain name resolves to the IP address `172.16.1.10`
- `user1@internal.example.com` is a email address of an sender that is internal to your protected domain, internal.example.com
- `user2@external.example.net` is a email address of an recipient that is external to your protected domain

Log messages

Log messages often contain clues that can aid you in determining the cause of a problem. FortiMail units can record log messages when errors occur that cause failures, upon significant changes, and upon processing events.

Depending on the type, log messages may appear in either the history, event, antivirus, or antispam logs. For example:

- To determine when and why an email was quarantined, you might examine the Classifier and Disposition fields in the history log.
- To determine if an antiSpam scan query was able to reach the FDN, you might examine the Message field in the antispam log.

During troubleshooting, you may find it useful to reduce the logging severity threshold for more verbose logs, to include more information on less severe events.

For example, when the FortiMail unit cannot reach the FDN or override server for FortiGuard Antispam queries, the associated log message in the antispam log has a severity level of Notification. If your severity threshold is currently greater than Notification (such as Warning or Error), the FortiMail unit will not record that log message, and you will not be notified of the error. Often this error might occur due to temporary connectivity problems, and is not critical. However, if you are frequently encountering this issue, you may want to lower the severity threshold to determine how often the issue is occurring and whether the cause of the problem is persistent.

Similar to how the FortiMail unit will not record log messages below the severity threshold, if the FortiMail unit is not enabled to record event, history, antivirus, and antispam log messages, you will not be able to analyze the log messages for events of that type. During troubleshooting, be sure that log messages are enabled for the type of event that you want to analyze.

To configure the severity threshold, go to Log & Report > Log Setting and set the logging level on one or both of the tabs. To enable logging of different types of events, select applicable options under Logging Policy Configuration on either or both tabs.

If this menu path is not available, first select Advanced to switch to the advanced mode of the GUI.

Greylist and sender reputation displays

If an SMTP client is unable to send email despite being able to initiate SMTP connections to or through the FortiMail unit, and is receiving SMTP error codes that indicate temporary failure or permanent rejection, verify that the SMTP client has not been temporarily blocked by the greylist or sender reputation features.

To view the lists of SMTP clients and their statuses with those features, go to Monitor > Greylist > Display and Monitor > Reputation > Sender Reputation respectively.

These menu items are only available in the advanced mode of the GUI.

Mail queues and quarantines

If email has not successfully passed to or through the FortiMail unit, but you have been able to successfully initiate the SMTP connection and send the email and have not received any SMTP error codes, verify that delivery has not been delayed and that the email message has not been quarantined.

To view the mail queues, go to Monitor > Mail Queue, then select a mail queue tab. To view the per-recipient or system quarantine, go to Monitor > Quarantine, then select either the Personal Quarantine or System Quarantine tab.

These menu items are only available in the advanced mode of the GUI.

Packet capture

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiMail units have a built-in sniffer. To use the built-in sniffer, go to *System* > *Utility* > *Traffic Capture*, or connect to the CLI and enter the following command:

```
diagnose sniffer packet <interface_str> '<filter_str>' <verbosity_level_int> <packet_count_
    int>
```

where:

- `<interface_str>` is the name of a network interface, such as `port1`, or enter `any` for all interfaces.
- `'<filter_str>'` is the sniffer filter that specifies which protocols and port numbers that you do or do not want to capture, such as `'tcp port 25'`, or enter `none` for no filters.
- `<verbosity_level_int>` is an integer indicating the depth of packet headers and payloads to display.
- `<packet_count_int>` is the number of packets the sniffer reads before stopping. Packet capture output is printed to your CLI display until you stop it by pressing Ctrl + C, or until it reaches the number of packets that you have specified to capture.

Packet capture can be very resource intensive. To minimize the performance impact on your FortiMail unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

For example, you might selectively capture packets for FortiGuard Antispam queries occurring through port1 (commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded):

```
FortiMail-400 # diag sniffer packet port1 'udp port 8889' 3
2.685841 172.16.1.10.47319 -> 212.95.252.120.8889: udp 64
0x0000 0009 0f84 27fe 0009 0f15 02e8 0800 4500 ....'.........E.
0x0010 005c 0000 4000 4011 44ff ac14 78a5 d45f .\..@.@.D...x.._
0x0020 fc78 b8d7 22b9 0048 9232 6968 726a b3c5 .x.."..H.2ihrj..
0x0030 776c 2d2f 5a5f 545e 4555 5b5f 425b 545f wl-/Z_T^EU[_B[T_
0x0040 4559 6b6a 776b 646e 776c 6b6a 772b 646e EYkjwkdnwlkjw+dn
0x0050 776c 6b6a 776b 646e 776c 6b6a 776b 86a9 wlkjwkdnwlkjwk..
0x0060 db73 21e1 5622 c618 7d6c .s!.V"..}l
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is usually preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark.

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

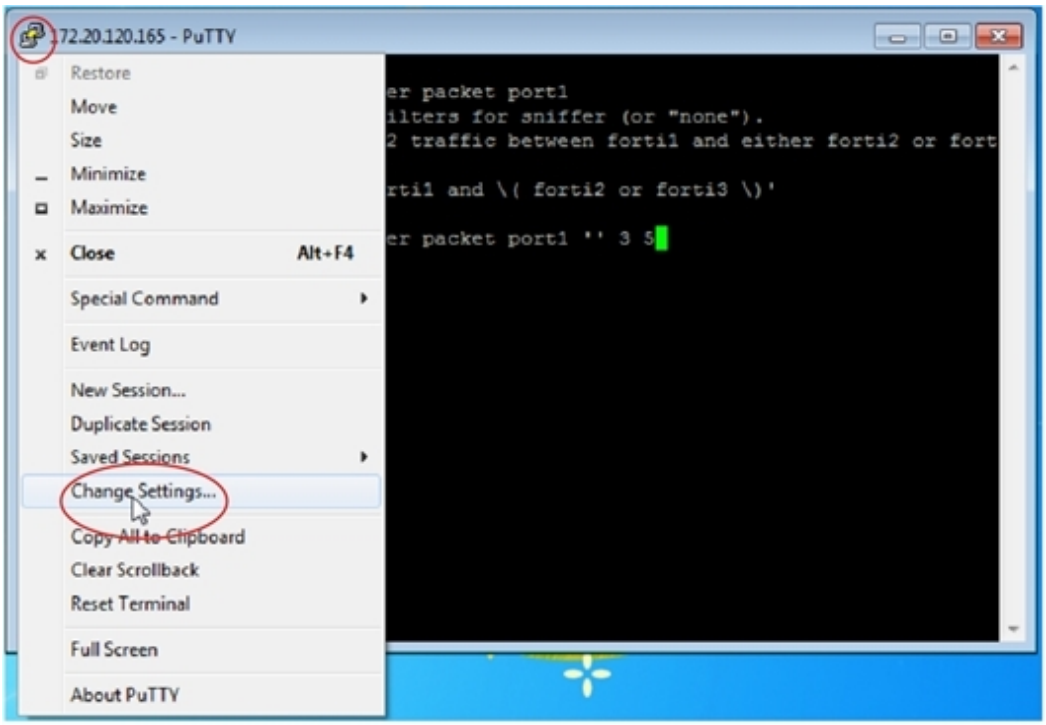
- terminal emulation software such as PuTTY
- a plain text editor such as Notepad
- a Perlinterpreter
- network protocol analyzer software such as Wireshark

To view packet capture output using PuTTY and Wireshark

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the FortiMail appliance using either a local serial console, SSH, or Telnet connection. For details, see the FortiMail CLI Reference.
3. Type the packet capture command, such as:
   ```
   diagnose sniffer packet port1 'tcp port 25' 3
   ```

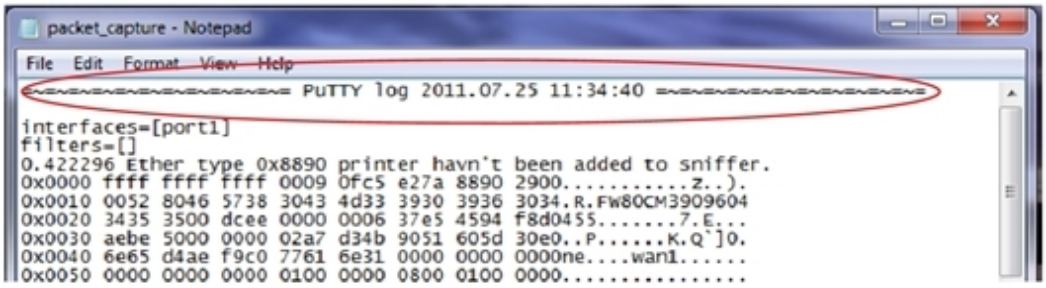
but do **not** press Enter yet.

4. In the upper left corner of the window, click the PuTTY icon to open its dropdown menu, then select Change Settings.



A dialog appears where you can configure PuTTY to save output to a plain text file.

5. In the Category tree on the left, go to Session > Logging.
6. In Session logging, select Printable output.
7. In Log file name, click the Browse button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file (you do not need to save it with the `.log` file extension).
8. Click Apply.
9. Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.



13. Delete the first and last lines, which look like this:
    `=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2011.07.25 11:34:40 =~=~=~=~=~=~=~=~=~=~=~=~=`
    `FortiMail-2000 #`

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethereal) using the fgt2eth.pl Perl script.

The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use fgt2eth.pl, open a command prompt, then enter a command such as the following:

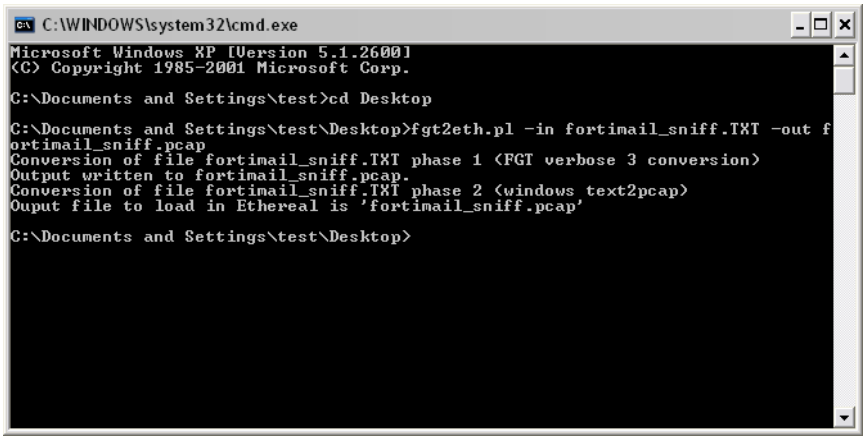
Methods to open a command prompt vary by operating system.
On Windows 10, click Start (Windows logo) then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

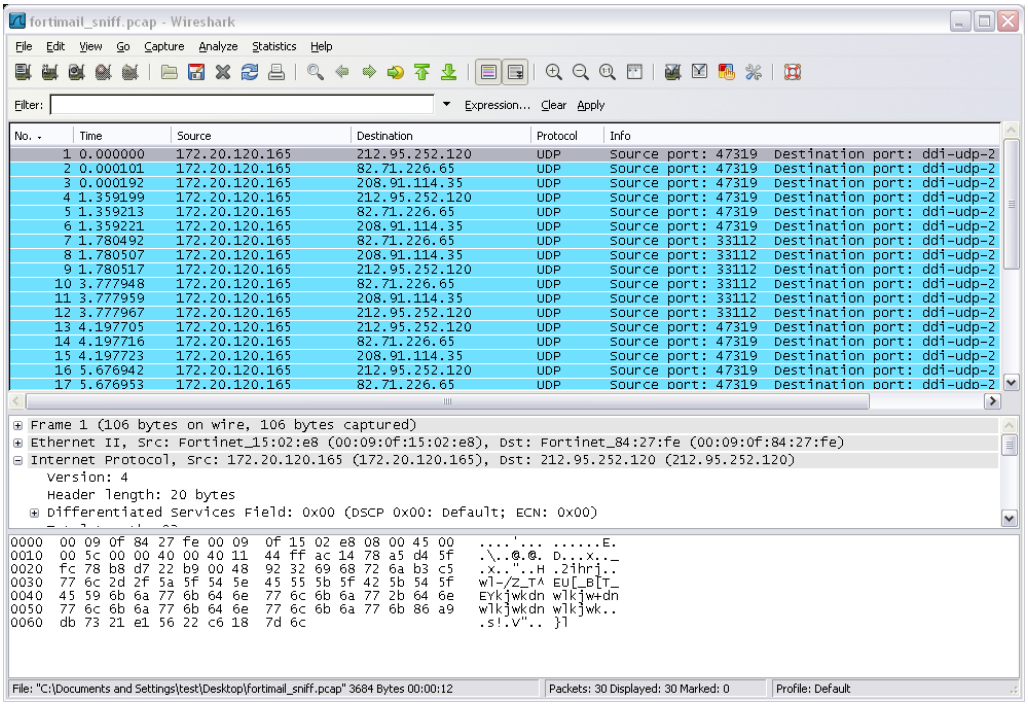
- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

Converting sniffer output to .pcap format



15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Viewing sniffer output in Wireshark



Backing up the configuration

Once you have tested your basic installation and verified that it functions correctly, create a backup. This “clean” backup can be used to:

- troubleshoot a non-functional configuration by comparing it with this functional baseline
- rapidly restore your installation to a simple yet working point

The following procedures only produce a backup of the configuration file. If you have also configured other settings such as block/safe lists, dictionaries, and the Bayesian databases, you should back them up as well.

To back up the configuration file via the GUI

1. Log in to the GUI as the `admin` administrator.
   Other administrator accounts do not have the required permissions.
2. Go to System > Maintenance > Configuration.
3. Select *System configuration* (and *User configuration* if you have already configured user preferences).
4. Click Backup.

   If your browser prompts you, navigate to the folder where you want to save the configuration file. Click Save.

   Your browser downloads the configuration file. Time required varies by the size of the configuration and the specifications of the appliance’s hardware as well as the speed of your network connection.

To back up the configuration file via the CLI

1. Log in to the CLI as the `admin` administrator using either the local serial console, the CLI Console widget in the GUI, or an SSH or Telnet connection.
   Other administrator accounts do not have the required permissions.
2. Enter the following command:
   `execute backup full-config tftp <file-name_str> <server_ipv4> [<backup-password_str>]`
   where the variables and options are as follows:

Variable	Description
`<file-name_str>`	Type the file name of the backup.
`<server_ipv4>`	Type the IP address or domain name of the server.
`[<backup-password_str>]`	Optional. Type the password that will be used to encrypt the backup file. **Caution:** Do not lose this password. You will need to enter this same password when restoring the backup file in order for the appliance to successfully decrypt the file. If you cannot remember the password, the backup cannot be used.

For example, the following command backs up a FortiMail-3000C's configuration file to a file named `FortiMail-3000C.conf` in the current directory on the TFTP server 172.16.1.10, encrypting the backup file using the password `P@ssw0rd1`:

For example, the following command backs up a FortiMail-3000C's configuration file to a file named `FortiMail-3000C.conf` in the current directory on the TFTP server 172.16.1.10, encrypting the backup file using the password `P@ssw0rd1`:

```
FortiMail-3000C # execute backup full-config tftp FortiMail-3000c.conf 172.16.1.10
     P@ssw0rd1
```

Time required varies by the size of the database and the specifications of the appliance's hardware, but could take several minutes.

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

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 serial number and current system status of the FortiMail unit, including uptime, system resource usage, alert messages, host name, firmware version, 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 greyed 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 User-add 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.

Using the CLI Console

Go to *Dashboard* > *Console* to access the CLI without exiting from the GUI.

Alternatively, if you want to open the CLI console in a pop-up dialog that you can resize, reposition, and keep open while you go to other areas of the GUI, click the *CLI Console* button that is in the bar at the top right corner of the GUI, next to the *Help* button.

For information about commands, see the FortiMail CLI Reference.

Using FortiView

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

This section includes:

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 266 and Domain mail statistics on page 266.

   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 361 and Configuring policies on page 333.
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. For details, see Configuring mailbox statistics on page 554.

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 559.

View threat statistics

Go to *FortiView* > *Threat Statistics* > *Threat Statistics* to view the summary of spam and virus mail. The FortiSandbox scan results are also summarized under *FortiView* > *Threat Statistics* > *FortiSandbox Statistics*.

View outbreak statistics

The *FortiView* > *Outbreak Statistics* > *Spam Outbreak* tab contains chart summaries of the number of email messages in each time period that the FortiMail unit detected a spam outbreak. Email messages are tracked as either Not Spam, Spam, or as being Monitored.

The *FortiView* > *Outbreak Statistics* > *Virus Outbreak* tab contains chart summaries of the number of email messages in each time period that the FortiMail unit detected a virus outbreak. Email messages are tracked as either Clean or containing a Virus.

The *FortiView* > *Outbreak Statistics* > *FortiSandbox* tab contains chart summaries of the number of email messages in each time period that the FortiSandbox unit is scanning. Email messages are tracked as either Clean, containing a Malicious File, or containing a Malicious URL.

Viewing top user statistics

The *FortiView* > *Top User Statistics* > *Top Recipient* and *FortiView* > *Top User Statistics* > *Top Sender* tabs display the top email, top virus, and top spam recipients and senders.

By default, this tab is hidden. To make this tab visible, use the following CLI command to enable it:

```
config system global
   set mailstat-service enable
end
```

Viewing current IP sessions

The *FortiView* > *Session* > *Session* tab displays information about the TCP sessions in established state, to and from the FortiMail unit.

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 Logging to the hard disk on page 543.

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 516.
- *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 118.

For more information, see FortiMail log types on page 537.

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 266.
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 117.
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 117.
   - 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 119.

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 117.

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*.

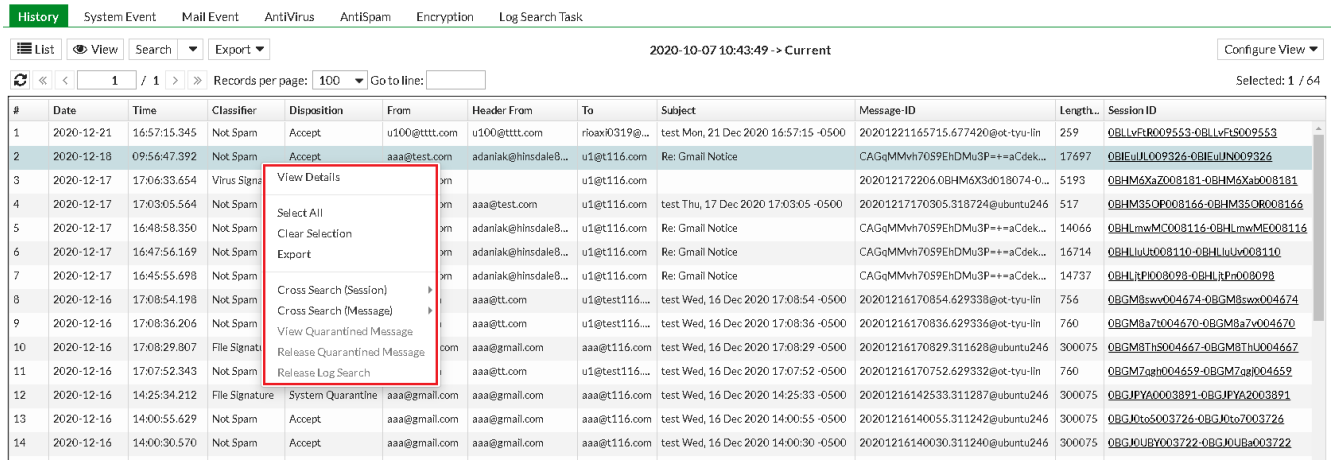
To change the order of the columns

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 119.
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 119.
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 120.
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 120.
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.
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.

GUI item	Description
	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 539.
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 539.

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. 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.

GUI item	Description
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 146.

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 three 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 121.

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 124.

Domain quarantine

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

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 126.

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 377
- Configuring antivirus profiles, file signatures, and actions
- Configuring content profiles and content action profiles on page 404
- Configuring content profiles and content action profiles

Sample Submission

You may also submit samples of spam email to a specified email account so it may either be reviewed by an administrator or sent directly to FortiGuard. See Managing the spam sample submissions on page 127.

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 121. For information on configuring the schedule and recipients of the quarantine report, see Configuring global quarantine report settings on page 473.

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 377 and Configuring content profiles on page 404.

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 122.

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 478.

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 474. 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 280 for quarantine report settings that are domain-specific, or Configuring global quarantine report settings on page 473 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 480.
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 419.
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 301, 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 418 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 377 and/or Configuring content action profiles on page 413.
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 417 is enabled. on page 1226, 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 354.
9. Either email users or FortiMail administrators can manage email in the per-recipient quarantines.

   For details, see Managing the personal quarantines on page 121 and Releasing and deleting email via quarantine reports on page 478.

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.
   A dialog appears.
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 479.

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 402, Configuring antispam action profiles on page 395, and Configuring content action profiles on page 413.

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.

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)	Starting from 6.2.0 release, you can 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 Message*s. • Release to: Original recipient(s) or other recipient(s) you specify.
Folder (dropdown list)	From the dropdown list, select a folder to view.

GUI item	Description
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 479. To view email messages quarantined in that mailbox, double-click its row. For more information, see Managing the system quarantine on page 124.
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.

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 479.

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 126.
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.
Session ID	Lists the session ID of each email.

GUI item	Description
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 123.

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 profiles on page 170 for more information. Note that domain/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 124 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.
   A dialog appears.
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

Once the sample submission service is enabled and email addresses are set to receive sample submissions of spam or non-spam, you can search for email messages based on whether they have been submitted as spam, non-spam (or ham), or if they have been detected to contain spam by FortiGuard.

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 detected 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 submit and view sample submissions, the service must first be enabled. See Configuring spam sample submission service on page 264 for more information.

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 according to the criteria you specify: • Start date • End date • Message type: Either *Not Submitted Only* or *All Messages*. • Submit to: Either *FortiGuard* or *Other recipient(s)* you specify.
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 479.
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.
From	Lists the display name of the sender as it appears in the message header, such as `"User 1"`.

GUI item	Description
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.
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 queue

FortiMail units prioritize mail delivery according to queues:

- **Regular mail queue**
  When the initial attempt to deliver an email fails, the FortiMail unit moves the email to the regular mail queue.
- **Slow mail queue**
  After 2 more failed delivery attempts, the FortiMail unit moves the email to the slow mail queue. This allows the FortiMail unit to resend valid email quickly, instead of repeatedly trying to resend email that is probably invalid (for example, email destined to an invalid MTA).

Once an undelivered email is in the deferred queue for 5 minutes, the mail appears under *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 interruptions to network connectivity. FortiMail units will periodically retry delivery (administrators can also manually initiate a retry). If the email is subsequently sent successfully, the FortiMail unit simply removes the email from the queue. It does not notify the sender. But if delivery continues to be deferred, 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 end of the time limit for delivery retries, 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, such as if the sender's SMTP server is unreachable or if the sender address is invalid or empty, the FortiMail unit will save a copy of the email in the dead mail folder. For more information, see Managing undeliverable mail on page 131.

When you delete a deferred email, the FortiMail unit sends an email message, with the deleted email attached to it, to notify 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.

GUI item	Description
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 the delayed incoming email destined to protected domains after one failed delivery attempt. After two more failed delivery retries, the mail will be moved to the Incoming-slow mail queue. • *Outgoing*: Displays the delayed outgoing email destined to unprotected domains after one failed delivery attempt. After two more failed delivery retries, the mail will be moved to the Outgoing-slow mail queue. • *IBE*: Displays the delayed IBE email after one failed delivery attempt. For information about IBE email, see Configuring IBE encryption. After two more failed delivery retries, the mail will be moved to the IBE-slow mail queue. • *Default-slow*: For FortiMail email process usage. • *Incoming-slow*: Displays the delayed incoming email after three failed delivery attempts. • *Outgoing-slow*: Displays the delayed outgoing email after three failed delivery attempts. • *IBE-slow*: Displays the delayed IBE email after three failed delivery attempts. • *Delivery control*: Displays the email throttled by delivery control policies (see Rate limiting for delivery on page 346). After three attempts, the mail will be moved to the outgoing-slow queue.
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 GeoIP locations/country names.
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.
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 enabled spam outbreak protection in an antispam profile, FortiMail will temporarily hold suspicious email for a certain period of time (configurable with CLI command `config system fortiguard antispam set outbreak-protection-period`) if the enabled FortiGuard antispam check (block IP and/or URL filter) returns no result. 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.

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 under *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 398). 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 284.

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.

View the mail queue size status in the GUI under *Dashboard* > *Status* in the *Queue Status* widget, or view the mail queue status using the following CLI command:

```
diagnose system mailqueue status
```

Viewing DMARC report statistics

If you have enabled:

- DMARC report analysis
- DMARC report generations for protected domains (see DMARC section on page 383)

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 278.

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 133.
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 133.

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 383.

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 489.

To use greylisting, you must enable the greylist scan in the antispam profile. For more information, see Configuring antispam profiles on page 377.

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 354, and Controlling email based on IP addresses on page 348), **or** if the matching access control rule's *Action* is *RELAY* (see Order of execution on page 26).

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 493 and Manually exempting senders from greylisting on page 494.

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 137.

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 136.
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.
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 493. • *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 137. *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`

GUI item	Description
	`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 493.

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 134. For more information on consolidation requirements, see Automatic greylist entries on page 492.

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.
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 493.

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 362.

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 139.
Clear (button)	Click to remove any search filter conditions.
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 362.
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 on page 471.

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 471), 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 471.
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 on page 501.

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 on page 504. 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 361.

You can alternatively blocklist MSISDNs/subscriber IDs manually. For more information, see Manually blocklisting endpoints on page 503.

You can exempt MSISDNs/subscriber IDs from automatic blocklisting. For more information, see Exempting endpoints from endpoint reputation on page 503.

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 141.
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*.

Managing archived email

You can archive email according to criteria you specify. For details, see Email archiving workflow on page 528.

You can view and search archived email through the GUI, and through IMAP using the email archiving administrator account. You can also download them, forward them to an email address, and use them to train the Bayesian databases.

For more information on Bayesian database training, see Training the Bayesian databases on page 508.

To view archived email

1. Go to *Monitor* > *Archive* > *Archive Account*.
2. Select the email archive account you want to view and click *View*. For details about email archive accounts, see Configuring email archiving accounts on page 528.
3. From the *Archive Folder* dropdown list, select *Inbox* to view the good mail mailboxes, or select *Bulk* to view the spam mailboxes.
4. Double-click the name of the email archive mailbox that you want to view.
   A list of archived email appears.

GUI item	Description
View (button)	To view the message, click its check box and click *View*. You can also view the message by double-clicking the message.
Send (button)	Select the check box of each email that you want to send to an email address as a mailbox (.mbox) file, then click this button.
Export (button)	Select the check box of email that you want to download and click *Export* to download a mailbox (.mbox) file or an archive (.tar.gz) file containing individual email (.eml) files.
Train Bayesian Database (button)	Mark the check box of each email message to use to train Bayesian databases then click this button. For more information, see To train Bayesian databases with archived mail on page 142.
Back (button)	Click to return to the list of archive mailboxes.

To train Bayesian databases with archived mail

1. Go to *Monitor* > *Archive* > *Archive Account*.
2. Select the email archive account you want to view and click *View*. For details about email archive accounts, see Configuring email archiving accounts on page 528.
3. From the *Archive Folder* dropdown list, select *Inbox* to view the good mail mailboxes, or select *Bulk* to view the spam mailboxes.
4. Double-click the name of the email archive mailbox that you want to use to train the Bayesian databases.

5. In the check box column, mark the check box of each email that you want to use to train the Bayesian databases. To use all messages for training, select the check box above the first message to mark the check boxes of all email on the current page.
6. Click *Train Bayesian Database*.
7. Select whether to use the messages as spam or non-spam (known as innocent messages) email.
8. Select the database you want to train: global or per-domain (group).
   - Global requires no further information.
   - For per-domain database training, select the domain.
9. Click *Apply*.

Searching the archived email

You can search the email archive for email messages based on their contents, senders, recipients, and time frames.

You can search archived email in both the current mailbox and rotated mailboxes, whether email is archived on the local disk or remote host. However, you can view only the archived email on the local disk.

The search action involves two steps:

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

See below for detailed instructions.

To search the email archives

1. Go to *Monitor* > *Archive* > *Archive Account*.
2. Select the email archive account you want to search and click *View*. For details about email archive accounts, see Configuring email archiving accounts on page 528.
3. From the *Archive Folder* dropdown list, select *Inbox* to search the good mail mailboxes, or select *Bulk* to search the spam mailboxes.
4. Click *Search* button.
   A new tab called *Archived Email Search* appears, displaying all search tasks if there are any.
5. Click *New* to add a search task.
6. Configure the search criteria. Note that for time range, the end time is excluded. For exmaple, if you specify a time range from 2018/10/03 to 2018/10/09, archives dated October 9, 2018 will not be included in the search.
7. Click *Create* to execute and save the task. The task name is the time when the task is created. The *Archived Email Search* tab displays the search tasks and their search status as follows:
   - *Done*: The FortiMail unit has finished the search. Click *View Search Result* to see the search results.
   - *Pending*: The search task is in the waiting list.
   - *Running*: The search task is still running. Click *Stop* to pause the search.
   - *Stopped*: The search task has stopped. Click *Resume* to restart the task.

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 550.

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 266 and Domain mail statistics on page 266.

   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.

Centrally monitoring the HA cluster

The *Centralized Monitor* menu allows administrators on the primary FortiMail unit of an HA cluster to monitor the state and activity of each HA cluster member, including CPU, memory, disk usage, email throughput, and other mail statistic summaries.

For active-active HA clusters, if a FortiAnalyzer is not used to aggregate logs, then administrators can use centralized monitoring to make log searches across the cluster members. This streamlines the monitoring process, avoiding the need to log into each individual cluster member.

If there is a firewall or NAT device between members of the HA cluster, you must also open required port numbers. See Appendix C: Port Numbers on page 611

By default, this feature is disabled and hidden. Purchase the feature license and enable the feature. See Centralized monitor on page 266.

Viewing the cluster status

Go to *Centralized Monitor* > *Overview* > *Overview Status* to manage and review the aggregate HA cluster dashboard.

Similarly to the FortiMail unit's dashboard under *Dashboard* > *Status*, administrators may manage and review various widgets that display current HA cluster status and summaries. Administrators may customize, move around, and monitor the following widgets:

- System Information
- System Resource
- Statistics History
- Statistics Summary Chart
- Statistics Summary

Viewing HA cluster mail statistics

Go to the various tabs under *Centralized Monitor* > *Mail Statistics* to view summaries for:

- the number of email messages,
- the size of email messages,
- the scan speed of email messages, and
- the transfer speed of email messages

All tabs may be viewed on a minute, hourly, daily, monthly, and yearly basis that the FortiMail HA cluster member(s) detected viruses, spam, or neither.

By default, all charts display statistics for **All** cluster members, however each chart may be filtered to show activity for specific cluster members by selecting the appropriate member under the icon .

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 use the *Mail Statistics* tab, first configure your FortiMail unit to detect spam and/or viruses. For more information, see Configuring profiles on page 361 and Configuring policies on page 333.

See also

Viewing mail statistics

Viewing HA cluster threat statistics

Go to *Centralized Monitor* > *Threat Statistics* > *Threat Statistics* to view the summary of spam and virus mail. The information presented by default displays statistics for **All** cluster members, but you can also show activity for specific cluster members.

Use the clock icon for each chart to display threat summaries based on an appropriate time schedule.

See also

View threat statistics

Searching the HA cluster logs

Go to *Centralized Monitor* > *Log Search* > *Log Search* to configure and conduct log searches across the cluster members based on various search criteria.

To configure HA log search

1. Go to *Centralized Monitor* > *Log Search* > *Log Search*.
2. Click *New*.
3. Configure the following search criteria. Note that the availability of the following options depends on the *Log type* selected:

GUI item	Description
Select devices	Either enable *All devices* to conduct the log search across all cluster members or select the members you wish to search from *Available* and move them to *Members*.
Log type	Select the type of log to search. Select from the following options: • *History* • *Mail Event* • *AntiVirus* • *AntiSpam*

GUI item	Description
	• *Encryption* • *System Event*
Description	Optionally, enter a description of the log you search for reference.
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.
Message-ID	Enter the unique identifier from the email header.
From	Enter all or part of the sender's email address as it appears in the log message. This option does not appear for any event or *Encryption* log searches.
Header From	This option appears only for *History* 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 any event log searches.
Session ID	Enter all or part of the session ID in the log message.
Log ID	Enter all or part of the log ID in the log message. This option does not appear for any event or *Encryption* or *System Event* log searches.
Client name/IP	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. This option appears only for *History* and *AntiSpam* log searches.
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 539.
Disposition	Enter the disposition in the log message. The disposition field specifies the action taken by the FortiMail cluster unit(s). For information about classifiers, see Classifiers and dispositions in history logs on page 539.
Match condition	• *Contain*: searches for the exact match. • *Wildcard*: supports wildcards in the entered search criteria.
Date	Select the date and time range of log messages to include in the search results.
Time span	Select the time span of log messages to include in the search results.

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 specified *End time* date. In that case, you would specify the *End time* date, and also specify the size of the span of time (10 days and 8 hours) before that date.

4. Click *Search*.
   The primary FortiMail HA unit searches your currently selected HA cluster members for log messages that match your search criteria, and displays any matching log messages.

See also

Viewing log messages

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 network settings

The *Network* submenu provides options to configure network connectivity and administrative access to the GUI or CLI of the FortiMail unit through each network interface.

About IPv6 Support

IP version 6 (IPv6) handles issues that did not exist when IPv4 was created, such as running out of IP addresses, fair distribution of IP addresses, built-in quality of service (QoS) features, better multimedia support, and improved handling of fragmentation. A bigger address space, bigger default packet size, and more optional header extensions provide these features with flexibility to customize IPv6 packets to future needs.

IPv6 has 128-bit addresses compared to IPv4's 32-bit addresses, effectively eliminating address exhaustion. This new very large address space reduces the need for network address translation (NAT) since IPv6 provides more than a billion IP addresses for each person on Earth. All hardware and software network components must support this new address size, so an upgrade that may take a while to complete and will force IPv6 and IPv4 to work side-by-side during the transition period.

FortiMail supports the following IPv6 features:

- Network interface
- Network routing
- High availability
- DNS
- Administrative access
- Webmail access
- Mail routing — multiple combinations of IPv4/6 server, IPv4/6 remote gateway
- Access control lists
- Grey list
- Local sender reputation
- IPv6 based policies
- Block/safe list
- LDAP
- IP pools

FortiMail will support the following IPv6 feature in future releases:

- Port forwarding for IPv6
- FortiGuard Antispam database populated with IPv6 addresses

About the management IP

When a FortiMail unit operates in transparent mode, you can configure one or more of its network interfaces to act as a Layer 2 bridge, without IP addresses of their own. However, the FortiMail unit must have an IP address for administrators to configure it through a network connection rather than a local console. The management IP address enables administrators to connect to the FortiMail unit through *port1* or other network ports, even when they are currently bridging.

By default, the management IP address is indirectly bound to *port1* through the bridge. If other network interfaces are also included in the bridge with *port1*, you can configure the FortiMail unit to respond to connections to the management IP address that arrive on those other network interfaces. For more information, see Do not associate with management IP on page 157.

Unless you configured an override server IP address, FortiMail units use this IP address to connect to the FortiGuard Distribution Network (FDN). Depending on your network topology, the management IP may be a private network address. In this case, it is not routable from the FDN and is unsuitable for use as the destination IP address of push update connections from the FDN. For push updates to function correctly, you must configure an override server. For details, see Configuring FortiGuard Antivirus service on page 262.

You can access the GUI, FortiMail webmail, and the per-recipient quarantines remotely using the management IP address.

About FortiMail logical interfaces

In addition to the FortiMail physical network interfaces, you can create the following types of logical interfaces on FortiMail:

- VLAN subinterfaces
- Redundant interfaces
- Loopback interfaces

VLAN subinterfaces

A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

VLANs use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

For information about adding VLAN subinterfaces, see Configuring the network interfaces on page 152.

Redundant interfaces

On the FortiMail unit, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on

that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

A physical interface is available to be in a redundant interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of a redundant interface
- it has no defined IP address and is not configured for DHCP
- it does not have any VLAN subinterfaces
- it is not monitored by HA

When a physical interface is included in a redundant interface, it is not listed on *System* > *Network* > *Interface* . You cannot configure the interface anymore.

For information about adding redundant interfaces, see Configuring the network interfaces on page 152.

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The FortiMail unit's loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiMail unit.

The loopback interface is useful when you use a Layer 2 load balancer in front of several FortiMail units. In this case, you can set the FortiMail loopback interface's IP address the same as the load balancer's IP address and thus the FortiMail unit can pick up the traffic forwarded to it from the load balancer.

For information about adding a loopback interface, see Configuring the network interfaces on page 152.

Configuring the network interfaces

The *System* > *Network* > *Interface* tab displays the FortiMail unit's network interfaces.

You must configure at least one network interface for the FortiMail unit to connect to your network. Depending on your network topology and other considerations, you can connect the FortiMail unit to your network using two or more of the network interfaces. You can configure each network interface separately. You can also configure advanced interface options, including VLAN sub-interfaces, redundant interfaces, and loopback interfaces. For more information, see About FortiMail logical interfaces on page 151, and Editing network interfaces on page 153.

If your FortiMail unit is not properly deployed and configured for the topology of your network, including network interface connections, email may bypass the FortiMail unit.

To view the list of network interfaces, go to *System* > *Network* > *Interface*>.

GUI item	Description
Interface name	Displays the name of the network interface, such as *port1*>. If the FortiMail unit is operating in transparent mode, this column also indicates that the management IP address is that of port1. For more information, see About the management IP on page 151.
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see About FortiMail logical interfaces on page 151.
Bridge Member	In transparent mode, this column indicates if the port is on the same bridge as the management IP. By default, all ports are on the bridge. For information on bridged networks in transparent mode, see Editing network interfaces on page 153
IP/Netmask	Displays the IP address and netmask of the network interface. If the FortiMail unit is in transparent mode, this field may display *Bridging* instead. This means that Do not associate with management IP has been disabled, and the network interface is acting as a Layer 2 bridge. If high availability (HA) is enabled, this field may display instead either: • *Bridged (isolated)* when Effective role is *Secondary*, and therefore the network interface is currently disconnected from the network • *Bridging (waiting for recovery)* when Effective role is *Failed*, and therefore the network interface is currently disconnected from the network, but a failover may soon occur, beginning connectivity. See also Virtual IP address (or Virtual IPv6 address) on page 237.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface. For more information about IPv6 support, see About IPv6 Support on page 150.
Access	Displays the administrative access and webmail access services that are enabled on the network interface, such as HTTPS for the GUI.
Status	Indicates the *up* (available) or *down* (unavailable) administrative status for the network interface. • *Green up arrow*: The network interface is up and can receive traffic. • *Red down arrow*: The network interface is down and cannot or receive traffic. To change the administrative status (that is, bring up or down a network interface), see Editing network interfaces on page 153.

Editing network interfaces

You can edit the FortiMail physical network interfaces to change their IP addresses, netmasks, administrative access protocols, and other settings. You can also create or edit logical interfaces, such as VLANs, redundant interfaces and the loopback interface.

Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiMail unit.

If your FortiMail unit operates in transparent mode and depending on your network topology, you may need to configure the network interfaces of the FortiMail unit.

- If all email servers protected by the FortiMail unit are located on the **same** subnet, no network interface configuration is necessary. Bridging is the default configuration for network interfaces when the FortiMail unit operates in transparent mode, and the FortiMail unit will bridge all connections occurring through it from the network to the protected email servers.
- If email servers protected by the FortiMail unit are located on **different** subnets, you must connect those email servers through separate physical ports on the FortiMail unit, and configure the network interfaces associated with those ports, assigning IP addresses and removing them from the bridge.

It is possible to configure a mixture of bridging and non-bridging network interfaces. For example, if some email servers belong to the same subnet, network interfaces for those email servers may remain in the bridge group; email servers belonging to other subnets may be attached to network interfaces that are not associated with the bridge.

You can restrict which IP addresses are permitted to log in as a FortiMail administrator through network interfaces. For details, see Configuring administrator accounts on page 168.

To create or edit a network interface

1. Go to *System* > *Network* > *Interface*>.
2. Double-click a network interface to modify it or select the interface and click *Edit*>. If you want to create a logical interface, click *New*.

   The *Edit Interface* dialog appears. Its appearance varies by:
   - the operation mode of the FortiMail unit (gateway, transparent, or server)
   - if the FortiMail unit is operating in transparent mode, by whether the network interface is *port1*, which is **required** to be configured as a Layer 2 bridge and associated with the management IP, and therefore **cannot** be configured with its own *IP* and *Netmask*
3. For gateway mode or server mode, configure the following:

GUI item	Description
Interface Name	If you are editing an existing interface, this field displays the name (such as port2) and media access control (MAC) address for this network interface. If you are creating a logical interface, enter a name for the interface.
Type	If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see About FortiMail logical interfaces on page 151.
VLAN	If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface for. Then specify a VLAN ID. Valid VLAN ID numbers are from 1 to 4094. (0 is used for high priority frames, and 4095 is reserved.)
Redundant	If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members.
Loopback	If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to “loopback”. You can only add one loopback interface on FortiMail.

GUI item		Description
Addressing mode		
Manual		Select to enter a static IP address, then enter the IP address and netmask for the network interface.
	IP/Netmask	Enter the IP address and netmask for the network interface. If the FortiMail unit is operating in gateway mode or server mode, this option is available only if Manual is selected. **Note:** IP addresses of different interfaces cannot be on the same subnet.
DHCP		Select to retrieve a dynamic IP address using DHCP. This option appears only if the FortiMail unit is operating in gateway mode or server mode.
	Retrieve default gateway and DNS from server	Enable to retrieve both the default gateway and DNS addresses from the DHCP server, replacing any manually configured values.
	Connect to server	Enable for the FortiMail unit to attempt to obtain DHCP addressing information from the DHCP server. Disable this option if you are configuring the network interface offline, and do not want the unit to attempt to obtain addressing information at this time.
Advanced Setting		
Access		Enable protocols that this network interface should accept for connections **to** the FortiMail unit itself (these options do not affect connections that will travel **through** the FortiMail unit). • *HTTPS*: Enable to allow secure HTTPS connections to the GUI, webmail, and per-recipient quarantine through this network interface. • *HTTP*: Enable to allow HTTP connections to the GUI, webmail, and per-recipient quarantine through this network interface. For information on redirecting HTTP requests for webmail and per-recipient quarantines to HTTPS, see Configuring global quarantine report settings on page 473. • *PING*: Enable to allow ICMP `ECHO` (ping) responses from this network interface. For information on configuring the network interface from which the FortiMail unit itself will send pings, see the FortiMail CLI Reference. • *SSH*: Enable to allow SSH connections to the CLI through this network interface. • *SNMP*: Enable to allow SNMP connections (queries) to this network interface. For information on further restricting access, or on configuring the network interface that will be the source of traps, see Configuring the network interfaces on page 152. • *TELNET*: Enable to allow Telnet connections to the CLI through this network interface.

GUI item	Description
	Caution: HTTP and Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiMail unit. For information on further restricting access of administrative connections, see Configuring administrator accounts on page 168.
Web access	Enable the GUI access type that this network interface should accept. • *Admin*: Enable to allow access the administrative GUI through this interface. • *Webmail*: Enable to allow webmail access through this interface.
Mail access	Enable the email access protocols that this network interface should accept: SMTP, SMTPS, IMAP, IMAPS, POP3, or POP3S.
MTU	Enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value; for example, RFC 2516 prescribes a value of 1492 for the PPPoE protocol.
Administrative status	Select either: • *Up*: Enable (that is, bring up) the network interface so that it can send and receive traffic. • *Down*: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

If the FortiMail unit is operating in transparent mode, configure the following:

GUI item	Description
Interface Name	Displays the name (such as port2) and media access control (MAC) address for this network interface. If you are creating a logical interface, enter a name for the interface.
Type	If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see About FortiMail logical interfaces on page 151.
VLAN	If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface for. Then specify a VLAN ID. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.

GUI item	Description
Redundant	If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members.
Loopback	If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to “loopback”. You can only add one loopback interface on FortiMail.
Addressing mode	
Do not associate with management IP	Enable to configure an IP address and netmask for this network interface, separate from the management IP, then configure IP/Netmask on page 153. This option appears only if the network interface is **not***port1*, which is required to be a member of the bridge.
IP/Netmask	Enter the IP address and netmask for the network interface. If the FortiMail unit is operating in transparent mode, this option is available only if Do not associate with management IP on page 157 is enabled.
Access	Enable protocols that this network interface should accept for connections **to** the FortiMail unit itself (these options do not affect connections that will travel **through** the FortiMail unit). • *HTTPS*: Enable to allow secure HTTPS connections to the GUI, webmail, and per-recipient quarantine through this network interface. • *HTTP*: Enable to allow HTTP connections to the GUI, webmail, and per-recipient quarantine through this network interface. For information on redirecting HTTP requests for webmail and per-recipient quarantines to HTTPS, see Configuring global quarantine report settings on page 473. • *PING*: Enable to allow ICMP `ECHO` (ping) responses from this network interface. For information on configuring the network interface from which the FortiMail unit itself will send pings, see the FortiMail CLI Reference. • *SSH*: Enable to allow SSH connections to the CLI through this network interface. • *SNMP*: Enable to allow SNMP connections (queries) to this network interface. For information on further restricting access, or on configuring the network interface that will be the source of traps, see Configuring the network interfaces on page 152. • *TELNET*: Enable to allow Telnet connections to the CLI through this network interface. **Caution:** HTTP and Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiMail unit. For information on further restricting access of administrative connections, see Configuring administrator accounts on page 168.

GUI item	Description
MTU	
Override default MTU value (1500)	Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value; for example, RFC 2516 prescribes a value of 1492 for the PPPoE protocol.
Administrative status	Select either: • *Up*: Enable (that is, bring up) the network interface so that it can send and receive traffic. • *Down*: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.
SMTP Proxy	When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified. Exceptions to SMTP connections that can be proxied or relayed include SMTP connections destined for the FortiMail unit itself. For those local connections, such as email messages from email users requesting deletion or release of their quarantined email, you must choose to either allow or block the connection. For more information about FortiMail transparent mode proxy and implicit SMTP relay, see Characteristics of transparent mode on page 45. **Note**: When a FortiMail unit proxies or relays traffic, whether the email will be scanned or not depends on the policies you specify. For more information about policies, see Configuring policies on page 333.
Incoming connections	Select how the proxy or built-in MTA will handle SMTP connections for that interface that are **incoming** to the IP addresses of email servers belonging to a protected domain. • *Pass through*: Permit connections but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • *Drop*: Drop connections. • *Proxy*: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see Configuring policies on page 333.

GUI item	Description
	Note: Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have selected *Proxy* more than once on this page. For an example, see For details, see Avoiding scanning email multiple times on page 199.
Outgoing connections	Select how the proxy or built-in MTA will handle SMTP connections for that interface that are **outgoing** to the IP addresses of email servers that are **not** a protected domain. • *Pass through*: Permit connections but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • *Drop*: Drop connections. • *Proxy*: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see Configuring policies on page 333. **Note:** Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have selected *Proxy* more than once on this page. For an example, see Avoiding scanning email multiple times on page 199.
Local connections	Select how the FortiMail unit will handle SMTP connections on each network interface that are destined for the FortiMail unit itself, such as quarantine release or delete messages and Bayesian training messages. • *Allow*: SMTP connections will be allowed. • *Disallow*: SMTP connections will be blocked.

To configure a non-bridging network interface

1. Go to *System* > *Network* > *Interface*.
2. Double-click the network interface to modify it or select the interface and click *Edit*.

port1 is required to be a member of the bridge and cannot be removed from it.

3. Enable *Do not associate with management IP*.

   This option appears only when the FortiMail unit is operating in transparent mode and the network interface is **not***port1*, which is required to be a member of the bridge.
4. In *IP/Netmask*, enter the IP address and netmask of the network interface.
5. Click *OK*.
6. Repeat this procedure for each network interface that is connected to an email server on a distinct subnet. When complete, configure static routes for those email servers. For details, see Configuring static routes on page 161. Also configure each protected domain to indicate through which network interface its email servers are connected. For details, see Configuring protected domains on page 280.

Configuring link status monitoring

Link status monitoring enables the FortiMail unit to track the status of its network interfaces and to bring an interface down or up based on the state of another associated interface.

Interface tracking

FortiMail units can process email before delivering it to your company's internal mail server. In this configuration, mail comes from an external interface into the FortiMail unit. Then the mail is processed for spam, viruses, and such. The mail is then forwarded over an internal interface to a company internal mail server for internal distribution.

For redundancy, companies can configure a secondary FortiMail unit that is connected to a secondary internal mail server. In this configuration the secondary FortiMail unit is normally not active with all mail going through the primary FortiMail unit. The secondary system is activated when the external interface on the primary FortiMail unit is unreachable. Mail is routed to the secondary system until the primary unit is can be reached and then the mail is delivered to the primary FortiMail unit once again. In this configuration the mail only goes to one FortiMail unit or the other - it is never divided between the two.

If the internal mail server becomes unreachable from the primary FortiMail unit's internal interface, the primary FortiMail unit needs to stop the incoming email or the email will continue to accumulate and not be delivered.

The FortiMail unit can track the status of the internal interface. When interface tracking sees the internal interface go down, it brings down the FortiMail external interface. This stops email from accumulating on the primary FortiMail unit. If your company has the redundant secondary FortiMail unit configured, email can be routed to it until the primary FortiMail unit can be reached again. Interface tracking also brings the external interface up when the internal interface comes back up.

With interface tracking, you can set which interfaces are associated. You can also set how often interface tracking checks the status of the interfaces. This is the maximum delay before the interfaces associated with the downed interface are brought down as well.

Configuring link status propagation

The *Propagate Link Status to Ports* section of the *Link Status* screen shows any interfaces whose status is linked to this interface.

Linking the state of an internal link to the external link prevents an accumulation of undeliverable mail from building up on the FortiMail unit when the internal link goes down.

To configure link status propagation

1. Go to *System* > *Network* > *Link Monitor*.
2. Select the *enable* button.
3. Enter the number of seconds between checks of the link status. If this is set to zero, the link status will not propagate to the other ports.
4. Enter the number of seconds to delay after a link state operation before checking the status.
5. Under *Link Status*, select the interface you want to propagate the status from, then click *Edit* for the interface.
6. In the *Link Status Setting* dialog, specify the ports you want to propagate the status to by moving the ports from the text area on the left to the right.
7. Click *OK*.

Configuring static routes

The *System* > *Network* > *Routing* tab displays a list of routes and lets you configure static routes and gateways used by the FortiMail unit.

Static routes direct traffic exiting the FortiMail unit. You can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. The router is aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations.

A default route is a special type of static route. A default route matches all packets, and defines a gateway router that can receive and route packets if no other, more specific static route is defined for the packet's destination IP address.

You should configure at least one static route, a default route, that points to your gateway. However, you may configure multiple static routes if you have multiple gateway routers, each of which should receive packets destined for a different subset of IP addresses.

To determine which route a packet will be subject to, the FortiMail unit compares the packet's destination IP address to those of the static routes and forward the packet to the route with the largest prefix match.

For example, if an SMTP server is directly attached to one of the network interfaces, but all other destinations, such as connecting clients, are located on distant networks such as the Internet, you might need to add only one route: a default route for the gateway router through which the FortiMail unit connects to the Internet.

To configure static routes

1. Go to *System* > *Network* > *Routing*.
2. Either click *New* to add a route or double-click a route to modify it.
3. In *Destination IP/netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.

   To create a default route that will match all packets, enter `0.0.0.0/0.0.0.0`.
4. Select the interface that this route applies to.
5. In *Gateway*, type the IP address of the next-hop router to which the FortiMail unit will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/netmask*. For an Internet connection, the next hop routing gateway routes traffic to the Internet.
6. Click *Create*.

Configuring DNS

FortiMail units require DNS servers for features such as reverse DNS lookups, FortiGuard connectivity, and other aspects of email processing. Your ISP may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

If the FortiMail unit is operating in gateway mode, you must configure the MX record of the DNS server for each protected domain to direct all email to this FortiMail unit instead of the protected SMTP servers. Failure to update the records of your DNS server may enable email to circumvent the FortiMail unit.

For improved FortiMail unit performance, use DNS servers on your local network.

Go to *System* > *Network* > *DNS* to configure the DNS servers that the FortiMail unit queries to resolve domain names into IP addresses.

Configuring dynamic DNS

If the FortiMail unit has a static domain name but a dynamic public IP address, you can configure the FortiMail unit to use dynamic DNS (DDNS) to update DNS servers on the Internet when the public IP address for its domain name changes. For information on setting a dynamic public IP address, see DHCP on page 155.

To configure dynamic DNS accounts

1. Go to *System* > *Network* > *DDNS*.
2. If you have not yet configured the dynamic DNS account that the FortiMail unit will use when it connects to the DDNS service provider, click *New*.

GUI item	Description
Server	Select a DDNS service provider to which the FortiMail unit will send DDNS updates.
User name	Enter the user name of your account with the DDNS service provider. The FortiMail unit will provide this to authenticate itself with the service when sending updates.
Password	Enter the password for the DDNS user name.
Update time	Enter the interval in hours between each time that the FortiMail unit will query the DDNS service provider's IP detection page if IP mode is *Auto detect*. **Caution:** Do not exceed the recommended frequency published by your DDNS service provider. Some DDNS service providers consider excessive connections to be abusive, and may ignore further queries from the FortiMail unit.

3. Click *Create*.
4. Double-click the row corresponding to the new DDNS account.
   The *Host/Domain Name Setting* area is now visible.
5. In the *Host/Domain Name Setting* area, click *Create New*, or, to modify an existing host/domain name, select its row and click *Edit*.
6. Configure the following:

GUI item	Description
Server	Displays the dynamic DNS service provider of this account.
Status	Enable to update the DDNS service provider when the FortiMail unit's public IP address changes. Disable to notify the DDNS service provider that this FQDN should use its offline redirect, if you configured any. If the FortiMail unit's public IP address changes, it will not notify the DDNS service provider.
Host name	Enter the public fully qualified domain name (FQDN) whose records the DDNS provider should update.

GUI item	Description
	Public DNS records for this domain name are updated by the DDNS service provider when the FortiMail unit sends its current public IP address. As such, it might not be the same as the host name and local domain name that you configured in Host name and Local domain name, which could be valid only for your internal network.
IP mode	Select which of the following ways the FortiMail unit should use to determine its current publicly routable IP address. • *Auto detect:* Periodically query the DDNS service provider's IP address detection web page to see if the FortiMail unit's public IP address has changed. The IP detection web page returns the apparent source IP address of the query. If this IP address has changed, the FortiMail unit then sends an update request to the DDNS service provider, causing it to update DNS records for the FQDN in Host name. This option is the most common choice. Also configure the interval of DDNS IP detection queries in Update time. **Note:** If this query occurs through a NAT device such as a router or firewall, its apparent source IP address will **not** be the private network IP address of any of the FortiMail unit's network interfaces. Instead, it will be the IP address of the NAT device's externally facing network interface. For example, a public virtual IP (VIP) on a FortiGate unit in NAT mode might be used to route email from the Internet to a FortiMail unit. DDNS updates are also routed out from the VIP to the DDNS service provider on the Internet. From the DDNS service provider's perspective, the DDNS update connection appears to come from the VIP, and therefore it updates the DNS records with the IP address of the VIP. The DDNS service provider does not know the private network address of the FortiMail unit. • *Bind interface*: Use the current IP address of one of the FortiMail unit's network interfaces. Choose this option only if the network interface has an IP address that is routable from the Internet — that is, it is **not** an RFC 1918 private network address. • *Static IP*: Use an IP address that you configure. You must manually update the accompanying field if the FortiMail unit's public IP address changes.
Type	Select one of the following: • *dynamic* (this is the default) • *static* • *custom*

7. To verify your DDNS configuration and connectivity, do not query DNS servers: depending on DNS caching, record propagation, and other effects, DNS queries may not be able to determine whether the update actually reached your DDNS service provider.

   Instead, log in to your DDNS service provider account and verify whether its host records have been updated. You can also view the FortiMail event log. Log messages such as this indicate DDNS update failure:

   ```
   DDNS daemon failed on update members.dyndns.org, domain fortimail.example.com, next try
        at 1251752285\n
   ```

Configuring port forwarding

Similar to port forwarding on FortiGate or third party routers and firewalls, FortiMail port forwarding allows computers on external networks such as the Internet to connect to a computer on a private local area network (LAN) that is behind the FortiMail unit. Port forwarding can be useful if FortiMail is deployed as a gateway, and you want external users to access an internal server through FortiMail.

For example, FortiMail port1 may be connected to the Internet. Its public IP address is 192.168.37.4. Behind the FortiMail unit, there is a private network: 10.10.10.0/24. Remote users need to access a device on the private network. The device is 10.10.10.42, and it listens on port 8000. To allow this, you configure port forwarding on FortiMail. When computers on the Internet try to communicate with 192.168.37.4 port 7000, FortiMail translates the connection and forwards it to to 10.10.10.42 port 8000. Computers on the Internet are unaware of this translation and see one host at the public IP address, rather than the private network behind the FortiMail unit.

To configure port forwarding

1. Go to *System* > *Network* > *Port Forwarding*.
2. Select *New* to configure a new forwarding rule or double-click a rule to modify it.
3. Configure the following settings:

GUI item	Description
Protocol	Select which protocols will receive port forwarding: *TCP* , *UDP*, or *Both*.
Host IP	Enter the IP address where FortiMail will listen for communications to forward.. This is usually the IP address of the receiving network interface on FortiMail. In the previous example, it is 192.168.37.4.
Host Port	Enter the port number where FortiMail will listen for communications to forward. In the previous example, it is 7000. See also Appendix C: Port Numbers on page 611.
Destination IP	Enter the IP address of the computer or other device that will receive communications. In the previous example, it is 10.10.10.42.
Destination Port	Enter the listening port number on the computer or other device that will receive communications. In the previous example, it is 8000.

4. Click *Create*.

Scanning SMTP traffic redirected from FortiGate

FortiMail and FortiGate support Web Cache Communication Protocol (WCCP) to redirect SMTP traffic from FortiGate to FortiMail. If the FortiGate unit is configured to redirect SMTP traffic to FortiMail for antispam scanning (for details, see the FortiGate documentation), on the FortiMail side, you must do corresponding configurations to accept the SMTP traffic from FortiGate.

To configure the WCCP communication with FortiGate

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

GUI item	Description
Enabled	Enable WCCP communication with FortiGate. See also Appendix C: Port Numbers on page 611.
Tunnel ID	Enter the WCCP tunnel ID assigned by FortiGate.
Local IP	Enter the IP address of the FortiMail interface that communicates with FortiGate.

GUI item	Description
Remote IP	Enter the IP address of the FortiGate interface that communicate with FortiMail.
Authentication	Enable if authentication is required on both sides.
Password	Enter the authentication password.

Configuring administrator accounts and access profiles

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

About administrator account permissions and domains

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 35.
- **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

The *Admin profile* defines the permissions that administrator accounts have to each area of the FortiMail software. Exact effects vary by the combination with the *Access level* of the administrator account.

Permission	*Access level*: System	*Access level*: Domain
Administrator (also known as *all*)	• View, create, and change all other administrator accounts except the `admin` administrator account • Change another administrator's password using the current password. The `admin` account can	• View, delete, and change other administrator accounts with *Read/Write* and *Read* permissions in the same protected domain, but cannot create new accounts

Permission	*Access level*: System	*Access level*: Domain
	also reset unknown passwords. See About the "admin" account on page 168. • View and change all parts of the FortiMail unit's configuration, including uploading configuration backup files and restoring firmware default settings • Release and delete quarantined email messages for **all** protected domains • Back up and restore databases • Manually update firmware and antivirus definitions • Restart and shut down the FortiMail unit	• View and change settings, including profiles and policies, only in its own protected domain and elsewhere if permitted • View profiles and policies created by an administrator whose *Access level* is *System*
Read/Write	• View and change its own administrator account settings • View and change parts of the FortiMail unit's configuration for **all** protected domains, and the FortiMail unit itself • Release and delete quarantined email messages for **all** protected domains • Back up and restore databases	• View and change its own administrator account settings • View and change parts of the FortiMail unit's configuration only in the same protected domain • View profiles and policies created by an administrator whose *Access level* is *System* • Release and delete quarantined email messages in the same protected domain.
Read/Update		
Read	• View and change only that administrator account's own settings • View the FortiMail unit configuration for **all** protected domains, and the FortiMail unit itself • Back up databases • For *Monitor* > *Quarantine*, *Mail Queue*, and *Archive* categories, administrators with either *Read* privileges or better can view email contents if *Content detail* is enabled	• View and change only that administrator account's own settings • View settings only in the same protected domain. • View profiles and policies created by an administrator whose *Access level* is *System*
Custom	Permissions vary by which is selected (*Read* etc.) in each area. • For *Monitor* > *Quarantine*, *Mail Queue*, and *Archive*, you can select action-specific permissions. If *Content detail* is enabled, administrators with *Read* privileges or better can view email contents. • For Monitor > Quarantine > System Quarantine, you can assign either *All folders* or some folders to the administrator. By default, all folders are assigned. To change the setting, click on *All folders*. In the popup box, disable *All folders*, and then move the folders from the *Available* list to the *Members* list.	

About the “admin” account

Unlike other administrator accounts whose *Admin profile* is `super_admin_prof` and *Access level* is *System*, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. Its name, permissions, and assignment to the `System` domain cannot be changed.

The `admin` administrator account always has full permission to view and change all FortiMail configuration options, including viewing and changing **all** other administrator accounts. It is the only administrator account that can reset another administrator’s password without having to enter the existing password. As such, it is the **only** account that can reset another administrator’s password if the existing password is unknown or forgotten (Other administrators can change an administrator’s password if they know the current password).

About the “remote_wildcard” account

You can use the wildcard administrator account so that many accounts from a RADIUS or LDAP server can log onto FortiMail.

To achieve this, you can use the preconfigured account named `remote_wildcard` account.

1. Go to *System* > *Administrator* > *Administrator*.
2. Double click the built-in account named `remote_wildcard`.
3. Configure the settings (see Configuring administrator accounts on page 168) and click *OK*.
   In *Authentication type*, select *RADIUS* or *LDAP*. The name, `remote_wildcard`, is not editable.

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 and domains on page 165.

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

- For the `admin` superuser, all administrators will be displayed.
- For administrators with the access profile named `super_admin_prof`, all administrators except for `admin` will be displayed.
- For all other administrators, only the administrators who are not using the `super_admin_prof` 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 479.

To configure administrator accounts

1. Go to *System* > *Administrator* > *Administrator*.
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 scope of the administrator account: • *System* • *Domain* • *Domain Group* For details, see About administrator account permissions and domains on page 165 and Configuring protected domains on page 280.  If *Access level* is *Domain*, the administrator cannot use the CLI 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*.
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 profiles on page 170.
Access mode	Select the allowed access methods: CLI, GUI, and/or REST API. For information on restricting administrative access protocols that can be used by administrator computers, see Editing network interfaces on page 153.
Authentication type	Select the local or remote type of authentication that the administrator will use: • *Local* • *RADIUS* • *PKI* • *LDAP* • *Single Sign On* Except for *Local*, most types require that you configure an authentication profile with associated settings. See Configuring authentication profiles on page 420 and Configuring PKI authentication on page 304.  The GUI login page may not include all types, depending on what you select when customizing the appearance. See the FortiMail CLI Reference.
Password	Enter a secure password for this administrator account. The password can contain any character except spaces.

GUI item	Description
	If you are changing your own password, the new password cannot be the same as the old one. After you change the password, you must log in again. However, if you are changing other administrators' passwords, these rules do not apply. This setting is only available when *Authentication type* is *Local*.
Confirm password	Enter this account's password again to confirm it. This setting is only available when *Authentication type* is *Local*.
RADIUS profile	If you selected the *RADIUS*or *RADIUS + Local* authentication type, select the name of the RADIUS profile that you want to use.
PKI profile	If you selected the *PKI* authentication type, select the name of the PKI profile that you want to use.
LDAP profile	If you selected the *LDAP* authentication type, select the name of the LDAP profile that you want to use.
Single sign on profile	If you selected the *Single Sign On* authentication type, select the name of the SSO profile that you want to use.
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 153.
Language	Select this administrator account's preference for the display language of the GUI. This setting overrides the default language configured under *System* > *Customization* > *Appearance*. See Customizing the GUI appearance on page 212.
Theme	Select this administrator account's preference for the display theme. This setting overrides the default theme configured under *System* > *Customization* > *Appearance*. See Customizing the GUI appearance on page 212.

Configuring administrator 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 account profile

1. Go to *System* > *Administrator* > *Admin Profile*.

GUI item	Description
Name	Displays the name of the administrator access profile.
Comment	Displays an optional description of the administrator access profile.
Ref.	Indicates whether or not the profile is being used in one or more administrator accounts. Click to show the list of referenced entities.

The access profile named `super_admin_prof` is required by the administrator account named `admin`, and cannot be deleted.

2. Either click *New* to add an account or double-click an access profile to modify it.
3. In *Profile name*, enter the name for this access profile.
4. For each row in the *Access Control* column, select the permissions such as *Read/Write* to grant to administrator accounts associated with this access profile. For more granular control of permissions, select *Custom*. For details, see About administrator account permissions and domains on page 165.
5. 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, options, and other system options

The *System* > *Configuration* submenu lets you configure the system time, various global GUI settings (such as idle timeout), and SNMP access.

Configuring the time and date

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 C: Port Numbers on page 611.

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

Configuring system options

The *System* > *Configuration* > *Option* tab lets you set the following global settings:

- system idle timeout
- LCD panel and button access restriction (for the models that have front LCD panel and control buttons)
- login disclaimer
- password enforcement policy
- administration port numbers on the interfaces

To configure the system options

1. Go to *System* > *Configuration* > *Option*.
2. Configure the following:

GUI item		Description
Idle timeout		Enter the amount of time that an administrator may be inactive before the FortiMail unit automatically logs out the administrator.  For better security, use a low idle timeout value.
LCD Panel (models with LCD panels)		
	PIN Protection	Enable to require administrators to enter the PIN before using the LCD display panel and control buttons on the FortiMail unit, then enter the 6-digit PIN number. This option appears only on FortiMail models whose hardware includes an LCD panel.  For better security, always configure an LCD PIN. Otherwise, anyone with physical access can reconfigure the FortiMail unit.
Login Disclaimer Setting		
	Login disclaimer	Enter text that you want to prompt the user to agree, such as an IT policy or legal disclaimer, then also configure when to display it: • *Display pre-login banner* • *Display post-login banner*
	Reset To Default (button)	If you have customized the disclaimer text but want to use the default text, click this button.
	Display pre-login banner	Enable to display the text in *Login disclaimer* before the login dialog.

GUI item		Description
	Display post-login banner	Enable to display the text in*Login disclaimer* after the login dialog, but before the GUI menu or CLI command prompt appears. Select which users receive the disclaimer: • *Admin* — Administrators. • *Webmail* — : Webmail and quarantine users. • *IBE* — : Encrypted email users.
Password Policy		
	Enforce password policy	Enable to require strong passwords, as configured in *Minimum password length* and *Password must contain*. If any password does not meet the requirements, FortiMail requires that user to change the password during the next login.  Set a strong password policy, especially for administrator accounts. If you don't, unauthorized persons could log into FortiMail and compromise security. Short, simple, and easily-guessed passwords are a security risk.  Password policy settings only apply to accounts that are local (defined on FortiMail). See also Authentication type on page 169.
	Allow empty password	Enable to ignore *Minimum password length* and *Password must contain* and allow empty passwords.  Empty passwords effectively disable authentication, and are a security risk.
	Minimum password length	Enter the minimum number of characters that a password must contain. The default value is 8.
	Password must contain	Select which types of characters are required to ensure password complexity: • *Uppercase letter* • *Lowercase letter* • *Number (0-9)* • *Non alphanumeric character* — Any character that is not a letter of the US-ASCII alphabet nor a number, such as: é ! ~ @ # %
	Apply password policy to	Select which accounts to apply the password policy to: • *Administrators* — Administrators. • *IBE users* — Encrypted email users. • *Local mail users* — : Webmail and quarantine users.
Administration Ports		Enter the TCP/UDP port numbers for administrative access on the network interfaces. See also Appendix C: Port Numbers on page 611.

See also

Customizing the GUI appearance

Configuring the network interfaces

Configuring SNMP queries and traps

You can configure the FortiMail appliance's simple network management protocol (SNMP) agent to allow queries for system information and to send traps (alarms or event messages) to an SNMP manager. In this way you can use an SNMP manager to monitor the FortiMail appliance.

Monitoring can include system events and thresholds, such as high availability (HA) cluster failover messages. On models which have monitored power supplies and RAID controllers, more event types are available. When a monitored power supply or a RAID controller is removed or added, the FortiMail unit will send configured notification for those events by log messages, alert email messages, and/or SNMP traps.

The FortiMail SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiMail system information and can receive FortiMail traps.

To configure SNMP traps and queries

1. On your SNMP manager:
   - Download the FortiMail management information blocks (MIBs) files from the Fortinet Support website. Load the Fortinet proprietary and standard MIBs into your SNMP manager. For instructions, see the documentation for your SNMP manager.
   - Get the name of the community that the SNMP manager belongs to. If you use SNMPv3, also get the names of SNMP users that should have access to information from FortiMail.
2. On FortiMail, for the network interface that connects to the SNMP manager, enable SNMP access. See Access on page 155.
3. Go *System* > *Configuration* > *SNMP*.
4. Expand the *SNMP Threshold* section.
5. Configure the following:

GUI item	Description
SNMP agent enable	Enable the SNMP service on the FortiMail unit.
Description	Optional. Type a comment about the FortiMail appliance. The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Location	Type the physical location of the FortiMail appliance, such as `floor2`. The location can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Contact	Type contact information for the administrator or other person responsible for this FortiMail appliance. The contact information can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).

6. Expand the *SNMP Threshold* section.
7. For each trap that occurs when a threshold is reached (*CPU Usage Threshold* etc.; see Configuring an SNMP community on page 175 and Configuring SNMP users on page 177), configure the settings:

GUI item	Description
Trigger	Enter the acceptable limit for resource usage. For example, you may want to monitor that FortiMail CPU usage remains under 80%, except for temporary spikes. You configure Trigger to be 80%, Threshold to `3`, Sample Freq (s) to 30 seconds, and Sample Period (s) to 600 seconds (10 minutes). If CPU usage exceeds 80% temporarily, but then decreases again before the next measurement and remains under the limit during the 10 minute period, then FortiMail does **not** send an SNMP trap. During another period, if the limit is exceeded 3 or more times, then FortiMail sends a trap. Multiple traps occur if the limit is exceeded more than 3 times.
Threshold	Enter the number of times that Trigger must be equaled or exceeded in order to reach the trap threshold.
Sample Period (s)	Enter the time period in seconds during which the FortiMail unit SNMP agent counts triggers. **Note:** Sample Period (s) must be greater than or equal to Sample Freq (s).
Sample Freq (s)	Enter the interval in seconds between measurements of the limit. This is the maximum rate at which FortiMail sends traps.

8. Click *Apply*.
9. Add at least one SNMP manager ("host") that is allowed to query, and which hosts will receive traps. Depending on your SNMP version, you may also need to configure users. See Configuring an SNMP community on page 175 and Configuring SNMP users on page 177.

Configuring an SNMP community

By default, FortiMail belongs to the community named `public`. Your FortiMail appliance must belong to at least one community. The FortiMail appliance will not respond to SNMP managers whose queries do not contain a matching community name. Similarly, traps from the FortiMail appliance will include community name, and an SNMP manager may not accept the trap if its community name does not match.

You can add up to 16 communities. Each community can be configured differently to receive different traps. Each community can have up to 8 SNMP managers.

To configure SNMPv1 or v2C access

1. Go to *System* > *Configuration* > *SNMP*.
2. Enable SNMP access. For details, see Configuring SNMP queries and traps on page 174.
3. Expand the *Community* section.
4. Either click *New* to add a community, or select a community and click *Edit*.
5. Configure the following:

GUI item	Description
Name	Type the name of the SNMP community to which at least one SNMP manager belongs.

GUI item	Description
	Caution: For better security, change the default community name, and only enable SNMP on trusted networks. The default community name `public` is a popular, well-known default. Attackers will often try this name first, and SNMP v2c and older does not support authentication nor encryption.
Enable	Enable to send traps to and allow queries from this community's SNMP managers.
Community Hosts IP Address	Double-click the entry to edit it, or click *Create* to add an entry. Type the IP address and subnet mask of the SNMP managers in this community. **Note:** By default, there is one entry: `0.0.0.0/0`. You must add the IP address of at least one specific SNMP manager. If there are no other host IP entries, queries from all IP addresses will be accepted, but traps are effectively disabled because there is no specific destination. **Caution:** For better security, change the default of `0.0.0.0/0`, which includes all IP addresses. FortiMail sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative devices.
Queries	Enable the SNMP v1 and/or v2c versions that you want FortiMail to accept for queries. Then in *Port*, enter the listening port on the FortiMail unit. See also Appendix C: Port Numbers on page 611.
Traps	Enable the SNMP v1 and/or v2c versions that you want FortiMail to use to send traps. Then in *Local Port*, enter the source port number from which FortiMail sends traps, and in *Remote Port*, enter the destination port number (listening port number) on the SNMP managers. See also Appendix C: Port Numbers on page 611.
SNMP Event	Enable the types of SNMP traps that you want the FortiMail appliance to send to the SNMP managers in this community. For more information on supported traps and queries, see SNMP MIB fields on page 179. Event types include: • *System Event* — FortiMail reboot, reload, upgrade, log disk formatting • *RAID Event* — Local storage. • *HA Event* • *Remote Storage Event* • *Interface IPChanged* While most traps are sent each time an event occrs, the following events occur only when a threshold has been exceeded: • *CPU Usage Threshold* • *Memory Usage Threshold* • *Log Disk Usage Threshold* • *Mailbox Disk Usage Threshold* • *Deferred Queue Threshold* • *Detected Virus Threshold* • *Detected Spam Threshold* To configure their thresholds, see Configuring SNMP queries and traps on page 174.

GUI item	Description
	Note: For events that don't have a configurable threshold, FortiMail examines the status at a regular interval. Therefore it may not always send a trap. For example, hardware status is examined every 60 seconds.Therefore if the power is off for a few seconds but returns before the next status check, no system event trap is sent.

6. Click *OK*.
7. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiMail appliance, test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiMail appliance. To test traps, cause one of the events that should trigger a trap.

Configuring SNMP users

Similar to SNMP v1 and v2C, SNMP v3 also requires that you define SNMP managers. However it provides some better security features.

If your SNMP manager supports SNMP v3, you can use authentication to specify which of its user accounts is permitted to access information about your FortiMail appliance. This provides more control over who can access potentially sensitive system information. You can add up to 16 SNMP users.

SNMP v3 also provides better security by supporting privacy (encryption in transit).

To configure SNMPv3 access

1. Go to *System* > *Configuration* > *SNMP*.
2. Enable SNMP access. For details, see Configuring SNMP queries and traps on page 174.
3. Expand the *User* section.
4. Under *Users*, click *New* to add a user or select a user and click *Edit*.
5. Configure the following:

GUI item	Description
User name	Enter the name of an SNMP user. This must match the name of the account as it is configured on your SNMP manager.
Enable	Enable to send traps to and allow queries from the user's SNMP managers.
Security level	Select either: • *No authentication, no privacy* — No encryption (privacy) and no authentication, similar to SNMP v1 and v2. **Caution:** For better security, do not use this option, except on management networks isolated from the rest of your network. Attackers could easily eavesdrop on sensitive system information and/or mimic a legitimate SNMP user. • *Authentication, no privacy* — Authentication only. No encryption (privacy). Also configure *Authentication protocol*. **Caution:** For better security, do not use this option, except on management networks isolated from the rest of your network. Attackers could easily eavesdrop on sensitive system information. • *Authentication, privacy* — Both encryption (secrecy) and authentication. Also

GUI item	Description
	configure *Authentication protocol* and *Privacy protocol*.
Authentication protocol	Select the hash to use for authentication, either: • *SHA-1* • *MD5* Also configure a salt in *Password*. Both the protocol and password on the SNMP manager and FortiMail must match. This option appears only if *Security level* is either *Authentication, no privacy* or *Authentication, privacy*.
Privacy protocol	Select the encryption algorithm, either: • *AES* • *DES* Also configure a salt in *Password*. Both the protocol and password on the SNMP manager and FortiMail must match. This option appears only if *Security level* is *Authentication, privacy*.

6. Similar to configuring the SNMP community, configure the other settings to specify the destination IP address for sending traps, allowed source IP addresses for receiving queries, and trap events. See Configuring an SNMP community on page 175.
7. Click *OK*.
8. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiMail appliance, test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiMail appliance. To test traps, cause one of the events that should trigger a trap.

FortiMail SNMP MIB files

FortiMail management information blocks (MIB) support most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II).

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

MIB file name	Description
fortimail.mib	Displays the proprietary Fortinet MIB includes detailed FortiMail system configuration information. Your SNMP manager requires this information to monitor FortiMail configuration settings. For more information, see SNMP MIB fields on page 179.
fortimail.trap.mib	Displays the proprietary Fortinet trap MIB includes FortiMail trap information. Your SNMP manager requires this information to receive traps from the FortiMail SNMP agent. For more information, see SNMP traps on page 179.

See also

SNMP traps

SNMP MIB fields

SNMP traps

All traps sent by FortiMail include the trap message as well as the FortiMail unit serial number and host name.

Trap	Description
fmlTrapCpuHighThreshold	Trap sent if CPU usage becomes too high.
fmlTrapMemLowThreshold	Trap sent if memory usage becomes too high.
fmlTrapLogDiskHighThreshold	Trap sent if log disk usage becomes too high.
fmlTrapMailDiskHighThreshold	Trap sent if mailbox disk usage becomes too high.
fmlTrapMailDeferredQueueHighThreshold	Trap sent if the number of deferred email messages becomes too great.
fmlTrapAvThresholdEvent	Trap sent when the number of detected viruses reaches the threshold.
fmlTrapSpamThresholdEvent	Trap sent when the number of spam email messages reaches the threshold.
fmlTrapSystemEvent	Trap sent when system shuts down, reboots, upgrades, etc.
fmlTrapRAIDEvent	Trap sent for RAID operations.
fmlTrapHAEvent	Trap sent when an HA event occurs. This trap includes the contents of the `fmlSysSerial`, `fmlHAEventId`, `fmlHAUnitIp`, and `fmlHAEventReason` MIB fields.
fmlTrapArchiveEvent	Trap sent when remote archive event occurs.
fmlTrapIpChange	Trap sent when the IP address of the network interface has been changed.

See also

FortiMail SNMP MIB files

SNMP MIB fields

SNMP MIB fields

The tables below list the names of the query fields and describe the status information available for each OID in the MIB.

System options MIB field

MIB field	Description
fmlSysModel	FortiMail model number, such as 400 for the FortiMail-400.
fmlSysSerial	FortiMail unit serial number.
fmlSysVersion	The firmware version currently running on the FortiMail unit.
fmlSysVersionAv	The antivirus definition version installed on the FortiMail unit.
fmlSysOpMode	The operation mode (gateway, transparent, or server) of the FortiMail unit.

MIB field	Description
fmlSysCpuUsage	The current CPU usage (%).
fmlSysMemUsage	The current memory utilization (%).
fmlSysLogDiskUsage	The log disk usage (%).
fmlSysMailDiskUsage	The mail disk usage (%).
fmlSysSesCount	The current IP session count.
fmlSysEventCode	System component events.
fmlRAIDCode	RAID system events.
fmlRAIDDevName	RAID device name.
fmlHAEventId	The ID of the most recent HA event. See also Using high availability (HA) on page 223.
fmlHAUnitIp	The IP address of the *port1* network interface on the FortiMail unit where the HA event occured.
fmlHAEffectiveMode	The effective role (applies to active-passive HA only), either as the primary unit or as the secondary unit. The effective role matches the configured mode of operation unless a failover has occurred.
fmlHAEventReason	The reason for the HA event.
fmlArchiveServerIp	IP address of the remote archive server.
fmlArchiveFilename	Archive mail file name.

System options MIB field

MIB field	Description
fmlSysOptIdleTimeout	Idle period after which the administrator is automatically logged out off the system.
fmlSysOptAuthTimeout	Authentication idle timeout value.
fmlSysOptsLan	Web administration language.
fmlSysOptsLcdProt	Whether LCD control buttons protection is enabled or disabled.

System session MIB fields

MIB field	Description
fmlIpSessTable	FortiMail IP sessions table.
fmlIpSessEntry	Particular IP session information.
fmlIpSessIndex	An index value that uniquely identifies an IP session.
fmlIpSessProto	The protocol of the connection.
fmlIpSessFromAddr	The session source IP address,
fmlIpSessFromPort	The session source port number.
fmlIpSessToAddr	The session destination IP address.

MIB field	Description
fmIpSessToPort	The session destination port number. See also Appendix C: Port Numbers on page 611.
fmIpSessExp	Time (in seconds) until the session expires.

Mail options MIB fields

MIB field	Description
fmMailOptionsDeferQueue	The current number of deferred email messages.

Configuring REST API and other web service settings

You can enable the REST API. You can also configure rate limiting for HTTPS requests to the FortiMail unit, including REST API requests.

1. Go to *System* > *Configuration* > *Web Service*.
2. Configure the following and click *Apply*:

GUI item	Description
Redirect HTTP to HTTPS	Enable to redirect HTTP web access to HTTPS.
Redirect to host	Enter the hostname of the FortiMail unit.
REST API	Enable REST API requests.
Rate Control	Expand *Rate Control* to define the maximum concurrent requests, maximum active sessions, and maximum request rate per second for the administrative GUI, webmail, Microsoft 365, and REST API access. Note that the ranges vary depending on FortiMail model: • VM08 supports a maximum of 400. • VM16 and higher supports a maximum of 500.
Repeat Offender Control	Enable to block the IP addresses that keep sending bad HTTP requests to FortiMail and causing FortiMail to return HTTP 404 or 405 errors. • *Offending request count*: Specify the number limit of bad requests within a specified period of time that will trigger offender IP blocking. The valid range is 1 to 50, and the default value is 3. Additionally, click *Exempt IP* to add those IP addresses you wish to exempt from the repeat offender block. • *Time period (minutes)*: Specify the period of time (in minutes) to count the bad requests. The valid range is 1 to 120, and the default value is 5. Use the default value as an example: if within a 5-minute interval, the bad requests from an IP address reach 3, the IP address will be blocked for the remaining of the 5-minutes interval. After the interval expires, the counter will restart for the next interval.

Configuring mail settings

Go to *System* > *Mail Setting* to configure assorted settings that apply to the SMTP server and webmail server that are built into the FortiMail unit.

Configuring mail server settings

You can configure SMTP server and relay settings of the *System* domain, which is located on the local host (that is, your FortiMail unit).

To configure local SMTP server settings

1. Go to *System* > *Mail Setting* > *Mail Server Settings*
2. Configure the following sections:
   - Configuring local host settings on page 182
   - Configuring SMTP service on page 183
   - Configuring IMAP service on page 184
   - Configuring POP3 service on page 184
   - Configuring mail queue settings on page 185
   - Configuring outgoing email options on page 185
   - Configuring DSN options on page 186
   - Configuring deferred message delivery on page 187
   - Configuring domain check options on page 188

Configuring local host settings

Provide the name and SMTP information for the mail server.

GUI item	Description
Host name	Enter the host name of the FortiMail unit. Displays the FortiMail unit's fully qualified domain name (FQDN) is in the format: `<host-name>.<local-domain-name>` such as `fortimail-400.example.com`, where `fortimail-400` is the Host name and `example.com` is the Local domain name. **Note:** The FQDN of the FortiMail unit should be different from that of protected SMTP servers. If the FortiMail unit uses the same FQDN as your mail server, it may become difficult to distinguish the two devices during troubleshooting. **Note:** You should use a different host name for each FortiMail unit, especially when you are managing multiple FortiMail units of the same model, or when configuring a high availability (HA) cluster. This will let you to distinguish between different members of the cluster. If the FortiMail unit is in HA mode, the FortiMail unit will add the host name to the subject line of alert email messages. For details, see Configuring alert email on page 556.
Local domain name	Enter the local domain name to which the FortiMail unit belongs.

GUI item	Description
	The local domain name is used in many features such as email quarantine, Bayesian database training, quarantine report, and delivery status notification (DSN) email messages. FortiMail unit's fully qualified domain name (FQDN) is in the following format: `<host-name>.<local-domain-name>` such as `fortimail-400.example.com`, where `fortimail-400` is the Host name and `example.com` is the Local domain name. **Note:** The IP address should be globally resolvable into the FQDN of the FortiMail unit if it will relay outgoing email. If it is not globally resolvable, reverse DNS lookups of the FortiMail unit's domain name by external SMTP servers will fail. For quarantine reports, if the FortiMail unit is operating in server mode or gateway mode, DNS records for the local domain name may need to be globally resolvable to the IP address of the FortiMail unit. If it is not globally resolvable, web and email release and delete for the per-recipient quarantines may fail. **Note:** The Local domain name is not required to be different from or identical to any protected domain. It can be a subdomain or different, external domain. For example, a FortiMail unit whose FQDN is fortimail.example.com could be configured with the protected domains example.com and accounting.example.net. When sending out quarantine reports, if the FortiMail local domain name is different from its protected domains, FortiMail will use its local domain name, because the local domain name is unique; however, if the FortiMail local domain is the same as one of its protected domains, FortiMail will use its FQDN to send out reports, so as to distinguish itself from the protected domains or other subdomains.
Default domain for authentication	If you set one domain as the default domain, users on the default domain only need to enter their user names without the domain part for webmail/SMTP/IMAP/POP3 authentication, such as `user1`. Users on the non-default domains must enter both the user name part and domain part to authentication, such as `user2@example.com`.

Configuring SMTP service

Use this section to configure SMTP service settings for the mail server. For the configured settings to take effect, enable SMTP Service.

GUI item	Description
SMTP server port number	Enter the port number on which the FortiMail unit's built-in will listens for SMTP connections. See also Appendix C: Port Numbers on page 611.
SMTPS server port number	Enter the port number on which the FortiMail unit's built-in MTA listens for secure SMTP connections. This option is unavailable if SMTP over SSL/TLS is disabled.
SMTP over SSL/TLS	Enable to allow SSL/TLS-secured connections from SMTP clients that request SSL/TLS. When disabled, SMTP connections with the FortiMail unit's built-in MTA must occur as clear text, unencrypted. **Note:** This option must be enabled to be able to receive SMTPS connections. However, it does **not** require them. To enforce client use of SMTPS, see Configuring access control receiving policies on page 337.

GUI item	Description
SMTP MSA service	Enable to let your email clients use SMTP for message submission on a separate TCP port number from deliveries or mail relay by MTAs. For details on message submission by email clients as distinct from SMTP used by MTAs, see RFC 2476.
SMTP MSA port number	Enter the TCP port number on which the FortiMail unit listens for email clients to submit email for delivery. See also Appendix C: Port Numbers on page 611.
Authentication	Enable SMTP, SMTPS, and/or SMTP over TLS authentication.
MTA-STS service	Enable MTA Strict Transport Security (MTA-STS) domain checking: • *Disable*: Disable MTA-STS domain checking. • *Check External Domain*: FortiMail performs MTA-STS checking only when delivering outgoing emails to external domains. • *Check All Domain*: FortiMail checks recipient domain MTA-STS records (including TLS version, format, and MTA-STS policy) for outgoing email to both internal and external domains. Once enabled, MTA-STS domain checking can be utilized in a TLS security profile. For more information, see To configure a TLS profile on page 453
Delivery tracking	If enabled, the history logs will record the following mail delivery statuses: • Delivered • Blocked • Failed • Queued You can view queued email (non-IBE email) in the history log from the right-click pop-up menu. For security reasons, IBE email queue is not accessible to view.

Configuring IMAP service

Use this section to configure IMAP service settings for the mail server. For the configured settings to take effect, enable IMAP Service.

GUI item	Description
IMAP port	Enter the IMAP port number. See also Appendix C: Port Numbers on page 611.
IMAPS port	Enter the IMAPS port number.

Configuring POP3 service

Use this section to configure POP3 service settings for the mail server. For the configured settings to take effect, enable POP3 Service.

GUI item	Description
POP3 port	Enter the POP3 port number.

GUI item	Description
	See also Appendix C: Port Numbers on page 611.
POP3S port	Enter the POP3S port number.

Configuring mail queue settings

Use these sections to configure mail queues and the use of Extended Simple Mail Transfer Protocol (ESMTP).

For more information on the FortiMail mail queue, see Managing the mail queue on page 129 and Managing undeliverable mail on page 131.

GUI item		Description
Mail Queue section		
	Maximum time for email in queue	Select the maximum number of hours that deferred email messages can remain in the deferred or quarantined email queue, during which the FortiMail unit periodically retries to send the message. After it reaches the maximum time, the FortiMail unit sends a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable.
	Maximum time for DSN email in queue	Select the maximum number of hours a delivery status notification (DSN) message can remain in the mail queues. After it reaches the maximum, the FortiMail unit moves the DSN email to the dead mail folder. If set to zero (0), the FortiMail unit attempts to deliver the DSN only once.
	Time before delay warning	Select the number of hours after an initial failure to deliver an email message before the FortiMail unit sends the first delivery status notification (DSN) message to notify the sender that the email message was deferred. After sending this initial DSN, the FortiMail unit continues trying to sending the email until reaching the limit configured in Maximum time for email in queue on page 185.
	Time interval for retry	Select the number of minutes between delivery retries for email messages in the deferred and spam mail queues. ***Note***: This interval setting only applies to the first three delivery retries. Starting from the fourth retry, 20 more minutes will be added to each subsequent retry. For example, if the time interval is set to five minutes, the fourth retry will be 25 minutes later; the fifth retry will be 45 minutes later; and the sixth retry will be 65 minutes later. For more information about mail queue, see Managing the mail queue on page 129.
	Dead mail retention period	Enter the number of days that undeliverable email and its associated DSN will be kept in the dead mail folder. After this time, the dead email and its DSN are automatically deleted.

Configuring outgoing email options

For outgoing email, you can specify to use an STMP relay, instead of the FortiMail built-in MTA, to deliver email.

Under some circumstance, connections from certain relays may by blocked by other parties. If you have other backup relays, you can use them instead.

For information about adding STMP relays, see Configuring SMTP relay hosts on page 188.

GUI item	Description
Deliver to relay host	Select a relay that you configured in Configuring SMTP relay hosts on page 188.
Disable ESMTP	Mark the check box to disable (ESMTP) for outgoing email. By default, FortiMail units can use ESMTP commands. ESMTP supports email messages with graphics, sound, video, and text in various languages. For more information on ESMTP, see RFC 1869.
Delivery Failure Handling	When email delivery fails, you can choose to use the mail queue settings (Configuring mail queue settings on page 185) to handle the temporary or permanent failures. You can also try another relay that you know might work.
Normal	Select this option if you want to queue the email and use the mail queue settings.
Deliver to relay host	Select another relay (backup relay) that you want to use for failed deliveries. Then specify how long the undelivered email should wait in the normal queue before trying the backup relay. You can also specify which types of failed connections the backup relay should take over and retry: • DNS failure: failed DNS lookups • Temporary failure from remote MTA (4XX reply code) • Permanent failure from remote MTA (5XX reply code) • Network failure -- connection • Network failure -- other

Configuring DSN options

Use this section to configure mail server delivery status notifications.

For information on failed deliveries, see Managing the mail queue on page 129 and Managing undeliverable mail on page 131.

GUI item	Description
DSN service	
Regular DSN service	Enable to allow the FortiMail unit to send DSN messages to notify email users of delivery delays and/or failure. Note that if the email message triggers an antispam or antivirus profile, no DSN message will be sent. If it triggers a content profile, a DSN message will still be sent. The following are the potential states in which DSN messages are sent: • SPF=Pass • SPF=None • SPF=Neutral • SPF=PERM-Error • SPF=TEMP-Error • SPF=Sender Alignment

GUI item	Description
	DSN messages are not sent for the following potential states: • SPF=Soft Fail • SPF=Hard Fail
Failure DSN (NDR)	Enable to send DSN (NDR) failure notifications.
Warning DSN	Enable to send DSN warning notifications.
Extended DSN service	Enable successful DSN service and positive delivery notification generation.
DSN email customization	
Failure DSN template	Enable to apply and additionally edit a custom failure DSN template.
Warning DSN template	Enable to apply and additionally edit a custom warning DSN template.
Success DSN template	Enable to apply and additionally edit a custom success DSN template.
Include original message as attachment	Enable to attach original email in delivery status notifications (DSN) or non-delivery reports (NDR).
EHLO/HELO option	Select the argument to use for DSN `EHLO`/`HELO`: • *Host Name*: use the host name of the FortiMail unit. This is the default setting. • *Domain Name*: use the local domain name of the FortiMail unit. • *Other Name*: use the customized name.
Sender displayname	Displays the name of the sender, such as `FortiMail administrator`, as it should appear in DSN email. If this field is empty, the FortiMail unit uses the default name of `postmaster`.
Sender address	Displays the sender email address in DSN. If this field is empty, the FortiMail unit uses the default sender email address of `postmaster@<domain_str>`, where `<domain_str>` is the domain name of the FortiMail unit, such as `example.com`.

Configuring deferred message delivery

You can choose to defer delivery of those email that may be resource intensive and reduce performance of the mail server:

- large email messages
- lower priority email from certain senders, for example, marketing campaign email and mass mailing

For improved FortiMail performance, schedule delivery during times when email traffic volume is low, such as nights and weekends.

To set a deferral period, configure both of the following:

- In *Start delivering messages at*, select the hour and minute of the day at which to begin delivering email messages.
- In *Stop delivering messages at*, select the hour and minute of the day at which to stop delivering email messages.

To configure the size limit or senders of deferred email, see Configuring content profiles on page 404.

Configuring domain check options

Use this section for LDAP compatibility.

If the domain lookup option is also enabled in the LDAP profile (see Configuring domain lookup options on page 435), the parent domain from the domain lookup query is used to hold domain association.

GUI item	Description
Perform LDAP domain verification for unknown domains	Enable to verify the existence of domains that are not configured as protected domains. Also configure LDAP profile for domain check. To verify the existence of unknown domains, the FortiMail unit queries an LDAP server for a user object that contains the email address. If the user object exists and the domain lookup is successful, the email is considered to be incoming and the corresponding incoming policies will be applied.
LDAP profile for domain check	Select the LDAP profile to use when verifying existence of unknown domains. The LDAP query is configured under *User Query Options* in an LDAP profile. If you also enable the domain lookup option in the LDAP profile, the option must be enabled for the domain. This option is available only if Perform LDAP domain verification for unknown domains is enabled.
Automatically create domain association for verified domain	Enable to automatically add unknown domains as domain associations if they are successfully verified by the LDAP query. See Configuring domain lookup options on page 435. For more information about domain association, see Domain Association on page 290. This option is available only if Perform LDAP domain verification for unknown domains is enabled.
Internal domain to hold domain association	Select the name of a protected domain with which to associate unknown domains, if they pass domain verification. However, if the domain lookup query (see Configuring domain lookup options on page 435) returned its own parent domain, that parent domain is used. This option is available only if Automatically create domain association for verified domain is enabled.

Configuring SMTP relay hosts

Configure one or more SMTP relays, if needed, to which the FortiMail unit will relay outgoing email. This is typically provided by your Internet service provider (ISP), but could be mail relays on your internal network.

When you configure mail server settings (Configuring outgoing email options on page 185), you can specify to use a relay host for outgoing email.

If the SMTP relay's domain name resolves to more than one IP address, for each SMTP session, the FortiMail unit will randomly select one of the IP addresses from the result of the DNS query, effectively load balancing between the SMTP relays.

If you do not configure a relay, for outgoing email delivered by the built-in MTA, the FortiMail unit will instead query the DNS server for the MX record of the mail domain in the recipient's email address (`RCPT TO:`), and relay the email directly to that mail gateway. For details, see When FortiMail uses the proxies instead of the built-in MTA on page 195.

Server relay is ignored if the FortiMail unit is operating in transparent mode, and Use client-specified SMTP server to send email (for outgoing connections) or Use this domain's SMTP server to deliver the mail (for incoming connections containing outgoing email messages) is enabled.

Server relay is ignored if email matches a profile where you have enabled Deliver to alternate host.

To configure SMTP relays

1. Go to *System* > *Mail Setting* > *Relay Host List*. You can configure a maximum of five relays.
2. Click *New*.
3. Configure the following:

GUI item	Description
Name	Enter a descriptive name for this relay host.
Host name/IP	Enter the domain name or IP address of an SMTP relay.
Port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).
Use SMTPS	Enable to initiate SSL/TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiMail unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.

Authentication Required	If the relay server requires use of the SMTP `AUTH` command, enable this option, click the arrow to expand the section and configure:
	• *User name*: Enter the name of the FortiMail unit's account on the SMTP relay.
	• *Password*: Enter the password for the FortiMail unit's user name.
	• *Authentication type*: Available SMTP authentication types include:
	  • *AUTO*: Automatically detect and use the most secure SMTP authentication type supported by the relay server.
	  • *PLAIN*: Provides an unencrypted, scrambled password.
	  • *LOGIN*: Provides an unencrypted, scrambled password.
	  • *DIGEST-MD5*: Provides an encrypted hash of the password.
	  • *CRAM-MD5*: Provides an encrypted hash of the password, with hash replay prevention, combined with a challenge and response mechanism.
	  • *NTLM*: Supports NT LAN Manager protocols and provides an hashed password.

See also

Configuring mail server settings

Configuring protected domains

Managing the mail queue

Configuring proxies (transparent mode only)

Troubleshoot MTA issues

Configuring global disclaimers

The *System* > *Mail Setting* > *Disclaimer* tab lets you configure system-wide disclaimer messages. A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential.

Disclaimers can be appended to both incoming and outgoing email. For an explanation of directionality, see Inbound versus outbound email on page 333.

If Allow per-domain settings on page 190 is enabled, you can configure disclaimer messages that are specific to each protected domain. For more information, see Disclaimer for a domain on page 292.

To configure disclaimer messages

1. Go to *System* > *Mail Setting* > *Disclaimer*.
2. Configure the following:

GUI item		Description
Allow per-domain settings		Enable to allow protected domains to select from either the system-wide disclaimer messages, configured below, or their own separate disclaimer messages. Disable to require that all protected domains use the system-wide disclaimer messages. If this option is disabled, domain-specific disclaimers cannot be configured. For information on configuring disclaimer messages specific to a protected domain, see Disclaimer for a domain on page 292.
Enable disclaimer message		Enable to insert customized disclaimers for incoming and/or outgoing mail.
Enable disclaimer exclusion list		Enable if you do not want to insert disclaimers to the email messages from certain senders or to certain recipients. For details about disclaimer exclusion list, see Configuring disclaimer exclusion list on page 191.
Disclaimer message		Enable a message from the table, or click *New* to configure a custom message. In the *Disclaimer Setting* popup window, configure the following:
	Status	Enable/disable the disclaimer message.
	Sender domain	The sender domain can be: • External • Internal • All
	Recipient domain	The recipient domain can be: • External • Internal • All
	Relationship strength	Specify the sender/recipient relationship strength level to apply the disclaimer message.

GUI item		Description
		FortiGuard Social Database contains the social mapping of the email communication flow. For example, if user1@example1.com and user2@exmaple2.com have regular communication, then their SRR is strong; if user1 and user2 have no history of communication before, then their SRR is weak.
	Custom message	Select the custom message. Or click *Edit* to modify an existing one, and configure the following: **Tag subject**: Enable and enter the text that appears in the subject line of the email, such as `[External Email]`. FortiMail will prepend this text to the subject line of email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, such as an external email 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 to insert a new header to the email and append a disclaimer message to the new header, then enter the disclaimer message. The maximum length is 256 characters. Enable and enter the message header key in the field, and the values in the *With value* field. FortiMail adds this text to the message header of the email before forwarding it to the recipient. The maximum length is 256 characters. Many email clients can sort incoming email messages into separate mailboxes, such as an external email mailbox, based on text appearing in various parts of email messages, including the subject line. 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: ALERT-External email from outside of our organization.` 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. **Add content:** Select whether to add the message to the start or end of the mail and then enter the content.

Configuring disclaimer exclusion list

In some cases, you may not want to insert disclaimers to some email messages. For example, you may not want to insert disclaimers to paging text or SMS text messages. To do this, you add the specific source IP netmasks, senders, sender domains, recipients, or recipients domains to the exclusion list, and when you configure the global disclaimer settings (see Configuring global disclaimers on page 190), you can enable the exclusion list.

To create a disclaimer exclusion list

1. Go to *System* > *Mail Setting* > *Disclaimer Exclusion List*.
2. Click *New* to create or new list or double click on an existing one to edit it.

3. Enter a sender pattern, recipient pattern, and/or source IP/mask.
   For example, for sender pattern, if you add *@example.com, all messages from example.com users will be exempted from disclaimer insertion.
   For source IP/mask, if you add 1.1.1.0/24, and both sender and recipient pattern are set to * (wildcard), then emails within the specified IP range are exempted from disclaimer insertion.
4. Click *Create*.

See also

Configuring global disclaimers

Customizing the GUI appearance

Selecting the mail data storage location

The *System* > *Mail Setting* > *Storage* tab lets you configure local or remote storage of mail data such as the mail queues, email archives, email users' mailboxes, quarantined email, and IBE encrypted email.

FortiMail units can store email either locally or remotely. FortiMail units support remote storage by a centralized quarantine, and/or by a network attached storage (NAS) server using the network file system (NFS) protocol.

NAS has the benefits of remote storage which include ease of backing up the mail data and more flexible storage limits. Additionally, you can still access the mail data on the NAS server if your FortiMail unit loses connectivity.

If the FortiMail unit is a member of an active-passive HA group, and the HA group stores mail data on a remote NAS server, disable mail data synchronization to prevent duplicate mail data traffic. For details, see Configuring HA on page 231.

If you store the mail data on a remote NAS device, you cannot back up the data. You can only back up the mail data stored locally on the FortiMail hard disk. Use backup software on the external NAS instead. For information about backing up mail data, see Configuring mailbox backups on page 274.

If you choose remote storage, mail data will not be duplicated locally. Mail data on remote storage cannot be transferred back to local storage either, if you choose to switch to local storage later.

Tested and Supported NFS servers

- Linux NAS
- FreeNAS
- Openfiler
- EMC VNXe3150 (version 2.4.2.21519(MR4 SP2))
- EMC Isilon S200 (OneFS 7.1.0.3)

Untested NFS servers

- Buffalo TeraStation
- Cisco Linksys NAS server

Non-Supported NFS servers

- Windows Server 2003 R2, 2008, 2016, 2019, and 2022

If you do not need consolidated storage for the mail queue and email user inboxes, the higher FortiMail models can act as a centralized quarantine server and IBE encrypted email storage server. If applicable to your model, the *Receive quarantined messages from clients* option and the *Receive IBE messages from clients* option appear on the *Storage* tab. Any FortiMail model can be a client.

To configure mail data storage

1. Go to *System* > *Mail Setting* > *Storage*.
2. Configure the following:

GUI item		Description
Option		
	Local	Select to store email on the FortiMail unit's local disk or RAID.
	NAS server	Select to store email on a remote network attached storage (NAS) server, such as a FortiAnalyzer unit.
	Test (button)	Click to verify the NAS server settings are correct and that the FortiMail unit can access that location. The test action basically tries to discover, login, mount, and unmount the remote device. This button is available only when *NAS server* is selected.

	Protocol	Select a type of the NAS server:
		• *NFS*: To configure a network file system (NFS) server. For this option, enter the following information:
		  • *Hostname/IP address*: The IP address or fully qualified domain name (FQDN) of the NFS server.
		  • *Port*: The port number on which the NFS server listens for connections. See also Appendix C: Port Numbers on page 611.
		  • *Directory*: The directory path of the NFS export on the NAS server where the FortiMail unit will store email.
		• *iSCSI Server*: To configure an Internet SCSI (Small Computer System Interface) server. For this option, enter the following information:
		  • *Username*: User name of the FortiMail unit's account on the iSCSI server.
		  • *Password*: Password of the FortiMail unit's account on the iSCSI server.
		  • *Hostname/IP address*: IP address or fully qualified domain name (FQDN) of the iSCSI server.
		  • *Port*: Port number on which the iSCSI server listens for connections. See also Appendix C: Port Numbers on page 611.
		  • *Encryption key*: Key that will be used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters.
		  • *iSCSI ID*: iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA).

GUI item	Description
	Status: When available. it indicates if the iSCSI share was successfully mounted on the FortiMail unit's file system. This field appears only after you configure the iSCSI share and click *Apply*. *Status* may take some time to appear if the iSCSI server is slow to respond. If *Not mounted* appears, the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiMail unit has both read and write permissions on the iSCSI server.
Refresh (button)	This button appears when you configure an iSCSI server. Click it to update the information in the *Status* field.
Click here to format this device **Click here to check file system on this device**	These two links appear when you configure an iSCSI server and click *Apply*. Click a link to initiate the described action (that is, format the device or check its file system). A message appears saying the action is being executed. Click *OK* to close the message and click *Refresh* to see a *Status* update. **Note**: If the iSCSI disk has never been formatted, FortiMail needs to format it before it can be used. If the disk has been formatted before, you do not need to format it again. unless you want to wipe out the data on it.
Centralized Quarantine	
Disabled	Select to store the quarantines on the FortiMail unit's local disk or RAID.
Receive quarantined messages from clients	Select to have this FortiMail unit act as a centralized quarantine server, then enter the IP addresses of all valid clients. This option is available on some high end models. FortiMail VM02, 400E, 1000D and 2000E models can host a maximum of 10 clients and FortiMail 3000 series and above models can host up to 20 clients. Any FortiMail model can be a client. Other FortiMail units acting as clients send all their quarantined email to this FortiMail unit. This FortiMail unit only accepts a connection if the client's IP address matches an IP address on the list of clients configured here.
Send quarantined messages to remote server	Select to have this FortiMail unit act as a centralized quarantine client. All quarantined email is saved on a centralized quarantine server, if available. When selected, enter the following information: • *Over SSL*: Select to send quarantined messages over SSL/TLS. • *Hostname/IP address*: Enter home name or IP address of the FortiMail unit that is acting as a centralized quarantine server.
Centralized IBE	
Disabled	Select to store IBE encrypted email on the FortiMail unit's local disk or RAID.
Receive IBE messages from clients	Select to have this FortiMail unit act as a centralized IBE mail storage server, then enter the IP addresses of all valid clients which are the FortiMail units that are configured to send IBE messages to this unit. This option is available on some high end models. FortiMail -400E, 1000D, 2000E and VM02 models can host a maximum of 10 clients and FortiMail 3000 series models and greater can host up to 20 clients. Any FortiMail model can be a client.

GUI item	Description
	Other FortiMail units acting as clients send all their IBE email to this FortiMail unit. This FortiMail unit will only accept a connection if the client's IP address matches an IP address on the list of clients configured here. **Note**: The protected domains on the IBE mail server must match the domains on the clients. Otherwise the secure mail recipients cannot retrieve their secure email from the server.
Send IBE messages to remote server over SSL	Select to have this FortiMail unit act as a centralized IBE storage client. All IBE email will be saved on the centralized IBE mail storage server, if available. When selected, enter the following information: • *Name*: Enter a name to identify this client to the centralized IBE mail storage server. This value must match the name of the client as it is configured on the centralized IBE mail storage server. Otherwise, the connection will fail. • *Host*: Enter the IP address of the FortiMail unit that is acting as a centralized IBE mail storage server.

Configuring proxies (transparent mode only)

In addition to the proxy settings under each network interface settings, you can also go to *System* > *Mail Setting* > *Proxies* to configure connection pick-up of the proxies and implicit relay.

Furthermore, the protected domains and session profiles also configure aspects of the proxies and implicit relay, such as transparency. For details, see Configuring protected domains on page 280 and Configuring session profiles on page 361.

This section contains the following topics:

About the transparent mode proxies

FortiMail has two transparent proxies: an incoming proxy and an outgoing proxy. The proxies' degree of transparency at the IP layer and at the SMTP layer varies by your configuration. Proxy behaviors are configured separately based on whether the SMTP connection is considered to be incoming or outgoing. Depending on your configuration, a FortiMail unit operating in transparent mode may implicitly use its built-in MTA instead.

Depending on your network topology, verify that email is not being scanned twice.

When FortiMail uses the proxies instead of the built-in MTA

When operating in transparent mode, a FortiMail unit has two ways of handling an SMTP connection: to proxy, or to relay. A FortiMail unit will proxy a connection only if you have enabled the proxy option applicable to the connection's

directionality, either:

- Use client-specified SMTP server to send email (for outgoing connections), or
- Use this domain's SMTP server to deliver the mail on page 287 (for incoming connections containing outgoing email messages)

  This option is ignored for email that matches an antispam or content action profile where you have enabled Deliver to alternate host.

Otherwise, it will use its built-in MTA instead.

Unlike in gateway mode, in transparent mode, the built-in MTA is used implicitly. SMTP clients do not explicitly connect to it, but unless proxied, all connections traveling through the FortiMail unit are implicitly handled by the built-in MTA. In this sense, while in transparent mode, the built-in MTA may initially seem to be similar to the proxies, which are also used implicitly, and not specifically requested by the SMTP client. However, the proxies or the built-in MTA may reroute connections to different destination IP addresses, and thereby may affect mail routing.

Because the outgoing proxy does not queue undeliverable email or apply authentication, while the built-in MTA and incoming proxy do, whether a proxy or the built-in MTA handles a connection may also affect the FortiMail unit's mail queues and authentication Verify.

Mail routing in transparent mode

Destination IP of connection	`RCPT TO:`	Configuration		Result
SMTP server (incoming connection)	**Not** a protected domain (outgoing email)	Use this domain's SMTP server to deliver the mail is enabled		Incoming queueing proxy establishes session with Use this domain's SMTP server to deliver the mail
		Use this domain's SMTP server to deliver the mail is disabled	Relay Server section is configured	Built-in MTA establishes session with Relay Server section
			Relay Server section is **not** configured	Built-in MTA performs MX lookup of the domain in `RCPT TO:` and establishes session with the resulting MTA
Not SMTP server (outgoing connection)	N/A	Use client-specified SMTP server to send email is enabled		Outgoing non-queueing proxy establishes session with the unprotected MTA
		Use client-specified SMTP server to send email is disabled	Relay Server section is configured	Built-in MTA establishes session with Relay Server section
			Relay Server section is **not** configured	Built-in MTA performs MX lookup of the domain in `RCPT TO:` and establishes session with the resulting MTA

You can determine whether a connection was handled using the built-in MTA or one of the proxies by viewing the Mailer column of the history log messages.

- `mta`: The connection was handled by the built-in MTA.
- `proxy`: The connection was handled by either the incoming proxy or the outgoing proxy.

For information on viewing the history log, see Viewing log messages on page 113.

See also

Incoming versus outgoing SMTP connections

Relaying using FortiMail's built-in MTA versus unprotected SMTP servers

Use client-specified SMTP server to send email

Incoming versus outgoing SMTP connections

At the network connection level, directionality is determined by the destination IP address.

- **Incoming connections**

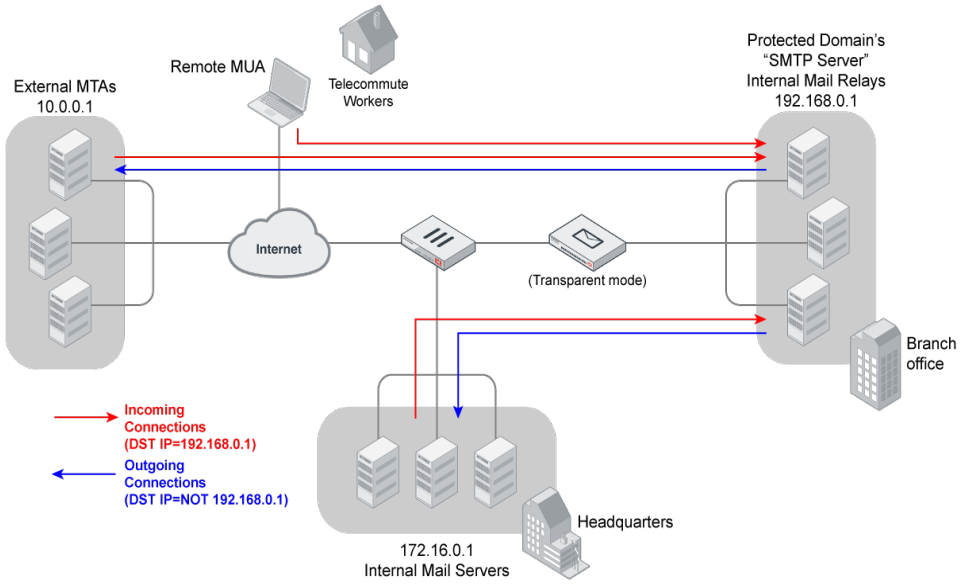
  The destination IP address matches a protected domain's SMTP server.

- **Outgoing connections**

  The destination IP address does **not** match any protected domain's SMTP server.

Connection level directionality does not consider a connection's source IP address, nor whether or not the recipient email address's (`RCPT TO:`) mail domain is a protected domain.

Incoming versus outgoing SMTP connections



Directionality at the connection level may be different than directionality at the level of email messages contained by the connection. Incoming connections can contain an outgoing email message. The opposite is also possible.

For example, in Incoming versus outgoing SMTP connections on page 197, connections from the internal mail relays to the internal mail servers are outgoing connections, but they contain incoming email messages. Conversely, connections

MUAs to the internal mail relays are incoming connections, but may contain outgoing email messages if the recipients' email addresses (`RCPT TO:`) are external.

For information on the concept of incoming versus outgoing at the application layer, see Inbound versus outbound email on page 333.

When the FortiMail unit is operating in transparent mode, directionality correlates with which proxy will be used, if any.

For example, in Incoming versus outgoing SMTP connections on page 197, the protected domain is example.com. Mailboxes for example.com are stored on servers located at the company's headquarters, separate from the mail relays, which are located at a branch office. All email is routed through the mail relays, and so the FortiMail unit is deployed in front of the mail relays at the branch office.

On the FortiMail unit, you have configured the protected domain's SMTP server to be 192.168.0.1, a mail relay, because all email must be routed through that mail relay. You have also enabled Use client-specified SMTP server to send email, so, for outgoing connections, the outgoing proxy will be used instead of the built-in MTA. However, you have not enabled Use this domain's SMTP server to deliver the mail on page 287, so, for incoming connections, the built-in MTA will be used, rather than the incoming proxy.

You can configure interception and transparency separately for each of the two proxies. Regardless of which proxy is used, the proxy may not be fully transparent unless you have configured it to be so. For details, see Transparency of the proxies and built-in MTA on page 198.

See also

Avoiding scanning email multiple times

Transparency of the proxies and built-in MTA

Relaying using FortiMail's built-in MTA versus unprotected SMTP servers

When FortiMail uses the proxies instead of the built-in MTA

Transparency of the proxies and built-in MTA

A FortiMail unit 's built-in MTA and proxies are not necessarily fully transparent, even if the FortiMail unit is operating in transparent mode.

If you want the FortiMail unit to behave truly transparently, you must:

- select the Hide this box from the mail server on page 362 option in each session profile
- select Hide the transparent box on page 286 in each protected domain

Otherwise, the source IP address of connection initiations, the destination IP address of reply traffic, and the SMTP greeting (`HELO`/`EHLO`) will contain either:

- the management IP address (for connections occurring through bridged network interfaces), or
- the network interface's IP address (for connections through out-of-bridge network interfaces)

In addition to preserving the original IP addresses and domain names, for connections to unprotected domains, to be hidden with regards to authentication, the FortiMail unit must pass SMTP `AUTH` commands through to the SMTP server instead of applying an authentication profile. To do this, you must enable Use client-specified SMTP server to send email

on page 203 in order to use the outgoing proxy instead of the built-in MTA. The outgoing proxy will transmit SMTP `AUTH` commands to the server, instead of applying the IP-based policy's authentication profile on behalf of the server.

See also

Incoming versus outgoing SMTP connections

Relaying using FortiMail's built-in MTA versus unprotected SMTP servers

When FortiMail uses the proxies instead of the built-in MTA

Avoiding scanning email multiple times

Depending on your network topology, in transparent mode, you may need to verify that the FortiMail unit is not scanning the same email multiple times.

Redundant scanning can result if all origins of outgoing email are not physically located on the same network as the protected domain's mail relay (SMTP server). This is especially true if your internal relays and mail servers are physically located on separate servers, and those servers are not located on the same network. Due to mail routing, an email could travel through the FortiMail unit multiple times in order to reach its final destination. As a result, if you have selected *Proxy* more than once in *System* > *Network* > *Interface*, it is possible that an email could be scanned more than once, decreasing the performance of your email system and unnecessarily increasing delivery time.

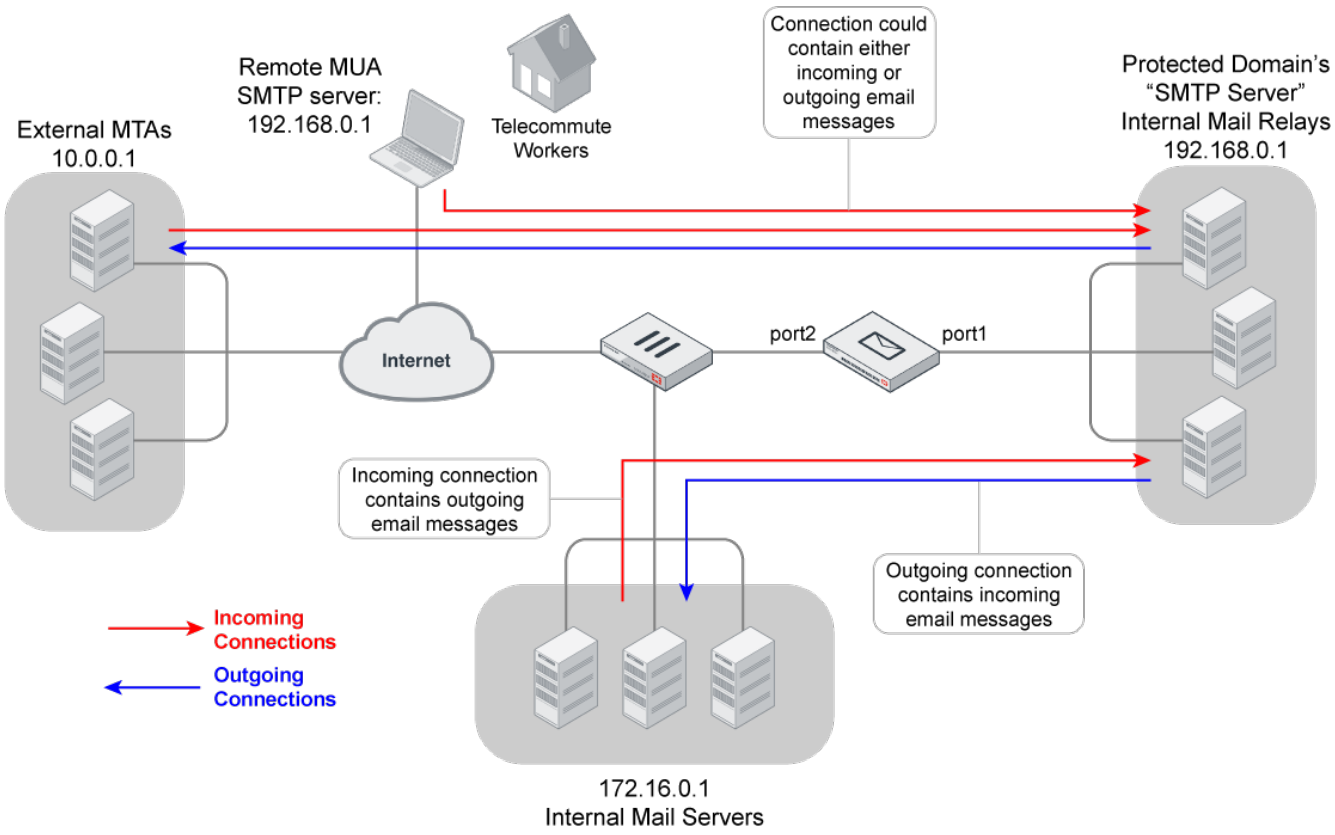
There are some topologies, however, when it is correct to select *Proxy* for multiple network interfaces, or even for both incoming and outgoing connections on the same network interface. It is important to understand the impact of the relevant configuration options in order to configure transparent mode proxy/relay pick-up correctly.

The following two examples demonstrate correct configurations for their topology, and illustrate the resulting mail routing.

Example 1

All email must be routed through the internal mail relays. Internal mail servers, internal MUAs, and remote MUAs all send mail through the mail relays, whether the recipient is a member of the protected domain or not. Because of this, the FortiMail unit is deployed directly in front of the internal mail relays, which are physically located on a network separate from the mail servers that store email for retrieval by email users. For each protected domain, SMTP server is configured with the IP address of an internal mail relay.

The following image and table shows the topology and configuration options that result in correct mail routing for this example.



Setting	Value
MUAs' SMTP server/MTA	The virtual IP on the FortiGate unit, or other public IP address, that routes to 192.168.0.1 (the internal mail relays)
each protected domain's SMTP server	192.168.0.1
each protected domain's Use this domain's SMTP server to deliver the mail	enabled
Use client-specified SMTP server to send email	enabled
port1's Incoming connections	Pass through **or** Drop
port1's Outgoing connections	Pass through
port2's Incoming connections	Proxy proxy
port2's Outgoing connections	Pass through **or** Drop

Because the FortiMail unit is deployed directly in front of the relays, which are not on the same network as either the remote MUAs or the internal mail servers, if proxy/relay pick-up is not configured correctly, outgoing email could be scanned twice: once as it travels from port2 to port1, and again as it travels from port1 to port2. In addition, if proxying is not configured correctly, email would be picked up by the built-in MTA instead of the proxy, and might never reach the internal mail relays.

To solve this, do **not** configure the FortiMail unit to use its built-in MTA to intercept incoming connections and deliver email messages. Instead, it should proxy the incoming connections, allowing them to reach the internal mail relays. Because all email was already scanned during the incoming connection, when the internal mail relay initiates the

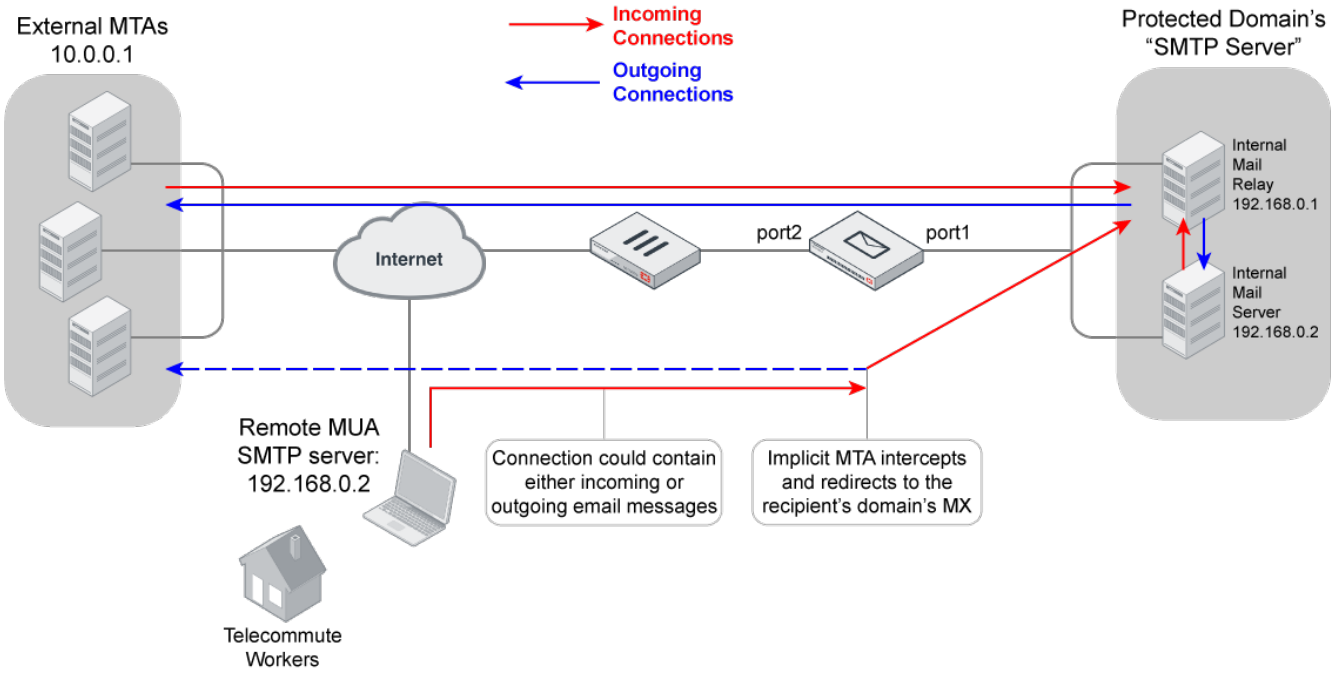
outgoing connection to either an external MTA or to the internal mail server, the FortiMail unit does not need to scan the email again. In addition, because the internal mail relays maintain the queues, the FortiMail unit does not need to maintain queues for outgoing connections. It can instead use its outgoing proxy, which does not queue, and will not reroute email. Finally, there should be no incoming connections on port1, nor outgoing connections on port2; so, configure them either as Pass through or Drop.

Example 2

All **incoming** email must be routed through the internal mail relays. The internal mail server also routes outgoing email through the relays. Because of this, the FortiMail unit is deployed directly in front of the internal mail relays, which are physically located on the same network as the mail servers that store email for retrieval by email users. For each protected domain, SMTP server is configured with the IP address of an internal mail relay.

Remote MUAs' outgoing email must not be routed through the internal mail relays.

The following image and table shows the topology and configuration options that result in correct mail routing for this example.



Setting	Value
MUAs' SMTP server/MTA	the virtual IP on the FortiGate unit, or other public IP address, that routes to 192.168.0.2 (the internal mail server, **not** the internal mail relays)
each protected domain's SMTP server	192.168.0.1
each protected domain's Use this domain's SMTP server to deliver the mail	disabled
Use client-specified SMTP server to send email	disabled

Setting	Value
port1's Incoming connections	Pass through
port1's Outgoing connections	Proxy
port2's Incoming connections	Proxy
port2's Outgoing connections	Proxy
Relay Server section	not configured
MX record for each protected domain on the internal DNS server	domain name resolving to 192.168.0.1 (the internal mail relays)

Unlike external MTAs making **incoming** connections to the relays, remote MUAs instead make **outgoing** connections through port2: their destination is the internal mail server, whose IP address is **not** configured in the protected domain (the protected domain's SMTP server is instead configured with the IP address of the internal mail relay). As a result, you can configure pick-up for these connections separately from those of external MTAs — they pass through the same port, but are distinct in their directionality.

In this case, we want to intercept connections for both external MTAs and remote MUAs. To solve this, we select Proxy for both Incoming connections on page 158 from external MTAs and Outgoing connections on page 159 (from remote MUAs) on port 2 (if we wanted to block remote MUAs only, we could simply select Drop for Outgoing connections on page 159 on port2).

However, the remote MUAs' configuration also means that the directionality of remote MUAs' connections coincides with that of the internal relays' connections to external relays: **both are outgoing**. Therefore if you configure the FortiMail unit to proxy outgoing connections instead of using the built-in MTA by enabling Use client-specified SMTP server to send email on page 203, **both** outgoing connections are proxied.

Remote MUAs' connections would all travel through the internal mail server, regardless of whether the recipient has an account on that mail server or not. Outgoing email would then need to be forwarded to the internal mail relay, and back out through the FortiMail unit. As a result, outgoing email from remote MUAs would travel extra mail hops. This would burden the internal network with traffic destined for an external network, and needlessly increases points of potential failure.

Additionally, because the FortiMail unit is deployed directly in front of both the relays and the mail server, which is not on the same network as remote MUAs, remote MUAs' outgoing email could be scanned twice: once as it travels from port2 to port1, and again as it travels from port1 to port2. This is resource-inefficient.

To solve this, the FortiMail unit should **not** be configured to use its proxy to intercept outgoing connections. Instead, it should use its built-in MTA. The built-in MTA forms its own separate connections based on the MX lookup of the recipient's domain, rerouting email if necessary. Notice that as a result of this lookup, although remote MUAs are configured to connect to the internal mail server, connections for incoming email are actually diverted by the built-in MTA through the internal mail relays. This has the benefit of providing a common relay point for all internal email.

Rerouting also prevents outgoing email from passing through the FortiMail unit multiple times, receiving redundant scans. This prevents externally-destined email from burdening the internal mail relays and internal mail servers.

Finally, there should be no incoming connections on port1, so it can be configured either as Pass through or Drop.

Relaying using FortiMail's built-in MTA versus unprotected SMTP servers

When not proxying, FortiMail units can use their own built-in SMTP relay to deliver email.

For example, If an email user at the branch office, behind a FortiMail unit, specifies the unprotected SMTP server 10.0.0.1 as the outgoing SMTP server, you can either let the email user send email using that specified unprotected SMTP server, or ignore the client's specification and insist that the FortiMail unit send the email message itself (see Incoming versus outgoing SMTP connections on page 197).

- If you permit the client to specify an unprotected SMTP server, the FortiMail unit will allow the email client to connect to it, and will not act as a formal relay. If the client's attempt fails, the outgoing proxy will simply drop the connection and will not queue the email or retry.
- If you insist that the client relay email using the FortiMail unit's built-in MTA rather than the client-specified relay, the FortiMail unit will act as an MTA, queuing email for temporary delivery failures and sending error messages back to the email senders for permanent delivery failures. It may also reroute the connection through another relay server, or by performing an MX lookup of the recipient's domain, and delivering the email directly to that mail gateway instead.

Enabling the FortiMail unit to allow clients to connect to unprotected SMTP servers may be useful if, for example, you are an Internet service provider (ISP) and allow customers to use the SMTP servers of their own choice, but do not want to spend resources to maintain SMTP connections and queues to external SMTP servers.

Unlike the outgoing proxy, the incoming proxy **does** queue and retry. In this way, it is similar to the built-in MTA.

For information on configuring use of the incoming proxy or outgoing proxy instead of using the built-in MTA, see Use client-specified SMTP server to send email on page 203 (for outgoing connections) and Use this domain's SMTP server to deliver the mail on page 287 (for incoming connections containing outgoing email messages).

See also

Incoming versus outgoing SMTP connections

Transparency of the proxies and built-in MTA

When FortiMail uses the proxies instead of the built-in MTA

Use client-specified SMTP server to send email

In FortiMail transparent mode, go to *System* > *Mail Setting* > *Preference* to enable this feature to use the outgoing proxy instead of the built-in MTA for outgoing SMTP connections. This allows the client to send email using the SMTP server that they specify, rather than enforcing the use of the FortiMail unit's own built-in MTA. The outgoing proxy refuses the connection if the client's destination SMTP server is not available. In addition, it will not queue email from the SMTP client, and if the client does not successfully complete the connection, the outgoing proxy will simply drop the connection, and will not retry.

Since authentication profiles may not successfully complete, the outgoing proxy will also ignore any authentication profiles that may be configured in the IP-based policy. The built-in MTA would normally apply authentication on behalf of the SMTP server, but the outgoing proxy will instead pass any authentication attempts through to the SMTP server, allowing it to perform its own authentication.

Disable to relay email using the built-in MTA to either the SMTP relay defined in Configuring SMTP relay hosts on page 188, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (RCPT TO:) domain. The email may not actually travel through the unprotected SMTP server, even though it was the relay originally specified by the SMTP client. For details, see When FortiMail uses the proxies instead of the built-in MTA on page 195.

If this option is enabled, consider also enabling Prevent open relaying on page 370. Failure to do so could allow clients to use open relays.

If this option is disabled, and an SMTP client is configured to authenticate, you must configure and apply an authentication profile. Without the profile, authentication with the built-in MTA will fail. Also, the mail server must be explicitly configured to allow relay from the built-in MTA in this case.

If this option is enabled, you cannot use IP pools. For more information, see Configuring IP pools on page 458.

For security reasons, this option does not apply if there is no session profile selected in the applicable IP-based policy. For more information on IP policies, see Controlling email based on IP addresses on page 348.

Customizing GUI, custom messages, email templates, and Security Fabric

Configuring custom messages

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

These custom message are used for login pages, IBE messages, and other system-relate message. The content, DLP, and antivirus replacement messages used in the action profiles are configured under Profile > Replacement Massage. For details, see Configuring replacement message profiles and variables on page 416.

All the disclaimers, custom messages, and IBE login page are customizable. When you create email template on the *System* > *Customization* > *Custom Email Template* tab, you can use many of the replacement messages.

Viewing the custom messages list

To view the custom message list, go to *System* > *Customization* > *Custom Message*.

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 reword existing messages or create new ones.

Modifying custom messages

You can modify the text and HTML code within a custom message to suit your requirements.

You can change the content of the custom message by editing the text and HTML codes and by working with custom message variables. For descriptions of the default custom message variables, see Default custom message variables on page 205.

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.

Some messages include a Subject and From area. You can edit their content too and add variables.

4. There is a limit of 8191 characters for each custom message.
5. If custom variables exist, you can add them to the text. To do so:
   - Click *Insert 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.
   - 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 205.
6. 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 messages that you will use frequently. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

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*.
   The *Edit Variable* page appears.
3. Click *New*.
   A dialog appears.
4. Configure the following:
   - In Name, enter the variable name to use in the custom message. Its format is: `%%<variable_name>%%`. For example, if you enter the word `virus`, this variable will appear as `%%virus%%` in the custom 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. Click Insert Variables to include any other existing variables, if needed. 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.

   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*.
5. Click *Create*.

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.	

Variable	Description	Location
%%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) of the quarantined email.	
%%QMSG_EMAIL_ DELETE%%	Under email actions in the quarantine summary, the Delete link that, if being 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 480.	
%%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 480.	
%%SPAM_PREFERENCE%%	The Click Here link under Other in the quarantine summary that, if being 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 header From of the email.	
%%ORIG_FROM_DOMAIN%%	The original header From domain of the 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 472)
- IBE (see FortiMail IBE configuration workflow on page 518)
- repackaging virus-infected email with new email body (see Configuring antivirus action profiles on page 402)
- notifying the recipeint for any FortiMail actions (see Configuring notification profiles on page 461)

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

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.
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 swatchs 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.

Customizing the GUI appearance

The *System* > *Customization* > *Appearance* tab lets you customize the default appearance of the administrator and webmail GUI with your own product name, product logo, and corporate logo.

You can customize the webmail interface language. If your preferred language is not currently installed, you can add it. You can also adjust the terms in existing language files. This can be useful for localizing terms within a language. For example, you could adjust the English language file to use spellings and terms specific to the locale of the United Kingdom, Australia, or the USA if your email users are most familiar with terminologies popular in those areas.

To customize the GUI appearance

1. Go to *System* > *Customization* > *Appearance*.
2. Click the arrow to expand Administration Interface and Webmail interface.

3. Configure the following to change appearance:

GUI item		Description
Admin Portal		
	Product name	Enter the name of the product. This name will precede *Administrator Login* in the title on the login page of the GUI.
	Product icon	Click *Change* to upload an icon that will be used as the favicon of the FortiMail GUI. The default icon is the Fortinet company icon.
	Custom top logo	Click *Change* to upload a graphic that will appear at the top of all pages in the GUI. The image's dimensions must be 460 pixels wide by 36 pixels tall. For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic. **Note:** Uploading a graphic overwrites the current graphic. The FortiMail unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again later.
	Login page	Select one of the following options: • *Default/Built-in*: uses the default login page. • *Single sign on only*: Use SSO configured in Configuring single sign-on (SSO).
	Default language	Select the default language for the display of the GUI and the login page. You can configure a separate language preference for each administrator account. For details, see Configuring administrator accounts on page 168.
	Default theme	Select the default display theme (red, green, blue, and light blue) for the display of the GUI and the login page. You can configure a separate theme preference for each administrator account. For details, see Configuring administrator accounts on page 168.
	System description	Optionally enter a description or comment.
Webmail Portal		
	Webmail login	Enter a word or phrase that will appear on top of the webmail login page, such as Webmail Login.
	Login user name hint	Enter a hint for the user name. This hint will appear when you hover your mouse cursor over the login name field.
	Login page	Select either: • *Customize*: Edit the page to create your own login page. • *Default/Built-in*: Use the default login page. • *Single sign on only*: Use SSO configured in Configuring single sign-on (SSO). If you have enabled single sign-on (SSO) and want to disable the username and password fields on the login page, see the FortiMail CLI Reference.
	Allow user to change theme	If selected, the webmail users will be able to customize the theme by themselves.

GUI item	Description
Show online help link	If selected, the Help button will appear on the webmail interface. The default help contents are provided by Fortinet. If you want to use your own organization's help contents, you can enable this option and enter the online help URL in the below field.
Custom online help URL	Enter the URL if you want to use your own online help file, instead of the default one that comes with FortiMail.
Custom webmail top logo	Click Change to upload an image that will appear at the top of all webmail pages. The image's dimensions must be 314 pixels wide by 36 pixels tall. **Note:** Uploading an image overwrites the current graphic. The FortiMail unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time.
Default language	Select the language in which webmail pages will be displayed. By default, the FortiMail unit will use the same language as the administrative GUI. For GUI language settings, see Configuring system options on page 172.
Default theme	Select a theme for the webmail GUI.
Webmail language customization	Displays the list of languages installed on the FortiMail unit in English and in their own language. • Create: Click to add a new language to the list. See To add a custom language on page 214. • Download: Select a language in the list, then click this button to download the language's resource file for that language. You can then edit the resource files using an XML editor that supports UTF-8. • Upload: Select a language in the list, then click this button to update the language's resource file for this language from your management computer to the FortiMail unit. In addition to uploading new language resource files, you can also use this button to update existing languages. • Delete: Select a language in the list, then click this button to remove the language. This option is available only for non-default languages.

4. Click Apply to save changes or Reset to return to the default settings.

To add a custom language

Note: The following steps require 7-Zip to decompress and compress archive file formats.

1. Go to *System* > *Customization* > *Appearance*.
2. Expand *Webmail Portal*, and expand *Webmail Language Customization*.
3. Underneath the list of language customizations, click Create.
4. In *Language name in English*, enter the name for the new language using English and US-ASCII encoding, such as `Welsh`.
5. In *Language name*, enter the name for the language using its own characters and UTF-8 encoding.
6. Click Create.
   The new language appears at the bottom of the webmail languages list.
7. Select the new language's row.
8. Click Download.

Your web browser downloads the file as a TGZ file.

9. Locate the downloaded file in Windows Explorer and extract the files using 7-Zip.
10. Open the extracted TAR file in an XML editor or plain text editor that supports UTF-8 encoding (Notepad++ for example).
11. For each `value` in the resource file, translate the word or phrase that is surrounded by double quotes (`"`). It will appear in the location indicated by the key's name.
    For example:
    ```
    <resource key="report_spam" value="Report Spam"/>
    ```
    indicates by `key="report_spam"` that the text is a label for the button that corrects the Bayesian scanner when it has not recognized an email that is spam. You could replace the contents of `value` (that is, `Report Spam`) with any text in your language that indicates the button's function.
12. Save the TAR file.
13. Right-click the TAR file and click *7-Zip* > *Add to archive*.
14. Set *Archive format* to *gzip* and click OK.
15. Return to the FortiMail GUI.
16. Select the new language's row.
17. Click Upload and select the compressed GZ file containing the translated resource file, then click Open.
18. Click Apply.
    To verify your language, log in to FortiMail webmail and review the text that appears on each button, field, and menu item. If the characters appear garbled, verify that your web browser is interpreting the web page using the correct encoding.

Enabling Security Fabric

FortiMail can connect to an upstream FortiGate root and become an integrated cluster member of a Security Fabric.

Go to *System* > *Customization* > *Security Fabric* to enable FortiMail to become a Security Fabric member. The Security Fabric FortiGate root can then establish a connection to the FortiMail unit using the IP address and port number specified.

This feature can also be configured in the CLI. For more information, see the FortiMail CLI Reference.

See also

Configuring administrator accounts

About administrator account permissions and domains

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 supports SSO for both the administrator and webmail GUI.

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.

Server mode SSO

When using SSO for domain authentication in server mode, you need to configure an LDAP profile for the domain users. Otherwise even if the users can log on to FortiMail webmail, they cannot send email unless you create local users first.

After applying the LDAP profile under the domain user profile (see Managing users on page 297), FortiMail can perform proper recipient verification and accept email if the user exists. Therefore, there would be no need to create local users.

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.
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.

GUI Item	Description
	• 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
Enabled	Enable or disable SSO.
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.
Allow dynamic IP from IdP	Enable to support dynamic client IP addresses from the IdP server within the same SAML session. And then specify the IP range. If no IP range is specified, any client IP address from the IdP server is allowed.

- 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 *Authentication type* and *Single sign on profile*, 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.

Configuring RAID

If your FortiMail model supports RAID, go to System > RAID to configure a redundant array of independent disks (RAID) for the FortiMail hard disks that are used to store logs and email.

Most FortiMail models can be configured to use RAID with their hard disks. The default RAID level should give good results, but you can modify the configuration to suit your individual requirements for enhanced performance and

reliability. For more information, see Configuring RAID on FortiMail models with software RAID controllers on page 219 or Configuring RAID on FortiMail models with hardware RAID controllers on page 221.

For some FortiMail models, you can configure the RAID levels for the local disk partitions used for storing email files or log files, depending on your requirements for performance, resiliency, and cost.

RAID events can be logged and reported with alert email. These events include disk full and disk failure notices. For more information, see About FortiMail logging on page 535, and Configuring alert email on page 556.

If your FortiMail model does not support RAID, the RAID menu won't be displayed.

See also

About RAID levels

Configuring RAID on FortiMail models with software RAID controllers

Configuring RAID on FortiMail models with hardware RAID controllers

About RAID levels

Supported RAID levels vary by FortiMail models.

Some models use software RAID controllers which support RAID levels 0 or 1. You can configure the log disk with a RAID level that is different from the email disk.

Some models use hardware RAID controllers requiring that the log disk and mail disk use the same RAID level.

Some models do not support RAID.

The available RAID levels depend on the number of hard drives installed in the FortiMail unit and different FortiMail models come with different number of factory-installed hard drives. You can added more hard drives if required. For details, see Replacing a RAID disk on page 222.

For more information about the supported RAID levels on your FortiMail unit, contact Fortinet Technical Support.

The following tables describe RAID levels supported by each FortiMail model.

FortiMail supported RAID levels

Number of Installed Hard Drives	Available RAID Levels	Default RAID Level
1	0	0
2	0, 1	1
3	0, 1 + hot spare, 5	5
4	5 + hot spare, 10	10
5	5 + hot spare, 10 + hot spares	10 + hot spares
6	10, 50	10

Number of Installed Hard Drives	Available RAID Levels	Default RAID Level
7 or more	10, 10 + hot spares, 50, 50 + hot spares	50 + hot spares

See also

Configuring RAID on FortiMail models with software RAID controllers

Configuring RAID on FortiMail models with hardware RAID controllers

Hot spares

FortiMail models with a hardware RAID controller have a hot spare RAID option. This feature consists of one or more disks that are pre-installed with the other disks in the unit. The hot spare disk is idle until an active hard disk in the RAID fails. Then the RAID immediately puts the hot spare disk into service and starts to rebuild the data from the failed disk onto it. This rebuilding may take up to several hours depending on system load and amount of data stored on the RAID, but the RAID continues without interruption during the process.

The hot spare feature has one or more extra hard disks installed with the RAID. A RAID 10 configuration requires two disks per RAID 1, and has only one hot spare disk. A RAID 50 configuration requires three disks per RAID 5, and can have up to two hot spare disks.

Configuring RAID on FortiMail models with software RAID controllers

Back up data on the disk before changing the RAID level. Changing the device's RAID level temporarily suspends all mail processing and erases all data on the hard disk. For more information on creating a backup, see Backup and restore on page 267.

To view and configure RAID levels

1. Go to *System* > *RAID* > *RAID System*.

GUI item	Description
Device	Displays the name of the RAID unit. This indicates whether it is used for log message data or for mailboxes, mail queues, and other email-related data. This is hard-coded and not configurable.
Unit	Displays the internal mount point of the RAID unit. This is hard-coded and not configurable.
Level	Displays the RAID level that indicates whether it is configured for optimal speed, failure tolerance, or both. For more information on RAID levels, see About RAID levels on page 218. To change the RAID level, click the row corresponding to the RAID device whose RAID level you want to change and select RAID level 0 or 1.
Resync Action	Displays the status of the RAID device. • idle: The RAID is idle, with no data being written to or read from the RAID disks. • dirty: Data is currently buffered, waiting to be written to disk. • clean: No data is currently buffered, waiting to be written to the RAID unit. • errors: Errors were detected on the RAID unit. • no-errors: No errors were detected on the RAID unit. • dirty no-errors: Data is currently buffered, waiting to be written to the RAID unit, and there are currently no detected RAID errors. For a FortiMail unit in active use, this is the expected setting. • clean no-errors: No data is currently buffered, waiting to be written to the RAID unit, and there are currently no RAID errors. For a FortiMail unit with an unmounted array that is not in active use, this is the expected setting.
Resync Status	If the RAID unit is not synchronized and you have clicked Click here to check array to cause it to rebuild itself, such as after a hard disk is replaced in the RAID unit, a progress bar indicates rebuild progress. The progress bar appears only when Click here to check array has been clicked and the status of the RAID is **not**`clean no-errors`.
Speed	Displays the average speed in kilobytes (KB) per second of the data transfer for the resynchronization. This is affected by the disk being in use during the resynchronization.
Apply (button)	Click to save changes.
Refresh (button)	Click to manually initiate the tab's display to refresh itself with current information.
ID/Port	Indicates the identifier of each hard disk visible to the RAID controller.
Part of Unit	Indicates the RAID unit to which the hard disk belongs, if any. To be usable by the FortiMail unit, you must add the hard disk to a RAID unit.
Status	Indicates the hardware viability of the hard disk.
Size	Indicates the capacity of the hard disk, in gigabytes (GB).
Delete (button)	Click to unmount a hard disk before swapping it. Note that the *Delete* button is grayed out if the disk is in use and operating normally in the array (*Status* shows *OK*). After replacing the disk, add it to a RAID unit, then click *Re-scan*.

See also

About RAID levels

Configuring RAID on FortiMail models with hardware RAID controllers

Configuring RAID on FortiMail models with hardware RAID controllers

To configure RAID

1. Go to *System* > *RAID* > *RAID System*.

GUI item	Description
Model	Displays the model of the hardware RAID controller.
Driver	Displays the version of the RAID controller's driver software.
Firmware	Displays the version of the RAID controller's firmware.
Set RAID level	Select the RAID level, then click Change. For more information about RAID levels, see About RAID levels on page 218.
Change (button)	Select the RAID style, then click this button to apply the RAID level.
Re-scan (button)	Click to rebuild the RAID unit with disks that are currently a member of it, or detect newly added hard disks, and start a diagnostic check. The progress is displayed in the Resync Status section.
List of RAID units in the array	
Unit	Indicates the identifier of the RAID unit, such as u0.
Type	Indicates the RAID level currently in use. For more information, see About RAID levels on page 218. To change the RAID level, use *Set RAID level*.
Status	Indicates the status of the RAID unit. • OK: The RAID unit is operating normally. • Warning: The RAID controller is currently performing a background task (rebuilding, migrating, or initializing the RAID unit). **Caution:** Do not remove hard disks while this status is displayed. Removing active hard disks can cause hardware damage. • Error: The RAID unit is degraded or inoperable. Causes vary, such as when too many hard disks in the unit fail and the RAID unit no longer has the minimum number of disks required to operate in your selected RAID level. To correct such a situation, replace the failed hard disks. • No Units: No RAID units are available. **Note:** If both Error and Warning conditions exist, the status appears as Error.
Size	Indicates the total disk space, in gigabytes (GB), available for the RAID unit. Available space varies by your RAID level selection. Due to some space being consumed to store data required by RAID, available storage space will **not** equal the sum of the capacities of hard disks in the unit.

GUI item	Description
Ignore ECC	Click turn on to ignore the Error Correcting Code (ECC). This option is off by default. Ignoring the ECC can speed up building the RAID, but the RAID will not be as fault-tolerant.
List of hard disks in the array	
ID/Port	Indicates the identifier of each hard disk visible to the RAID controller.
Part of Unit	Indicates the RAID unit to which the hard disk belongs, if any. To be usable by the FortiMail unit, you must add the hard disk to a RAID unit.
Status	Indicates the hardware viability of the hard disk. • OK: The hard disk is operating normally. • UNKNOWN: The viability of the hard disk is not known. Causes vary, such as the hard disk not being a member of a RAID unit. In such a case, the RAID controller does not monitor its current status.
Size	Indicates the capacity of the hard disk, in gigabytes (GB).
Delete (button)	Click to unmount a hard disk before swapping it. Note that the *Delete* button is grayed out if the disk is in use and operating normally in the array (*Status* shows *OK*). After replacing the disk, add it to a RAID unit, then click *Re-scan*.

To change RAID levels

Back up data on the disk before beginning this procedure. Changing the device's RAID level temporarily suspends all mail processing and erases all data on the hard disk. For more information on creating a backup, see Backup and restore on page 267.

1. Go to *System* > *RAID* > *RAID System*.
2. From Set RAID level, select a RAID level.
3. Click Change.

The FortiMail unit changes the RAID level and reboots.

Replacing a RAID disk

When replacing a disk in the RAID array, the new disk must have the same or greater storage capacity than the existing disks in the array. If the new disk has a larger capacity than the other disks in the array, only the amount equal to the smallest hard disk will be used. For example, if the RAID has 400 GB disks, and you replace one with a 500 GB disk, to be consistent with the other disks, only 400 GB of the new disk will be used.

FortiMail units support hot swap; shutting down the FortiMail unit during hard disk replacement is not required.

To replace a disk in the array

1. Go to *System* > *RAID* > *RAID System*.
2. In the row corresponding to the hard disk that you want to replace (for example, p4), select the hard disk and click *Delete*. Note that the *Delete* button is grayed out if the disk is in use and operating normally in the array (*Status* shows *OK*).
   The RAID controller removes the hard disk from the list.

3. Protect the FortiMail unit from static electricity by using measures such as applying an antistatic wrist strap.
4. Physically remove the hard disk that corresponds to the one you removed in the GUI from its drive bay on the FortiMail unit.
5. Replace the hard disk with a new hard disk, inserting it into its drive bay on the FortiMail unit.
6. Click Re-scan.
   The RAID controller will scan for available hard disks and should locate the new hard disk. Depending on the RAID level, the FortiMail unit may either automatically add the new hard disk to the RAID unit or allocate it as a spare that will be automatically added to the array if one of the hard disks in the array fails.
   The FortiMail unit rebuilds the RAID array with the new hard disk. Time required varies by the size of the array.

See also

About RAID levels

Configuring RAID on FortiMail models with software RAID controllers

Using high availability (HA)

Go to *System* > *High Availability* to configure the FortiMail unit to act as a member of a high availability (HA) cluster or group in order to increase processing capacity and/or availability, so that your deployment is still up even if some hardware fails.

About HA types

FortiMail supports two types of HA:

- **Member HA**: Multiple FortiMail units (2 units for active-passive HA and 2-24 units for active-active HA) can operate in one HA pair or cluster.
- **Group HA**: Multiple groups (each group contains multiple FortiMail units) can work together as active-passive or active-active HA groups.

For instance, if you have one data center to protect, you only need one member HA; if you have two data centers backing up each other, you can join the two member HA clusters to form group HA. The two HA clusters or groups can work together as active-active or active-passive groups, just as the individual units in member HA.

See also

Deploying member HA

Deploying group HA

About HA modes

FortiMail HA can operate in either:

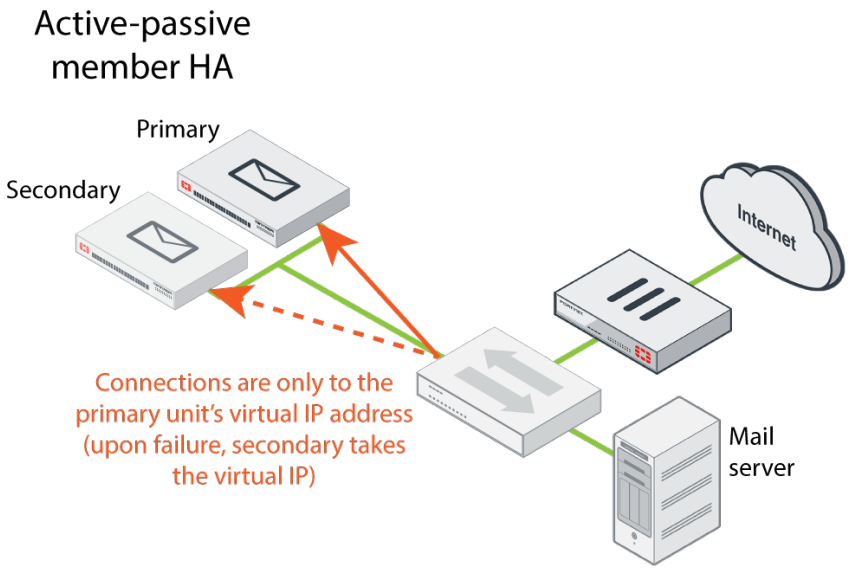
- active-passive mode
- active-active mode

Active-passive HA	Active-active HA
2 FortiMail units or groups in the HA pair	2-24 FortiMail units or groups in the HA cluster
Typically deployed behind a switch	Typically deployed behind a load balancer
Both configuration* and data synchronized^	Only configuration* synchronized
Only primary unit/group processes email	All units process email
No data loss^ when hardware fails	Data loss when hardware fails
No increased processing capacity	Increased processing capacity

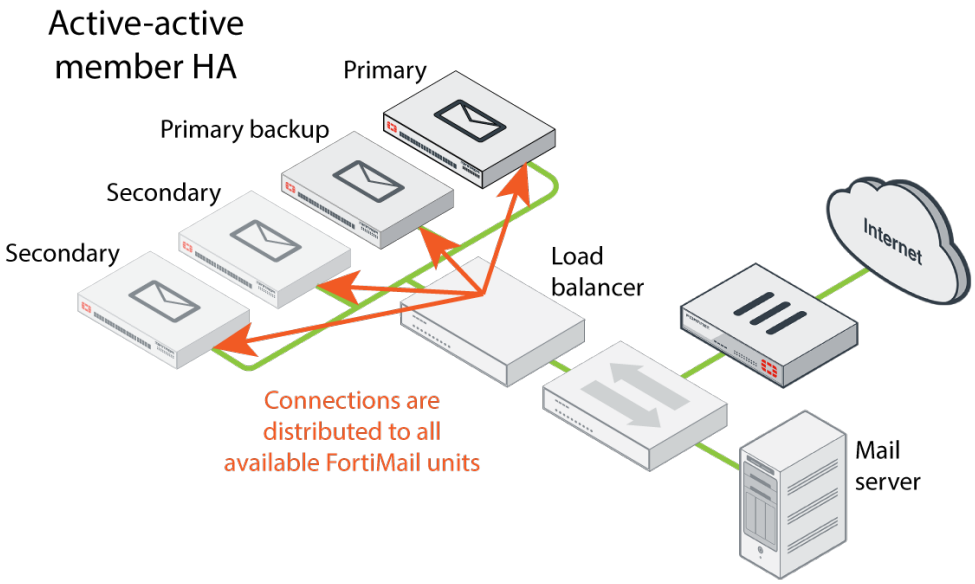
***** For exceptions, see Settings that are not synchronized by HA on page 228.

^ For exceptions, see Synchronization of MTA queue directories after a failover on page 229.

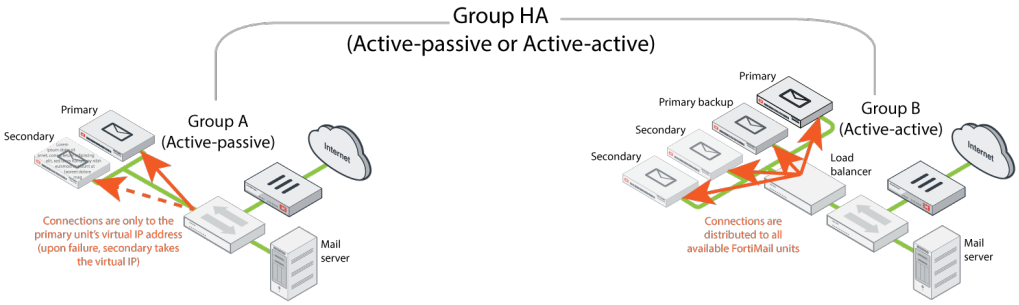
Active-passive member HA operating in gateway mode



Active-active member HA operating in gateway mode



Group HA



When a FortiMail unit fails, current SMTP sessions are interrupted. SMTP clients usually handle this gracefully, and restart a new connection. Traffic is redirected away from the failed FortiMail by different methods that vary by HA mode

- **Active-passive**: The secondary unit starts to use the virtual IP address of the failed unit, and uses ARP to automatically notify the switch or router that traffic should now be redirected to its network interface instead.
- **Active-active**: The load balancer stops sending email connections to failed FortiMail units. Only live FortiMail units continue to receive connections.

You can mix different FortiMail models in the same HA group. However:

- All FortiMail units in the HA group must have the same firmware version.
- Capacity and maximum configuration values are limited by the least powerful model.

To configure FortiMail units in an HA group, you usually connect only to the primary unit. The primary unit's configuration is almost entirely synchronized to secondary units, so that changes made to the primary unit are propagated to the secondary units.

Exceptions include:

- viewing log messages recorded about the secondary unit itself on its own hard disk
- configuring settings that are not synchronized (see Settings that are not synchronized by HA on page 228)

To use FortiGuard Antivirus or FortiGuard Antispam with HA, you must license all FortiMail units in the cluster. Only licensed devices can use the subscription services.

See also

About HA heartbeat and synchronization

About logging, alert email, and SNMP for HA

Storing mail data from HA groups on a NAS server

Example: Failover scenarios

Example: Active-passive HA group in gateway mode

About HA heartbeat and synchronization

Heartbeat and synchronization through the primary and secondary heartbeat network interfaces:

- monitors other units in the FortiMail HA group for failure
- synchronizes configuration changes from the primary unit to the secondary units
  For exceptions, see Settings that are not synchronized by HA on page 228.
- (active-passive only) synchronizes the mail queue, FortiMail system mail directory, and user home directories
  For exceptions, see Storing mail data from HA groups on a NAS server on page 230.

Synchronization intervals vary.

- **FortiGuard Antispam and FortiGuard Antivirus packages**: Not synchronized.
- **Mail queue**: Up to 20 minutes (not real time).
- **Configuration**: Real time.

If configuration synchronization did not occur when expected, or if you have inadvertently de-synchronized the secondary unit's configuration (for example, if a cable was accidentally disconnected), then you can manually initiate synchronization via GUI or the CLI command `diagnose system ha sync` on either the primary unit or the secondary unit.

Periodically, the secondary unit verifies that all configuration changes have been synchronized. If they have not, then the secondary unit will pull the configuration changes from the primary unit and reload the new configuration.

Secondary units also can push any changes made to its block and safe lists back to the primary unit. In active-active HA, these changes are then synchronized to all other secondary units.

The secondary unit expects to constantly receive heartbeat traffic from the primary unit. Loss of the heartbeat signal detects failure of the primary unit, and triggers the action that you select in On failure. For details, see Example: Failover scenarios on page 246.

Exceptions include system restarts and the `execute reload` CLI command. If the primary unit reboots or reloads its configuration, then it signals to the secondary unit to wait for the primary unit to complete the restart or reload. For details, see Failover scenario 2: System reboot or reload of the primary unit on page 247.

Behavior when the heartbeat signal is lost varies by HA mode and On failure:

- **Active-passive**: The secondary unit becomes the new primary unit and starts receiving email connections. Some in-progress email connections may be interrupted and must be restarted, but most email clients and servers can gracefully handle this.
- **Active-active**: If Primary backup has been selected, then your preferred backup unit will take over the role of the primary unit (Effective role becomes *Primary*).

  If a specific Primary backup is not selected, then each secondary unit continues to operate as a secondary unit. However, with no primary unit, changes to the configuration are not synchronized anymore.

For failover examples and steps required to restore the initially configured roles in each case, see Example: Failover scenarios on page 246.

Interface monitoring, hard drive monitoring, and remote service monitoring do not provide configuration and data synchronization, and therefore they are not a complete replacement for the heartbeat. However you can use them as another way to detect failure. See Interface section on page 236 and Service Monitor section on page 237.

See also

About HA types on page 223

About HA modes

About HA port numbers and protocols

About logging, alert email, and SNMP for HA

Settings that are not synchronized by HA

Storing mail data from HA groups on a NAS server

Synchronization of MTA queue directories after a failover

Example: Active-passive HA group in gateway mode

Example: Failover scenarios

About HA port numbers and protocols

The default protocol and port numbers for HA heartbeat, synchronization, and service monitoring communications are configurable. See HA base port on page 235, the `control-packet-option` setting in the FortiMail CLI Reference, and Appendix C: Port Numbers on page 611.

If a firewall is between the primary and secondary FortiMail unit, then verify that the firewall policy allows HA port numbers. Blocked HA ports can cause incorrect failover and synchronization failure.

Settings that are not synchronized by HA

All settings on the primary unit are synchronized to the secondary unit, except the following:

Settings	Explanation
Operation mode	You must set the operation mode (gateway, transparent, or server) of each HA group member before configuring HA. Many settings vary by operation mode, and therefore configurations cannot be synchronized if the operation mode is different.
Host name	Different host names are used to distinguish members of the HA cluster when connecting to the GUI and to indicate which unit failed. For details, see Hostname on page 233.
Static route	Static routes are not synchronized because some or all in the network interfaces on each FortiMail unit in the HA cluster may be connected to different subnets. See also Configuring static routes on page 161.
Interface configuration (gateway and server mode only)	Administrator connections to the GUI/CLI, alert email, and many other features require that you configure at least one network interface with an IP address. For details, see Configuring the network interfaces on page 152. Exceptions include virtual IP addresses on active-passive HA. Virtual IP addresses are synchronized because, upon failover, the secondary unit must starts to use them. This mechanism allows traffic to receive connections instead of the failed primary unit. See Virtual IP address (or Virtual IPv6 address) on page 237.
Management IP address (transparent mode only)	Each FortiMail unit in the HA cluster should be configured with different management IP addresses for GUI and CLI connectivity purposes. For details, see About the management IP on page 151.
SNMP system information	Each FortiMail unit in the HA cluster will have its own SNMP system information, including the *Description*, *Location*, and *Contact*. For details, see Configuring SNMP queries and traps on page 174.
RAID configuration	RAID settings are hardware-dependent and determined at boot time by looking at the drives (for software RAID) or the controller (hardware RAID), and are not stored in the system configuration. Therefore, they are not synchronized.
Some HA settings	• Shared password • Member Role
Product name and icon	The product name and icon under *System* > *Customization* > *Appearance* are not synchronized. All other appearance settings are synchronized.
Miscellaneous settings (active-active HA only)	In active-active HA, the following settings are not synchronized: • local domain name (see Local domain name on page 182) • default certificate (see Managing local certificates on page 251) • iSCSI initiator name • iSCSI ID for remote storage (see NAS server on page 193) • SNMP settings (see Configuring SNMP queries and traps on page 174) • IP pools (see Configuring IP pools on page 458) • quarantine report host name (see Web release host name/IP on page 474) • IBE settings of base URL, *Help* content URL, and *About* content URL (see Configuring IBE encryption on page 516)

Settings	Explanation
	• centralized IBE client IP address (see Centralized IBE on page 194) • centralized quarantine client IP address (see Centralized Quarantine on page 194) All system, domain, and user level block/safe lists are synchronized.  User data is synchronized at predefined time intervals, not in real time.

See also

About HA heartbeat and synchronization

Synchronization of MTA queue directories after a failover

During normal operation in active-passive HA, email messages are either:

- being received or sent by the primary FortiMail unit
- waiting to be delivered in the mail queue
- stored in the primary unit's mail data directories (email quarantines, email archives, and email inboxes of server mode)

When a failure occurs, sending and receiving is interrupted. The delivery attempt fails, and the sender usually retries to send the email message. However, stored messages remain in the primary unit's mail data directories.

To prevent data loss when a primary unit fails, you usually should enable Synchronize mail data directory (unless NAS storage is used), but do **not** need to enable Synchronize MTA queue directory. This is because of an automatic recovery mechanism in FortiMail HA failover.

1. The secondary or primary backup unit detects that the primary unit has failed, and becomes the new primary unit.
2. If the former primary unit can reboot, it detects the new primary unit, and becomes a secondary unit.

    Depending on the On failure setting, you may be required to click Restart HA on a failed primary unit.

3. The former primary unit pushes its mail queue to the new primary unit.

   This synchronization occurs through the heartbeat link between the primary and secondary units, and prevents duplicate email messages from forming in the primary unit's mail queue.
4. The new primary unit delivers email in its mail queues, including email messages synchronized from the new secondary unit.

As a result, if the failed primary unit can restart, no email is lost from the mail queue.

Even if you choose to synchronize the mail queue, because its contents change very rapidly and synchronization is periodic, there is a chance that some email will not have not been synchronized when a failover occurs.

See also

About HA heartbeat and synchronization

Storing mail data from HA groups on a NAS server

Storing mail data from HA groups on a NAS server

If you have FortiMail units operating in server mode and in an active-active HA group, you **must** store mail data centrally on a network attached storage (NAS) server — not on each FortiMail unit. Otherwise email users' messages and other mail data could be scattered across multiple FortiMail units.

For other HA and operating modes, however, it still may be better to store mail data on a NAS server.

For example, regular NAS server backups help to prevent mail data loss, even if a FortiMail unit has hardware failure. Also, during a temporary failure of a FortiMail unit, you can still access the mail data on the NAS server. When the FortiMail unit restarts, it can usually continue to access and use the mail data stored on the NAS server.

For active-active HA with a NAS server, only the primary unit sends quarantine reports to email users. The primary unit also acts as a proxy between email users and the NAS server when email users use FortiMail webmail to access quarantined email and to configure their own Bayesian filters.

For active-passive HA groups, the primary unit reads and writes all mail data to and from the NAS server in the same way as a standalone unit. If a failover occurs, the new primary unit uses the same NAS server for mail data. The new primary unit can access all mail data that the original primary unit stored on the NAS server. So if you are using a NAS server to store mail data, after a failover, the new primary unit continues operating with no loss of mail data.

If the FortiMail unit is a member of an active-passive HA group, and the HA group stores mail data on a remote NAS server, disable mail data synchronization to prevent duplicate mail data traffic.

For instructions on storing mail data on a NAS server, see Selecting the mail data storage location on page 192.

See also

About HA heartbeat and synchronization

Synchronization of MTA queue directories after a failover

About logging, alert email, and SNMP for HA

For faster discovery and diagnosis of network problems that have caused an HA failover, you can configure SNMP, Syslog, and/or alert email to monitor the HA cluster.

To configure logging and alert email, configure the primary unit and enable HA events. When the configuration changes are synchronized to the secondary units, all FortiMail units in the HA group record their own separate log messages and send separate alert email messages. Log data is not synchronized.

To distinguish alert email from each member of the HA cluster, configure a different host name for each member. For details, see Hostname on page 233.

To use SNMP to monitor HA failover, configure each cluster member to enable HA events for the SNMP community, such as:

- fmlTrapHAEvent
- fmlHAEventId
- fmlHAUnitIp

- fmlHAEffectiveMode
- fmlHAEventReason

See also

Configuring SNMP queries and traps

Logs, reports, and alerts

About HA heartbeat and synchronization

Configuring HA

Depending on your HA deployment scenarios, follow the steps below to deploy member HA or group HA.

Deploying member HA

The following procedures describe how to set up member HA with multiple FortiMail units.

1. Register all FortiMail units in the HA cluster with the Fortinet Technical Support web site:
   https://support.fortinet.com/
   If you use licensed features such as centralized HA monitoring, FortiGuard Antivirus, and/or FortiGuard Antispam, also purchase and register licenses for all units.
2. Connect the network interfaces that will be used for the heartbeat and synchronization between FortiMail units in the HA cluster. At least one heartbeat link is required.
   For example, you could use a network cable to connect FortiMail A's *port2* to FortiMail B's *port2*.

Don't disconnect the heartbeat once HA is enabled. If the heartbeat is accidentally interrupted for an active-passive HA group, such as when a network cable is temporarily disconnected, the secondary unit will assume that the primary unit has failed, and become the new primary unit. If no failure has actually occurred, both FortiMail units will be operating as primary units at the same time. This can cause an IP address conflict. In active-active HA groups, configuration synchronization can be disrupted. For details on correcting this, see Restore to configured role.

For better heartbeat reliability, create two heartbeat links: a primary and a secondary. Directly link the pair of heartbeat ports with an Ethernet crossover cable, or connect them through a dedicated local switch that is not connected to your overall network. This ensures enough bandwidth and low latency for the synchronization and heartbeat. If the heartbeat is interrupted, then a failover may occur. See also About HA heartbeat and synchronization on page 226.

3. If you are making an active-passive HA group, and the operation mode is gateway or server, add a Virtual IP address (or Virtual IPv6 address) and Virtual hostname to the network interface that will receive email connections. Update DNS records to use this virtual IP address, not the physical IP address. Wait for the DNS records to propagate to non-authoritative DNS servers before you enable HA.
4. If you are making an active-active HA group, configure storage of mail data on a NAS server. See Storing mail data from HA groups on a NAS server on page 230.(Active-passive members can also benefit from a NAS server, but do

not require it.)

For active-active HA, if the FortiMail unit is operating in server mode, you must store mail data externally on a NAS server. Failure to store mail data externally could result in mailboxes and other data scattered over multiple FortiMail units.

5. On each member of the HA group, go to *System* > *High Availability* > *Configuration* and:
   a. Configure the following:

GUI item	Description
State	Enable or disable HA.
Type	Select *Member*. For information about HA types, see About HA types on page 223.
HA mode	Select either *Active-Active* or *Active-Passive*. For details, see About HA modes on page 223.
On failure	Select what the HA group will do when it detects a failure, either: • *Switch off immediately*: On recovery, do not process email or join the HA group until you manually select the Effective role (see Restart HA and Restore to configured role). • *Wait for recovery*: On recovery, the failed primary unit's Effective role becomes *Secondary*. To manually restore the FortiMail unit to acting in its configured Member Role, see Restore to configured role. • *Wait for recovery and switch to configured role*: On recovery, the failed primary unit's Effective role automatically becomes *Primary* again, and the secondary unit that was temporarily acting as primary automatically becomes *Secondary* again. This option may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is recurring, resulting in many extra role changes. **Tip:** In most cases, you should select *Wait for recovery*.
Shared password	Enter an HA password for the HA group members. Before HA group members synchronize with each other, they verify that they have the same shared password. This prevents them from accidentally synchronizing with FortiMail units that do not belong to the same cluster. Therefore you must add the shared HA password to each unit in the HA group.

   b. Expand the *Member* section. For each FortiMail unit in the HA group, click *New* and configure the following:

GUI item	Description
Member Role	Select the role of the FortiMail unit in the HA group, either *Primary* or *Secondary* Each HA group member's role is not synchronized because this distinguishes the primary and secondary units. Effects of the role vary by HA mode. See About HA modes on page 223.
Use current device	Click to automatically fill out the following fields with the current device information.

GUI item	Description
IPv4 address (or IPv6 address)	Enter the IP address of the network interface that will listen for the heartbeat and synchronization on the primary or secondary (depending on which entry you are currently configuring in the table). If you want more heartbeat interfaces, click **+** and then add those IP addresses. Alternatively, if you are currently configuring the device that you are adding to the table, click *Use Current Device*. **Note:** You must also bring up and then enable Heartbeat status on the interface. If it is disabled, but the IP address is configured here, then HA will detect that the heartbeat link has failed.
Hostname	Displays the hostname of the primary or secondary (depending on which entry you are currently configuring in the table). **Note:** Do not configure the hostname here. It will not update the hostname used by the FortiMail unit's SMTP relay/proxy. Instead, configure Host name in the mail settings and Virtual hostname, and then click *Use Current Device* to automatically paste the hostname into this field.
Primary backup (Active-active secondary units only)	If HA mode is *Active-Active*, then there can be many secondary units. Enable this setting if Member Role is *Secondary*, and you want to select this member to become the new primary when a failure is detected. **Note:** Usually you should have a primary backup. Otherwise configuration synchronization will be interrupted upon failure. See About HA heartbeat and synchronization on page 226.
Comment	Optional. Enter a descriptive comment.

c. If the HA group is active-passive, configure the Virtual IP address (or Virtual IPv6 address) that will transfer upon failover.

d. If the HA group stores mail data on NAS, disable Synchronize mail data directory.

e. Optionally, configure:

- Advanced Option section on page 234
- Interface section on page 236
- Service Monitor section on page 237

f. Click *Apply* on the primary unit, and then on the secondary units.

6. If the HA group is active-active, configure the load balancer with either remote service monitoring or interface monitoring to detect failed FortiMail units, and to redirect connections to available FortiMail units.
7. Monitor the status of each cluster member. For details, see Monitoring HA status on page 239, Logs, reports, and alerts on page 535, and Centrally monitoring the HA cluster on page 146.

Deploying group HA

The following procedures describe how to set up group HA with multiple FortiMail unit groups.

1. Register all of the FortiMail units as described in Deploying member HA on page 231.
2. Connect the FortiMail unit interfaces as described in Deploying member HA on page 231.
3. On the primary unit, go to *System* > *High Availability* > *Configuration*.
   Configure the HA settings as described in Deploying member HA on page 231
4. On the primary unit, go to *System* > *High Availability* > *Configuration*.

From Type, select *Group*. Then expand the *Group* section, and click *New*. Configure the following settings. Repeat this step to create all of the primary and secondary groups.

GUI item	Description
Name	Specify a group name.
Group role	Specify the group role: *Off*, *Primary*, or *Secondary*.
Member mode	Specify the group member mode: either *Active-Active (A-A)* or *Active-Passive (A-P)*.
Comment	Optional. Enter a descriptive comment.

5. On other member units, go to *System* > *High Availability* > *Configuration*.

   Click *Join an existing HA cluster* and configure the following settings. Then click *Confirm and Join*.

   This option is only available if the unit has no HA configured yet. If HA has been configured before, skip this step and go to the next step.

GUI item	Description
Primary device IP	Specify primary unit's IP address.
Shared password	Enter the shared password configured on the primary unit.
Join with name	Specify the member's name in the cluster.
Join HA group	Enable this option.
Group name	Select a group name.

6. If you have already configured HA on a unit and you want the unit to join a group, go to *System* > *High Availability* > *Configuration*. From Type, select *Group*. Then join a group by editing the existing member in the *Member* list.

You must select the *Group* HA type first. If you select *Member* HA type, the option to join a group will not be available when you edit a member.

The primary unit in the primary group will collect and populate the HA information to other primary units in the secondary groups, which will populate the information to the secondary units in their own groups.

See also

About HA types on page 223

About HA modes

About HA heartbeat and synchronization

Settings that are not synchronized by HA

Example: Active-passive HA group in gateway mode

Example: Failover scenarios

Advanced Option section

1. Go to *System* > *High Availability* > *Configuration*.
2. Expand the *Advanced Option* section.
3. Configure the following and then click *Apply*:

GUI item	Description
Synchronize mail data directory (Active-Passive only)	Enable if the HA group does not store its mail data on a NAS server, in order to synchronize system quarantine, per-recipient quarantines, email archives, email users' preferences, and (server mode only) mailboxes with the HA group members.See Storing mail data from HA groups on a NAS server on page 230. If mail data changes frequently, you can manually initiate a data synchronization when significant changes are complete. For details, see Start configuration sync.
Synchronize MTA queue directory (Active-Passive only)	Enable if you want to synchronize the mail queue with the HA group members.  If the primary unit experiences a hardware failure and you cannot restart it, and if this option is disabled, MTA queue directory data could be lost.  Enabling this option can affect the FortiMail unit's performance, because periodic synchronization of the mail queue can be processor and bandwidth-intensive. Additionally, because the content of the MTA queue directories is very dynamic, periodically synchronizing MTA queue directories between FortiMail units may not guarantee against loss of all email in those directories. Even if MTA queue directory synchronization is disabled, after a failover, a separate synchronization mechanism may successfully prevent loss of MTA queue data. For details, see Synchronization of MTA queue directories after a failover on page 229 and Managing the mail queue on page 129.
HA base port	Enter the first of multiple port numbers (see Appendix C: Port Numbers on page 611) that will be used for: • heartbeat signals • synchronization control • data synchronization • configuration synchronization  For both active-active and active-passive HA, in addition or alternatively to configuring the heartbeat, you can configure service monitoring. For details, see Service Monitor section on page 237 and About HA heartbeat and synchronization on page 226.  In addition to automatic immediate and periodic configuration synchronization, you can also manually initiate synchronization. For details, see Start configuration sync.
Heartbeat lost threshold	Enter the total amount of time, in seconds, that a FortiMail unit can be unresponsive until and HA detects a failure and performs the action in On failure.

GUI item	Description
	 The heartbeat verifies availability every 1 second. To prevent unnecessary failover when the primary unit is temporarily experiencing very heavy load and therefore heartbeat responses are slow, configure a longer threshold (for example, 3 seconds or more) to allow the secondary unit enough time to send more heartbeat signals to confirm unresponsiveness. To determine the best heartbeat threshold, it is useful to know your FortiMail unit's performance baseline and peaks. See also Establish a system baseline on page 584 and Troubleshoot resource issues on page 598.
	 If you have service level agreements (SLA), then you may be required to keep this time short. If the failure detection time is too long, email delivery could be delayed or fail until HA detects the failure. This reduces service uptime.
Remote services as heartbeat	Enable to avoid the the On failure action if both the primary and secondary heartbeat links temporarily fail, but remote service monitoring detects that the FortiMail unit is still available.
	 The On failure action can still occur if the HA process restarts due to system reboot or HA daemon restart. Then it examines the physical heartbeat links first. If they are not found, then failure is detected. This setting provides an extra HA heartbeat only, **not synchronization**. To avoid synchronization problems, do not use remote service monitoring as a heartbeat for a long time. This feature is intended only as a temporary heartbeat until you reestablish a normal primary or secondary heartbeat link.

Interface section

In a basic HA deployment, the heartbeat interface provides a basic signal to other HA group members about the health of the primary FortiMail unit. However, you can use an additional signals. Interface monitoring periodically tests the local network interfaces on the primary unit . If a malfunctioning interface is detected, HA performs the action configured in On failure.

1. Optionally, configure the interface monitoring interval and failure detection threshold. See Service Monitor section on page 237.
2. Go to *System* > *High Availability* > *Configuration*.
3. Expand the *Interface* section.
4. Select a row for a network interface in the table, and then click *Edit*.
5. Configure the following settings:

GUI item	Description
Heartbeat status	Enable if this interface will listen for HA heartbeat and synchronization communications.  You must enable at least one of the heartbeat interfaces that you defined in IPv4 address (or IPv6 address). Otherwise HA will detect a failure.
Port	Displays the name of the network interface that you are configuring. Optionally, you can click the name to view or configure its settings. See also Configuring the network interfaces on page 152.
Virtual IP address (or Virtual IPv6 address)	Enter a virtual IP address that the primary unit will have on this network interface. Upon failure detection, the secondary will become the new primary and start to use the virtual IP address. For gateway mode and server mode deployments, DNS records should be configured to point to the virtual IP address, not physical IP addresses.See also About HA modes on page 223, Configuring the network interfaces on page 152, About IPv6 Support on page 150. This setting is available only if HA mode is *Active-Passive*.  The interface IP address must be different from, but on the same subnet as, the IP addresses of the other heartbeat network interfaces of other members in the HA group. When configuring other FortiMail units in the HA group, use this value as the: • *Remote peer IP* (for active-passive HA) • *Primary configuration* (for secondary units in active-active HA) • *Peer systems* (for the primary unit in active-active HA)
Virtual hostname	Enter a virtual hostname. Similar to behavior with the virtual IP address, the virtual hostname belongs to the current primary unit. Upon failover, the secondary unit becomes the new primary unit, and so it starts to use the virtual hostname instead. This setting is available only if HA mode is *Active-Passive*.
Enable port monitor	Enable to monitor a physical network port for failure. If the port fails, a failure is detected by the HA cluster.

Service Monitor section

Failed FortiMail units, in the simplest HA deployments, are detected by an interrupted heartbeat. However HA can also detect failure of hardware and network services. Heartbeats detect the general responsiveness of a primary unit, but do not test each daemon (for example, POP3 or webmail service), hard drive, and physical network ports used by non-heartbeat traffic. Therefore you can add hardware and service monitoring to be more specific. Alternatively, if the heartbeat link is briefly disconnected, remote services monitoring can prevent an unnecessary failover by temporarily acting as a secondary heartbeat.

With remote service monitoring, the secondary unit connects to the SMTP, POP3, and/or web service (HTTP) on the primary unit to detect failure. For server mode, IMAP service can also be monitored.

With local network interface monitoring and hard drive monitoring, the primary unit monitors its own network interfaces and hard drives.Hard drive monitoring tests that the local hard drive is still accessible, and disk space exists for mail data. If the hard disk is not responsive, or if the mail data disk is 95% full, then a failure is detected.

Network interface monitoring tests all network interfaces where:

- Status is enabled (the network interface is up)
- *Enable port monitor* is enabled

Alert email, log messages, and SNMP traps (if configured) indicate the specific cause.

For example, if service monitoring detects failure of *port2* on the primary unit, it records this log message:

```
date=2005-11-18 time=18:20:31 device_id=FE-4002905500194 log_id=0107000000 type=event
     subtype=ha pri=notice user=ha ui=ha action=unknown status=success msg="monitord: local
     problem detected (port2), shutting down"
```

and sends this alert email:

```
Subject: monitord: local problem detected (port2), shutting down [primary-host-name]
This is the FortiMail HA unit at 10.0.0.1.
A local problem (port2) has been detected, telling remote to take over and shutting down.
```

To configure hardware and service monitoring

1. Go to *System* > *High Availability* > *Configuration*.
2. Expand the *Service Monitor* section.
3. Select a row in the table and click *Edit*.

   For *Remote SMTP*, *Remote IMAP*, *Remote POP*, and *Remote HTTP* services, configure the following and click *OK*:

GUI item	Description
Enable	Enable or disable monitoring for the selected service.
Name	Displays the service name.
Port	Enter the listening port number of the service on the primary FortiMail and (active-active HA only) secondary. See also Appendix C: Port Numbers on page 611.
Timeout	Enter the amount of time in seconds to wait for a response to the connection.
Interval	Enter the time in seconds between each test.
Retries	Enter the number of consecutively failed tests that indicate a failure.

   For interface monitoring, configure the following and click *OK* (to configure which ports are monitored, see Interface section on page 236):

GUI item	Description
Interval	Enter the time in seconds between each test.
Retries	Enter the number of consecutively failed tests that indicate a failure.

   For local hard drive monitoring, configure the following and click *OK*:

GUI item	Description
Enable	Enable or disable monitoring that the local hard drive.
Interval	Enter the time in seconds between each test.
Retries	Enter the number of consecutively failed tests that indicate a failure.

See also

About HA heartbeat and synchronization

About logging, alert email, and SNMP for HA

Example: Active-passive HA group in gateway mode

Example: Failover scenarios

Monitoring HA status

After you configure HA (see Configuring HA on page 231), to view the roles and synchronization status of the HA group, go *System* > *High Availability* > *Status*. You can also manually initiate synchronization and reset the current Effective role to match the initial Configured role.

GUI item	Description
State	Displays the configured HA mode.
Configured role	Displays the configured Member Role. In active-active HA, the secondary unit that is the primary backup (if configured) will display *Secondary*, like other secondary units. After a failure has been detected, the FortiMail unit may not be acting in the role that it was initially configured for, and then this will not match Effective role. For details, see Combinations of configured and effective HA role on page 240.
Effective role	Displays the role that this FortiMail unit is currently operating in, either: • *Primary*: Acting as primary unit. • *Secondary*: Acting as secondary unit. • *Off*: For primary units, this indicates that interface or remote service monitoring has detected a failure and therefore the primary unit went offline and halted HA processes. For secondary units, this indicates that it detected an HA synchronization failure; if sync immediately fails again, then the action in On failure will occur. See also Restart HA. • *Failed*: Service monitoring or network interface monitoring has detected a failure and the diagnostic connection is currently determining if the problem has been corrected or it must perform the action in On failure. • *Holdoff*: For secondary units, this indicates that the primary unit is rebooting and asked to wait longer than the usual Heartbeat lost threshold so that the reboot can complete. If the primary does not return, then a failure is detected and it must perform the action in On failure. After a failure has been detected, the FortiMail unit may not be acting in the role that it was initially configured for, and then this will not match Configured role. For details, see Combinations of configured and effective HA role on page 240. For information on restoring the FortiMail unit to the initially configured role, in Action, click *Restore to configured role*.
Member Status	A table with some basic statuses about all FortiMail units that belong to the HA group, including: • *SN*: Serial number.

GUI item	Description
	• *IP*: IPv4 address (or IPv6 address) of the network interface for the primary heartbeat. • *Version*: Firmware version. A FortiMail unit must run the same firmware version in order to join the HA group, so that the configuration can be synchronized. • *Configured*: Configured role. In addition, if a secondary unit has been configured as the *Primary Backup*, it is denoted with an icon. • *Effective*: Effective role. • *Status*: Whether or not the HA cluster is synchronized. • *Up Time*: Duration of time that the HA cluster member has been operational. • *Last Seen*: When this FortiMail unit's HA daemon last communicated with the others in the HA group to make sure that they are available. See also Heartbeat lost thresholdand HA base port.
Action	Depending on the context, one or more the following actions may be available: • *Start configuration sync*: Click to manually initiate configuration synchronization with other FortiMail units in the HA cluster. See also Settings that are not synchronized by HA on page 228. • *Restore to configured role*: Click to manually reset the Effective role to match the unit's Configured role. • *Restart HA*: If the primary unit's Effective role is *Off*, and then you have fixed the cause of the failure, click to restart HA processes.

See also

Centrally monitoring the HA cluster

About HA heartbeat and synchronization

About logging, alert email, and SNMP for HA

Configuring HA

Service Monitor section

Example: Failover scenarios

Combinations of configured and effective HA role

Member Role	Effective role	Result
Primary	Primary	Normal for the primary unit of an HA group.
Secondary	Secondary	Normal for the secondary unit of an HA group. In active-active HA, this can also occur if the primary unit has failed. Most of the secondary units continue to be secondary. If you selected one of them to be the primary backup, however, then its Effective role becomes *Primary*.

Member Role	Effective role	Result
Primary	Off	Either the: • primary unit failed, and On failure is *Switch off immediately* • FortiMail unit is starting to operate in HA mode and its HA processes such as configuration synchronization are stopped. To return it to the originally configured role, see Recovering from a heartbeat link failure on page 249.  This is caused by a stopped heartbeat, not remote service monitoring or hardware/interface monitoring.
Secondary	Off	The secondary unit has detected a failure, or the FortiMail unit is starting to operate in HA mode. After the secondary unit starts and connects with the primary unit to form an HA group, the first configuration synchronization may fail. To prevent both the secondary and primary units from simultaneously acting as primary units, the Effective role becomes *Off*. If the next synchronization fails, then the secondary unit's Effective role becomes *Primary*.
Primary	Failed	Remote service monitoring or local network interface monitoring on the primary unit has detected a failure. Once the problem that caused the failure has been corrected, the Effective role changes from *Failed* to either *Secondary* or *Primary*, depending on the On failure setting.
Primary	Secondary	The primary unit failed. A secondary unit automatically became the new primary unit. When the failed unit restarted, it detected that there was already a primary unit in the HA group, and so now the failed unit is the new secondary unit. If you want the failed unit to return to acting as the primary unit, in Action, you must manually select *Restore to configured role*.
Secondary	Primary	The secondary unit detected that the primary unit failed, and then the secondary unit became the new primary unit. If you want it to return to acting as the secondary unit, in Action, you must manually select *Restore to configured role*.

See also

About HA heartbeat and synchronization

Monitoring HA status

Configuring HA

Service Monitor section

Recovering from a heartbeat link failure

Example: Active-passive HA group in gateway mode

Example: Failover scenarios

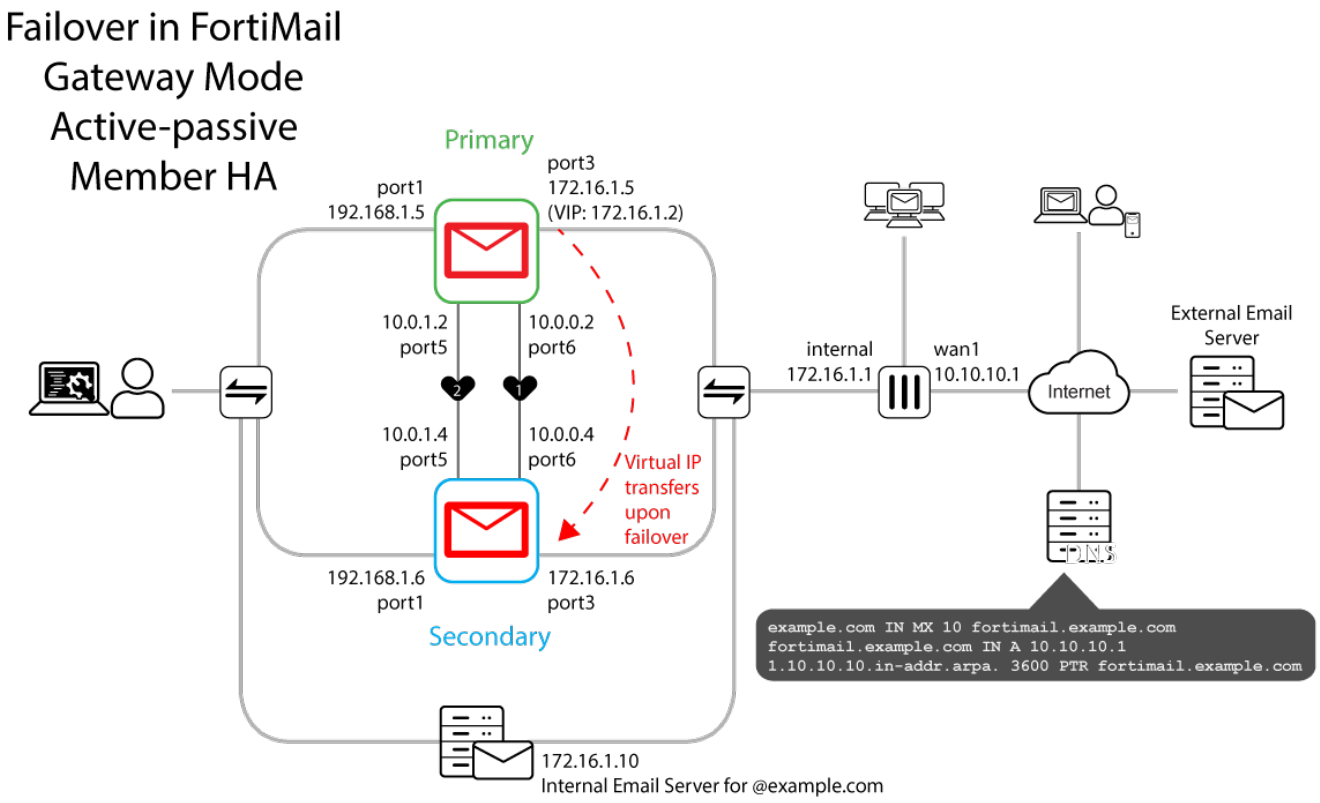
Example: Active-passive HA group in gateway mode

In this example, two FortiMail units in gateway mode are configured as an active-passive HA group.

This example describes HA configuration for this scenario. Before beginning, verify that both of the FortiMail units are:

- operating in gateway mode
- connected as shown in the diagram Virtual IP address for active-passive HA failover on page 242, except for the virtual IP address (VIP) that will be configured during this example

Virtual IP address for active-passive HA failover



For both FortiMail units:

port1	• connected to a switch which is connected only to administrator computers • administrative access is enabled only on this port
port3	• connected to a switch which is connected to the remaining private network and, indirectly through a FortiGate, the Internet • email connections occur only through this port
port5	• connected directly to the other FortiMail unit • heartbeat and synchronization occurs through this port
port6	• connected directly to the other FortiMail unit • heartbeat and synchronization occurs through this port

When a failover occurs, the secondary unit starts to act as the new primary. Then it must receive email connections. To make this happen, you will configure Virtual IP address (or Virtual IPv6 address). Email connections are to the VIP (not

the regular *port3* IP address). Initially, the VIP is on the original primary unit's *port3*. After failover, the secondary unit becomes the new primary and starts to use the VIP on its *port3* instead.

About standalone versus HA deployment

If you want to convert a standalone FortiMail unit to a member of an HA group, it may help to understand how HA and standalone deployments are similar and different.

For example, compare the diagram Virtual IP address for active-passive HA failover on page 242 with a standalone deployment.

Example network interfaces on a standalone FortiMail

Network interface	IP address	Description
port1	192.168.1.5	Administrative connections to the FortiMail unit
port2, port4	Default	Not connected.
port3	172.16.1.2	• Email connections to the FortiMail unit • Internal DNS `PTR`, `A` and `AAAA` records resolve to this IP address
port5	Default	Not connected.
port6	Default	Not connected.

On both, administrators connect to the IP address of *port1*. DNS records and email connections use the IP address of *port3*.

However on HA, *port3* on the primary unit has an additional IP address: the virtual IP address (VIP). Instead of the regular IP address, private network DNS records and email connections point to the VIP. When the primary fails, the secondary unit becomes the new primary, and starts to use the *port3* VIP. This causes the network to automatically redirect connections there.

On HA, additionally, *port6* is connected. This link is used only by HA heartbeat and synchronization between the primary and secondary unit.

Configuring the DNS records and firewall

In the diagram Virtual IP address for active-passive HA failover on page 242, SMTP clients on the private network connect to the virtual IP address of the primary unit. For SMTP clients on the Internet, however, they connect through the public network, using an IPv4 virtual IP (VIP) on the FortiGate unit. FortiGate policies allow, NAT, and route connections to another VIP on the primary FortiMail unit.

Because of NAT, the public DNS server on the Internet must not use private network IP addresses:

- `A` and/or `AAAA` records resolve `fortimail.example.com` into the**public** VIP on the FortiGate unit — not the **private** network VIP on the FortiMail primary unit
- `PTR` records to enable external email servers to use a reverse DNS query to resolve the **public** VIP on the FortiGate unit into `fortimail.example.com`
- `MX` records to indicate that `fortimail.example.com` is the email gateway for `example.com`, like usual

Configuring the primary unit for HA operation

In the standalone gateway mode configuration shown in About standalone versus HA deployment on page 243, the FortiMail unit's *port3* IP address is 172.16.1.2. The FortiGate unit is configured to NAT email connections to and from that private network IP address.

To achieve the same result with an active-passive HA group, you will add a virtual IP address of 172.16.1.2 to *port3* on the primary unit. Email connections occur through this virtual IP address, instead of the physical IP address. You will also add a heartbeat link between the HA members on *port6*.

To configure the primary unit for HA

1. Before you start, verify that the IP address and DNS records match what is shown in Example: Active-passive HA group in gateway mode on page 242.
2. On the primary unit, go to *System* > *Network* > *Interface*.
3. Configure *port6* to `10.0.0.2/255.255.255.0` and *port5* to `10.0.1.2/255.255.255.0`.
4. Go to *System* > *High Availability* > *Configuration*.
5. Configure the following:

GUI item		Value
	HA mode	Active-Passive
	On failure	Wait for recovery then switch to configured role
	Shared password	YOUR_HA_PASSWORD
Member section		
1		
	Member Role	Primary
	IPv4 address (or IPv6 address)	10.0.0.2
		10.0.1.2
	Hostname	Click *Use Current Device*
2		
	Member Role	Secondary
	IPv4 address (or IPv6 address)	10.0.0.4
		10.0.1.4
Interface section		
port3		
	Heartbeat status	Disable
	Virtual IP address (or Virtual IPv6 address)	172.16.1.2/255.255.255.0
port5		
	Heartbeat status	Enable
port6		
	Heartbeat status	Enable

6. Click *Apply*.

   The FortiMail unit enables active-passive HA mode, and, after determining that there is no other primary unit, sets its Effective role to *Primary* and adds the virtual IP 172.16.1.2 to *port3*.

7. To confirm that the FortiMail unit is acting as the primary unit, go to *System* > *High Availability* > *Status* and compare the Configured role and Effective role. Both should be *Primary*.

   If the Effective role is **not** *Primary*, then the FortiMail unit is **not** acting as the primary unit. Determine the cause of the failover, then restore the Effective role to that matching its configured HA mode of operation.

Configuring the secondary unit for HA operation

The following procedure describes how to prepare a FortiMail unit for HA operation as the secondary unit according to the diagram Virtual IP address for active-passive HA failover on page 242.

Before beginning this procedure, verify that you have completed the required preparations described in Example: Active-passive HA group in gateway mode on page 242. Also verify that you configured the primary unit as described in Configuring the primary unit for HA operation on page 244.

To configure the secondary unit for HA

1. On the secondary unit, go to *System* > *Network* > *Interface*.
2. Configure *port6* to be `10.0.0.4/255.255.255.0` and *port5* to be `10.0.1.4/255.255.255.0`.
3. Go to *System* > *High Availability* > *Configuration*.
4. Configure the following:

GUI item		Value
	HA mode	Active-Passive
	On failure	Wait for recovery then switch to configured role
	Shared password	YOUR_HA_PASSWORD
Member section		
1		
	Member Role	Primary
	IPv4 address (or IPv6 address)	10.0.0.2
		10.0.1.2
2		
	Member Role	Secondary
	IPv4 address (or IPv6 address)	10.0.0.4
		10.0.1.4
	Hostname	Click *Use Current Device*
Interface section		
port3		
	Heartbeat status	Disable

GUI item		Value
	Virtual IP address (or Virtual IPv6 address)	172.16.1.2/255.255.255.0
port5		
	Heartbeat status	Enable
port6		
	Heartbeat status	Enable

5. Click *Apply*.
   The FortiMail unit changes to active-passive HA, and, after determining that the primary unit is available, sets its Effective role to *Secondary*.
6. Go to *System* > *High Availability* > *Status*.
7. To confirm that the FortiMail unit is acting as the secondary unit, go to *System* > *High Availability* > *Status*. Compare the Configured role and Effective role. Both should be *Secondary*.
   If the Effective role is **not** *Secondary*, then the FortiMail unit is **not** acting as the secondary unit. Determine the cause of the failover, then restore the Effective role to match Configured role.

If the heartbeat interfaces are not connected, then the secondary unit cannot connect to the primary unit and a failure will be detected. The secondary unit will change its Effective role to *Primary*.

Example: Failover scenarios

Once HA is configured, it starts to automatically monitor the HA group for failures.

Various causes can be detected as a failure, and depending on the On failure setting, the HA group may automatically fail over in order to maintain service availability for overall uptime.

Automatic failover can be configured for active-active HA groups, but in this example, we show active-passive HA. The following abbreviations are used:

- P1 is the configured primary unit
- S2 is the configured secondary unit

Failover scenario 1: Temporary failure of the primary unit

In this scenario, the primary unit (P1) fails because of a software crash or a recoverable hardware failure (in this example, the P1 power cable is unplugged). HA logging and alert email are configured for the HA group.

When the secondary unit (S2) detects that P1 has failed, S2 becomes the new primary unit and continues processing email.

During this process:

1. The FortiMail HA group is operating normally.
2. The power cable is accidentally disconnected from P1.
3. S2's primary heartbeat test detects that P1 has failed.
   How soon this happens depends on the Heartbeat lost threshold of S2.

4. The Effective role of S2 changes to *Primary*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is changing its Effective role to *Primary*.

```
This is the HA machine at 172.16.1.6.
The following event has occurred
'PRIMARY heartbeat disappeared'
The state changed from 'SECONDARY' to 'PRIMARY'
```

6. S2 records the following event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is changing its Effective role to *Primary*.

```
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=notice user=ha ui=ha
     action=unknown status=success msg="monitord: peer stop responding (heartbeat),
     assuming PRIMARY role"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="monitord: main loop stopping"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="backupd: main loop stopping"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="configd: main loop stopping"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="configd: main loop starting, entering
     primary mode"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="backupd: main loop starting, entering
     primary mode"
2009-11-30 13:33:34 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="monitord: main loop starting, entering
     PRIMARY mode"
```

7. After P1 recovers from the hardware failure, what happens next depends on P1's On failure setting.

Failover scenario 2: System reboot or reload of the primary unit

If you need to reboot or reload the configuration (not shut down) P1, such as during a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload <httpd...>`, or by clicking *System* > *Reboot* from the top-right corner of the GUI:

- P1 will send a command to S2 to wait for the heartbeat and service monitoring signal to resume, so that S2 will not take over the primary role during P1's reboot.
- P1 will also send an alert email similar to the following:

```
This is the HA machine at 172.16.1.5.
The following critical event was detected
The system is rebooting (or reloading)!
```

- S2 will wait up to 15 minutes for P1 to return. If P1 fails during the reboot, S2 will become primary.
- S2 will send an alert email, indicating that S2 received the wait command from P1.

```
This is the HA machine at 172.16.1.6.
The following event has occurred
'peer rebooting (or reloading)'
The state changed from 'SECONDARY' to 'HOLD_OFF'
```

When P1 is up again:

- P1 will send another command to S2 and ask S2 to change its Effective role from *Holdoff* to *Secondary*, and to resume monitoring P1's services and heartbeat.
- S2 will send an alert email, indicating that S2 received instruction commands from P1.

```
This is the HA machine at 172.16.1.6.
The following event has occurred
'peer command appeared'
The state changed from 'HOLD_OFF' to 'SECONDARY'
```

- S2 logs the event in the HA logs.

Failover scenario 3: System reboot or reload of the secondary unit

If you reboot or reload the configuration of S2 such as during a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload <httpd...>`, or by clicking *System* > *Reboot* from the top-right corner of the GUI, then the behavior of P1 and S2 is as follows:

- P1 will send an alert email about S2, similar to the following:

```
This is the HA machine at 172.16.1.5.
The following event has occurred
'ha: SECONDARY heartbeat disappeared'
```

- S2 will send an alert email similar to the following:

```
This is the HA machine at 172.16.1.6.
The following critical event was detected
The system is rebooting (or reloading)!
```

- P1 will also log this event in the HA logs.

Shutdown (halt) is in the general purpose logs and alert email, but is not in alert email about HA specifically.

Failover scenario 4: Primary heartbeat link fails

If the primary heartbeat link fails, such as when the cable becomes accidentally disconnected, and if you have not configured a secondary heartbeat link, the FortiMail units in the HA group cannot verify that other units are operating and assume that the other has failed. As a result, the Effective role of the secondary unit (S2) changes to *Primary*, and **both**FortiMail units are acting as primary units.

Two primary units connected to the same network may cause IP address conflicts on your network because matching interfaces will have the same IP addresses. Additionally, because the heartbeat link is interrupted, the FortiMail units in the HA group cannot synchronize configuration changes or mail data changes.

Even after reconnecting the heartbeat link, both units will continue operating as primary units. To return the HA group to normal operation, you must connect to the GUI of S2 to manually return it to acting as a secondary unit.

1. The FortiMail HA group is operating normally.
2. The heartbeat link Ethernet cable is accidentally disconnected.
3. S2's HA heartbeat test detects that the primary unit has failed.
   How soon this happens depends on the HA daemon configuration of S2.
4. The Effective role of S2 changes to *Primary*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is changing its Effective role to *Primary*.

```
This is the HA machine at 172.16.1.6.
The following event has occurred
'PRIMARY heartbeat disappeared'
The state changed from 'SECONDARY' to 'PRIMARY'
```

6. S2 records the following event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is changing its Effective role to *Primary*.

```
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=notice user=ha ui=ha
     action=unknown status=success msg="monitord: peer stop responding (heartbeat),
     assuming PRIMARY role"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="monitord: main loop stopping"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="backupd: main loop stopping"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="configd: main loop stopping"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="backupd: main loop starting, entering
     primary mode"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="configd: main loop starting, entering
     primary mode"
2005-01-30 16:27:18 log_id=0107000000 type=event subtype=ha pri=information user=ha
     ui=ha action=unknown status=success msg="monitord: main loop starting, entering
     PRIMARY mode"
```

Recovering from a heartbeat link failure

If a hardware failure is not permanent (for example, an temporarily disconnected cable, not a failed port on one of the FortiMail units), then you may want to return both FortiMail units to operating in their configured Member Role.

To return to normal roles after the heartbeat link fails

1. Reconnect the primary heartbeat interface by reconnecting the Ethernet cable for the heartbeat link.
   Even though the Effective role of S2 is *Primary*, S2 continues to attempt to find the other primary unit. When the heartbeat link is reconnected, S2 finds P1 and determines that P1's Effective role is also *Primary*. So S2 sends a heartbeat signal to tell P1 to stop operating as a primary unit. The Effective role of P1 changes to *Off*.
2. P1 sends an alert email similar to the following, indicating that P1 has stopped operating as the primary unit.

   ```
   This is the HA machine at 172.16.1.5
   The following event has occurred
   'SECONDARY asks us to switch roles (user requested takeover)'
   The state changed from 'PRIMARY' to 'OFF'
   ```
3. P1 records the following event log messages (among others) indicating that P1's Effective role is changing to *Off*.

   ```
   2005-11-30 17:13:06 log_id=0107000000 type=event subtype=ha pri=notice user=ha ui=ha
        action=unknown status=success msg="monitord: remote detected problem, shutting
        down"
   2005-11-30 17:13:16 log_id=0107000000 type=event subtype=ha pri=information user=ha
        ui=ha action=unknown status=success msg="monitord: main loop stopping"
   2005-11-30 17:13:16 log_id=0107000000 type=event subtype=ha pri=information user=ha
        ui=ha action=unknown status=success msg="backupd: main loop stopping"
   2005-11-30 17:13:16 log_id=0107000000 type=event subtype=ha pri=information user=ha
        ui=ha action=unknown status=success msg="configd: main loop stopping"
   2005-11-30 17:13:16 log_id=0107000000 type=event subtype=ha pri=information user=ha
        ui=ha action=unknown status=success msg="backupd: main loop starting, entering off
        mode"
   2005-11-30 17:13:16 log_id=0107000000 type=event subtype=ha pri=information user=ha
        ui=ha action=unknown status=success msg="configd: main loop starting, entering off
        mode"
   ```

   The configured Member Role of P1 is *Primary*, but the Effective role is *Off*.

   The configured Member Role of S2 is *Secondary*, but the Effective role is *Primary*.

   P1 synchronizes the content of its MTA queue directories to S2. Email in these directories can now be delivered by S2.
4. Connect to the GUI of P1, and go to *System* > *High Availability* > *Status*.

5. Look for synchronization messages.

   Do not continue to the next step until P1 has synchronized with S2.
6. Connect to the GUI of S2, go to *System* > *High Availability* > *Status*, and in Action, select *Restore to configured role*.

   The HA group should return to normal operation. P1 records the following event log message (among others) indicating that S2 asked P1 to return to being the primary unit.

   ```
   2005-11-30 18:10:00 log_id=0107000000 type=event subtype=ha pri=notice user=ha ui=ha
        action=unknown status=success msg="monitord: being asked to assume original role"
   ```
7. P1 and S2 synchronize their MTA queue directories. All email in these directories can now be delivered by P1.

Managing certificates

You can use the *System* > *Certificate* submenu to generate certificate requests, install signed X.509 certificates, import CA root certificates and certificate revocation lists, and back up and restore installed certificates and private keys.

FortiMail uses certificates for public key infrastructure (PKI) authentication in secure connections. PKI can be used to authenticate a user, server, or client software. To prove that they can be trusted, when the connection occurs, the software presents a certificate with its identity. The software on the opposite side of the connection verifies that the certificate is currently valid, is being used for the intended purpose, and has been cryptographically signed by a known, trusted certification authority (CA). Depending on the connection, both the client and server sides of the connection may be required to present their certificates in order to authenticate each other.

Certificates can also be used for encryption. For an example of how to use certificates for PKI authentication of FortiMail administrators and email users, see Appendix F: PKI Authentication on page 628.

Depending on the features you use, you may need to configure multiple types of certificates on FortiMail.

Certificate type	Purpose
CA certificates	FortiMail compares trusted CA certificates to the CA signature on certificates presented by client software (including administrators and webmail users' web browsers). For details, see Configuring PKI authentication on page 304 and Managing certificate authority certificates on page 256.
Server certificates	FortiMail must present its server certificate when a client requests a secure connection for the: • GUI (HTTPS connections only) • webmail (HTTPS connections only) • secure email, such as SMTPS, IMAPS, and POP3S For details, see Managing local certificates on page 251.
Client certificates	FortiMail must present its client certificate if another server requests that FortiMail identify itself during a secure connection for: • LDAPS • SSO For details, see Managing local certificates on page 251 and Configuring single sign-on (SSO) on page 215.
Personal certificates	Mail users' personal certificates are used for S/MIME encryption. For details, see Configuring certificate bindings on page 521.

Managing local certificates

System > *Certificate* > *Local Certificate* displays both signed certificates and unsigned certificate requests.

If you do not have a server certificate for FortiMail, you can generate a certificate signing request and, once a CA has signed it, import the certificate. This installs the certificate for local use by the FortiMail unit.

FortiMail units require a local server certificate that it can present to prove its identity when clients request secure connections, including the:

- GUI (HTTPS connections only)
- webmail (HTTPS connections only)
- secure email, such as SMTPS, IMAPS, and POP3S

A local client certificate may also be required if FortiMail makes secure connections to another server, where FortiMail must authenticate itself, such as in SSO and some LDAPS configurations. The certificate for SSO is not located together with other client certificates; instead see Configuring single sign-on (SSO) on page 215.

GUI item	Description
View (button)	Select a certificate and click *View* to display its issuer, subject, and range of dates within which the certificate is valid.
Delete (button)	Removes the selected certificate.
Generate (button)	Click to generate a local certificate request. For more information, see Generating a certificate signing request on page 252.
Download (button)	Click the row of a certificate file or certificate request file in order to select it, then click this button to download a certificate (.cer) or certificate request (.csr) file. You can send the request to your certificate authority (CA) to obtain a signed certificate for the FortiMail unit. For more information, see Downloading a certificate signing request on page 254.
Set status	Click the row of a certificate in order to select it, then click this button to use it as the *Default* (that is, currently chosen for use) certificate. The *Status* column changes to indicate that the certificate is the current (*Default*) certificate. This button is not available if the selected certificate is already *Default*.
Import (button)	Click to import a signed certificate for local use. For more information, see Importing a certificate on page 254.
Name	Displays the name of the certificate file or certificate request file.
Subject	Displays the Distinguished Name (DN) located in the `Subject` field of the certificate. If the certificate has not yet been signed, this field is empty.
Status	Displays the status of the local certificates or certificate signing request. • *Default*: Indicates that the certificate was successfully imported, and is currently selected for use by the FortiMail unit. • *OK*: Indicates that the certificate was successfully imported, but is not selected as the certificate currently in use. To use the certificate, click the row of the certificate in order to select it, then click *Set status*. • *Pending*: Indicates that the certificate request has been generated, but must be downloaded, signed, and imported before it can be used as a local certificate. For details, see Installing a local certificate on page 252.

See also

Generating a certificate signing request

Downloading a certificate signing request

Importing a certificate

Installing a local certificate

To install a local certificate that FortiMail can use, either:

- Import an existing certificate. Both server and client certificates can use this procedure. For details, see Importing a certificate.
- Generate a new certificate. Server certificates can use this procedure. For details, see:
  a. Generating a certificate signing request
  b. Downloading a certificate signing request
  c. Submitting a certificate request to your CA for signing
  d. Importing a certificate

Generating a certificate signing request

You can generate a certificate signing request (CSR) file, based on the information you enter to identify the FortiMail unit. Certificate request files can then be submitted for verification and signing by a certificate authority (CA) in order to make a server certificate.

Alternatively, you may be able to generate a CSR and download a certificate directly on CA servers such as Microsoft Active Directory and Let's Encrypt. See your CA documentation.

To generate a certificate request on FortiMail

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click Generate.
   A dialog appears.
3. Configure the following:

GUI item	Description
Certification name	Enter a unique name for the certificate request, such as `fmlocal`.
Subject Information	Information that the certificate is required to contain in order to uniquely identify the FortiMail unit.
Certification name	Select which type of identifier will be used in the certificate to identify the FortiMail unit: • *Host IP* • *Domain name* • *E-mail* Which type you should select varies by whether or not your FortiMail unit has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate.

GUI item		Description
		For example, if your FortiMail unit has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the GUI by the domain name of the FortiMail unit, you might prefer to generate a certificate based on the domain name of the FortiMail unit, rather than its IP address. • *Host IP* requires that the FortiMail unit have a static, public IP address. It may be preferable if clients will be accessing the FortiMail unit primarily by its IP address. • *Domain name* requires that the FortiMail unit have a fully-qualified domain name (FQDN). It may be preferable if clients will be accessing the FortiMail unit primarily by its domain name. • *E-mail* does not require either a static IP address or a domain name. It may be preferable if the FortiMail unit does not have a domain name or public IP address.
	IP	Enter the static IP address of the FortiMail unit. This option appears only if *ID Type* is *Host IP*.
	Domain name	Type the fully-qualified domain name (FQDN) of the FortiMail unit. The domain name may resolve to either a static or, if the FortiMail unit is configured to use a dynamic DNS service, a dynamic IP address. For more information, see Configuring the network interfaces on page 152 and Configuring dynamic DNS on page 162. If a domain name is not available and the FortiMail unit subscribes to a dynamic DNS service, an `unable to verify certificate` message may appear in the user's browser whenever the public IP address of the FortiMail unit changes. This option appears only if *ID Type* is *Domain name*.
	E-mail	Type the email address of the owner of the FortiMail unit. This option appears only if *ID Type* is *E-mail*.
Optional Information		Information that you may include in the certificate, but which is not required.
	Organization unit	Type the name of your organizational unit, such as the name of your department (Optional). To enter more than one organizational unit name, click the + icon, and enter each organizational unit separately in each field.
	Organization	Type the legal name of your organization (Optional).
	Locality(City)	Type the name of the city or town where the FortiMail unit is located (Optional).
	State/Province	Type the name of the state or province where the FortiMail unit is located (Optional).
	Country	Select the name of the country where the FortiMail unit is located (Optional).
	E-mail	Type an email address that may be used for contact purposes (Optional).
Key type		Displays the type of algorithm used to generate the key: RSA or Elliptic Curve.
Key size		Select a security key size of *1024 Bit*, *1536 Bit*, *2048 Bit*, or *4096 Bit*. Larger keys are slower to generate, but provide better security.

GUI item	Description
Curve name	Select an elliptic curve name of *secp256r1*, *secp384r1*, or *secp521r1*. Elliptic Curve Digital Signature Algorithm (ECSDSA) provides a similar encryption strength to RSA but with a shorter key length.

4. Click *OK*.
   The certificate is generated, and can be downloaded to your management computer for submission to a certificate authority (CA) for signing. For more information, see Downloading a certificate signing request on page 254.

Downloading a certificate signing request

After you have generated a certificate request, you can download the request file to your management computer in order to submit the request file to a certificate authority (CA) for signing.

For other related steps, see Installing a local certificate on page 252.

To download a certificate request

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click the row that corresponds to the certificate request in order to select it.
3. Click *Download*, then select *Download* from the pop-up menu.
   Your web browser downloads the certificate request (.csr) file.

Submitting a certificate request to your CA for signing

After you have download the certificate request file, you can submit the request to you CA for signing.

For other related steps, see Installing a local certificate on page 252.

To submit a certificate request

1. Using the web browser on your management computer, go to the web site for your CA.
2. Follow your CA's instructions to place a Base64-encoded PKCS #12 certificate request, uploading your certificate request.
   If clients and servers that will be validating the certificate require specific fields such as `Subject Alternative Name` and `Key Usage`, then verify that the CA includes those fields when it signs the certificate.
3. Follow your CA's instructions to download their root certificate and Certificate Revocation List (CRL), and then install the root certificate and CRL on each remote client.
4. When you receive the signed certificate from the CA, install the certificate on the FortiMail unit. For more information, see Importing a certificate on page 254.

See also

Managing local certificates

Generating a certificate signing request

Importing a certificate

Importing a certificate

Importing a certificate may be useful when:

- restoring a certificate backup
- installing a certificate that has been generated on another system
- installing a certificate, after the certificate request has been signed by a certificate authority (CA)

If you generated the certificate request using the FortiMail unit, after you submit the certificate request to CA, the CA will verify the information and register the contact information in a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate and return it to you for installation on the FortiMail unit. To install the certificate, you must import it. For other related steps, see Installing a local certificate on page 252.

If the FortiMail unit's local certificate is signed by an intermediate CA rather than a root CA, before clients will trust the FortiMail unit's local certificate, you must demonstrate a link with trusted root CAs, thereby proving that the FortiMail unit's certificate is genuine. You can demonstrate this chain of trust either by:

- installing each intermediate CA's certificate in the client's list of trusted CAs
- including a signing chain in the FortiMail unit's local certificate

To include a signing chain, before importing the local certificate to the FortiMail unit, first open the FortiMail unit's local certificate file in a plain text editor, append the certificate of each intermediate CA in order from the intermediate CA who signed the FortiMail unit's certificate to the intermediate CA whose certificate was signed directly by a trusted root CA, then save the certificate. For example, a local certificate which includes a signing chain might use the following structure:

```
-----BEGIN CERTIFICATE-----
<FortiMail unit's local server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 1, who signed the FortiMail certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 2, who signed the certificate of intermediate CA 1 and whose
     certificate was signed by a trusted root CA>
-----END CERTIFICATE-----
```

To import a local certificate

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click *Import*.
3. Select the type of the import file or files:
   - *Local Certificate*: Select this option if you are importing a signed certificate issued by your CA. For other related steps, see Installing a local certificate on page 252.
   - *PKCS12 Certificate*: Select this option if you are importing an existing certificate whose certificate file and private key are stored in a PKCS #12 (.p12) password-encrypted file.
   - *Certificate*: Select this option if you are importing an existing certificate whose certificate file (.cert) and key file (.key) are stored separately. The private key is password-encrypted.
4. Configure the following:

GUI item	Description
Certificate name	Enter the location of the previously .cert or .pem exported certificate (or, for PKCS #12 certificates, the .p12 certificate-and-key file), or click *Browse* to locate the file.
Key file	Enter the location of the previously exported key file, or click Browse to locate the file. This option appears only when *Type* is *Certificate*.
Password	Enter the password that was used to encrypt the file, enabling the FortiMail unit to decrypt and install the certificate.

GUI item	Description
	This option appears only when *Type* is *PKCS12 certificate* or *Certificate*.

See also

Managing local certificates

Downloading a certificate signing request

Managing certificate authority certificates

Go to *System* > *Certificate* > *CA Certificate* to view and import the certificates of certificate authorities (CA) that FortiMail should trust.

CAs validate and sign other certificates in order to indicate to third parties that those other certificates are authentic.

Secure connections that use transport layer security (TLS) and S/MIME encryption use CA certificates to validate the signatures on other certificates. For more information, see Configuring TLS security profiles on page 453 and Configuring certificate bindings on page 521. Depending on the configuration of each PKI user, CA certificates may also be required to authenticate PKI users. For more information, see Configuring PKI authentication on page 304.

GUI item	Description
View (button)	Select a certificate and click *View* to display certificate details including the certificate name, issuer, subject, and the range of dates within which the certificate is valid.
Delete (button)	Removes the selected certificate.
Download (button)	Click the row of a certificate in order to select it, then click *Download* to download a copy of the CA certificate (.cer).
Import (button)	Click to import a CA certificate.
Name	Displays the name of the CA certificate.
Subject	Displays the Distinguished Name (DN) located in the `Subject` field of the certificate.

See also

Managing local certificates

Viewing trusted certificate authority certificates

Managing OCSP server certificates

Managing the certificate revocation list

System > *Certificate* > *Certificate Revocation List* lets you view and import certificate revocation lists (CRL).

To ensure that your FortiMail unit accepts only valid (not revoked) certificates, you should upload a current certificate revocation list, which may be provided by certificate authorities (CA), whenever a certificate is revoked. Alternatively, you

can use online certificate status protocol (OCSP) to query for certificate statuses. See Managing OCSP server certificates on page 257.

GUI item	Description
Delete (button)	Removes the selected list.
View (button)	Select a certificate revocation list and click *View* to display details.
Download (button)	Select a certificate revocation list and click *Download* to download a copy of the CRL file (.cer).
Import (button)	Click to import a certificate revocation list.
Name	Displays the name of the certificate revocation list.
Subject	Displays the Distinguished Name (DN) located in the `Subject` field of the certificate revocation list.

See also

Managing local certificates

Managing certificate authority certificates

Managing OCSP server certificates

Managing OCSP server certificates

Go to *System* > *Certificate* > *Remote* to view and import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA).

OCSP lets you revoke or validate certificates by query (see Appendix C: Port Numbers on page 611), rather than by importing certificate revocation lists (CRL; see Managing the certificate revocation list on page 256).

Remote certificates are required if you enable OCSP for PKI users. For more information, see Configuring PKI authentication on page 304.

GUI item	Description
Delete (button)	Removes the selected certificate.
View (button)	Select a certificate and click View to display certificate details including the certificate name, issuer, subject, and the range of dates within which the certificate is valid.
Download (button)	Click the row of a certificate in order to select it, then click *Download* to download a copy of the OCSP server certificate (.cer).
Import (button)	Click to import an OCSP server certificate.
Name	Displays the name of the OCSP server certificate.
Subject	Displays the Distinguished Name (DN) located in the `Subject` field of the certificate.

Viewing trusted certificate authority certificates

Go to *System* > *Certificate* > *Trusted CA* to view all trusted root certificate authorities (CA) downloaded from FortiGuard.

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

FortiMail keeps this list of trusted CA certificates up to date from FortiGuard.

GUI item	Description
View (button)	Select a certificate and click *View* to display certificate details including the certificate name, issuer, subject, and the range of dates within which the certificate is valid.
Download (button)	Click the row of a certificate in order to select it, then click *Download* to download a copy of the CA certificate (.cer).
Name	Displays the name of the CA certificate.
Subject	Displays the Distinguished Name (DN) located in the `Subject` field of the certificate.

See also

Managing local certificates

Managing certificate authority certificates

Managing OCSP server certificates

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 398). 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.
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 398). 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 260.
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.

GUI item	Description
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.
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 *FortiSanbox type* depending on your FortiCare contract. Also configure other scan settings (see Using FortiSandbox antivirus inspection on page 259).
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

FortiMail uses various Fortinet FortiGuard services, such as Antivirus, Antispam, and URL protection.

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 on page 590.

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
FortiGuard server port	Connect to FortiGuard Antivirus servers on either port 443 or 8890. The default port is 443.
Use override server	Enable to override the default FDN server to which the FortiMail unit connects for updates.
Override server IP address	Enter the IP address of the override public or private FDN server.
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*.

GUI item	Description
	• *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. • *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 535.

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. Also select the *FortiGuard server port* (53 by default or 8888) and protocol (UDP or HTTPS).

3. Specify a spam outbreak protection level. Higher level means more strict filtering.
4. If you want to use an override server, such as a local FortiManager unit, instead of the default FDN server, specify it by enabling the option and entering the server address.
5. Optionally enable cache and specify the cache TTL time. Enabling cache can improve performance.
6. Use FortiGuard servers either in the United States only, or in any location in the world.
7. 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 379). 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

You can designate an email address to receive and review sample submissions of spam for an administrator to review, or send directly to FortiGuard. Spam submissions can be made using the *Report Spam* plugin within Microsoft Outlook available for download at https://support.fortinet.com/.

Emails that have been submitted can be reviewed under *Monitor* > *Quarantine* > *Sample Submission*. For more information, see Sample Submission on page 121.

To configure a spam sample submissions service

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. Under *Sample Submission*, verify that *Enable submission service* is enabled.
3. If you have multiple protected domains, enable *Domain Submission* to allow domain administrators to view submissions from their own domains only.
4. Select whether you want an administrator to manually review spam sample submissions or you want the submissions to be sent directly to FortiGuard.

5. Define a *Retention period* of between 0-60 days, after which the sample submission will be deleted.
6. Enter the email addresses to receive spam and non-spam (or ham) sample submissions.

For the email addresses:

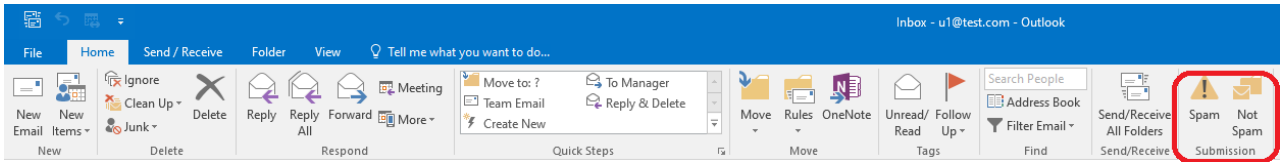
- The two email accounts cannot be the same.
- The two accounts are reserved for spam and non-spam submissions; they cannot receive other email.

  Therefore, you cannot use any email accounts in use for spam and non-spam submissions.

7. Click *Apply*.

To use the report spam plugin for Microsoft Outlook

1. Go to https://support.fortinet.com/ and log into your account.
2. Go to *Support* > *Firmware Download*.
3. Go to *FortiMail* > *Plugins*.
4. Double-click the appropriate install file to start the installation process, and follow the on-screen instructions.
5. After the plugin is successfully installed, restart Outlook. Upon reopening Outlook, you can *Report Spam* to report any uncaught suspicious email, and use *Not Spam* to report any caught spam email that you wish to mark as not spam.



Configuring licensed features

The following features are configurable with valid applicable licenses.

Configuring email continuity

When FortiMail is running in either gateway or transparent mode, with this feature enabled, end users are allowed to access inbound emails in instances where the email server behind the FortiMail unit goes offline. This feature is only available with a valid license from FortiGuard.

To configure email continuity

1. Go to *System* > *FortiGuard* > *Licensed Feature*.
2. In the *Email Continuity* section, set *Status* to *Enable*. Alternatively, you may select either *Disable* or *Disable and Purge Email* (to disable the feature and purge email from the email continuity service after the configured retention period expires).
3. Adjust the *Retention period* according to your requirements. The higher the number, the higher the number of days emails are kept before they are removed. The default setting is 30. The valid range is 1-60.

The actual retention period is whichever is the smaller value of this setting and the email retention period set for incoming email when configuring a resource profile. See Configuring resource profiles.

By default, this feature is disabled.

4. Enable *Authentication cache status* to allow FortiMail to caches user's password, enabling users to authenticate in the event of an LDAP server outage.
5. Define the *Authentication cache period* in days. The default setting is 20. The valid range is 1-60.

Configuring advanced management (feature license required)

If you have an advanced management feature license, you can go to *System* > *FortiGuard* > *Licensed Feature* and in the *Advanced Management* section, enable the following settings.

GUI item	Description
Centralized monitor	For details, see Centrally monitoring the HA cluster on page 146.
User management	For details, see Configuring user import profiles on page 308
Mailbox accounting service	For details, see Configuring mailbox statistics on page 554 and Viewing mail statistics on page 110.
Domain group support	For details, see To configure domain groups on page 284.
History log access for domain level administrator	For details, see Access level on page 169 and Viewing log messages on page 113.
Domain mail statistics	For details, see Viewing mail statistics on page 110.
MTA advanced control	For details, see Configuring advanced MTA control settings on page 374.
Intra domain protection	Enable or disable applying both inbound and outbound policies when an email is sent between protected domains. When this setting is disabled, if an email is sent between two protected domains, then FortiMail only applies the matching inbound policy. This means that, for example, an inbound policy with antispam would apply, but not an outbound policy with DLP. This behavior may be correct if all protected domains belong to the same company. However for an MSSP with multiple tenants, both policies should apply. In that case, enabled this setting so that FortiMail applies **both** inbound and outbound policies.
DMARC report analysis	For details, see Viewing DMARC report statistics on page 132.

Configuring image analysis

When you configure a content profile (see Configuring scan options on page 406), you can choose to scan images in the email body and attachments. You can fine-tune the file size that the FortiMail unit will scan, and how these images are detected. Separate thresholds exists for each category of images that you may want to block, such as violence or adult images. For details on thresholds, see the FortiMail CLI Reference.

To configure image analysis settings

1. Go to *System* > *FortiGuard* > *Licensed Feature*.
2. In the *Adult Image Analysis* section, enable *Status*.
3. In *Minimum image size (KB)* and *Maximum image size (KB)*, enter the range of image sizes to scan.
4. Click *Apply*.

System maintenance

The *Maintenance* menu contains features for use during scheduled maintenance: updates, backups, and restoration.

The *Maintenance* menu can also be used to install firmware. See also Managing firmware and configuration on page 567.

Backup and restore

Before installing FortiMail firmware or making significant configuration changes, back up your FortiMail configuration. Backups let you revert to your previous configuration if the new configuration does not function correctly. Backups let you compare changes in configuration.

A complete configuration backup consists of several parts:

- core configuration file (fml.cfg), including the local certificates
- Bayesian databases
- mail queues
- system, per-domain, and per-user block/safe list databases
- email users' address books
- images and language files for customized appearance of the GUI and webmail

In addition, although they are not part of the configuration, you may want to back up the following data, which may not be retrievable after the configuration is reset:

- email archives
- log files (cannot be restored)
- generated report files (cannot be restored)
- mailboxes

Items which cannot be backed up include:

- personal address books (separate from the global address book; these can only be backed up by each email user individually using the webmail interface)
- quarantines (can be backed up by using a NAS server)
- SSH keys for remote administrative access
- greylist auto-exempt state
- sender reputation state
- automatic MSISDN reputation blocklist state

Although mailboxes and quarantines cannot be downloaded to your management computer, you can configure the FortiMail unit to back up mail data by storing it externally, on a NAS server. For details, see Selecting the mail data storage location on page 192.

To back up the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. If you want to back up the configuration now, in the Backup Configuration area:
   - Enable System configuration, *User configuration*, or *IBE data*.
   - For user configuration and IBE data, click *Update* to get the latest configurations.
   - Click Backup.
   - If you want to encrypt the backup file, enable *Encryption* and enter the password. When you restore the encrypted backup file, you'll be prompted to enter the password.

   Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection.
3. If you want to set up scheduled backup, in the Scheduled Backup area:
   - Specify the schedule.
   - Enable *Local Backup* or *Remote Backup* or both.
   - For local backup, you can view the backup configuration files by backup types: All, Scheduled, or Automatic (automatic configuration backups are always done by the system before firmware upgrade or configuration restore.
   - For remote backup, specify the remote server information and login credentials.
   - Click Apply.

To back up, restore, reset, or repair the Bayesian databases

1. Go to *System* > *Maintenance* > *Database Maintenance*.
2. Click the relevant links.
   You must update the Bayesian database before you back it up.

To back up the mail queues

1. Go to *System* > *Maintenance* > *Mail Queue*.
2. Click Backup Queue.
   Your management computer downloads the database file. Time required varies by the size of the file and the speed of your network connection.

To back up the block/safe list database

1. Go to *System* > *Maintenance* > *Block/Safe List Maintenance*.
2. Click Export Block/Safe List.
   The database will be saved on your management computer as a .fml file. This database file contains the system-wide, per-domain and per-user block lists and safe lists.

To import the block/safe list database

1. Go to *System* > *Maintenance* > *Block/Safe List Maintenance*.
2. Click Import Block/Safe List.
   The file to be imported must be the .fml file that has been exported from FortiMail.

To back up email users' accounts (server mode only)

1. Go to *Domain & User* > *User* > *User*.
2. Click Export .CSV.
   Your management computer downloads the user account spreadsheet file. Time required varies by the size of the file and the speed of your network connection.

To back up the global address book (server mode only)

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Click Export.
3. On the pop-up menu, select CSV.
   You are prompted for a location to save the file. Follow the prompts and click Save.

   Your management computer downloads the address book spreadsheet file. Time required varies by the size of the file and the speed of your network connection.

To back up customized appearances of the administrative GUI and webmail GUI

1. Go to *System* > *Customization* > *Appearance*.
2. In Administration interface, for each image file, save the image to your management computer.
   Methods vary by web browser. For example, you might need to click and drag the images into a folder on your management computer in order to save them to that folder. For instructions, see your browser's documentation.
3. Click the arrow to expand Webmail interface.
4. For each webmail language, click the name of the language to select it, then click Download.
   Your management computer downloads the language file. Time required varies by the size of the file and the speed of your network connection.
5. To back up email archives go to *System* > *Maintenance* > *Mail Data*.

   In addition to downloading email archives to your management computer, you can configure the FortiMail unit to store email archives on an SFTP or FTP server. For details, see Managing archived email on page 142 and Configuring email archiving accounts on page 528.
6. Continue using the instructions in Configuring mailbox backups on page 274.

See also

Backing up your configuration using the CLI

Backing up and restoring the mailboxes

Backing up your configuration using the CLI

If you only want to back up the core configuration file, you can perform this backup using the CLI.

The core configuration file does not contain all configuration data. Failure to perform a complete backup could result in data loss of items such as Bayesian databases, dictionary databases, mail queues, and other items. For details on performing a complete backup, see Backup and restore on page 267.

To back up the configuration file using the CLI, enter the following command:

```
execute backup config tftp <filename_str> <tftp_ipv4>
```

where:

- `<filename_str>` is the name of the file located in the TFTP server's root directory
- `<tftp_ipv4>` is the IP address of the TFTP server

See also

Backup and restore

Backing up and restoring the mailboxes

Scheduling configuration backup

Instead of backing up your configuration manually (see the previous sections), you can also configure a schedule to back up the configuration automatically to the FortiMail local hard drive or a remote FTP/SFTP server.

To schedule the configuration backup

1. Go to *System* > *Maintenance* > *Configuration*.
2. Under *Scheduled Backup*, configure the schedule time and the maximum backup number. When the maximum number is reached, the oldest version will be overwritten.
3. Enable *Local backup* if you want to back up locally.
4. Enable *Remote backup* and configure the FTP/SFTP server credentials if you want to back up remotely.
5. Click *Apply*.

See also

Backup and restore

Backing up your configuration using the CLI

Restoring the configuration

Only the super admin user can restore system configuration and the firmware.

In the *Restore Configuration* area under *System* > *Maintenance* > *Configuration*, you can restore the backup FortiMail configuration from your local PC. Note that if the backup file is encrypted, you'll be prompted to enter the password. For details, see Restoring the configuration on page 572.

Restoring the firmware

Only the super admin user can restore system configuration and the firmware.

In the *Restore Firmware* area under *System* > *Maintenance* > *Configuration*, you can install a FortiMail firmware from your local PC. For details, see Installing firmware on page 569.

Backing up and restoring the mailboxes

The *System* > *Maintenance* > *Mail Data* tab lets you back and restore all mail data, including system quarantine, email users' personal quarantines, user preferences, archived email, and server mode webmail mailboxes. You can also monitor the status of any backup or restoration that is currently in progress.

Mail data backup only works for local storage. If you have configured remote storage (see Selecting the mail data storage location on page 192), mail data cannot be backed up.

Viewing the mailbox backup/restoration status

Go to *System* > *Maintenance* > *Mail Data* to view the progress if you are backing up or restoring mail data.

If backup and restoration are enabled, the appearance of this tab varies by:

- whether the FortiMail unit is currently backing up or restoring mailboxes
- whether the FortiMail unit has previously backed up or restored any mailboxes
- whether the previous backup or restoration attempt was successful

Backing up and restoring mailboxes from *System* > *Maintenance* > *Mail Data*

GUI item	Description
Automatically refresh interval	Select the interval in seconds to set how often the GUI automatically refreshes its display of this tab.
Refresh	Click to manually refresh the tab's display.

GUI item		Description
(button)		
Status		Indicates the current activity of mailbox data backup or restoration. If backup and restoration are currently disabled, the *Status* area of the *Mail Data* tab displays the message: *Backup/Restore is currently disabled*. To enable mailbox backups, see Configuring mailbox backups on page 274.
	State	Displays he current mailbox backup or restoration status, one of: • *IDLE*: No backup or restoration is currently occurring. To begin a backup, at the bottom of the status section, click *Click here to start a backup*. To begin a restoration, in the *Restore options* section, click *Restore*. • *BACKING UP*: The FortiMail unit is currently creating a backup copy of the mailboxes to the backup media configured in Device. • *RESTORING*: The FortiMail unit is currently restoring a backup copy of the mailboxes from the backup media . • *STOPPING*: You have canceled a backup or restoration that was in progress, and the FortiMail unit is halting the backup or restoration process. • *CHECKING*: The FortiMail unit is currently checking the file system integrity of the backup media. This state occurs only if you have configured a block-level backup media (either a USB disk or iSCSI server). • *FORMATTING*: The FortiMail unit is currently formatting the file system of the backup media. This state occurs only if you have configured a block-level backup media (either a USB disk or iSCSI server). If after some time the progress remains at 0%, or eventually silently reverts to an *IDLE* state without the backup or restoration having finished, then the operation has failed. Verify connectivity with the backup media (this is especially true with NFS, SSH, and iSCSI backup methods, where network connectivity issues can cause the FortiMail unit's attempt to mount the backup file system to fail). Also verify that you have configured the backup media correctly in Configuring mailbox backups on page 274 and configured the restoration item correctly in Restoring mailboxes from backups on page 276. **Note:** If a backup or restoration has failed, you may need to reboot the FortiMail unit before you can try again.
	Objects Copied (Total)	Indicates the number of files transferred to or from the backup media so far, and the total amount that will be transferred when the backup or restoration is complete.
	Bytes Copied (Total)	Indicates the number of bytes of data transferred to or from the backup media so far, and the total amount that will be transferred when the backup or restoration is complete.
	Percentage Complete	Indicates the percentage of bytes of data transferred to or from the backup media so far.

GUI item	Description
	If after some time the progress remains at 0%, or eventually silently reverts to an *IDLE* state without the backup or restoration having finished, the operation has failed. Verify connectivity with the backup media (this is especially true with NFS, SSH, and iSCSI backup methods, where network connectivity issues can cause the FortiMail's attempt to mount the backup file system to fail). Also verify that you have configured the backup media correctly in Device and configured the restoration item correctly in Restoring mailboxes from backups on page 276.
Status	Indicates the step of the backup or restoration that is currently occurring, such as *OK (stopping file systems)*.

Total number of errors is	Indicates the number of errors that occurred during the previous backup attempt. If any errors occurred, they may also be individually listed.
	For example, if the backup media is an NFS server, and the NFS share could not be mounted, such as if the FortiMail unit could not contact the NFS server or did not have permissions to access the share, an error message similar to the following would appear:
	`failed to mount archive filesystem [protocol=nfs,host=192.168.1.10,port=2049,directory=/home/fortimail]`
	`stopped, waiting for requested shutdown`
	`watch dog stopped, killing backup process`
	This field appears only if the previous backup attempt was not successful.

Last Backup	Indicates the date and time of the previous backup attempt. If a backup has not yet occurred, this field displays the message, *No backup has been run*.
Last Restore	Indicates the date and time of the previous restoration attempt. If a restoration has not yet occurred, this field is empty.
Click here to start a backup	Click to manually initiate an immediate mailbox backup to the media configured in Device. Time required to complete a backup varies by the size of the backup and the speed of your network connection, and also by whether the backup is a full or incremental backup. Alternatively, you can schedule the FortiMail unit to automatically back up the mailboxes. For details, see Configuring mailbox backups on page 274. This link does not appear if a backup or restoration is currently in progress.
Click here to format backup device	If you use a USB device for backup, click this link to format the device for use with FortiMail.
Click here to check file system on backup device	If you use a USB device for backup, click this link to determine if the device is compatible for use with FortiMail.
Click here to stop the current backup	Click to cancel a backup that is currently in progress. Time required to cancel the backup varies by the backup media, but may be up to 30 seconds. This link appears only if a backup is currently in progress.
Click here to stop the current restore	Click to cancel a restore that is currently in progress. Time required to cancel the restore varies by the restore media, but may be up to 30 seconds. This link appears only if a restore is currently in progress.

See also

Viewing the mailbox backup/restoration status

Configuring mailbox backups

Restoring mailboxes from backups

Configuring mailbox backups

Use the *Backup Options* area of the *Mail Data* tab to configure which backup media to use when you back up or restore email users' mailboxes. You can also configure the schedule the FortiMail unit uses to automatically perform backups.

You can only back up mail data when you store the data locally on the FortiMail hard disk. If you store the mail data on a NAS device, you cannot back up the data. Use backup software on the external NAS instead. For information about selecting a storage device, see Selecting the mail data storage location on page 192.

While a backup or restoration is occurring, you cannot change the configuration of this area, and this area will display the message:

```
Backup/Restore is busy, no configuration changes can be made.
```

However, you can view the status of the backup or restoration to determine if there are any errors. You can also manually initiate an immediate backup if the backup media was unavailable at the time of a previously scheduled backup. For details, see Backing up and restoring the mailboxes on page 271.

Before you can manually initiate a backup, or in order to configure automatic scheduled backups, you must first enable backups and configure the backup media.

To configure backups

1. Go to *System* > *Maintenance* > *Mail Data*.
2. Configure the following in the *Backup Options* section:

GUI item	Description
Enable	Mark this check box, configure all other options in this area, then click *Apply* to enable backups and restoration of email users' mailboxes.
Copies of full backups	Enter a number of full backups to keep on the backup device.
Schedule [full] **Schedule [incremental]**	The *Schedule* options are disabled if *Protocol* is *External USB (auto detect)*. Full backup will back up the entire mail data, while incremental backup will back up the newer data since the previous backup. To minimize performance impacts, consider scheduling backups during a time of the day and day of the week when email traffic volume is typically low, such as at night on the weekend. If the backup media is not available when the backup is scheduled to occur, the FortiMail unit will re-attempt the backup at the next scheduled time. Regardless of whether or not scheduled backups are enabled, you can manually initiate backups. For details, see Backing up and restoring the mailboxes on page 271.

GUI item		Description
Device		
	Protocol	Select one of the following types of backup media: • *NFS*: A network file system (NFS) server. • *SMB/CIFS*: A Microsoft Windows-style file share. • *SSH File System*: A server that supports secure shell (SSH) connections. • *External USB Device*: An external hard drive connected to the FortiMail unit's USB port. • *External USB Device (auto detect):* An external disk connected to the FortiMail unit's USB port. Unlike the previous option, this option only creates a backup when you connect the USB disk, or when you manually initiate a backup using Backing up and restoring the mailboxes on page 271, rather than according to a schedule. • *iSCSI Server*: An Internet SCSI (Small Computer System Interface), also called iSCSI server.
	The availability of the following options varies by the device chosen.	
	Username	Enter the user name of the FortiMail unit's account on the backup server.
	Domain	If you choose *SMB/CIFS* as the backup media and if the account name has a domain part, then enter the domain name.
	Password	Enter the password of the FortiMail unit's account on the backup server.
	Hostname/IP address	Enter the IP address or fully qualified domain name (FQDN) of the NFS, Windows, SSH, or iSCSI server.
	Port	Enter the port number on which the backup server listens for connections.
	Directory	Enter the path of the folder on the backup server where the FortiMail unit will store the mailbox backups, such as: `/home/fortimail/mailboxbackups` **Note:** Do not use special characters such as a tilde (~). Special characters will cause the backup to fail.
	Share	Enter the path of the folder on the backup server where the FortiMail unit will store the mailbox backups, such as: `FortiMailMailboxBackups` **Note**: Do NOT type / before the path name.
	Encryption key	Enter the key that will be used to encrypt data stored on the backup media. Valid key lengths are between 6 and 64 single-byte characters.
	iSCSI ID	Enter the iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA).

See also

Viewing the mailbox backup/restoration status

Backing up and restoring the mailboxes

Restoring mailboxes from backups

Restoring mailboxes from backups

The *Restore Options* area of the *Mail Data* tab lets you selectively restore email users' mailboxes from mailbox backups. The restored mailboxes will be merged with the current mailboxes.

If a backup or restoration is currently in progress, this area will display the message:

Backup/Restore is busy, no restore can be started till it finishes.

If after some time the progress remains at 0%, or eventually silently reverts to an *IDLE* state without the restoration having finished, the operation has failed. Verify connectivity with the backup media (this is especially true with NFS, SSH, and iSCSI backup methods, where network connectivity issues can cause the FortiMail's attempt to mount the backup file system to fail). Also verify that you have configured the backup media correctly in Device.

To restore mailboxes from backup

1. Go to *System* > *Maintenance* > *Mail Data*.
2. Configure the following in the *Restore Options* section:

GUI item	Description
Created by this device	Select to restore mailboxes from backups identified by the current fully qualified domain name (FQDN) (or, if its local domain was not configured, the hostname) of this FortiMail unit. If you changed the host name and/or local domain name of the FortiMail unit, the backup files are still identified by the previous FQDN. In this case, do not select this option. Instead, use the *Created by* option.
Created by	Select to restore mailboxes from backups identified by an oldFQDN, or the FQDN of another FortiMail unit. Usually, you enter the FQDN of this same FortiMail unit, but you may enter the FQDN of another FortiMail unit if you want to import mailboxes from it. For example, you may be upgrading from FortiMail A to a FortiMail B, and have a backup of the mailboxes from the FortiMail A, `fortimail.example.com`. On FortiMail B, configure it to also use the same backup storage media, then enter `fortimail.example.com` in this field to import mailboxes from FortiMail A.
For this domain	Mark this check box if you want to restore only the mailboxes of a specific protected domain, then select the name of the protected domain from the dropdown list. If you want to restore only the mailbox of a specific email user within this protected domain, also configure *For this user*.
For this user	Mark this check box if you want to restore only the mailbox of a specific email user, then enter the name of the email user account, such as `user1`. This option is available only if *For this domain* is enabled.
Restore (button)	Click to restore mailboxes from the most recent full or incremental backup stored on the backup media configured on Configuring mailbox backups on page 274. Time required to complete a restoration varies by the size of the backup and the speed of your network connection, and also by whether the backup was a full or incremental backup.

GUI item	Description
	Note: To restore from a specific full and incremental version of backup, you can use the command `execute backup-restore old-restore`. For details, see the FortiMail CLI Reference.

3. To manually initiate restoration of mail data, click *Restore*.

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 263.

Traffic capture

When troubleshooting networks, it helps to look inside the contents of the packets. This helps to determine if the packets, route, and destination are all what you expect. Traffic capture can also be called packet sniffing, a network tap, or logic analyzing.

Packet sniffing tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- finding missing traffic
- seeing if sessions are setting up properly
- locating ARP problems such as broadcast storm sources and causes
- confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks
- confirming routing is working as you expect
- intermittent missing PING packets.

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, how the port enters and exits the FortiRecorder unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start sniffing packets, you need to have a good idea of what you are looking for. Sniffing is used to confirm or deny your ideas about what is happening on the network. If you try sniffing without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to sniff enough packets to really understand all of the patterns and behavior that you are looking for.

To capture the traffic

1. Go to *System* > *Utility* > *Traffic Capture*.
2. Click *New*.
3. Enter a description for the file generated from the captured traffic.
4. Enter the time period for performing the packet capture.

5. Specify which interface you want to capture.
6. If you want to limit the scope of traffic capture, in the *IP/HOST* field, enter a maximum of 3 IP addresses or host names for which you want to capture.
7. Select the filter for the traffic capture:
   - *Use protocol*: Only UDP or TCP traffic on the specified port number will be captured.
   - *Capture all*: All network traffic will be captured.
8. For *Exclusion*, enter the IP addresses/host names and port numbers for which do not want to capture.
9. Click *Create*.

Regular expression validator

Go to *System* > *Utility* > *Regex Validator* to validate and test regular expressions and string text. See also Syntax on page 617.

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, since FortiMail couldn't scan the content of an email attachment with .msg files attached.

On-demand DMARC reports

If DMARC checks and DMARC reports are enabled (see DMARC section on page 383 and DMARC Report Generation on page 506), then FortiMail automatically periodically sends DMARC reports.

If you have the feature license for it (see DMARC report analysis on page 266), 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.

GUI item	Description
	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 506.
Report to address	Select the 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. • *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.

3. Click lick *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.

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
- the 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 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 290.

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.

Before you begin, if the protected domain will use an IP pool profile, first configure the IP pool profile. For details, see Configuring IP pools on page 458.

To configure protected domains

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	Displays 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 (transparent and gateway mode only)	Indicates how the SMTP server will receive email from the FortiMail unit for the protected domain: • *Host* • *MX Record (this domain)* • *MX Record (alternative domain)* • *IP Group* • *LDAP Domain Mail Host*
SMTP server (transparent and gateway mode only)	Displays the host name or IP address and port number of the mail exchanger (MX) for this protected domain. 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 (transparent and gateway mode only)	Displays the SMTP server or LDAP server used for recipient address verification if it is enabled.
Sub (transparent and gateway mode only)	The number indicates how many subdomains this domain has.
Association (transparent and gateway mode only)	The number indicates how many domain associations this domain has. For more information on domain associations, see Domain Association on page 290.
MTA Status (transparent and gateway mode only)	Displays the recipient SMTP server status.

GUI item	Description
Disk Usage (%) (transparent and gateway mode only)	Displays 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 general information as it applies to the current 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.
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 (transparent and 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 423).

GUI item	Description
	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 (transparent and 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. 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 333 and Avoiding scanning email multiple times on page 199. This field appears only if Relay type is *Host*.
Fallback SMTP server (transparent and 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 (transparent and 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 (transparent mode and 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*.

GUI item	Description
	See also Appendix C: Port Numbers on page 611.
Alternative domain name (transparent and 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 423), 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 266.
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 you wish 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 transparent mode options
   - Configuring removal of invalid quarantine accounts
   - Configuring LDAP Options
   - Configuring advanced settings
   - Configuring mail migration settings (server mode only)

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.

This feature can impact performance and be noticeable during peak traffic times. For a lesser performance impact, you can alternatively periodically automatically remove quarantined email messages for invalid email user accounts, rather than actively preventing them during each email message.

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 C: Port Numbers on page 611.
	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 423. 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 307

GUI item	Description
	Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).

Configuring transparent mode options

This section appears only when the FortiMail unit operates in transparent 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.
   A multisection dialog appears. Its options vary with the operation mode.
3. Expand the transparent mode settings section.
4. Configure the following:
5.

GUI item	Description
This server is on	Select the network interface (a port) to which the protected SMTP server is connected. **Note:** Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface.

Hide the transparent box	Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in:
	• the SMTP greeting (`HELO`/`EHLO`) in the envelope and in the `Received:` message headers of email messages
	• the IP addresses in the IP header
	This masks the existence of the FortiMail unit to the protected SMTP server.
	Disable to replace the SMTP client's IP address or domain name with that of the FortiMail unit.
	For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in bold):
	`Received: from 192.168.1.1 (`**`EHLO 172.16.1.1`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`[172.16.1.1]`**` with SMTP id kAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT`
	But if the option is disabled, the message headers would contain:
	`Received: from 192.168.1.1 (`**`EHLO fortimail.example.com`**`) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800`
	`Received: from smtpa ([172.16.1.2]) by `**`fortimail.example.com`**` with SMTP id kAOFJl4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT`
	Note: If the protected SMTP server applies rate limiting according to IP addresses, enabling this option can improve performance. The rate limit will then be separate for each client connecting to the protected SMTP server, rather than shared among all connections handled by the FortiMail unit.

GUI item	Description
	Note: Unless you have enabled Take precedence over recipient based policy match on page 353 in the IP-based policy, this option supercedes the Hide this box from the mail server on page 362 option in the session profile, and may prevent it from applying to incoming email messages.
Use this domain's SMTP server to deliver the mail	Enable to use the protected SMTP server, instead of the FortiMail built-in MTA, to deliver ***outgoing*** email messages from the SMTP clients whose sending MTA is the protected SMTP server. For example, if the protected domain example.com has the SMTP server 192.168.1.1, and an SMTP client for `user1@example.com` connects to it to send email to `user2@external.example.net`, enabling this option would cause the FortiMail unit to pass the mail message via its built-in MTA to the protected SMTP server, which will deliver the message. Disable to relay email using the built-in MTA to either the SMTP relay defined in Configuring SMTP relay hosts on page 188, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (`RCPT TO:`) domain. The email may not actually travel through the protected SMTP server, even though it was the relay originally specified by the SMTP client. This option does not affect incoming connections containing incoming email messages, which will always be handled by the built-in MTA. For details, see When FortiMail uses the proxies instead of the built-in MTA on page 195. **Note:** This option will be ignored for email that matches an antispam or content action profile.

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 284), 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 multisection 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 423.
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.

Configuring LDAP Options

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 Options* section.
4. Configure the following:

GUI item	Description
User alias / address mapping profile (transparent and 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 423.
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 423.
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 423.

Configuring advanced settings

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

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 473 and Customizing GUI, custom messages, email templates, and Security Fabric on page 204.

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. Click to expand Advanced Setting.
4. Click to expand Quarantine Report Setting.
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 121.
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 Configuring group query options on page 427. 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 473.

GUI item	Description
	• *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

The Domain Association section that appears when configuring a protected domain lets you 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 the FortiMail unit 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.
5. 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.
6. Click Create.
   The name of the associated domain appears in the Members area.
7. Repeat the previous steps for all domains that you want to associate with this protected domain.
8. When done, click Create or OK.

DKIM and ARC Setting

The FortiMail unit will sign outgoing email messages using the domain key for this protected domain if you have selected it when configuring sender validation in the session profile. For more information, see Configuring session profiles on page 361.

FortiMail also supports Authenticated Received Chain (ARC) validation and sealing.

DKIM signing requires a public-private key pair. The private key is kept on and used by the FortiMail unit to generate the DKIM signatures for the email messages; the public key is stored on the DNS server in the DNS record for the domain name, and used by receiving parties to verify the signature.

You can generate the key pair by creating a domain key selector; you can also manually import an existing key pair in PEM format.

After you generate or import the key pair, you can export the DNS record that contains the public key. The following is a sample of the exported DNS record:

```
example_com._domainkey IN TXT "t=y; k=rsa;
      p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5xvUazqp2sBovpfumPuR5xC+yDvGbfndyHZuVQdSHhwdK
      AdsfiyOa03iPniCfQEbuM0d+4/AoPyTXHHPFBBnChMMHkWgHYlRDm5UMjrH5J1zDT5OyFxUEur+NtfS6LF29Te
      +6vSS+D3asfZ85V6WJDHSI9JV0504uwDeOOh/aewIDAQAB"
```

This DNS record can be generated either in multiple string or single string format.

Then you can publish the public key by adding it to the DNS zone file as a text record for the domain name on the DNS server. The recipient SMTP server, if enabled to use DKIM verification, will use the public key to decrypt the signature and compare the hash values of the email message in order to verify that the hash values match.

FortiMail performs DKIM signing for an associated domain with its parent domain DKIM key. You must publish the DKIM public key for the associated domain in order for the receiving MTA to validate the DKIM signature.

To configure DKIM and ARC settings

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Double-click to modify an existing protected domain. ***Note:*** You can only configure DKIM and ARC setting for existing domains.
3. Click to expand Advanced Setting.
4. Click DKIM and ARC Setting.
5. Configure both the *DKIM signing option* and *ARC sealing option*:
   - *Disable*:Disable DKIM signing/ARC sealing.
   - *Incoming*:Perform DKIM signing/ARC sealing for email sent from one protected domain to the same domain.
   - *Outgoing*:Perform DKIM signing/ARC sealing for email sent from one protected domain to other domains,

including other protected domains and all external domains.
- *All*:Perform DKIM signing/ARC sealing for both the incoming and outgoing email.

6. Under *Key Selectors*, click *New* to configure the key pair required for DKIM signing.
7. If you want to generate a key pair, enter a new selector to use for the DKIM key, such as `example_com2`, then select *Auto Generation* and click *OK*.
8. If you want to import an existing key pair, enter a selector name, then select *Manual Import*, and upload the public key and private key. Optionally enter a password for the private key. Note that the key files must be in PEM format.
9. Click Create.
   The selector name for the key pair appears in the list of domain key selectors. The key pair is generated and public key can be exported for publication on a DNS server.

When a new key is created or imported, it is not active by default. This allows you to publish the public key on the DNS server before you activate the key. Also note that only one key pair can be active at a time.

10. Click to select the domain key, then click Download.
    Optionally, specify whether you want to download the domain key in either multi-string or single-string format.
    Your web browser downloads the plain text file which contains the exported DNS record (.dkim) file.
11. Publish the public key by inserting the exported DNS record into the DNS zone file of the DNS server that resolves this domain name. For details, see the documentation for your DNS server.
12. Now you can activate the key by selecting the key and then clicking *Activate*.

Disclaimer for a domain

The Disclaimer section that appears when configuring a protected domain lets you configure disclaimer messages specific to this protected domain. This option is only available when Allow per-domain settings is enabled under *System* > *Mail Setting* > *Disclaimer*.

A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential. For disclaimers added to outgoing messages, you need to 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.

If the FortiMail unit is operating in transparent mode, to use disclaimers, you must enable clients to send email using their specified SMTP server. For more information, see Use client-specified SMTP server to send email on page 203.

To configure a per-domain disclaimer messages

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 to expand Disclaimer.

You cannot configure the domain disclaimer unless the *Allow per-domain settings* option is enabled under*System* > *Mail Setting* > *Disclaimer*.

5. 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 messages. For more information, see Configuring global disclaimers on page 190. • *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 190. This option is only available only when you have enabled per-domain disclaimer messages. For more information, see Configuring global disclaimers on page 190.

Sender address rate control

For users under this domain, you can rate control how much each user can send email.

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 to expand *Sender Address Rate Control*.
5. For email users under this domain, you can configure the following rate control settings per user:
   - Maximum number of messages per half hour. The default value is 30.
   - Maximum number of recipients per half hour. The default value is 60.
   - Maximum data size per half hour (MB). The default value is 100 MB.
   - Maximum number of spam messages per half hour. The default value is 5.
   - Send email notification upon rate control violations and select a notification profile (see Configuring notification profiles on page 461).

See also

Use client-specified SMTP server to send email

Configuring global disclaimers

Incoming versus outgoing email

Configuring protected domains

Other advanced domain settings

The following procedure is part of the domain configuration process. For information about domain configuration, see Configuring protected domains on page 280.

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. Click to expand the *Advanced Setting* section.
4. Click to expand the *Other* section.
5. Configure the following:

GUI item	Description
Webmail theme	Either use the system setting or choose a color to overwrite the system setting.
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 the GUI appearance on page 212.
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 215.
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.

GUI item	Description
	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. • *Use other name*: Specify a greeting name if you want to use a customized host name. For example, if you choose to use an IP group for this domain, you can specify a greeting name for this IP pool to use. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.
IP pool	You can use a pool of IP addresses as the source IP address when sending email from this domain, or as the destination IP address when receiving email destined to this domain, or as both the source and destination IP addresses. • If you want to use the IP pool as the source IP address for this protected domain, according to the sender's email address in the envelope (`MAIL FROM:`), select the IP pool to use and select *Delivering* as the *Direction*. • If you want to use the IP pool as the destination IP address (virtual host) for this protected domain, according to the recipient's email address in the envelope (`RCPT TO:`), select the IP pool to use and select *Receiving* as the *Direction*. You must also configure the MX record to direct email to the IP pool addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well. • If you want to use the IP pool as both the destination and source IP address, select the IP pool to use and select *Both* as the *Direction*. Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address. If the FortiMail unit is operating in transparent mode, and you have enabled Hide the transparent box on page 286 or Use client-specified SMTP server to send email on page 203, you cannot use IP pools. For more information on IP pools, see Configuring IP pools on page 458.
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 373.
Use global Bayesian database	Enable to use the global Bayesian database instead of the Bayesian database for this protected domain.

GUI item	Description
	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 507 and Training the Bayesian databases on page 508.
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 497.

Domain level service settings (server mode only)

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 set limits on the usage of FortiMail resources. The domain administrators are not allowed to modify these settings.

The following procedure is part of the domain configuration process. For information about domain configuration, see Configuring protected domains on page 280.

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. Click *Other* under *Advanced Setting*.
4. Configure the following under *Service Setting*:

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.

Configuring customer information

Use this section to configure the customer account information.

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 *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	Optionally, enter a description.

Configuring mail migration settings (server mode only)

If you enable the mail migration feature, this section will appear. For details, see Migrating email from other mail servers (server mode only) on page 330.

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 602.

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.

GUI item	Description
	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 on page 267.
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 299. 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 280. You may also want to back up the existing email user accounts. For details, see Backup and restore on page 267.
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 423.
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.
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 280.

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 Configuring user authentication options on page 428.

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 418 is enabled. For details, see Workflow to enable and configure authentication of email users on page 419 and Configuring resource profiles on page 418.
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 333.

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 423.

6. Click OK.

See also

Managing the disk usage of email users mailboxes

Configuring user preferences

Configuring user aliases

Configuring address mappings

Configuring PKI authentication

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 418.

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* • *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 the GUI appearance on page 212.
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 487.
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.

GUI item	Description
	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. For more information on safe lists and block lists, see Managing the personal block lists and safe lists on page 487.
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 487) 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

Configuring PKI authentication

Configuring PKI authentication

Go to *Domain & User* > *User* > *PKI User* to configure public key infrastructure (PKI) user authentication.

PKI users can authenticate by presenting a valid client certificate, rather than by entering a user name and password.

A PKI user can be either an email user or a FortiMail administrator.

When a PKI user connects to the FortiMail unit with a web browser, the browser presents the PKI user's certificate to the FortiMail unit. If the certificate is valid, the FortiMail unit then authenticates the PKI user. To be valid, a client certificate must:

- not be expired
- not be revoked by either certificate revocation list (CRL) or, if enabled, online certificate status protocol (OCSP)
- be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail unit
- contain a `CA` field whose value matches the CA certificate
- contain a `Issuer` field whose value matches the `Subject` field in the CA certificate
- contain a `Subject` field whose value contains the subject, or is empty
- contain a `Common Name` (CN) or `Subject Alternative` field, if LDAP Query is enabled, whose value matches the email address of a user object retrieved using the *User Query Options* of the LDAP profile.

Web browsers may have their own certificate validation requirements in addition to FortiMail requirements. For example, personal certificates may be required to contain the PKI user's email address in the `Subject Alternative Name` field, and that `Key Usage` field contain `Digital Signature, Data Encipherment, Key Encipherment`. For browser requirements, see your web browser's documentation.

If the client certificate is **not** valid, depending on whether you have configured the FortiMail unit to require valid certificates, authentication will either fail absolutely, or fail over to user name and password authentication.

If the certificate is valid and authentication succeeds, the PKI user's web browser is redirected to either the GUI (for PKI users that are FortiMail administrators), or FortiMail webmail or the personal quarantine (for PKI users that are email users).

For details and examples about how to use PKI authentication for FortiMail email users and administrators, see Appendix F: PKI Authentication on page 628.

To view and configure PKI users

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

GUI item	Description
Name	Displays the user name of the PKI user.
Domain	Displays the protected domain to which the PKI user is assigned. If Domain on page 305 is empty, the PKI user is an administrator.
CA	Displays the name of the CA certificate used when validating the CA's signature of the client certificate. For more information, see Managing certificate authority certificates on page 256.
Subject	Displays a string used to match part of the value in the `Subject` field of the client certificate. It does not have to match the entire subject. If empty, matching values are not considered when validating the client certificate presented by the PKI user's web browser.
LDAP	If LDAP query on page 306 is enabled, the LDAP configuration of this PKI user is shown in three parts: • Whether the LDAP query setting is enabled (indicated by `E`) or disabled (indicated by "–"). • Displays the name of the LDAP profile used for the query. For more information, see Configuring LDAP profiles on page 423. • Displays the name of the field in the client certificate (either Subject Alternative or CN) whose value must match the email address of a user object in the LDAP directory. For example, `E/ldapprof/Subject Alternative` indicates that LDAP query is enabled, and will use the LDAP profile named `ldapprof` to validate the `Subject Alternative` field of the client certificate.
OCSP	If this is enabled, the OCSP configuration of this PKI user is shown in three parts: • Whether OSCP is enabled (indicated by `E`) or disabled (indicated by "–"). • Displays the URL of the OCSP server. • Displays the action to take if the OCSP server is unavailable. If set to ignore, the FortiMail unit allows the user to authenticate. If set to revoke, the FortiMail unit behaves as if the certificate is currently revoked, and authentication fails. For example, `E/https://www.example.com/Revoke` indicates OCSP is enabled, using the OSCP server at https://www.example.com, and if the OSCP server is unavailable, the FortiMail unit prevents the user from authenticating.

2. Click New to add PKI authentication for an email user or administrator account or double-click an account to modify it.
3. Configure the following:

GUI item	Description
User name	For a new user, enter the name of the PKI user. There is no requirement to use the same name as the administrator or email user's account name, although you may find it helpful to be so. For example, you might have an administrator account named `admin1`.You might therefore find it most straightforward to **also** name the PKI user `admin1`, making it easy to remember which account you intended to use these PKI settings.

GUI item	Description
Domain	Select either the protected domain to which the PKI user is assigned, or, if the PKI user is a FortiMail administrator, select System. You can see only the domains that are permitted by your administrator profile.
CA	Select either None or the name of the CA certificate to use when validating the CA's signature of the client certificate. For more information, see Managing certificate authority certificates on page 256. If you select None, you **must** configure Subject on page 306.
Subject	Enter the value which must match the `Subject` field of the client certificate, or leave this field empty. If empty, matching values are not considered when validating the client certificate presented by the PKI user's web browser. The FortiMail unit will use a CA certificate to authenticate a PKI user only if the subject string you enter here also appears in the CA certificate subject. If no subject is entered here, the subject not considered when the FortiMail unit selects the certificate to use. If you do not configure Subject on page 306, you **must** configure CA on page 306.
LDAP query	Enable to query an LDAP directory, such as Microsoft Active Directory, to determine the existence of the PKI user who is attempting to authenticate, then also configure LDAP profile on page 306 and Query field on page 306. **Note:** If this option is enabled, no local user configuration is necessary. Instead, the FortiMail unit creates the personal quarantine folder and other necessary items when PKI authentication queries the LDAP server.
	LDAP profile — From the dropdown list, select the LDAP profile to use when querying the LDAP server. • If no profile exists, click New to create one. • If a profile exists but needs modification, select it and click Edit. In both cases, the Edit LDAP Profile dialog appears. For more information, see Configuring LDAP profiles on page 423. This option is available only if LDAP query on page 306 is enabled.
	Query field — Select the name of the field in the client certificate (either CN or Subject Alternative) which contains the email address of the PKI user. This email address will be compared with the value of the email address attribute for each user object queried from the LDAP directory to determine if the PKI user exists in the LDAP directory. This option is available only if LDAP query on page 306 is enabled.
OCSP	Enable to use an Online Certificate Status Protocol (OCSP) server to query whether the client certificate has been revoked, then also configure URL, Remote certificate, and Unavailable action.
	URL — Displays the URL of the OCSP server. See also Appendix C: Port Numbers on page 611. This option is available only if OCSP is enabled.
	Remote certificate — Select the remote certificate that is used to verify the identity of the OCSP server. For more information, see Managing OCSP server certificates on page 257. This option is available only if OCSP is enabled.

GUI item	Description	
	Unavailable action	Select the action to take if the OCSP server is unavailable. If set to Ignore, the FortiMail unit allows the user to authenticate. If set to Revoke, the FortiMail unit behaves as if the certificate is currently revoked, and authentication fails. This option is available only if OCSP is enabled.

You need to take additional steps to activate and complete a PKI user's configuration.

To complete PKI user configuration

1. To enable PKI authentication on your FortiMail unit for all PKI users, open the CLI and enter the following command:
```
config system global
   set pki-mode enable
end
```
2. For each PKI user, import the client certificate into the user's web browser on each computer the PKI user will use to access the FortiMail unit. For details on installing certificates, see the documentation for your web browser. Client certificates must be valid. For information on how FortiMail units validate the client certificates of PKI users, see Configuring PKI authentication on page 304.
3. In the GUI, import the CA certificate into the FortiMail unit. For more information, see Managing certificate authority certificates on page 256.
4. For PKI users that are FortiMail administrators, select the PKI authentication type and select a PKI user to which the administrator account corresponds. For more information, see Configuring administrator accounts and access profiles on page 165.
5. For PKI users that are email users, enable PKI user authentication in the incoming recipient-based policies which match those email users. For more information, see Controlling email based on sender and recipient addresses on page 354.

Control access to each PKI user's computer. Certificate-based PKI authentication controls access to the FortiMail unit based on PKI certificates, which are installed on each email user or administrator's computer. If anyone can access the computers where those PKI certificates are installed, they can gain access to the FortiMail unit, which can compromise the security of your FortiMail unit.

See also

Configuring local user accounts (server mode only)

Configuring user preferences

Configuring user aliases

Configuring address mappings

Configuring PKI authentication

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

Note that this advanced management feature is only available when *User management* is enabled under *System* > *FortiGuard* > *Licensed Feature*. For more information, see Configuring advanced management (feature license required) on page 266.

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 308 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 266.
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. See also Appendix C: Port Numbers on page 611.
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*.

GUI item	Description
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.
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 423.

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

Configuring user alias options

Configuring 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:` • `Resent-Sender:` • `Delivery-Receipt-To:` • `Disposition-Notification-To:`	External email address

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 423.

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 313.
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. 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 313. 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

Configuring address mapping options

Configuring 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 518.

This section contains the following topics:

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. 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 317.
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.
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:

GUI item	Description
	• 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 317.
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)

See also

Configuring expired users

Configuring IBE authentication

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 516.

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.

GUI item	Description
	Note that **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 317.
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 317.
Expiry Time	Displays when the user's registration expired.
Last Access	Displays the time stamp when the user was last active.

See also

Configuring active users

Configuring IBE authentication

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 319.

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 423.

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 non-LDAP-authenticated users to get registered on FortiMail, you can use 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 423.
LDAP profile	Select the LDAP profile you want to use to authenticate the domain users.

User registration process with two-factor authentication

As of FortiMail 6.4.0, the enforcement of security questions has been removed and replaced with two-factor authentication, via email and/or SMS text message.

See Configuring IBE services on page 519 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.

See also

Configuring active users

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 315.
Expired User Count	Displays the expired mail users in a domain. For more information about active users, see Configuring expired users on page 316.

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 322.

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 280.
First name	Enter a first name (given name).
Last name	Enter a last name (family or surname).
Display name	
Email	Enter an email address.

GUI item	Description
	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 322.

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 324.

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 423.
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 323.

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 322.

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 321.

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 280.
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 320.

   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.

GUI item	Description
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 438.

   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.
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 320 and Synchronizing the address book via LDAP on page 324.

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 423.
LDAP mapping	Select an LDAP attribute-to-address-book mapping that defines which contact information will be synchronized. See also Configuring LDAP attribute mapping for the address book on page 323.
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 previous synchronization.
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 320. 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 326).
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 326).
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 326).

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 326).
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 C: Port Numbers on page 611.
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 331.

c. Create a domain for the to-be-migrated users. For details, see Creating domains for mail migration on page 332.

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 420.
     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 354.
     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 330.

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 C: Port Numbers on page 611.
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 330.

1. Go to *Domain & User* > *Domain* > *Domain.*
2. Click *New*.
3. Configure the settings as described in Configuring protected domains on page 280.

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 331.
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 361), 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 337)
- Recipient-based policies (see Controlling email based on sender and recipient addresses on page 354)
- IP-based policies (see Controlling email based on IP addresses on page 348)

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

Use access control rules and delivery rules to control which SMTP clients can send email through an SMTP relay and how SMTP will deliver email that it proxies or relays.

Recipient-based policies are applied to individual email messages based on the recipient's email address.

IP-based policies are applied based on the IP address of the connecting SMTP client and, if the FortiMail unit is operating in transparent mode, the SMTP server.

See also

What is a policy?

Whether to use IP-based or recipient-based policies

Order of execution of policies

Which policy/profile is applied when an email has multiple recipients?

Whether to use IP-based or recipient-based policies

Since there are two types of policies, which type 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 appropriate **Authentication type** and **Authentication profile** under **Authentication and Access** 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

Arrange policies in the policy list by placing the most specific policy at the top and more general policies at the bottom.

For example, a recipient-based policy created with an asterisk (*) entered for the user name is the most general policy possible because it will match all users in the domain. When you create more specific policies, you should move them above this policy. Otherwise, the general policy would always match all email for the domain, and no other recipient-based policy would ever be applied.

FortiMail units execute policies in the following order:

1. As a general rule, recipient-based policies override IP-based policies. This means that if an email message matches both a recipient-based policy and an IP-based policy, the settings in the recipient-based policy will be applied and the IP-based policy will be ignored. The exception is described in the next step.
2. The FortiMail unit looks for a matching IP-based policy.
   The FortiMail unit evaluates each policy for a match with the IP address of the SMTP client and, for transparent mode, the server. Evaluation occurs in the order of each policy's distance from the top of the list of IP-based policies. Once a match is found, the FortiMail unit does not evaluate subsequent IP-based policies.

If you have enabled *Take precedence over recipient based policy match* in the IP-based policy, the FortiMail unit applies the profiles in the IP-based policy. In this case, it ignores recipient-based policies in the following two steps and jumps to step The FortiMail unit applies the profiles in the matching IP-based policy, only if: There is no recipient-based policy match in step 3. Or you have enabledTake precedence over recipient based policy match in the IP-based policy.Or although there is a recipient-based policy match, the profile does not exist in the policy. However, the profile exists in the matching IP-based policy. on page 336.

3. The FortiMail unit looks for a matching recipient-based policy.
   The FortiMail unit evaluates each policy for a match with the domain name portion of the recipient's email address (`RCPT TO:`), also known as the domain-part. Incoming policies are evaluated for matches before outgoing policies. Evaluation occurs in the order of each policy's distance from the top of the list of recipient-based policies. Once a match is found, the FortiMail unit does not evaluate subsequent recipient-based policies.
4. The FortiMail unit applies the profiles in the matching recipient-based policy, if any.
5. The FortiMail unit applies the profiles in the matching IP-based policy, only if:
   - There is no recipient-based policy match in step 3.
   - Or you have enabled*Take precedence over recipient based policy match* in the IP-based policy.
   - Or although there is a recipient-based policy match, the profile does not exist in the policy. However, the profile exists in the matching IP-based policy.

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.

See also

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

Which policy/profile is applied when an email has multiple recipients?

When applying recipient-based policies, an email message with multiple recipients is treated as if it were multiple email messages, each with a single 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 will look for a matching recipient-based policy. If none is found, the FortiMail unit will evaluate each subsequent recipient email address for a matching policy. The FortiMail unit will apply only the first matching policy; it will not evaluate subsequent recipients for a matching policy. If no matching recipient-based policy is found, the FortiMail unit will apply the antivirus profile from the IP-based policy, if any.

If no recipient-based or IP-based policy matches, no profiles is applied.

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 152.

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.

See also

Configuring access control receiving policies

Configuring delivery rules

Rate limiting for delivery

Troubleshoot MTA issues

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:

- 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
- 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 280.

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
- specified 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 348.

For information about the sequence in which access control rules are used relative to other antispam methods, see Order of execution on page 26.

Do **not** create an access control policy where:

- Sender is `*`
- Recipient is `*`
- 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.

GUI item	Description

Sender	Select how you will define the sender email addresses that match the policy, either:
	• *User Defined*: 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.
	• *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 459.
	• *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 423.
	• *LDAP Verification*: Select the LDAP query to a directory server such as Microsoft Active Directory. See also Configuring LDAP profiles on page 423.
	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.
	• *Regular Expression*: Enter a regular expression that can match multiple email addresses. To validate the expression and verify correct matching, click *Validate*. See also Appendix D: Wildcards and regular expressions on page 616 and Using wildcards and regular expressions with access control on page 341.

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.
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. 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 address, enter `0.0.0.0/0`. • *IP Group*: Select an IP address group. See also Configuring IP groups on page 460. • *GeoIP Group*: Select a geographic IP address group. See also Configuring GeoIP groups on page 460.

GUI item	Description
	• *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.
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. • Regular expression. **Tip:** To verify syntax and correct matching, click *Validate*. See also Appendix D: Wildcards and regular expressions on page 616 and Using wildcards and regular expressions with access control on page 341. 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.
Authentication status	Select whether to match this policy based upon whether 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 453.
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. If all scans pass, the email is delivered. • *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 and but continue with others such as antivirus.

GUI item	Description
	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 *Safe*, except **do not greylist**. • *Receive*: Like *Relay*, except **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:** Usually, the *Receive* action is 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 617 and Example regular expressions on page 619.

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 *Regular Expression* is **not selected** for the setting, enter an asterisk (`*`) in the pattern field.
- If *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 *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).

See also

Example: Access control rules with wild cards

Example: Access control rules with regular expressions

Controlling SMTP access and delivery

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 pattern	*
Authentication status	Authenticated
TLS profile	tlsprofile1
Action	Relay

See also

Configuring access control receiving policies

Example: Access control rules with regular expressions

Controlling SMTP access and delivery

Using wildcards and regular expressions with access control

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 pattern	Authentication status	Action
1	-/*	-/user932@example.com	0.0.0.0/0	-/*	Any	Reject
2	R/^\s*$	-/*	0.0.0.0/0	-/*	Any	Reject
3	-/*	-/*@example.com	172.20.120.0/24	-/mail.example.org	Any	Relay
4	-/*@example.org	-/*	0.0.0.0/0	-/*	Any	Reject

ID	Sender	Recipient	Source	Reverse DNS pattern	Authentication status	Action
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 ActionThe 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 pattern, 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*.

See also

Configuring access control receiving policies

Example: Access control rules with wild cards

Controlling SMTP access and delivery

Using wildcards and regular expressions with access control

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: • *User Defined*: An email address or wild card pattern that can match multiple email addresses. In the text field below the dropdown list, enter the pattern. 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. • *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 459. • *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 423. **Note**: In the LDAP query string, use `$m` to match sender email addresses. • *Regular Expression*: A regular expression that can match multiple email addresses. In the text field below the dropdown list, enter the regular expression. **Tip:** To verify that the regular expression is valid and only matches the email addresses that you intend, click *Validate* See also Appendix D: Wildcards and regular expressions on page 616 and Using wildcards and regular expressions with access control.
Recipient	Select how you will define the recipient email addresses (`RCPT TO:`) in the SMTP envelope that match the policy. Options are the same as Sender. **Note**: For the *LDAP Group* option, use `$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:

GUI item	Description
	• *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 address, enter `0.0.0.0/0`. • *IP Group*: Select an IP address group. See also Configuring IP groups on page 460.
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 453.
IP pool profile	Select an IP pool profile that FortiMail will use as its source IP address when it delivers email. For details, see Configuring IP pools on page 458.
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 455, Configuring certificate bindings on page 521, and Configuring content action profiles on page 413. **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 293), 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.
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.

See also

What is a policy?

How to use policies

Incoming versus outgoing email

Which policy/profile is applied when an email has multiple recipients?

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. For information about IP pools, see Configuring IP pools on page 458.

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 337.

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*.

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 334.

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 and domains on page 165.

To view the list of IP-based policies, go to *Policy* > *IP Policy* > *IP Policy*.

GUI item	Description
Move (button)	Click a policy to select it, click Move, then select either: • the direction in which to move the selected policy (Up or Down), 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 FortiMail units match the policies in sequence, from the top of the list downwards.
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:** This may be different from the order in which they appear on the page, which indicates order of evaluation. FortiMail units evaluate policies in sequence. More than one policy may be applied. For details, see Order of execution of policies on page 335 and Which policy/profile is applied when an email has multiple recipients? on page 336
Source	Displays the IP address, IP group, GeoIP, or Internet Service Database (ISDB) entry of the SMTP source to which the policy applies. The ISDB is a comprehensive public IP address database that combines IP address range, IP owner, port number, and IP security credibility. The data comes from the FortiGuard service system. Information is regularly added to this database, for example, geographic location, IP reputation, popularity, DNS, and so on. All this information helps users define Internet security more effectively. You can use the contents of the database as criteria for inclusion or exclusion in a policy.
Reverse DNS pattern	Displays whether a reverse DNS look-up is used for matching.
Destination	Displays the IP address of the destination IP to which the policy applies.
Session	Displays the name of the session profile applied by this policy. To modify the or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring session profiles on page 361.
AntiSpam	Displays the name of the antispam profile applied by this policy. To modify or view the a profile, click its name. The profile appears in a pop-up window. For details, see Configuring antispam profiles on page 377.
AntiVirus	Displays the name of the antivirus profile applied by this policy. To modify the 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 398.
Content	Displays the name of the content profile applied by this policy. To modify the or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring content profiles on page 404.
DLP (if DLP is enabled on GUI)	Displays the name of the DLP profile applied by this policy. To modify the or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring DLP profiles on page 527.
IP Pool	Displays the name of the IP pool profile applied by this policy.

GUI item	Description
	The IP addresses in the IP pool is used as the source IP address for the SMTP sessions matching this policy. The IP pool profile is ignored if the Take precedence over recipient based policy match on page 353 option is disabled. • An IP pool in an IP policy will be used to deliver incoming emails from FortiMail to the protected server. It will also be used to deliver outgoing emails if the sender domain doesn't have a delivery IP pool or, although it has a delivery IP pool, Take precedence over recipient based policy match is enabled in the IP-based policy. • An IP pool (either in an IP policy or domain settings) will be used to deliver emails to the protected domain servers if the mail flow is from internal to internal domains. • When an email message's `MAIL FROM` is empty "<>", normally the email is a NDR or DSN bounced message. FortiMail will check the IP address of the sender device against the IP list of the protected domains. If the sender IP is found in the protected domain IP list, the email flow is considered as from internal to internal and the IP pool will be skipped. FortiMail will also skip the DNS query if servers of the protected domains are configured as host names and MX record.
Authentication (not in server mode)	Displays the name of an authentication profile applied to the IP policy. To modify the profile, click its name. The profile appears in a pop-up window. For details, see Configuring authentication profiles on page 420
Exclusive	Indicates whether or not Take precedence over recipient based policy match on page 353 is enabled in this policy. See Order of execution of policies on page 335 for an explanation of that option. • Green check mark icon: The option is enabled. Recipient-based policies will not be applied if a connection matches this IP-based policy. • Red X icon: The option is disabled. Both the IP-based policy and any applicable recipient-based policies will be applied.

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	Select or clear to 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 460. • GeoIP group. See Configuring GeoIP groups on page 460. • ISDB To match all clients, enter `0.0.0.0/0`.

GUI item	Description
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. • Regular expression. **Tip:** To verify syntax and correct matching, click *Validate*. See also Appendix D: Wildcards and regular expressions on page 616 and Controlling email based on IP addresses on page 348. 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	If the FortiMail unit runs in transparent mode, enter the IP address of the SMTP server to whose connections this policy will apply. • IP address and subnet mask • IP group. See Configuring IP groups on page 460. To match all servers, enter `0.0.0.0/0`. If the FortiMail unit runs in gateway or server mode, the destination will be the FortiMail unit itself. But if you use virtual hosts on the FortiMail unit, you can specify which virtual host (IP/subnet or IP group) the email is destined to. Otherwise, you do not have to specify the destination address. If you use virtual hosts, you must also configure the MX record to direct email to the virtual host IP addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well.
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. Note that this action is for transparent only.
Comment	Enter a comment if necessary. 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 on page 351 is Scan. ***Warning***: If you are configuring an IP-bases 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 on page 351 is Scan.
	AntiVirus	Select the name of an antivirus profile to have this policy apply. This option is applicable only if Action on page 351 is Scan.
	Content	Select the name of a content profile to have this policy apply. This option is applicable only if Action on page 351 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 on page 351 is Scan.
	IP pool	Select the name of an IP pool profile, if any, that this policy will apply. • An IP pool in an IP policy will be used to deliver incoming email from FortiMail to the protected server. It will also be used to deliver outgoing emails if the sender domain doesn't have a delivery IP pool or, although it has a delivery IP pool, Take precedence over recipient based policy match is enabled in the IP-based policy. • An IP pool (either in an IP policy or domain settings) will be used to deliver emails to the protected domain servers if the mail flow is from internal to internal domains. • When an email message's `MAIL FROM` is empty "<>", normally the email is a NDR or DSN bounced message. FortiMail will check the IP address of the sender device against the IP list of the protected domains. If the sender IP is found in the protected domain IP list, the email flow is considered as from internal to internal and the IP pool will be skipped. FortiMail will also skip the DNS query if servers of the protected domains are configured as host names and MX record. This option is applicable only if Action on page 351 is Scan. For details about IP pools, see Configuring IP pools on page 458.
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 419.
	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 359 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 122.
	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 359 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile on page 359. **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 337.
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 334. 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 on page 351 is Scan. **Note:** Enabling this option also causes the FortiMail unit to ignore the option Hide the transparent box on page 286 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* 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 353. 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 334.

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 348.
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.

Before you can configure a recipient policy, you first must have configured:

- at least one protected domain (see Configuring protected domains on page 280)
- 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 297 or Configuring LDAP profiles on page 423)
- at least one PKI user, if you will allow or require email users to access their per-recipient quarantine using PKI authentication (see Configuring PKI authentication on page 304)

About the default system policy

Starting from FortiMail 5.4.0, an inbound and outbound default system-level recipient policy has been added. If enabled, the default system policy will be checked before any other policies. If the email matches the default system policy, no other policies will be checked.

The default system policy provides the following conveniences:

- If many domains will be using identical policies, you can just modify the default system policy for the domains to use.
- When troubleshooting profiles and policies, you can temporarily use the system policy for all domains while disabling other policies, so that you can examine the profiles and policies.

If the system policies are not visible, turn on the *Show system policy* switch.

To view recipient-based policies

Go to *Policy* > *Recipient Policy* > *Inbound* or *Policy* > *Recipient Policy* > *Outbound* to view a list of applicable policies.

GUI item	Description
Move (button)	FortiMail units match the policies for each domain in sequence, from the top of the list downwards. Therefore, you must put the more specific policies on top of the more generic ones. To move a policy in the policy list: **1.** Select a domain. **Note**: If *Domain* is set to *All*, the *Move* button is disabled. When *Domain* is set to a particular domain, *Show system policy* must be disabled in order to move domain policies. **2.** Click a policy to select it. **3.** Click Move, then select either: • the direction in which to move the selected policy (Up or Down), 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.
Domain (dropdown list)	• All: Select to display both system-level and domain-level policies. • System: Select to display system-level policies. • <domain>: Select one domain to display this domain's policies. Use the *Show system policy* switch to display or hide the system-level policies when you view all policies or domain-level policies. If you are a domain administrator, you can only see the domains that are permitted by your administrator profile.
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:** This may be different from the order in which they appear on the page, which indicates order of evaluation. FortiMail units evaluate policies in sequence. More than one policy may be applied. For details, see Order of execution of policies on page 335 and Which policy/profile is applied when an email has multiple recipients? on page 336

GUI item	Description
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 617.
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 617.
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 377.
AntiVirus	Displays the antivirus 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 antivirus profiles, file signatures, and actions on page 398.
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 404.
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 524.
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 418.
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 420 or Configuring LDAP profiles on page 423.

To configure recipient-based policies

1. Go to *Policy* > *Recipient Policy* > *Inbound* or *Policy* > *Recipient Policy* > *Outbound*, either click New to add a policy or double-click a policy to modify it.
   A multisection dialog appears.
2. Select Enable to determine whether or not the policy is in effect.
3. For *Domain*, select either *System* or the domain name that this profile will be used for.
4. Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.
5. Configure the following sections, as applicable:
   - Configuring the sender and recipient patterns on page 357
   - Configuring the profiles section of a recipient policy on page 358
   - Configuring authentication for inbound email on page 358
   - Configuring the advanced settings of inbound policies on page 359

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 617. • *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 address group*: Select an email group from the dropdown list. For details about creating an email group, see Configuring email groups on page 459.

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. • *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 617. • *Email address group*: Select an email group from the dropdown list. For details about creating an email group, see Configuring email groups on page 459.

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 377. **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 398.
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 404.
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 527.
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 418.

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 419.

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 359 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 122.
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 on page 359 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile on page 359. **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 337.

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 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	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 360. For more information on configuring PKI users and what defines a valid certificate, see Configuring PKI authentication on page 304.

GUI item	Description
(Inbound policy only)	
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.

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 361
- Configuring sender reputation options on page 362
- Configuring endpoint reputation options on page 364
- Configuring sender validation options on page 365
- Configuring session settings on page 367
- Configuring unauthenticated session settings on page 369
- Configuring SMTP limit options on page 371
- Configuring error handling options on page 372
- Configuring header manipulation options on page 373
- Configuring list options on page 373
- Configuring advanced MTA control settings on page 374

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 361.

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 if needed. 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 • the 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 Hide the transparent box on page 286.
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 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 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" on page 259, 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 361.

You can also view the sender reputation statuses by going to *Monitor* > *Sender Reputation*. See Viewing sender reputation statuses on page 137.

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. 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.

GUI item	Description
	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 379.
	• *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:
	`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 361.

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 on page 501.

   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 362.
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.
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 on page 504.
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

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 361.

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 Sender Validation. Configure the settings to confirm sender and message.
   DomainKeys validation is a predecessor of DKIM and works in the same way. Because some domains still use DomainKeys validation, it is provided for backward compatibility.

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. Validation results are used to adjust the sender reputation scores, MSISDN reputation scores, and deep header scans.

Enabling sender validation can improve performance by rejecting invalid senders before more resource-intensive antispam scans are performed.

4. Configure the following:

GUI item	Description
SPF check	If the sender domain DNS record lists SPF authorized IP addresses, use SPF check to compare the client IP address to the IP addresses of authorized senders in the DNS record (RFC 4408). An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score. If the DNS record for the domain name of the sender does not publish SPF information, the FortiMail unit omits the SPF client IP address validation. **Note:** No SPF check is performed for direct connections from RFC 1918 private IP addresses. **Note:** If you select to *Bypass* SPF checking in the session profile, SPF checking will be bypassed even though you enable it in the antispam profile. **Note:** Before FortiMail 4.3.1 release, only SPF hardfailed (-all) email is treated as spam. Starting from 4.3.2 to 6.0.2 release, you can use a CLI command (`set spf-checking {strict | aggressive}` under `config antispam settings`) to control if the SPF softfailed (~all) email should also be treated as spam. For details, see the FortiMail CLI Guide. Starting from 6.0.3, this command is removed.
Enable DKIM check	If a DKIM signature is present (RFC 4871), enable this to query the DNS server that hosts the DNS record for the sender's domain name to retrieve its public key to decrypt and verify the DKIM signature. An invalid signature increases the client sender reputation score and affects the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DKIM information or the message is not signed, the FortiMail unit omits the DKIM signature validation.
Enable DKIM signing for outgoing message	Enable to sign outgoing email with a DKIM signature. This option requires that you first generate a domain key pair and publish the public key in the DNS record for the domain name of the protected domain. If you do not publish the public key, destination SMTP servers cannot validate your DKIM signature. For details on generating domain key pairs and publishing the public key, see DKIM and ARC Setting on page 291. Before 6.2.0 release, Envelope From domain is used for DKIM signatures. After 6.2.0 release, Header From domain is used instead. If there is no DKIM key for the Header From domain, then the key for the Envelope From domain will be used. ***Note***: Outbound quarantined email messages will not be DKIM signed when they are released.

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	If a DomainKey signature is present, use this option to query the DNS server for the sender's domain name to retrieve its public key to decrypt and verify the DomainKey signature. An invalid signature increases the client sender reputation score and affects the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DomainKey information or the message is not signed, the FortiMail unit omits the DomainKey signature validation.
Bypass bounce verification check	If bounce verification is enabled, enable to omit verification of bounce address tags on incoming bounce messages. This bypass does not omit bounce address tagging of outgoing messages. For more information, see Configuring bounce verification and tagging on page 497.
Sender address verification with LDAP	Enable to verify sender email addresses on an LDAP server. Also select an LDAP profile from the dropdown list. Or click *New* to create a new one. For details about LDAP profiles, see Configuring LDAP profiles on page 423.

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 361.

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 413.
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 italics: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT` ***`EHLO ^^&^&^#$`***

GUI item	Description
	`501 5.0.0 Invalid domain name` Valid characters for domain names include: • alphanumerics (A to Z and 0 to 9) • 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	Enable to return SMTP reply code 503, and to reject a SMTP command, if the client or server uses SMTP commands that are syntactically incorrect. `EHLO` or `HELO`, `MAIL FROM:`, `RCPT TO:` (can be multiple), and `DATA` commands must be in that order. `AUTH`, `STARTTLS`, `RSET`, or `NOOP` commands can arrive at any time. Other commands, or commands in an unacceptable order, return a syntax error. The following example shows invalid command in bold italics: `220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:41:15 GMT`

GUI item	Description
	EHLO example.com 250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you RCPT TO:<user1@example.com> 503 5.0.0 Need MAIL before RCPT
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 361.

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 Unauthenticated Session Setting.
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** The following example shows the invalid command in bold italics: 220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 20 Nov 2013 10:42:07 -0500 ehlo abc.qq 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

GUI item	Description
	250-DELIVERBY 250 HELP mail from:aaa@333 550 5.5.0 Invalid EHLO/HELO domain. quit 221 2.0.0 FortiMail-400.localdomain closing connection Connection closed by foreign host.
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. 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 italics: 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.

GUI item	Description
	This option is effective only if you have enabled Use client-specified SMTP server to send email on page 203 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 on page 188), 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 MS365 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 361.

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 333), 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

GUI item	Description
	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.
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 `RSET`s.

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 361.

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 client	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.

GUI item	Description
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 361.

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 295.
Custom	Enable to remove other headers that have been inserted by other MTAs (not this FortiMail), then click Edit to configure which headers should be removed.
Header inserted by this unit	Enable to remove the headers that are inserted by this FortiMail unit, except `DKIM-Signature:`. **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 361.

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 sue 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 of block lists and safe lists on page 482.

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 320.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans, including SPF validation.

4. Configure the following:

GUI item	Description
Enable sender safe list checking	Enable to check the sender addresses in the email envelope (`MAIL FROM:`), email 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 email envelope (`MAIL FROM:`), email 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 email 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 email 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 361.

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 266.

   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 arrow 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 settings on page 185.
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 375.
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 375.
Mail routing	Select a mail routing profile or click *New* to create one. For details about creating mail routing profiles, see Configuring mail routing profiles in a session profile on page 376.
Access control	Select an access control profile or click *New* to create one. For details, see Configuring access control profiles in a session profile on page 376.
DSN	Select a DNS profile or click *New* to create one. For details, see Configuring DSN profiles in a session profile on page 376.
Remote logging	Select a remote logging profile or click *New* to create one. Note that the remote logging profiles used here are the same as the system-wide remote logging profiles. For details, see Logging to a Syslog server or FortiAnalyzer unit on page 545.

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 374), 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 Configuring address mapping options on page 433.

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 374), 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 Hos*t: Relay to a pre-defined relay host.
6. Enter the SMTP port number. See also Appendix C: Port Numbers on page 611.
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 374), 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 337.
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 374), the *DSN* tab will appear. Configure this setting to overwrite the global setting configured in Configuring mail queue settings on page 185.

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 on page 26.

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 423 and Configuring scan override options on page 434.

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 261.
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 390.
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 and domains on page 165.
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 spam. For each scan in the profile, you can use its *Action* setting to override this default and select a more specific behavior.

GUI item	Description
	See also Configuring antispam action profiles on page 395.

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 385, Banned word section on page 386, and Image spam section on page 388. 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 504.

GUI item	Description
	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.

GUI item		Description
		 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 465.
	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 465.
	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 463.
		 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 488.

Greylisting can improve performance by blocking most spam before it undergoes other resource-intensive antispam scans.

SPF section

If the DNS record lists IP addresses that are authorized to send email for the domain name, then you can enable SPF verification to compare the SMTP client's IP address to that DNS record (RFC 4408). If SPF information does not exist in the DNS record, then IP address validation is omitted.

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.

SPF verifications 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.

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.
None	Select which *Action* to perform if a SPF record does not exist on the DNS server.

If you select *Bypass* in the session profile (see Configuring sender validation options on page 365), then even if you enable SPF in the antispam profile, FortiMail skips SPF.

Before FortiMail 4.3.1 release, only SPF hardfailed (-all) email is treated as spam. Starting from 4.3.2 to 6.0.2 release, you can use a CLI command (`set spf-checking {strict | aggressive}` under `config antispam settings`) to control if the SPF softfailed (~all) email should also be treated as spam. For details, see the FortiMail CLI Reference. Starting from 6.0.3, this command is removed.

DKIM section

DomainKeys Identified Mail (DKIM) utilizes public and private keys to digitally sign outbound emails to prove that email has not been tampered with in transit.

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.
None	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.

FortiMail also verifies DMARC alignment, where at least one of the domains authenticated by SPF or DKIM must align with the sender domain 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.
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.
None	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.

FortiMail combines non-final actions set in the antispam profile with the actions set in the DMARC DNS record policy.

If the antispam profile DMARC actions are non-final, such as *Tag subject* and *Notify*, then they are combined with the actions in the DMARC DNS record policy: none, reject, or quarantine.

This happens when either the FortiMail configuration is either:

```
config antispam settings
   set dmarc-failure-action use-policy-action
```

or, if the policy option in the sender's DMARC record is `p=none`:

```
config antispam settings
   set dmarc-failure-action use-profile-action-with-none
```

You can generate DMARC reports with the following CLI command, from the system level and domain level, respectively:

- `config antispam dmarc-report-generation`
- `config domain-setting`

For more details, see the FortiMail CLI Reference.

ARC section

Authenticated Received Chain (ARC) permits intermediate email servers (such as mailing lists or forwarding services) to sign an email's original authentication results. This allows a receiving service to validate an emal if the email's SPF and DKIM records are rendered invalid by an intermediate server's processing. For more information, see RFC 8617.

If ARC override to SPF, DKIM, and/or DMARC is also enabled, then the ARC result takes precedence over SPF, DKIM, or DMARC results.

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 393.
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 390.
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 392.
Sender alignment	Enable to scan for sender email address and name mismatches.

GUI item	Description
	Sender alignment compares the message header (`From:` (and any others you select in *Apply to*) 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 378.

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 465.

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 379.

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 D: Wildcards and regular expressions on page 616.

You can also apply this scan to PDF attachments. See Scan PDF attachment on page 378.

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 D: Wildcards and regular expressions on page 616.

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 449.) 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.
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 508.

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. 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 480. 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 377, 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 390.
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).

GUI item	Description
	You can only see the domains that are permitted by your administrator profile. See About administrator account permissions and domains on page 165.
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 D: Wildcards and regular expressions on page 616.
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 384.

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 390.
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 and domains on page 165.
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 617.

GUI item	Description
	 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 384.

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 390.
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 and domains on page 165.
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@example1.com and user2@exmaple2.com have regular communication, then their SRR is strong; if user1 and user2 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:` 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 392.
	• *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",

GUI item	Description
	"bank account", "conference attendee", etc. • *Dictionary profile*: Select the dictionary profile. See Configuring dictionary profiles on page 449. • *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 384.

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 390.
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 and domains on page 165.
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. 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.

GUI item	Description
	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.
Archive to account	Enable to send the email to an archiving account. Click *New* to create a new archiving account or click *Edit* to modify an existing account. For details about archiving accounts, see Email archiving workflow on page 528.
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 461 and Customizing email templates on page 212.
Final action	For details about final and non-final actions, see Order of execution on page 26.
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 121. 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 124. 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 461 and Customizing email templates on page 212.
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 126.

GUI item	Description
	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 461 and Customizing email templates on page 212.
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 377.

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 402.

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 and domains on page 165.
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 402.

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 400.
	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 258.
	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.

GUI item	Description
FortiSandbox	Enable this option to send potentially harmful 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 259.
Scan mode	*Submit and wait for result* means to wait for scan results before delivering the email. *Submit only* means to submit the email to FortiSandbox but still deliver the mail without waiting for scan results.
Attachment analysis	Enable to send email attachments to FortiSandbox. If desired, configure different actions for different scan results.
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 398).

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
- .ppsm
- .ppt
- .pptm
- .pptx
- .reg
- .scr
- .sldm
- .swf
- .tar

- .gz
- .hta
- .inf
- .jar
- .js
- .jse
- .msi
- .msp
- .pdf
- .pif
- .potm
- .ppam
- .vbe
- .ws
- .wsc
- .wsf
- .wsh
- .xlam
- .xls
- .xlsm
- .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 465.

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 and domains on page 165.
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:

GUI item	Description
	`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. **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 GUI, custom messages, email templates, and Security Fabric on page 204.
Remove URL detected by FortiSandbox	Removes suspicious URLs from email, as detected by FortiSandbox.
Archive to account	Redirect email to a specified archive account.
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 461 and Customizing email templates on page 212.
Final action	Select one of the following actions:

GUI item	Description

	• *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".
	• *System quarantine*: Enable to redirect email to the system quarantine. For more information, see Managing the system quarantine on page 124.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 126.
	• *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 212.
	• *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 413.
6. Configure the following sections:
   - Configuring attachment scan rules on page 405
   - Configuring scan options on page 406
   - Configuring content disarm and reconstruction (CDR) on page 407
   - Configuring archive handling on page 408
   - Configuring password decryption options on page 409
   - Configuring content monitor and filtering on page 410
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 411.

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 404.

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.

GUI item	Description
File filter	Select the file filter. See Configuring file filters on page 411.
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 404.

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.
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 412.
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 334.

GUI item	Description
	For information on scheduling deferred delivery, see Configuring mail server settings on page 182.
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 267.

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 468.

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 404.

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 413.

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:
	• *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 469.
	  • *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.

GUI item	Description

	• *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 404.

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.

GUI Item	Description
	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 409. 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 404.

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 412.

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 404.

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 449.
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 413.

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 405. 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 D: Wildcards and regular expressions on page 616.

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 404.

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 365).

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 413.
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 406) and archived files (see Configuring archive handling on page 408). To decrypt the documents, you need passwords. See also Configuring password decryption options on page 409.

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 182.
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 182.
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 GUI, custom messages, email templates, and Security Fabric on page 204.
Archive to account	Enable to send the email to an archiving account. As long as this action is enabled, no matter if the email is delivered or rejected, it will still be archived. Click *New* to create a new archiving account or click *Edit* to modify an existing account. For details about archiving accounts, see Email archiving workflow on page 528.

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 461 and Customizing email templates on page 212.
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 121. 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 124. 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 461 and Customizing email templates on page 212.
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 126. 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 461 and Customizing email templates on page 212.
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.
Encrypt with profile	Enable to apply an encryption profile, then select which encryption profile to use. For details, see Configuring encryption profiles on page 455.

GUI item	Description
	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 344.
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 377.

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 377.

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 404), 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 398).

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 297 and Configuring user preferences on page 301.

To view and 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.
   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 the name of the profile. The profile name is editable later.
Disk quota (MB)	Enter the disk space quota in Megabytes for this profile (set the value between 0-60000; default value is 1000). Note that 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:

GUI item	Description
	• *User preference access*: Determine whether users can access user preference options, including idle timeout and ability to automatically check for new messages. • *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 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 is license based, and must be enabled under FortiGuard services. See Configuring email continuity on page 265 for more information. 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.

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 354 and Controlling email based on IP addresses on page 348.

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 337.
2. For secure (SSL/TLS) authentication:
   - Upload a local certificate. For details, see Managing local certificates on page 251.
   - Enable *SMTP over SSL/TLS*. For details, see Configuring mail server settings on page 182.
   - 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 453 and Configuring access control receiving policies on page 337.

- 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 also configure a remote certificate revocation authority. For details, see Configuring PKI authentication on page 304, Managing certificate authority certificates on page 256, and Managing OCSP server certificates on page 257.

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 420)
   - LDAP (see Configuring LDAP profiles on page 423)
   - RADIUS (see Configuring authentication profiles on page 420)
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 297 and Configuring resource profiles on page 418.
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 354 and Controlling email based on IP addresses on page 348.
   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 354.

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 423.

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 419.

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 C: Port Numbers on page 611.
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 435. 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 354, Controlling email based on IP addresses on page 348, and Configuring local user accounts (server mode only) on page 297.

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 C: Port Numbers on page 611.
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 168), 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 354, Controlling email based on IP addresses on page 348, and Configuring local user accounts (server mode only) on page 297.

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 438.

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*.
Comment	Displays the comment in the profile.
Name	Displays the name of 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 Options* is enabled.
Auth	Indicates whether *User Authentication Options* is enabled.
Alias	Indicates whether *User Alias Options* is enabled.
Routing	Indicates whether *Mail Routing Options* is enabled.
Address Map	Indicates whether *Address Mapping Options* 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 Options* 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.
   A dialog appears.
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 C: Port Numbers on page 611.
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 C: Port Numbers on page 611.
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 251. Click *Test LDAP Query* to test the connection. A pop-up window appears. For details, see To verify user query options on page 445. **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: • 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)

GUI item	Description
	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 Options	
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.

4. Configure the following sections:
   - Configuring user query options on page 425
   - Configuring group query options on page 427
   - Configuring user authentication options on page 428
   - Configuring user alias options on page 429
   - Configuring mail routing on page 432
   - Configuring address mapping options on page 433
   - Configuring scan override options on page 434
   - Configuring domain lookup options on page 435
   - Configuring remote access override options on page 436
   - Configuring LDAP chain query on page 437
   - Configuring advanced options on page 437

Configuring user query options

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 423.

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. Click the arrow to expand *User Query Options* section.
4. Configure the query to retrieve the distinguished names (DN) of user objects by their email addresses:

GUI item	Description
Schema	Click *Schema* to 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 426. 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 dereferencing 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	Specify 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 Options* to resolve aliases. For details, see Configuring user alias options on page 429.

Configuring group query options

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 423.

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. Click the arrow to expand *Group Query Options* section.

   For more information on determining user group membership by LDAP query, see Controlling email based on sender and recipient addresses on page 354 or Controlling email based on IP addresses on page 348.
4. Configure the following:

GUI item	Description
Use LDAP tree node as group	Enable to use objects within the Base DN of *User Query Options* 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 Options* as if they were members of such a group.
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.

GUI item	Description
	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. For more information on sending quarantine reports to the group owner, see Quarantine Report Setting on page 289 and Managing the personal quarantines on page 121.
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.

Configuring user authentication options

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 423.

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. Click the arrow to expand the *User Authentication Options* section.
   For more information on authenticating users by LDAP query, see Controlling email based on sender and recipient addresses on page 354.
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`).

GUI item	Description
	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 Options*, 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 Options*.

Configuring user alias options

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 423.

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. Click the arrow to expand the *User Alias Options* 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 425. This option is preconfigured and read-only if, in *User Alias Options*, 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*.

GUI item	Description
	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 431. For more information on required object types and their attributes, see Preparing your LDAP schema for FortiMail LDAP profiles on page 438. 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 425. 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 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.

GUI item	Description
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. • *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.
Use separate bind (configure the following if Default Bind Options on page 425 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 425.

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.

Configuring 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 423.

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. Click the arrow to expand the *Mail Routing Options* section.

The *Mail Routing Options* section query occurs after recipient tagging processing. If you have enabled recipient tagging, the *Mail Routing Options* section 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 Options*.

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.

GUI item	Description
	This attribute must be present in user objects.
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. 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.

Configuring address mapping options

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 423.

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. Click the arrow to expand the *Address Mapping Options* 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.

Configuring scan override options

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 423.

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. Click the arrow to expand the *Scan Override Options* section.

If the *Scan Override Options* 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 440. If enabled, this attribute setting takes precedence over the generic antispam attribute setting in the domain lookup options (see Configuring domain lookup options on page 435). 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 440. If enabled, this attribute setting takes precedence over the generic antivirus attribute setting in the domain lookup options (see Configuring domain lookup options on page 435). 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 440. If enabled, this attribute setting takes precedence over the generic content attribute setting in the domain lookup options (see Configuring domain lookup options on page 435). If you enable this option but leave the attribute field blank, the content profile in the matched recipient-based policy will be used.

Configuring domain lookup options

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 423.

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 you set the Relay Type to other methods, the following settings will not apply.

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 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. Click the arrow to expand the *Domain Lookup Options* 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 the following: `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.

GUI item	Description
	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. 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.

Configuring remote access override options

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 423.

When you add a FortiMail administrator (see Configuring administrator accounts on page 168), 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 remote 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. Click the arrow to expand the *Remote Access Override Options* 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.

Configuring LDAP chain query

If you use different attributes for similar or same values on different LDAP servers, you may want to query all of the LDAP servers one by one (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 423.

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. Click the arrow to expand the *LDAP Profile Chain.*
4. From the LDAP profile list, select the profile you want to add to the chain and click the plus sign.
5. Repeat the above step to add more profiles.

Configuring advanced options

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 423.

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. Click the arrow to expand the *Advanced Options* 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 with the new information.

GUI item	Description
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. *Active Directory* appears only if Use secure connection is *SSL*.
Password schema	Select your LDAP server's user schema style, either *OpenIdap* 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 284.

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 Options*, 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 Options*, 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 Options*, 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 Options* 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 Options			
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 Options			

Object type	Attribute	Value	Query result
(Objects from *User Query Options*.)	`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 Options*.
(Objects from *User Query Options*.)	`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 Options			
(Objects from *User Query Options*.)	`userPassword`	Any.	Query verifies user identity by binding with the user password for any user defined by *User Query Options*.
User Alias Options			
Email alias object classes such as `nisMailAlias`, or user objects from *User Query Options*, depending on whether your schema resolves email aliases directly or indirectly, respectively. For details, see Base DN on page 425.	`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 425.
User group object classes such as `group` or `groupOfNames`.	`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.

Object type	Attribute	Value	Query result
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 425.			This attribute is required only if aliases resolve to user email addresses indirectly. For details, see Base DN on page 425.
Mail Routing Options			
(Objects from *User Query Options*.)	`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 Options*.
	`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 Options*.
Scan Override Options			
(Objects from *User Query Options*.)	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 Options*.
	No default attribute name.	Varies by schema. May be: • `TRUE`, `YES`, `1`, `ENABLE` or `ENABLED` (on) • `FALSE`, `NO`, `0`,	Query retrieves whether or not to perform **antispam** processing, or which profile to use, for any user defined by *User Query Options*.

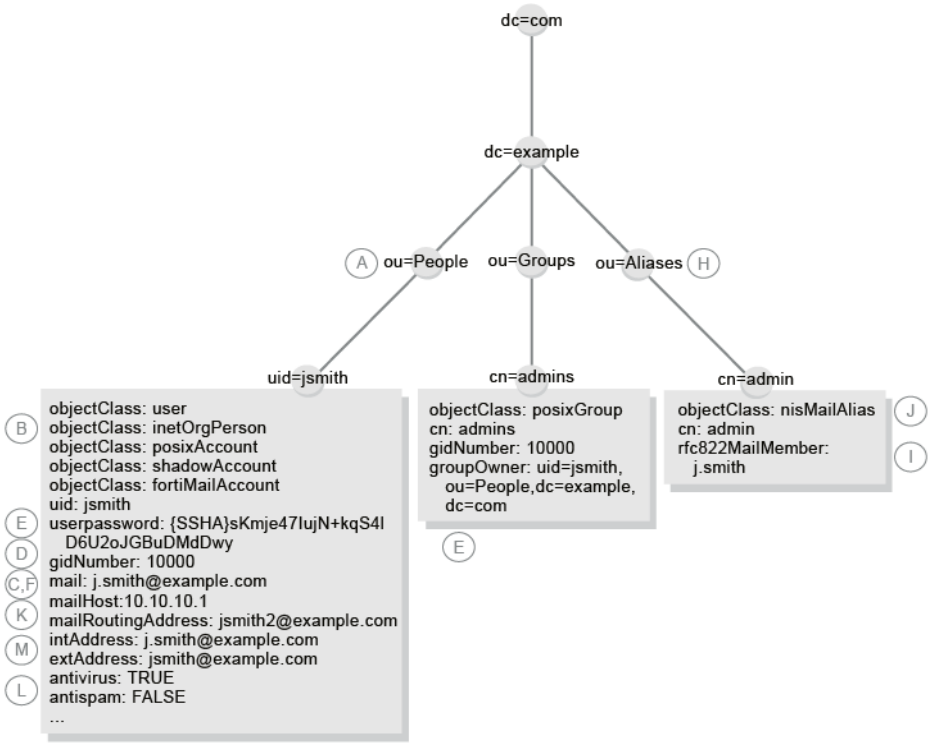
Object type	Attribute	Value	Query result
		`DISABLE`, or `DISABLED`, or any other value not associated with “on” (off) • the name of an antivirus profile	
Address Mapping Options			
(Objects from *User Query Options*.)	No default attribute name.	A user’s **internal** email address.	Query retrieves the user’s **internal** email address
	No default attribute name.	A user’s **external** email address.	Query retrieves the user’s **external** email address.
Enable webmail password change			
(Objects from *User Query Options*.)	`userPassword`	Any.	Query, upon successful bind using the existing password, changes the password for any user defined by *User Query Options*.

Each LDAP profile query filter string may indicate expected value syntax by the FortiMail variables used in the query filter string.

- `$b`: the query filter expects the attribute’s value to be a bind DN
- `$d`: the query filter expects the attribute’s value to be a domain name
- `$f`: the query filter expects the attribute’s value to be a sender domain name
- `$m`: the query filter expects the attribute’s value to be a recipient email address
- `$s`: the query filter expects the attribute’s value to be a sender email address
- `$u`: the query filter expects the attribute’s value to be 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
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.
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 Options* section should be blank. Otherwise, you must enter a valid bind DN and its password.

LDAP Query Failure Message	Meaning and Solution
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 Options*, 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 Options* 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 Options*.
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 Options*, 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 user query options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *User Query Options section* 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 group query options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Group Query Options section* 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 Options* section.
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 group query options group owner

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Group Query Options* 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 Options*.
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 options

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 user query options

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 mail routing options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Mail Routing Options* 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 scan override options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Scan Override Options* (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 address mapping options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *Address Mapping Options* 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 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 Webmail Password Options 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 377 and Configuring content profiles and content action profiles on page 404.

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 516.

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.

GUI item	Description
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 617. 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 388 and Configuring content monitor and filtering on page 410.
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 451, Configuring antispam profiles on page 377, and Configuring content profiles on page 404.

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 449.

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 377 and Configuring content profiles on page 404.

Configuring security profiles

Go to *Profile* > *Security* to create transport layer security (TLS) profiles and encryption profiles.

This section includes:

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 337.

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 on page 256.
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 455.
(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*.
   A dialog appears.
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.

GUI item	Description
	 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.
	Note that the MTA-STS feature may only take effect when enabled under *System* > *Mail Setting* > *Mail Server Settings*, or via the CLI Console:
	`config system mailserver`
	`set smtp-mtasts-status {check-all-domain | check-external-domain | disable}`
	`end`
	For more information, see Configuring SMTP service on page 183

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.
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.  The CA issuer string format must use **no** spaces, and must use slashes "/" to separate the certificate components. For example: /CN=Fortinet/O=Fortinet Ltd. 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 on page 256. Check CA issuer must be enabled for CA issuer to have any effect.

GUI item	Description
	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 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 344 and Configuring content action profiles on page 413.

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 521.

For more information about using S/MIME encryption, see Using S/MIME encryption on page 457.

For more information about using IBE, see Configuring IBE encryption on page 516.

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 344 and Configuring TLS security profiles on page 453.
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.
   A dialog appears.
3. For a new profile, enter the name of the profile in Profile name.
4. In Protocol, select S/MIME or IBE.
   The availability of the following options varies by your selection in Protocol.
5. If you selected IBE as the protocol:

- 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).

6. 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 457 and Configuring certificate bindings on page 521.
7. 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).
8. 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.
9. 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 on page 250.
   - 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 521.
   - create an S/MIME encryption profile. For details, see Configuring encryption profiles on page 455.
   - 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 344), 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 354, Controlling email based on IP addresses on page 348, Configuring content action profiles on page 413, and Configuring content profiles on page 404).

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 on page 250.
   - 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 IP pools

The *Profile* > *IP Pool* > *IP Pool* tab displays the list of IP pool profiles.

IP pools define a range of IP addresses, and can be used in multiple ways:

- To define source IP addresses used by the FortiMail unit if you want **outgoing** email to originate from a range of IP addresses (see IP pool on page 295)
- To define destination addresses used by the FortiMail unit if you want ***incoming*** email to destine to the virtual host on a range of IP addresses (see IP pool on page 295)

Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.

- An IP pool in an IP policy will be used to deliver incoming emails from FortiMail to the protected server. It will also be used to deliver outgoing emails if the sender domain doesn't have a delivery IP pool or, although it has a delivery IP pool, takes precedence over recipient based policy match when enabled in the IP-based policy.
- Since the release of v7.0.1, an IP pool (either in an IP policy or domain settings) will be used to deliver emails to the protected domain servers if the mail flow is from internal to internal domains.
- When an email message's sender email address is empty (`MAIL FROM: <>`), normally the email is a NDR or DSN bounced message. FortiMail will check the IP address of the sender device against the IP list of the protected domains. If the sender IP is found in the protected domain IP list, the email flow is considered as from internal to internal and the IP pool will be skipped. FortiMail will also skip the DNS query if servers of the protected domains are configured as host names and MX record.
- Avoid using large IP pools because whenever an IP pool is referenced, FortiMail will send out gratuitous ARP for each IP address in the IP pool. Too many gratuitous ARP broadcasts may flood the network.

To manage IP pool profiles

1. Go to *Profile* > *IP Pool* > *IP Pool*.
2. Either click New to add a profile or double-click a profile to modify it. The profile name is editable later.
3. Configuring the following:

GUI item	Description
Pool name	Enter a name. The name must contain only alphanumeric characters, hyphens (-) and underscores (_). Spaces are not allowed.
IP Group	Click *New* to create a new IP group, which can be an IP/netmask or IP range. For example, 192.168.1.0/24.
Comment	Optionally enter a descriptive comment.
SMTP Certificate	If you want to bind a certificate to this IP pool profile for TLS purpose, under *SMTP Certificate*, select a certificate and specify if the certificate will be used for mail receiving, delivery, or both. For example, if FortiMail protects several mail servers for several customers, you may want to bind the customer's own certificate to the customer's IP pool.

GUI item	Description
	 When **Certificate** is set to **None**, FortiMail will use the default certificate during the session certificate exchange.
SMTP Session	By default, FortiMail uses its system host name as the greeting name in the SMTP sessions. In some cases, for example, when different IP pools are bound to different domains, you may want to use different host names for different IP pools. To to this, under *SMTP Session*, select *Use other name* and specify the host name to use. This setting is applicable when FortiMail is connecting as a server or a client.

To apply the IP pool, select it when configuring a protected domain (you can use the IP pool for delivering and/or receiving directions) or when configuring an IP-based policy. For details, see IP pool on page 295, and/or IP Pool on page 349.

Configuring email, IP and GeoIP groups

The *Profile* > *Group* tab displays the list of email and IP group and override profiles.

This sections includes:

- Configuring email groups
- Configuring IP groups
- Configuring GeoIP groups
- Configuring GeoIP override

Configuring email groups

Email groups include groups of email addresses that can be used when configuring access control rules and recipient-based policies. For information about access control rules and polices, see Configuring access control receiving policies on page 337 and Controlling email based on sender and recipient addresses on page 354.

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. The profile name is editable.
3. Optionally enter a comment.
4. Select whether this profile will be applied system-wide or to a specific domain.
5. For a new group, enter a name for this email group.
   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. The 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*.

Configuring IP groups

IP groups include groups of IP addresses that can be used when configuring access control rules, IP-based policies, and reports. See also Configuring access control receiving policies on page 337, Controlling email based on IP addresses on page 348, and Configuring report profiles and generating reports on page 550.

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. For a new group, enter a name in *Group name*.
   The name must contain only alphanumeric characters. Spaces are not allowed.
4. Optionally enter a comment.
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.

Configuring GeoIP groups

Starting from 6.2 release, FortiMail utilizes the GeoIP database to map the geolocations of client IP addresses. You can use GeoIP groups in access control rules and IP-based policies to geo-targeting spam and virus devices. For information about access control rules and polices, see Configuring access control receiving policies on page 337 and Controlling email based on IP addresses on page 348.

You can also override geolocation mappings that may not be correct in the GeoIP database. For details, see Configuring GeoIP override.

To configure a GeoIP group

1. Go to *Profile* > *Group* > *GeoIP Group*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new group, enter a name in *Group name*.
   The name must contain only alphanumeric characters. Spaces are not allowed.
4. Optionally enter a comment.
5. If you want to create a group to include all countries and regions, enable this option and click Create. Otherwise, disable this option and move the available countries, regions, or override groups to the member list, and click Create. You can have a maximum of 30 countries and regions in one group.

Configuring GeoIP override

GeoIP service looks up the IP address geographic locations in the GeoIP database. However, in some cases, the lookup might not be accurate, for example, when clients use proxies.

With FortiMail, you can override the GeoIP lookup by manually specifying the geographic locations of some IP addresses and ranges. When you create GeoIP groups (see Configuring GeoIP groups on page 460), you can use the override geographic locations in the groups.

When entering IP addresses for GeoIP overrides, only IPv4 addresses are supported.

To configure a GeoIP override

1. Go to *Profile* > *Group* > *GeoIP Override*.
2. Click *New*.
3. Specify a geographic location name for the client IP addresses.
4. Optionally enter a comment.
5. Click *New* to specify the IPv4 addresses that you want to include in the geographic location.
6. Click *Create*.
   To test a lookup, click *IP Geography Query*.

Configuring notification profiles

When FortiMail takes actions against email messages, you may wan 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 395, Configuring antivirus action profiles on page 402, and Configuring content action profiles on page 413.

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 advanced domain settings on page 293), 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 212.
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 377.

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 465.

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 463.

4. Click *Create*.
5. To apply the URL rating category profile, you can select it in:
   - antispam profiles (see FortiGuard section on page 379)
   - click protection (see Configuring CDR URL click protection and removal options on page 469)
   - FortiSandbox scanning (see Using FortiSandbox antivirus inspection on page 259)

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 467.

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 465.
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 463.

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. 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 616.

GUI item	Description
	• *Regular Expression* — Flexible and full-featured pattern matching. See Syntax on page 617. **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 463)

4. Click *Create*.
   The override is applied to features that use URL filter profiles. See also Configuring URL filter profiles on page 463.

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.

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 610.

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 467.
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 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 256. • *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 400, Configuring custom URL rating categories on page 463, and FortiGuard section on page 379.

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 463.
- **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 400.

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 407) 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 407.

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.

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 463.
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 URLs of images that are stored on remote web servers. 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 on a web server or CDN. Email clients download and display the image later, when each person reads their email. Normal 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 remotely stored images to detect valid recipient addresses even when SMTP recipient verification is disabled, and to bypass email antispam and antivirus scans by transmitting the content over HTTPS instead of SMTP.

GUI item		Description
		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 463.
	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 259).
		• *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 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 apply click handling on 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 463.
	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 apply FortiIsolator on URLs of images that are stored on remote web servers.
URL Removal		

GUI item	Description
Category	Select which URL rating category a URL must match in order to be removed. See Configuring URL filter profiles on page 463.
Include image source attribute	Enable to remove 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 463.
Include image source attribute	Enable to neutralize 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 407.

Configuring authentication reputation

FortiMail comes with an authentication mechanism to block IP addresses if failed login attempts from that IP address reach the threshold.

You can control access to FortiMail by access types:

- **CLI**: access via SSH
- **Mail**: mail access via SMTP(S), IMAP(S), POP3(S)
- **Web**: admin and webmail access via HTTP(S)

The blocking duration is based on the login history of the IP address. The more the IP address has been blocked in the past, the longer the IP address will be blocked. The maximum time an IP address can be blocked is 45 days. For example, if you set the initial block period to 10 minutes, depending on the user's number of violations, the actual maximum block time can be up to two hours. If you set it to 30 minutes, the actual block time can be up to 12 hours. If you set it to more than 70 minutes, the actual block time can be up to 45 days. Therefore, to avoid false positives, it is not recommended to use longer initial block time setting. The recommended setting is less than 30 minutes. The default setting is 10 minutes.

If a user has consecutive successful logins within a period of time, the user's IP address will be automatically added to an auto/dynamic exempt list.

You can also manually exempt IP addresses from failed login attempt tracking and blocking.

To monitor the blocked IP address information, go to *Monitor* > *Reputation* > *Authentication Reputation*. See Viewing authentication reputation statuses on page 140.

To configure authentication reputation settings

1. Go to *Security* > *Authentication Reputation* > *Setting*.
2. Configuring the following:

GUI item	Description
Status	Select *Enable*, *Disable*, or *Monitor only*. *Monitor only* means that failed login attempts will be counted and scored but will not be blocked.
Access Tracking	Enable or disable what types of login access will be tracked: CLI, Mail or Web.
Initial block period	Specify how long the IP address will be blocked after its failed login attempts reach the threshold for the first time. The actual block time will be increased for repeated offenders. See above for more descriptions.

To manually exempt IP addresses from authentication reputation tracking

1. Go to *Security* > *Authentication Reputation* > *Exempt*.
2. Click *New*.
3. Enter the IP address and netmask.
4. Click *Create*.

To manage the auto exempt list

1. Go to *Security* > *Authentication Reputation* > *Auto Exempt*.
2. The exempted IP addresses are displayed.
3. To remove an IP address from the list, select the IP address and click *Delete*.

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 395) and content action profiles (see Configuring content action profiles on page 413).
- Configure the system quarantine administrator account who can manage the system quarantine. See Configuring the system quarantine setting on page 479.
- 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 480.
- 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 473.
- Configure domain-wide quarantine report settings for specific domains. See Quarantine Report Setting on page 289.
- View and manage personal quarantines and system quarantines. See Managing the quarantines on page 120.
- 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 603.

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 395 and Configuring content action profiles on page 413. For general steps about how to use email quarantine, see Configuring email quarantines and quarantine reports on page 472.

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 289.

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 474 and About the HTML formatted quarantine report on page 476.

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 212.
Webmail Access Setting		

GUI item		Description
	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 on page 151. 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 280.
	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 Configuring group query options on page 427. 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 478.

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 GUI, custom messages, email templates, and Security Fabric on page 204.

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: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsIOYjUyM2MjUjRSxVNzoyLA==

Date: Thu, 04 Sep 2008 11:48:50
Subject: [SPAM] Buy now!!!! lowest prices
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsIOYjUyM2NDIjRSxVNToyLA==

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 477)
- contain links to release individual email messages (see Sample HTML quarantine report on page 477)

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 478.

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 474.

The contents of quarantine reports are customizable. For more information, see Customizing GUI, custom messages, email templates, and Security Fabric on page 204.

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
```

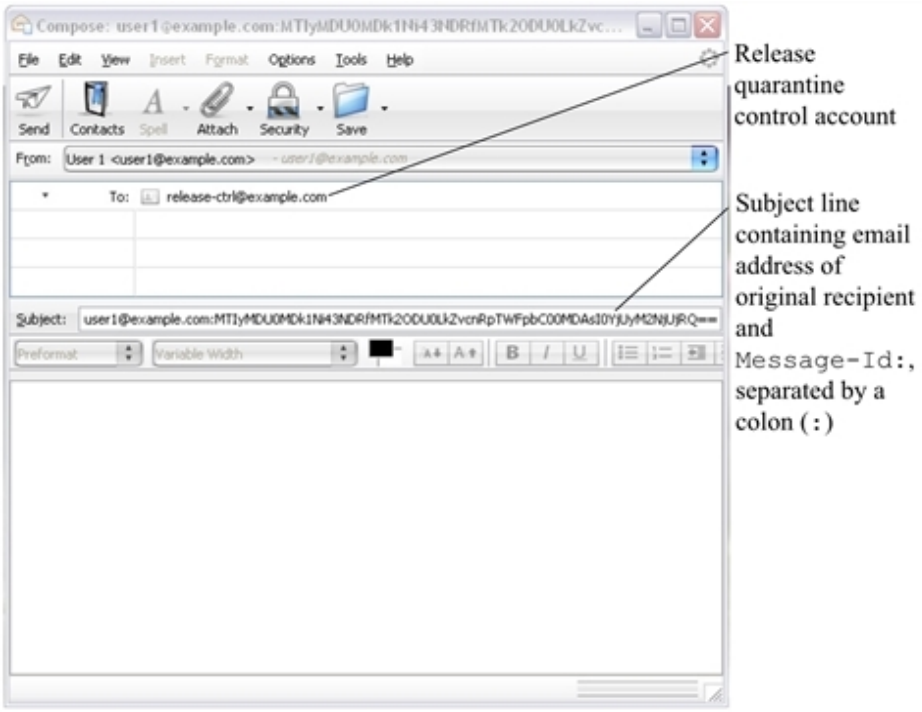
Releasing and deleting email via quarantine reports

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 480.

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 473.

For more information on the differences between plain text and HTML format quarantine reports, see About the plain text formatted quarantine report on page 474 and About the HTML formatted quarantine report on page 476.

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`. The FortiMail unit's host name and local domain name are configured under *System* > *Mail Setting* > *Mail Server Setting*.

For more information on releasing and deleting quarantined items through email, see Releasing and deleting email via quarantine reports on page 478.

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

The *Security* > *Block/Safe List* submenu lets you reject, discard, or allow email messages based on email addresses, domain names, and IP addresses. It also lets you back up and restore the block lists and safe lists.

Multiple types of block lists and safe lists exist: system-wide, per-domain, per-user, and per-session profile. There are several places in the GUI where you can configure these block lists and safe lists.

- For system-wide, per-domain, and per-user block lists and safe lists, go to *Security* > *Block/Safe List*. For details, see Managing the global block and safe list on page 484, Managing the per-domain block lists and safe lists on page 485, and Managing the personal block lists and safe lists on page 487.
- For per-user block lists and safe lists, you can alternatively go to *Domain & User* > *User* > *User Preference*. For details, see Configuring user preferences on page 301.
- For session profile block lists and safe lists, go to *Profile* > *Session* > *Session* and modify the session profile. For details, see Configuring session profiles on page 361.

In addition to FortiMail administrators being able to configure per-user block lists and safe lists, email users can configure their own per-user block list and safe list by going to the Preferences tab in FortiMail webmail. For more information, see the online help for FortiMail webmail.

For more information on order of execution, see Order of execution of block lists and safe lists on page 482.

All block and safe list entries are automatically sorted into alphabetical order, where wildcard characters (* and ?) and numbers sort before letters.

See also

Order of execution of block lists and safe lists

As one of the first steps to detect spam, FortiMail units evaluate whether an email message matches a block list or safe list entry.

Generally, safe lists take precedence over block lists. If the same entry appears in both lists, the entry will be safelisted. Similarly, system-wide lists take precedence over session lists, session lists over per-domain lists, and per-domain lists over per-user lists.

The following table is the sequence in which the FortiMail unit evaluates email for matches with block list and safe list entries. If the FortiMail unit finds a match, it does not look for any additional matches, and cancels any remaining antispam scans of the message (but not the antivirus and content scans).

Block and safe list order of operations

Order	List	Examines	Action taken if match is found
1	System safe list	Sender address, Client IP	Accept message
2	System block list	Sender address, Client IP	Invoke block list action
3	Session recipient safe list	Recipient address	Accept message for matching recipients
4	Session recipient block list	Recipient address	Invoke block list action
5	Session sender safe list	Sender address, Client IP	Accept message for all recipients
6	Session sender block list	Sender address, Client IP	Invoke block list action
7	Domain safe list	Sender address, Client IP	Accept message
8	Domain block list	Sender address, Client IP	Invoke block list action
9	User safe list	Sender address, Client IP	Accept message for this recipient
10	User block list	Sender address, Client IP	Discard message

When the sender email address or domain is examined for a match:

- email addresses and domain names in the list are compared to the sender address in the email envelope (`MAIL FROM:`), email header (`From:`) and (`Reply-to:`)
- IP addresses are compared to the IP address of the SMTP client delivering the email, also known as the last hop address

When the recipient is examined for a match, email addresses and domain names in the list are compared to the recipient address in both the envelop and header. An IP address in a recipient safe or block list is not a valid entry, because IP addresses are not used.

System-wide, per-domain, and per-user block lists and safe lists are executed before any policy match. In contrast, per-session profile block lists and safe lists require that the traffic first match a policy. When configuring a session profile (see Configuring session profiles on page 361), you can create block and safe lists that will be used with the session profile. Session profiles are selected in IP-based policies, and as a result, per-session profile block lists and safe lists are not applied until the traffic matches an IP-based policy.

For information on order of execution relative to other antispam methods, see Order of execution on page 26.

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

Configuring block list settings

Order of execution

About block list and safe list address formats

Since the release of 7.0.0, FortiMail supports three block and safe list entry types:

1. **Email:** Matches email address, supporting wildcard entries. Matches both header from and envelope from.
   Email entries must be entered in the following format:
   "user@example.com"

   Email entries prior to upgrading to 7.0.0 or higher utilize the following format
   "example.com"
   Such entries are automatically updated once FortiMail is upgraded to 7.0.0 or higher, in this example, "*@example.com".

2. **IP/Netmask:** Matches IP/Netmasks, entered in the following format:
   "172.20.0.1/32"

   Prior to 7.0.0, only IP address was supported. Any such entries are automatically updated to those with a netmask, for example "172.20.0.1/32" once FortiMail is upgraded to 7.0.0 or higher.
   Supports CIDR notation.

3. **Reverse DNS:** Enter the hostname/FQDN which will match reverse DNS lookup (PTR) results for connecting client MTA IPs.

Acceptable input for block and safe list entries may vary by the type of the block or safe list, but may be:

- an IP address or subnet (CIDR notation is supported)
- all or part of an email address using wildcards

Domain name portions (for example, example.com) and user name portions (for example, user1) may use wild cards (`?` and `*`).

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 IPs.

The following formats are **not** valid:

- 172.168.1
- example.com
- @spam. example.com

See also

Order of execution of block lists and safe lists

Configuring the block lists and safe lists

Managing the global block and safe list

The *System* tab lets you configure system-wide block and safe lists to block or allow email by sender. It also lets you 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 To configure block list settings on page 488 for more information.

You can alternatively back up all system-wide, per-domain, and per-user block and safe lists together. For details, see Backup and restore on page 267.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans, including SPF validation.

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 view the global block list or safe list, go to *Security* > *Block/Safe List* > *System*. The page displays two links:

- Block List
- Safe List

To add an entry to the system-wide block list or safe list

1. Go to *Security* > *Block/Safe List* > *System*.
2. Do one of the following:
   - 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 483.
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 of block lists and safe lists

About block list and safe list address formats

Backup and restore

Managing the per-domain block lists and safe lists

The Domain tab lets you configure block and safe lists that are specific to a protected domain in order to block or allow email by sender. It also lets you back up and restore the per-domain block lists and safe lists.

You can alternatively back up all system-wide, per-domain, and per-user block lists and safe lists together. For details, see Backup and restore on page 267.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans.

To view and edit per-domain block 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 280.
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 483.

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 of block lists and safe lists

About block list and safe list address formats

Backup and restore

Managing the personal block lists and safe lists

Security > *Block/Safe List* > *Personal* lets you add or modify email users' personal block or safe lists in order to block or allow email by sender. It also lets you back up and restore the per-user block lists and safe lists.

In addition to FortiMail administrators configuring per-user block lists and safe lists, email users can configure their own per-user block list and safe list by going to the Preferences tab in FortiMail webmail. For more information, see the online help for FortiMail webmail.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans.

To view and add to personal 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 box, type the user name of the email user whose per-user block list or safe list you want to modify, and click Enter to search the user.
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 483.
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.

If you add the user's email address to the same user's personal safe list, the FortiMail unit will ignore this entry. This is a precautious measure taken to guard against spammers from sending spam in disguise of that user's email address as the sender address.

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 of block lists and safe lists

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 one of the following actions:
   - *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 377.
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. Additionally, 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 of block lists and safe lists

Configuring greylisting

Go to *Security* > *Greylist* to configure greylisting and to view greylist-exempt senders.

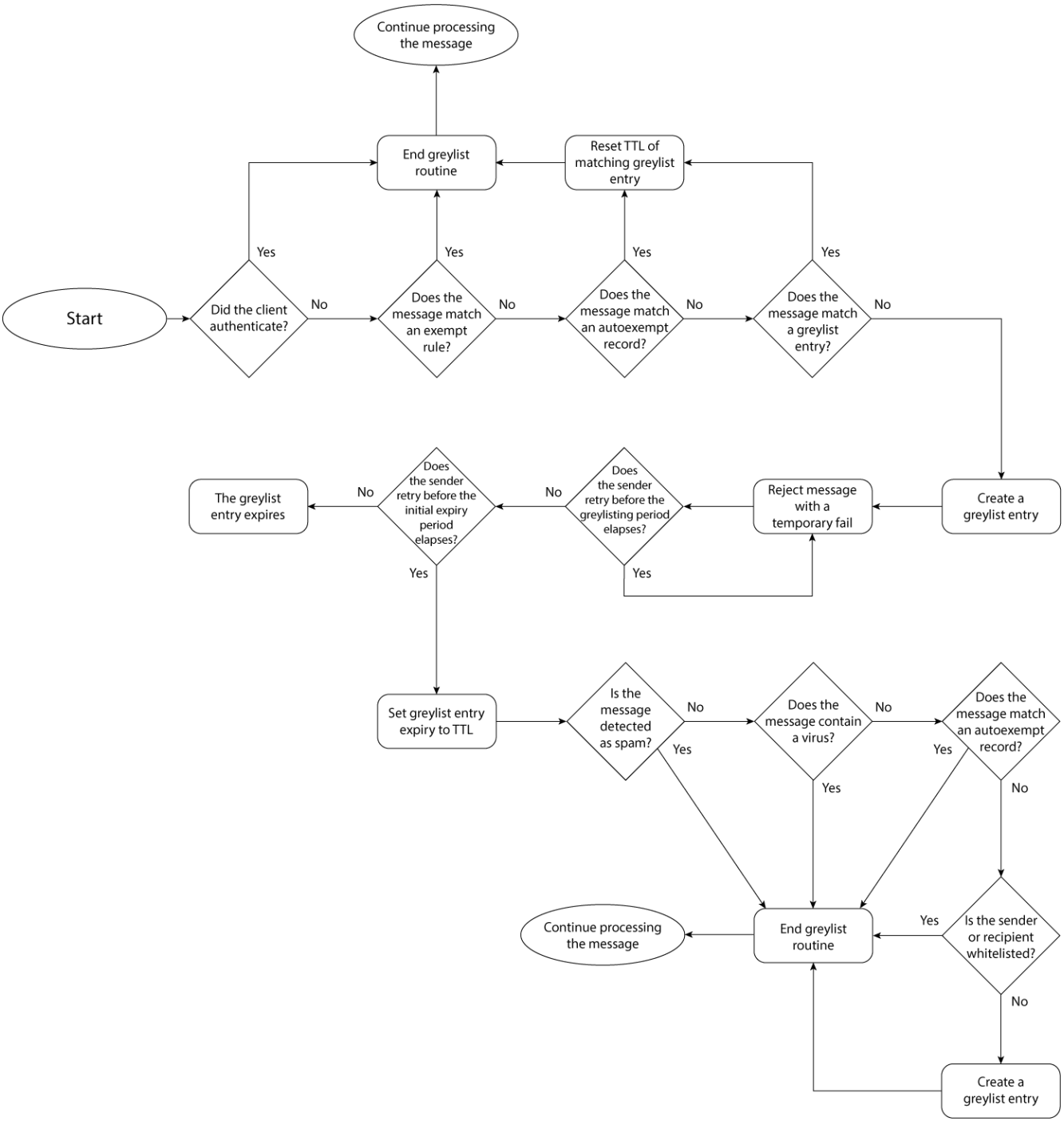
About greylisting

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 on page 26.

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 493)
2. consolidated automatic greylist entries, also known as autoexempt entries (see Automatic greylist entries on page 492)
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 492 and Automatic greylist entries on page 492.

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 134) 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 491. For information on configuring the greylisting delay, window, and entry expiry/TTL, see Configuring the greylist TTL and initial delay on page 493.

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 493.

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 134)
- individual (see Viewing the pending and individual automatic greylist entries on page 134)
- consolidated (see Viewing the consolidated automatic greylist exemptions on page 137)

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 494.

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 489.

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

GUI item	Description
	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 134.
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 134.

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 on page 26.

For more information on the automatic greylisting process, see About greylisting on page 489. For more information on manual greylist entries, see Manual greylist entries on page 493.

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 617. • **-/**: 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 617. • **-/**: 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 617. • **-/**: 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 617.
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 617.
Sender IP/Netmask	Enter the IP address and netmask that defines SMTP clients that match this entry.

GUI item	Description
	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 617.

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 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, the following must be true:

- bounce verification is enabled
- a bounce address key must exist and be activated
- in the protected domain to which the sender belongs, the "Bypass bounce verification" option is disabled (see Configuring protected domains on page 280)
- the recipient domain is not 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 280)
- in the session profile, the Bypass Bounce Verification check option is disabled (see Configuring session profiles on page 361)
- the sender email address (`MAIL FROM:`) in the message envelope is empty
- the DSN sender is not in the verification example 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 as required:

GUI item	Description
Staus	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 280 and Configuring session profiles on page 361.
Tag expiry (days)	Enter the number of days after creation when bounce message keys will expire and their resulting tags will fail verification.
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

GUI item	Description
	you selected in the policy that matches the email message. For more information on actions, see Configuring antispam action profiles on page 395.
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 instance, *.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, so that emails may be forwarded by an MTA if necessary without being rejected by the receiving server which may have a strict SPF policy in place.

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*.

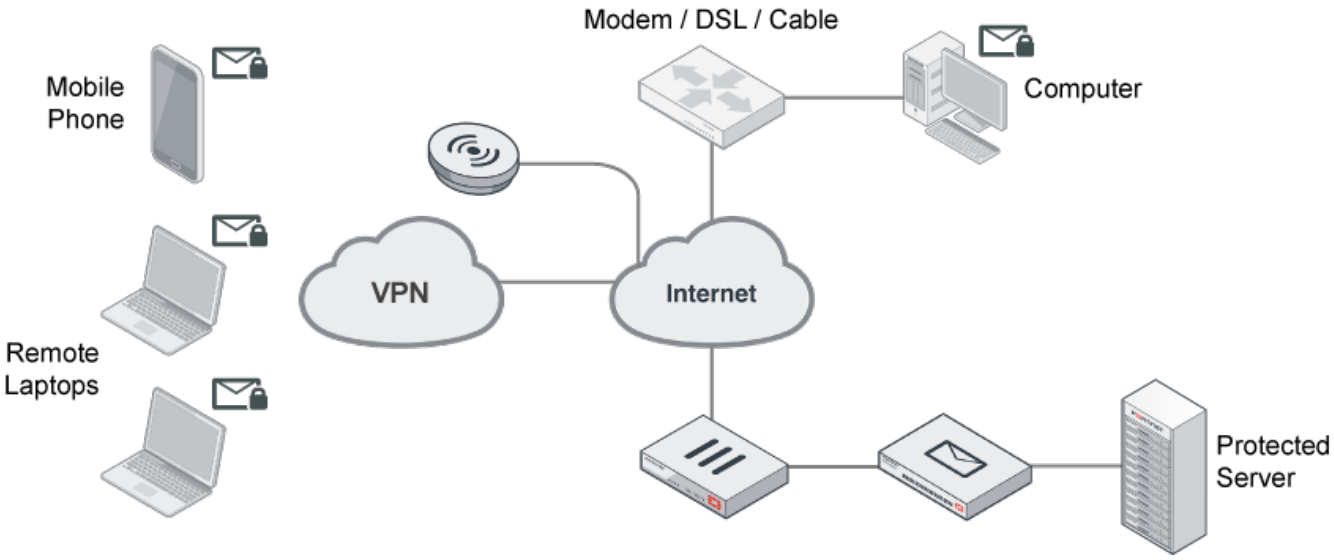
Configuring endpoint reputation

Go to *Security* > *Endpoint Reputation* to manually blocklist carrier end points, to exempt them from automatic blocklisting due to their reputation score, and to view the list of automatically blocklisted carrier end points.

About endpoint reputation

A carrier end point is any device on the periphery of a carrier's or Internet service provider's (ISP) network. It could be, for example, a subscriber's GSM cellular phone, wireless PDA, or computer using DSL service.

Carrier end points



Unlike MTAs, computers in homes and small offices and mobile devices such as laptops and cellular phones that send email may not have a static IP address. Cellular phones' IP addresses especially may change very frequently. After a device leaves the network or changes its IP address, its dynamic IP address may be reused by another device. Because of this, a sender reputation score that is directly associated with an SMTP client's IP address may not function well. A device sending spam could start again with a clean sender reputation score simply by rejoining the network to get another IP address, and an innocent device could be accidentally blocklisted when it receives an IP address that was previously used by a spammer.

To control spam from SMTP clients with dynamic IP addresses, you can use the endpoint reputation score method instead.

The endpoint reputation score method does not directly use the IP address as the SMTP client's unique identifier. Instead, it uses the subscriber ID, login ID, MSISDN, or other identifier (an MSISDN is the number associated with a mobile device, such as a SIM card on a cellular phone network). The IP address is only temporarily associated with this identifier while the device is joined to the network.

When a device joins the network of its service provider, such as a cellular phone carrier or DSL provider, it may use a protocol such as PPPoE or PPPoA which supports authentication. The network access server (NAS) queries the remote authentication dial-in user server (RADIUS) for authentication and access authorization. If successful, the RADIUS server then creates a record which associates the device's MSISDN, subscriber ID, or other identifier with its current IP address.

The server, next acting as a RADIUS client, sends an accounting request with the mapping to the FortiMail unit (the FortiMail unit acts as an auxiliary accounting server if the endpoint reputation daemon is enabled). The FortiMail unit then stores the mappings, and uses them for the endpoint reputation feature.

When the device leaves the network or changes its IP address, the RADIUS server acting as a client requests that the FortiMail unit stop accounting (that is, remove its local record of the IP-to-MSISDN/subscriber ID mapping). The FortiMail unit keeps the reputation score associated with the MSISDN or subscriber ID, which will be re-mapped to the new IP address on the next time that the mobile device joins the network.

The endpoint reputation feature can be used with traditional email, but it can also be used with MMS text messages.

The multimedia messaging service (MMS) protocol transmits graphics, animations, audio, and video between mobile phones. There are eight interfaces defined for the MMS standard, referred to as MM1 through MM8. MM3 uses SMTP to transmit text messages to and from mobile phones. Because it can be used to transmit content, spammers can also use MMS to send spam.

You can blocklist MSISDNs or subscriber IDs to reduce MMS and email spam.

In addition to manually blocklisting or exempting MSISDNs and subscriber IDs, you can configure automatic blocklisting based on endpoint reputation score. If a carrier end point sends email or text messages that the FortiMail unit detects as spam, the endpoint reputation score increases. You can configure session profiles to log or block, for a period of time, email and text messages from carrier end points whose endpoint reputation score exceeds the threshold during the automatic blocklisting window. For information on enabling endpoint reputation scans in session profiles and configuring the score threshold and automatic blocklisting duration, see Configuring session profiles on page 361. For information on configuring the automatic blocklisting window, see Configuring the endpoint reputation score window on page 504.

To use the endpoint reputation feature

1. Enter the following CLI command to start the endpoint reputation daemon:
```
config antispam setting
   set carrier-endpoint-status enable
end
```
2. On the GUI, go to *Security* > *Endpoint Reputation* and configure the settings described in Manually blocklisting endpoints on page 503, Exempting endpoints from endpoint reputation on page 503, and Configuring the endpoint reputation score window on page 504.
3. Go to *Profile* > *Session* > *Session*. Mark the check box of the Enable Endpoint Reputation on page 365 option, then select either Reject or Monitor from Action on page 365. For details, see Configuring session profiles on page 361.
4. Go to *Policy* > *IP Policy* > *IP Policy*. Select the session profile in an IP-based policy. For details, see Controlling email based on IP addresses on page 348.
5. If you enable antispam, antivirus, and history logging, you can go to *Monitor* > *Log* to view endpoint reputation-related log messages. For details, see Configuring logging on page 542 and Viewing log messages on page 113.

Manually blocklisting endpoints

The Blocklist tab lets you manually blocklist carrier end points by subscriber ID, MSISDN, or other identifier.

MSISDN numbers or subscriber IDs listed on the block list will have their email or text messages blocked as long as their identifier appears on the block list.

You can alternatively blocklist subscriber IDs or MSISDNs automatically, based on their reputation score. For more information, see Viewing endpoint reputation statuses on page 140.

To edit a manual carrier endpoint block list

1. Go to *Security* > *Endpoint Reputation* > *Blocklist*.
2. Click New to add an entry (entries cannot be edited, only deleted).
   A single-field dialog appears.
3. In Endpoint ID, type the MSISDN, subscriber ID, or other identifier for the carrier end point that you want to add to the list.
4. Click Create.

Exempting endpoints from endpoint reputation

The Exempt tab lets you manually exempt carrier end points (by MSISDN, subscriber ID, or other identifiers) from automatic blocklisting due to their endpoint reputation score.

To add an exemption

1. Go to *Security* > *Endpoint Reputation* > *Exempt*.
2. Click New to add an entry (entries cannot be edited, only deleted).
   A dialog appears.
3. In Endpoint ID, type the MSISDN, subscriber ID, or other identifier for the carrier end point that you want to exempt.
4. Click Create.

Filtering manual endpoint block list entries

You can filter manual endpoint block list entries on the *Blocklist* and *Exempt* tabs based on the MSISDN, subscriber ID, or other identifier of the sender.

To filter entries

1. Go to *Security* > *Endpoint Reputation* > *Blocklist* or *Security* > *Endpoint Reputation* > *Exempt*.
2. Click the *Search* button.
3. In the *Value* field, enter the identifier of the carrier endpoint, such as the subscriber ID or MSISDN, for the entry or entries that you want to display.
   A blank field matches any value. Use an asterisk (`*`) as a wildcard to match multiple patterns, such as typing `46*` to match 46701123456, 46701123457, and so forth. Regular expressions are not supported.
4. Select *Case Sensitive* if capitalization is part of the search requirement.

5. Under *Operation*, select *Contain* or *Wildcard* to set the search method.
6. Click *Search*.
   The tab appears again showing just entries that match your filter criteria. To remove the filter criteria and display all entries, click the tab to refresh its view.

Configuring the endpoint reputation score window

The Setting tab lets you configure the window size for calculating the reputation score for automatic endpoint reputation-based blocklisting.

In addition to manually blocklisting or exempting carrier end points based on their MSISDNs or subscriber IDs, you can configure automatic blocklisting based on endpoint reputation score. If an MSISDN or subscriber ID sends email or text messages that the FortiMail unit detects as spam or infected, the endpoint reputation score increases. You can configure session profiles to log or block, for a period of time, email and text messages from carrier end points whose reputation score exceeds the threshold during the automatic blocklisting window. For information on enabling endpoint reputation scans in session profiles and configuring the score threshold and automatic blocklisting duration, see Configuring session profiles on page 361.

For more information on the role of the automatic blocklisting window in the endpoint reputation scan, see Configuring endpoint reputation on page 501.

To configure the automatic endpoint blocklisting window

1. Go to *Security* > *Endpoint Reputation* > *Setting*.
2. In *Auto blocklist window size*, enter the number of previous minutes in which events will be used to calculate the current endpoint reputation score.
   For example, if the window of time was 15, detections of spam or viruses within the last 0-15 minutes are counted towards the current score; but, detections of spam or viruses older than 15 minutes would not count towards the current score.
3. Click *Apply*.

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 395, Configuring antivirus action profiles on page 402, and Configuring content action profiles on page 413), you can select an action: • *Deliver to alternate host* • *Deliver to original host* • *System quarantine* • *Personal quarantine* • *Disclaimer insertion*

GUI item	Description
	• *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*, you can choose to insert the disclaimer in selected or all messages. For *Subject tag location*, you can choose to insert the tag at the start or end of the subject line.
Enforce delivery action if 'delivery to original/alternate host' is enabled	If the action in a profile is one of the final actions, such as *System quarantine*, while the action in another profile is to deliver to the original host or alternate host, you can enable this option to override the final action.
Execute attachment scan on spam email under personal quarantine	For spam that is sent to personal quarantine, you can either continue or stop further 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.
AntiSpam	
DMARC failure action	Select either: • *Action profile* — Use the action specified in the antispam profile. • *Action profile with none* — If the policy option in the sender's DMARC record is `p=none`, use that action. Else use the action in the antispam profile. • *DMARC record policy* — Use the actions specified in the `policy` option of the sender's DMARC record.

GUI item	Description
	The default setting is *Action profile with none*. This system-wide setting can be overridden by a per-domain setting. For details, see the FortiMail CLI Reference.
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 DMARC report analysis on page 266 and On-demand DMARC reports on page 278. • *Disable* — Do not collect DMARC check data. Do not generate a report. • *Monitor Only* — Collect DMARC check data, but do not generate a report.
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 `syslocal`. 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 lience is valid. See also DMARC report analysis on page 266.
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 377), 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 377.

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 508.

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 295.

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 295.

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 295.

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 511.
   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 on page 142.

   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 511.
   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 514, Accept training messages from user on page 389, and Training Bayesian databases on page 602.

   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 508.

You can alternatively back up, restore, and reset all Bayesian databases at once. For more information, see Backup and restore on page 267.

Domain administrators cannot access the global Bayesian settings.

For details, see About administrator account permissions and domains on page 165.

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 295.
- 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 512
   - To back up a Bayesian database on page 512
   - To restore a Bayesian database on page 513
   - To reset a Bayesian database on page 513

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 on page 142.

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 512 or Backup and restore on page 267.

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 on page 267.

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 512 or Backup and restore on page 267.

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.

GUI item	Description
"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.

This section contains the following topics:

- About FortiMail IBE
- FortiMail IBE configuration workflow
- Configuring IBE services

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 517 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.

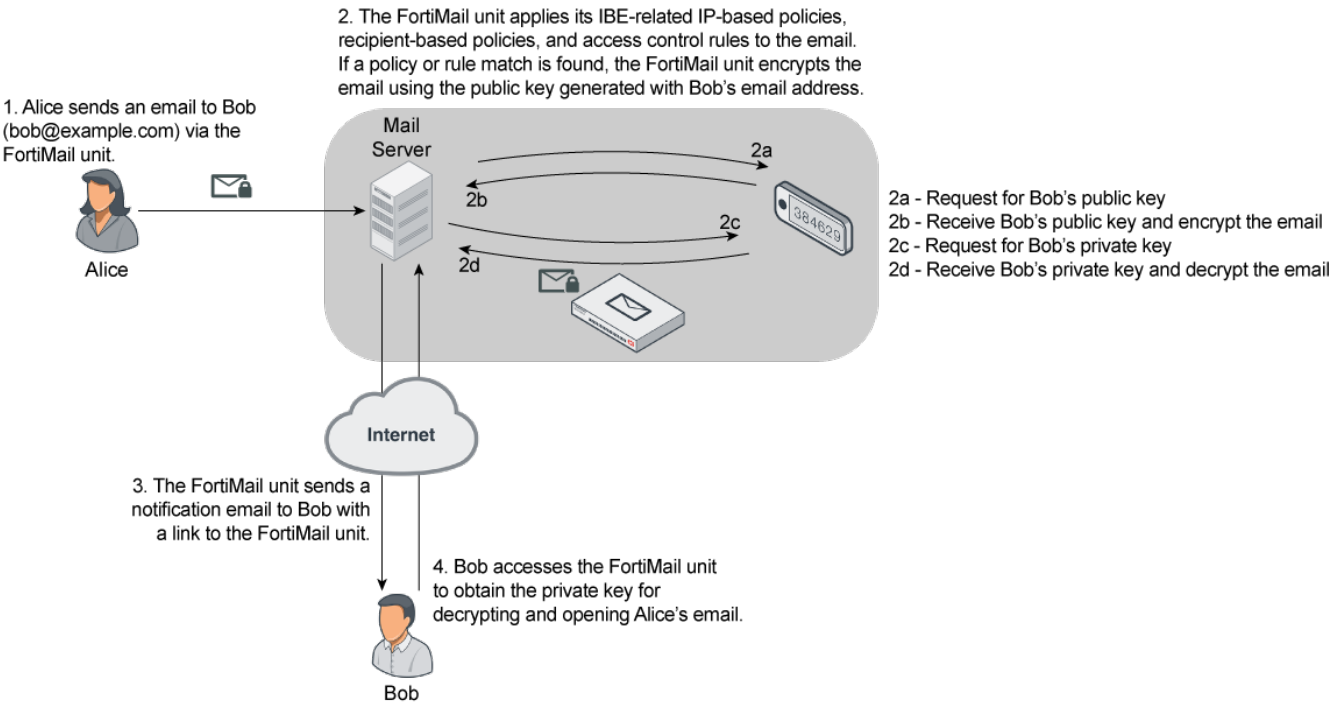
If this is the first time the recipient receives such a notification, the recipient must follow the instructions and links to register on the FortiMail unit before reading email.

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.

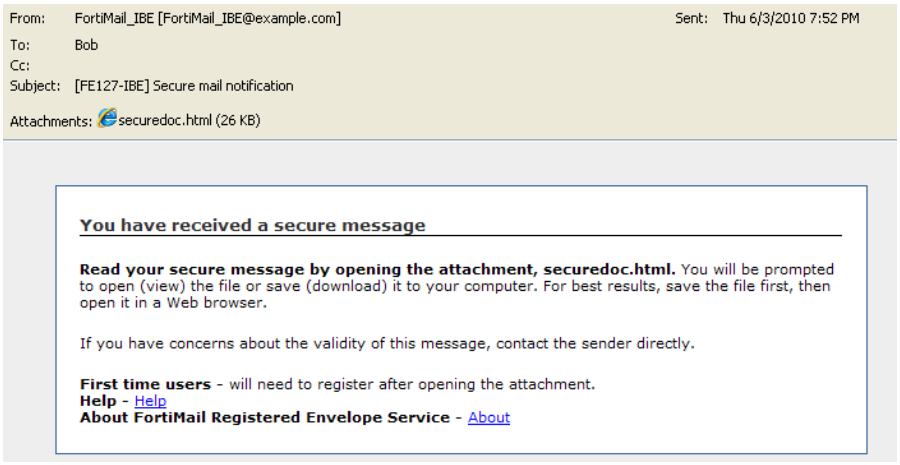
When the recipient opens the mail on the FortiMail unit, the email is decrypted automatically.

Due to more confining security restrictions imposed by the iOS system, email attachments included in IBE PUSH (for details about IBE PUSH and PULL methods, see Configuring encryption profiles on page 455) 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 PCs 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.

See also

About FortiMail IBE

FortiMail IBE configuration workflow

Configuring IBE services

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 519.
- Manage IBE users. See Configuring IBE users on page 315.
- Configure an IBE encryption profile. See Configuring encryption profiles on page 455.

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 413.
- 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 404.
- 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 354, and Controlling email based on IP addresses on page 348.

  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 449)
  - 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 542.
- View logs of IBE encryption. See Viewing log messages on page 113.

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 344.
- Configure IBE email storage.
- Configure log settings for IBE encryption. See Configuring logging on page 542.
- View logs of IBE encryption. See Viewing log messages on page 113.

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.

See also

About FortiMail IBE

Configuring IBE services

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 518.

To configure IBE service

1. Go to *Encryption* > *IBE* > *IBE Encryption*.
2. Configure the following:

GUI item	Description
Enable IBE service	Select to enable the IBE service you configured.
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 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 that 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.

GUI item	Description
	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.
IBE base URL type	IBE base URL is used for IBE users to register or authenticate to access their encrypted email. You can choose to use one of the two types of base URL: • *System*:the system-based URL is the FortiMail unit's IP address or FQDN, for example, https://192.168.100.20 or https://hostname.local_domain.com (as you configured in Configuring mail server settings on page 182). • *Domain*:the domain-based URL is a combination of the FortiMail unit's host name and the protected domains. For example, https://fortimail.protected_domain_a.com and https://fortimail.protected_domain_b.com. This is useful if you have multiple protected domains and want the protected domain IBE users to use different IBE portals. However, if the IBE user is not from the protected domain, the system-based URL will be used.
IBE base URL	For *System* type IBE base URL, you can use the FortiMail FQDN, or enter the FortiMail unit IP address. For *Domain* type IBE base URL, the URL will be dynamically set as the combination of the FortiMail hostname and IBE user's protected domain name, as described above.
"Help" content URL	You can create a help file on how to access the FortiMail secure email and enter the URL for the file. The mail recipient can click the "Help" link from the secure mail notification to view the file. If you leave this field empty, a default help file link will be added to the secure mail notification.
"About" content URL	You can create a file about the FortiMail IBE encryption and enter the URL for the file. The mail recipient can click the "About" link from the secure mail notification to view the file. If you leave this field empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification.
Allow custom user control	If your corporation has its own user authentication tools, enable this option and enter the URL. **"Custom user control" URL**: This is the URL where you can check for user existence. **"Custom forgot password" URL**: This is the URL where users get authenticated.
Authentication Setting	FortiMail supports the customization of IBE authentication settings, supporting two-factor authentication through the use of one-time password (OTP) tokens and passwords. Users may authenticate themselves through either SMS or email. Additionally, authenticated sessions may be time limited, to ensure historical emails are not accessed from the encrypted mailbox. Use this section to define the authentication mode, email and SMS secure token delivery options, and secure token and maximum attempt timeouts and limits. See the User registration process with two-factor authentication on page 318 for more information on the user workflow.
Notification Setting	Under *Account Status Notification*, enable the types of account notifications you wish to 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 212.

GUI item	Description
	Depending on the IBE email access method (either PUSH or PULL) you defined in Configuring encryption profiles on page 455, 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 455) 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 on page 256.

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 251.
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 457, Configuring encryption profiles on page 455, and Configuring delivery rules on page 344. 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
- Defining the sensitive data
- Configuring DLP rules
- Configuring DLP profiles

DLP configuration workflow

DLP is enabled by default on high-end platforms. For performance reasons, it is disabled by default on low-end platforms.

To use the DLP feature

1. Enable the DLP feature using the following hidden command.
```
config system global
   set data-loss-prevention enable
end
```
2. Define the sensitive data first. See Defining the sensitive data on page 524.
3. Define the DLP scan rules which specify the information to be checked in the email traffic. See Configuring DLP rules on page 526.
4. Define DLP profiles, which use one or more rules. See Configuring DLP profiles on page 527. 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 413.
5. Apply the DLP profiles to the IP or recipient based policies. See Controlling email based on sender and recipient addresses on page 354 and Controlling email based on IP addresses on page 348.

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 617.
- **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 525.
- **File filters**: Also used in the content profiles. See Configuring file filters on page 411.

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.
- 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.

To configure a fingerprint document source

1. Go to *Data Loss Prevention* > *Sensitive Data* > *Fingerprint Source*.
2. Click *New* and configure the following:

GUI item	Description
Name	Enter a descriptive name for the document source.
Server type	This refers to the type of server share that is being accessed. The default is SMB/CIFS (Windows Share protocol) but this will also work on Samba shares.
Server address	Enter the IP address of the server.
User name	Enter the user name of the account the FortiMail unit uses to access the server network share.
Password	Enter the password of the account the FortiMail unit uses to access the server network share.
Path	Enter the path to the document folder.
File pattern	You may enter a filename pattern to restrict fingerprinting to only those files that match the pattern. To fingerprint all files, enter an asterisk (“*”).
Checking period	Check the files document source daily if the files are added or changed regularly.
Advanced	
Fingerprint files in subdirectories	By default, only the files in the specified path are fingerprinted. Files in subdirectories are ignored. Select this option to fingerprint files in subdirectories of the specified path.
Remove fingerprints for detected files	Select this option to retain the fingerprints of files deleted from the document source. If this option is disabled, fingerprints for deleted files will be removed when the document source is scanned next time.
Keep previous fingerprints for modified files	Select this option to retain the fingerprints of previous revisions of updated files. If this option is disabled, fingerprints for previous version of files will be deleted when a new fingerprint is generated.

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/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 413). 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 descriptive 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 413.
Comment	Optionally 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.

Archiving email

You can archive email messages according to various criteria and reasons. For example, you may want to archive email sent by certain senders or email contains certain words.

Email archiving workflow

To use the email archiving feature, you must do the following:

1. Create email archive accounts to send archived email to. See Configuring email archiving accounts on page 528. Starting from version 4.2, you can create multiple archive accounts and send different categories of email to different accounts. For the maximum number of archive accounts you can create, see Appendix B: Maximum Values on page 610.
2. Create email archive policies or exemption policies to specify the archiving criteria. See Configuring email archiving policies on page 532 and Configuring email archiving exemptions on page 534. Or, when creating antispam action profiles and content action profiles, choose to archive email as one of the actions. See Configuring antispam profiles and actions on page 377 and Configuring content profiles and content action profiles on page 404.
3. Assign the administrator account access privilege to the email archive. See Configuring administrator accounts and access profiles on page 165.
4. You can search or view the archived email as the FortiMail administrator. See Managing archived email on page 142. You can also access email archives remotely through IMAP. See Configuring email archiving accounts on page 528.
5. If you are archiving the MicroSoft Exchange Journaling email, you must specify the journaling source first. See Archiving email from Microsoft Exchange journaling on page 531.

See also

Configuring email archiving accounts

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring email archiving accounts

Before you can archive email, you need to set up and enable email archiving accounts, as described below. The archived emails will be stored in the archiving accounts. You can create multiple archive accounts and send different categories of email to different accounts. For the maximum number of archive accounts you can create, see Appendix B: Maximum Values on page 610.

When email is archived, you can view and manage the archived email messages. For more information, see Managing archived email on page 142. You can also access the email archive remotely through IMAP.

To enable and configure an email archive account

1. Go to *Email Archiving* > *Archive Account* > *Archive Account*.

GUI item	Description
Status	Select to enable an email archiving account. Clear the check box to disable it.
Account	Lists email archive accounts.
Index Type	Indicates if archive indexing is in use and how much is indexed. Indexing speeds up content searches. The choices are: None: email is not indexed. Header: email headers are indexed. Full: the entire message is indexed.
Storage	Indicates the type of archive storage: Local or Remote.
(Green dot in column heading)	Indicates whether the archive is currently referred to by an archive policy. If so, a red dot appears in this column and the entry cannot be deleted.

2. Click New to create an account or double-click an account to modify it.
   A multisection dialog appears.
3. Configure the following sections, and click Create:
   - Configuring account settings on page 529
   - Configuring rotation settings on page 530
   - Configuring destination settings on page 530

Configuring account settings

The following procedure is part of the email archive account configuration process. For general procedures about how to configure an archive account, see Configuring email archiving accounts on page 528. For information about how to use the email archiving feature, see Email archiving workflow on page 528.

1. Go to *Email Archiving* > *Archive Account* > *Archive Account*.
2. Click *New* to create a new account or double click on an existing account to edit it.
3. For a new account, enter its name.
   This account name holds archived email. You also use this account name as the login user name if you want to access archived email remotely through IMAP. Do not include spaces in the name.
4. In *Password*, enter the password for IMAP access if you want to access archived email remotely.
5. In Forward to, if you require it, enter an email address to which the FortiMail unit will forward a copy when it archives an email.
6. For *Index type*, specify whether you want to index the archived email. Email indexing helps to search the email messages in the archives more quickly. You can choose to index the email headers or the entire email messages.
7. Enable Email archiving status. If the account is not enabled, you cannot select it in other places where it is used.
8. Enable *IMAP access* if you want to access email archives through IMAP access.

Configuring rotation settings

The following procedure is part of the email archive account configuration process. For general procedures about how to configure an archive account, see Configuring email archiving accounts on page 528. For information about how to use the email archiving feature, see Email archiving workflow on page 528.

1. Go to *Email Archiving* > *Archive Account* > *Archive Account*.
2. Click *New* to create a new account or double click on an existing account to edit it.
3. Under *Rotation Setting*, enter the Mailbox rotation size and Mailbox rotation time.
   When the mailbox reaches either the rotation size or time specified, whichever comes first, the email archiving mailbox is automatically renamed. The FortiMail unit generates a new mailbox file, where it continues saving email archives. You can access all rotated mailboxes through search.
4. In Archiving option when disk quota is full, specify what the FortiMail unit should do if it runs out of disk space. Select Overwrite to removes the oldest email archive folder in order to make space for the new archive or select Do not archive to stop archiving more email.
   Whenever an archiving account reaches its disk quota, FortiMail may send an alert email to the administrator, if you enable this feature under *Log and Report* > *Alert Email*. For details, see Configuring alert categories on page 557.

You cannot manually delete specific archived email messages. The only way to delete all of the email archives is to format the mail data disk.

Configuring destination settings

The following procedure is part of the email archive account configuration process. For general procedures about how to configure an archive account, see Configuring email archiving accounts on page 528. For information about how to use the email archiving feature, see Email archiving workflow on page 528.

1. Go to *Email Archiving* > *Archive Account* > *Archive Account*.
2. Click *New* to create a new account or double click on an existing account to edit it.
3. Under *Destination Setting,* select an archiving destination:
   - Local (the FortiMail unit's local hard drive, or a NAS server if you configure a NAS server as the remote storage target.
   - Remote (a remote FTP or SFTP storage server).
4. If Local is the archiving destination, enter the disk space quota in Local disk quota.
   If you are archiving to the local disk, the disk quota for all the archiving accounts cannot exceed 80% of the total mail partition. If this quota is met, or 95% of the total disk space is used, FortiMail will automatically remove the oldest email archive folder in order to make space for the new archive.

   If you are archiving to a NAS server, there is no limit for the local disk quota of all the archiving accounts. But the local quota for a single archive account is limited with the valid range from 1GB to 80% of the total mail partition. The default value is 5GB.

   You can also configure how long the archive folders will be kept. Older folders than the specified retention period will be removed. The valid range is 0 to 3650 days. The default value is 0 day, meaning that no archive folders will be removed.
5. If Remote is the archiving destination, configure the following:

GUI item	Description
Protocol	Select the protocol that the FortiMail unit will use to connect to the remote storage server, either SFTP or FTP.
IP address	Enter the IP address of the remote storage server.
User name	Enter the user name of an account the FortiMail unit will use to access the remote storage server, such as `Fortimail`.
Password	Enter the password for the user name of the account on the remote storage server.
Remote directory	Enter the directory path on the remote storage server where the FortiMail unit will store archived email, such as `/home/fortimail/email-archives`.
Remote cache quota	Enter the FortiMail cache quota that is allowed to be used for remote host archiving. The above statement regarding the local disk quota also applied to the cache quota.

Archiving email from Microsoft Exchange journaling

Microsoft Exchange servers can record("journal") email and then send it to another server, such as FortiMail, for archiving.

For both FortiMail and the Exchange server to communicate, you must configure both sides. The document only describes the FortiMail side of configurations.

To archive the journaled email from an Exchange server

1. Add a journaling source (that is, the Exchange server). See the following procedure.
2. Create an archive account for the journaled email. See Configuring email archiving accounts on page 528.
3. Create an archive policy to specify what email should be archived. See Configuring email archiving policies on page 532.

To add a journaling source

1. Go to *Email Archiving* > *Archive Account* > *Archive Journaling Source*.
2. Click *New* and configuring the following:

GUI item	Description
Status	Enable the journaling source.
Host	Enter the IP address or host name of the Exchange server.
Sender	Enter the archive email sender address. Note that this is not the sender address in the email messages being archived. It is the email account that sends out the journaling email on the Exchange server.
Recipient	Enter the email account that receives journaling email on the FortiMail server. On the Exchange server, you must also specify this receiving account. **Note:** This is not the recipient address in the email messages that you are archiving.
Comments	Optionally enter a comment.

GUI item	Description
Email scanning	Enable to scan the incoming journaled email with the configured recipient-based or IP policies. For details about policies, see Controlling email based on sender and recipient addresses on page 354 and Controlling email based on IP addresses on page 348. Note that without matching policies, enabling this option only will not scan the email.
Email archiving	Enable to archive the email from the journal report.
Email continuity	Enable or disable email continuity, taking email from journal reports to users' mailboxes. When enabled, users can access inbound emails in instances where the email server protected by the FortiMail unit goes offline. **Note:** This command is only available when the FortiMail unit is operating in either gateway or transparent mode.

See also

Email archiving workflow

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring email archiving policies

You do not need to archive all email. Use the Archive Policy tab to specify the types of email to archive. The criteria you specify are called policies. You can also create exemptions to these policies (see Configuring email archiving exemptions on page 534).

To view and configure archiving policy

1. Go to *Email Archiving* > *Policy* > *Archive Policy*.

GUI item	Description
Move (button)	Click a policy to select it, click Move, then select either: • Up or Down, or • After or Before, which opens a dialog, then in Move right after or Move right before indicate the policy's new location by entering the ID of another policy FortiMail units match the policies in sequence, from the top of the list downwards.
Status	To enable an email archiving policy, mark its check box.
ID	Displays policy identification numbers. IDs are generated by the FortiMail unit.
Type	Displays the policy type. The five types are pre-defined. See step In Policy type, qualify what types of email to archive: on page 533.
Account (column)	Displays email archive account names.
Pattern	Displays the pattern that the FortiMail unit will use when evaluating email for a match with the policy.

2. Click New to add an entry or double-click an entry to modify it.
   A dialog appears.
3. From the *Account* dropdown list, select the archive account where you want to archive email. Optionally, click *New* to create an archive account or click *Edit* to edit an existing account. For details about archive accounts, see Configuring email archiving accounts on page 528.
4. In Policy type, qualify what types of email to archive:
   - Sender Address: The FortiMail unit checks the sender email address for the specified pattern. Use an asterisk (`*`) wildcard when specifying a partial address.
   - Recipient Address: The FortiMail unit checks the recipient email address for the specified pattern. Use an asterisk (`*`) when specifying a partial address.
   - Keyword in Subject: The FortiMail unit checks the message subject line for the specified pattern.
   - Keyword in Body: The FortiMail unit checks the message body for the specified pattern.
   - Attachment File Name: The FortiMail unit checks the file names of any message attachments for the specified pattern. Use an asterisk (`*`) wildcard when specifying a partial address.
   - Outbreak Protection: The FortiMail unit checks the deferral reason for outbreak protection. Select from the following deferral reasons:
     - FortiSandbox
     - Spam
     - Virus
5. In Pattern, specify what attributes the messages must have to be archived. Enter a pattern based on the selected policy type. For example, if you select Sender Address and enter `*@example.com` as the pattern, the FortiMail unit archives email from the example.com domain.
6. Enable Policy status.
7. Click Create.

See also

Email archiving workflow

Configuring email archiving accounts

Configuring email archiving exemptions

After setting up email archiving policies, use the *Exempt Policy* tab to prevent the FortiMail unit from archiving certain email.

To view and configure archiving exemptions

1. Go to *Email Archiving* > *Policy* > *Exempt Policy*.

GUI item	Description
Move (button)	Click a policy to select it, click Move, then select either: • Up or Down, or • After or Before, which opens a dialog, then in Move right after or Move right before indicate the policy's new location by entering the ID of another policy FortiMail units match the policies in sequence, from the top of the list downwards.
Status	To enable an email archiving exemption policy, mark its check box.
ID	Displays the identification numbers of the policy. IDs are generated by the FortiMail unit.
Type	Displays the policy type. The three types are pre-defined. See step In Policy type, select one of the following on which to base the exemption: on page 534 of Click New to add an entry or double-click an entry to modify it. on page 534.
Account (column)	Displays the email archive account names.
Pattern	Displays the pattern that the FortiMail unit will use when evaluating email for a match with the policy.

2. Click New to add an entry or double-click an entry to modify it.
   A dialog appears.
3. From the *Account* dropdown list, select the archive account that you want to apply the exemption to. Click *New* to create an archive account or *Edit* to edit an account.
4. In Policy type, select one of the following on which to base the exemption:
   - Sender: The FortiMail unit checks the sender email address for the specified pattern. Use an asterisk (`*`) wildcard when specifying a partial address.
   - Recipient: The FortiMail unit checks the recipient email address for the specified pattern. Use an asterisk (`*`) wildcard when specifying a partial address.
   - Spam Email: The FortiMail unit does not archive email it determines as spam. The spam email includes email detected by antispam profiles and email detected by content profiles which have the "Treat as spam" action enabled.
5. In Pattern, specify what attributes the messages must have to be exempted from the archive. Enter a pattern for the selected policy type, such as `*@example.com`. If you select Spam emails as the policy type, no pattern is required.
6. Enable Policy status.
7. Click Create.

Logs, reports, and alerts

The Log and Report menu lets you configure logging, reports, and alert email.

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 538.

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 542. It can also use log messages as the basis for reports. For more information, see Configuring report profiles and generating reports on page 550.

Accessing FortiMail log messages

There are several ways you can access FortiMail log messages:

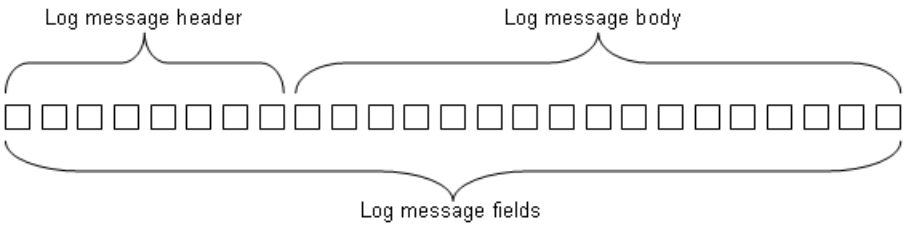
- On the FortiMail GUI, you can view log messages by going to *Monitor* > *Log*. From here you can download log messages to your computer by clicking *Export* and view them later.
- Go to *Log & Report* > *Log Setting* > *Remote* and add a FortiAnalyzer unit as a remote host in order to send log messages 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 539.

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 455.

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 unit stores all log messages equal to or exceeding the severity level you select. For example, if you select Error, the FortiMail unit stores log messages whose severity level is Error, Critical, Alert, or Emergency.

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

Hex Number	Classifier	Hex Number	Classifier
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
0x1F	Access Control List Relay Denied	0x49	DLP Requires Encryption
0x20	Safelist Word	0x4A	Access Control List Safe

Hex Number	Classifier	Hex Number	Classifier
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
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

Hex number	Disposition	Hex Number	Disposition
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* submenu 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 unit to store log messages locally (that is, in RAM or to the hard disk), remotely (that is, on a Syslog server or FortiAnalyzer unit), or the FortiAnalyzer Cloud (license required).

Your choice of storage location may be affected by several factors, including the following:

- Local logging by itself may not satisfy your requirements for off-site log storage.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see Log message severity levels on page 538.

For information on viewing locally stored log messages, see Viewing log messages on page 113.

When the following system resource usages exceed the predefined thresholds, the events will be logged.

- CPU usage: 85%
- Memory usage: 85%
- System load: 85%
- Mail disk usage: 95%
- Log disk usage: 95%

See also

Logging to a Syslog server or FortiAnalyzer unit

Logging to the hard disk

Logging to FortiAnalyzer Cloud on page 548

Logging to the hard disk

You can store log messages locally on the hard disk of the FortiMail unit.

To ensure that local hard disk has sufficient disk space to store new log messages and that it does not overwrite existing logs, you should regularly download backup copies of the oldest log files to your management computer or other storage, and then delete them from the FortiMail unit (alternatively, you could configure logging to a remote host).

You can view and download these logs from the Log submenu of the Monitor tab. For more information, see Viewing log messages on page 113.

For logging accuracy, you should also verify that the FortiMail unit's system time is accurate. For details, see Configuring the time and date on page 171.

To configure logging to the local hard disk

1. Go to *Log & Report* > *Log Setting* > *Local*.
2. Configure the following settings:

Setting	Description
Status	Select to enable logging to this location.
Log file size	Enter the maximum file size of the current log file in megabytes (MB).
Log time **At hour**	Enter the maximum age (in days) of the log file, and the hour of the day (24-hour format) when FortiMail will rotate the current log file. Valid range is from 1 to 365 days. When a log file reaches either the age or file size limit, the FortiMail unit closes the current log file and starts a new one ("rotates"): it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23rd hour of the 10th day (23:00). **Note**: Large log files may decrease display and search performance.

Setting	Description
Log level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For details, see Log message severity levels on page 538. **Caution:** 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.
Log retention period	Enter how long (in days) the logs will be kept. Valid range is 0 to 1461 days. 0 means no limit.
Log options when disk full	Select what you want to do when the log partition of the local disk is almost full, meaning that less than 5 percent of the disk space or 1.5 GB, whichever is smaller, is left. • Do not log: Discard all new log messages. • Overwrite: Delete the oldest log file in order to free disk space, and store the new log messages. Oldest files of all log types will be deleted until 15 percent of the disk space or 22.5 GB, whichever is smaller, is reached.

Logging Policy Configuration	Select which categories of log messages to send to the remote server:
	• *System Event*
	  • *Configuration-Admin*: Configuration changes by an administrator, such as editing policies, profiles, and domains.
	  • *Configuration-User*: Configuration changes by a quarantine or webmail user, such as personal safe/block lists.
	  • *Admin activity*: Administrative events such as logins and viewing log messages.
	  • *System activity*: System events, such as rebooting the FortiMail unit or IP address configuration via DHCP.
	  • *HA*
	  • *Update*: Both successful and unsuccessful attempts to download firmware and FortiGuard updates.
	  • *DNS*
	• *Mail Event*
	  • *Webmail*
	  • *POP3*
	  • *IMAP*
	  • *SMTP*
	• *History*: SMTP relay or proxy events related to mail delivery.
	• *AntiVirus*
	• *AntiSpam*
	• *Encryption*: IBE events. See also Configuring encryption profiles on page 455.

3. Click Apply.

See also

Log message severity levels

Logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely on a Syslog server or a FortiAnalyzer unit. For information about how many remote Syslog servers your FortiMail model can support, see Appendix B: Maximum Values on page 610.

Logs stored remotely cannot be viewed from theFortiMail GUI. If you require this, also enable local storage. For details, see Logging to the hard disk on page 543.

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 the time and date on page 171.

To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log & Report* > *Log Setting* > *Remote*.
2. Click *New* to create a new entry or double-click an existing entry to modify it.
   A dialog appears.
3. Configure the following settings:

Setting	Description
Status	Select to enable logging to this location.
Name	Enter a unique name for this configuration.
Server name/IP	Enter the IPv4, IPv6, or domain name (FQDN) address of the Syslog server or FortiAnalyzer that will store the logs.
Server port	If the remote host is a FortiAnalyzer unit, type `514`. If the remote host is a Syslog server, type the port number on which the Syslog server listens. See also Appendix C: Port Numbers on page 611.
Protocol	Select the protocol used to communicate with the remote log server. • *Syslog*: Any compatible third-party Syslog server or FortiAnalyzer. If the server uses Syslog over TCP or secure transport, also configure *Mode*. • *OFTPS*: FortiAnalyzer only. Also configure *Hash algorithm*.
Mode	Enter the transport layer protocol used for delivering the log to the remote Syslog server: • *TCP*: Slower, but more reliable than UDP: the server asks the FortiMail unit to retransmit if the server did not correctly receive the log message, compliant with RFC 6587 (Transmission of syslog Messages over TCP). **Note:** Requires that the log server supports the octet counting method. • *TCP (legacy)*: TCP, but with legacy options for message delimiters instead of octet counting, compliant with RFC 3195 (Reliable Delivery for

Setting	Description
	Syslog) and, for example, old versions of Kiwi Syslog Server. • *TCP over TLS*: TCP, but more secure: data in the channel is encrypted during transit using TLS, compliant with RFC 5427 (Transport Layer Security Transport Mapping for Syslog). FortiMail requires that the server present a valid certificate to identify itself, and the server may also require that FortiMail unit present a valid client certificate to authenticate. Otherwise, the connection fails. Also configure *Local certificate*. • *TCP over TLS (legacy)*: TLS, but with the same legacy options as `tcp-legacy`. • *UDP*: Faster, but less reliable than TCP, and not secure: the server does not confirm if it did not correctly receive the log message, and does not encrypt log messages in transit. This setting is applicable if *Protocol* is *Syslog*. **Caution:** Do not use UDP or TCP without encryption if logs are transmitted through untrusted networks such as the Internet. Sensitive information could be intercepted by unauthorized persons, compromising the security of your network. Use a TLS option instead. For stronger security, you can configure encryption settings. For details, see `config system global` in the FortiMail CLI Reference.
Local certificate	Select which certificate to use in TLS to encrypt the Syslog session to the remote Syslog server. This setting is available if *Mode* is *TCP over TLS* or *TCP over TLS (legacy)*.
Hash algorithm	Select the hash algorithm to use in OFTPS encryption. This setting is available if *Protocol* is *OFTPS*.
Matched session only	Select this option if you want to send only the matched session logs to this storage location. Otherwise, all logs will be sent. This option appears if you enabled advanced MTA control (see Configuring advanced MTA control settings on page 374).
Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For details, see Log message severity levels on page 538.
Facility	Select the facility identifier that the FortiMail unit will use to identify itself when sending log messages. To easily identify log messages from the FortiMail unit when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CSV format	Enable if you want to send log messages in comma-separated value (CSV) format. **Note**: Do not enable this option if the log destination is a FortiAnalyzer unit. FortiAnalyzer units do not support logs in CSV format.
Comment	Enter a descriptive comment.
Logging Policy Configuration	Select which categories of log messages to send to the remote server:

Setting	Description

	• *System Event*
	  • *Configuration-Admin*: Configuration changes by an administrator, such as editing policies, profiles, and domains.
	  • *Configuration-User*: Configuration changes by a quarantine or webmail user, such as personal safe/block lists.
	  • *Admin activity*: Administrative events such as logins and viewing log messages.
	  • *System activity*: System events, such as rebooting the FortiMail unit or IP address configuration via DHCP.
	  • *HA*
	  • *Update*: Both successful and unsuccessful attempts to download firmware and FortiGuard updates.
	  • *DNS*
	• *Mail Event*
	  • *Webmail*
	  • *POP3*
	  • *IMAP*
	  • *SMTP*
	• *History*: SMTP relay or proxy events related to mail delivery.
	• *AntiVirus*
	• *AntiSpam*
	• *Encryption*: IBE events. See also Configuring encryption profiles on page 455.

4. Click *Create*.
5. If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiMail unit was added to the FortiAnalyzer unit's device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the FortiAnalyzer Administration Guide.
6. To verify logging connectivity, from the FortiMail unit, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

   For example, if you have chosen to record event log messages to the remote host if they are more severe than information, you could log in to the GUI or download a backup copy of the FortiMail unit's configuration file in order to trigger an event log message.

   If the remote host does not receive the log messages, verify the FortiMail unit's network interfaces (see Configuring the network interfaces on page 152 and About the management IP on page 151) and static routes (see Configuring static routes on page 161), and the policies on any intermediary firewalls or routers. If ICMP `ECHO (ping)` is enabled on the remote host, you can use the `execute traceroute` command to determine the point where connectivity fails. For details, see the FortiMail CLI Reference.

See also

Log message severity levels

Logging to the hard disk

Logging to FortiAnalyzer Cloud on page 548

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 Logging to the hard disk on page 543.

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 the time and date on page 171.

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 538.
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

Logging to the hard disk

Logging to a Syslog server or FortiAnalyzer unit

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

Emptying the current log file

You can empty the current log file to remove all of the log messages contained in that file, without deleting the log file itself.

This can be useful in cases such as when you want to delete all old log messages from the FortiMail unit's hard disk, because rolled log files can be deleted but the current log file cannot.

Only the current log file can be emptied. Rolled log files cannot be emptied, but may be deleted instead. For more information, see Deleting rotated log files on page 550.

Back up the current log file before emptying the current log file. When emptying the log file, log messages are permanently removed, and cannot be recovered. For instructions on how to download a backup copy of the current log file, see Downloading log files on page 548.

To empty the current log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as *History*.
3. In the row corresponding to the current log file, click *Empty Log*.
   A confirmation dialog appears, such as:
   ```
   Are you sure you want to delete: alog?
   ```
4. Click *OK*.

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.

Only rolled log files can be deleted. Current log files cannot be deleted, but may be emptied instead. For more information, see Emptying the current log file on page 549.

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 548.

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, such as:

   ```
   Are you sure you want to delete: 2008-06-16-14:45:15_2007-10-16-22:52:20.alog?
   ```
4. Click *OK*.

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:

   ```
   Are you sure you want to delete: selected log files?
   ```
6. Click *OK*.

See also

Viewing log messages

Configuring logging

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 542.

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 266.
   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 144.

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 144.
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 552.
   - Schedule on page 553.
   - Recipient Domain and Sender Domain on page 553.
   - Conditions on page 554.
   - Email Notification on page 554
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*).

GUI item	Description
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*.
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

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*.

To configure the report profile

1. Purchase the feature license and enable the feature. See Mailbox accounting service on page 266.

   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 144.
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 555
   - Domain on page 555
   - Email Notification on page 556
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 <<.

Configuring alert email

The Alert Email submenu lets you configure the FortiMail unit to notify selected users (including administrators) by email when specific types of events occur and are logged. For example, if you require notification about virus detections, you can have the FortiMail unit send an alert email message whenever the FortiMail unit detects a virus.

To set up alerts, you must configure both the alert email recipients (see Configuring alert recipients on page 556) and which event categories will trigger an alert email message (see Configuring alert categories on page 557).

Alert email messages also require that you supply the FortiMail unit with the IP address of at least one DNS server. The FortiMail unit uses the domain name of the SMTP server to send alert email messages. To resolve this domain name into an IP address, the FortiMail unit must be able to query a DNS server. For information on DNS, see Configuring DNS on page 161.

See also

- Configuring alert recipients
- Configuring alert categories

Configuring alert recipients

Before the FortiMail unit can send alert email messages, you must create a recipient list.

To configure recipients of alert email messages

1. Go to *Log & Report* > *Alert Email* > *Configuration*.

GUI item	Description
Test (button)	Clicking on the button will send a test alert email to all configured recipients in the list.
Alert Email Account	Displays the names of email accounts receiving email alerts.

2. Click New to add the email address of a recipient.

A single-field dialog appears.

3. In Email to, enter a recipient email address.
4. Click Create.
5. Repeat the previous steps to add more users.

See also

Configuring alert email

Configuring alert categories

Configuring alert categories

Before the FortiMail unit can send alert email messages, you must specify which events cause the FortiMail unit to send an alert email message to your list of alert email recipients (see Configuring alert recipients on page 556).

To select events that will trigger an alert email message

1. Go to *Log & Report* > *Alert Email* > *Category*.
2. Select one or more of the following event categories check boxes:

GUI item	Description
System events	Send an alert email message when an important system event occurs. These include system reboot/reload, firmware upgrade/downgrade, and log disk/mail disk formatting.
Disk is full	Send an alert email message when the hard disk of the FortiMail unit is full.
Remote archiving/NAS failures	Send an alert email message when the remote archiving feature encounters one or more failures. See Configuring email archiving accounts on page 528.
HA events	Send an alert email message when any high availability (HA) event occurs. When a FortiMail unit is operating in HA mode, the subject line of the alert email includes the host name of the cluster member. If you have configured a different host name for each member of the cluster, this lets you identify which FortiMail unit in the HA cluster sent the alert email message. For more information, see About logging, alert email, and SNMP for HA on page 230.
Disk quota of an account is exceeded	Send an alert email message when an email user's account exceeds its quota of hard disk space. This option is available only if the FortiMail unit is in server mode.
Email Archive quota is exceeded	Send an alert email message when any email archiving account reaches its quota of hard disk space. For information about email archiving account quota, see Configuring rotation settings on page 530.

GUI item	Description
Deferred emails	Send an alert email message if the deferred email queue contains greater than this number of email messages. Enter a number between 1 and 10 000 to define the alert threshold, then enter the interval of time between each alert email message that the FortiMail unit will send while the number of email messages in the deferred email queue remains over this limit.
FortiGuard license expiry time	Send an alert email when the FortiGuard license is to expire in the number of days entered. Enter a number between 1 and 100.
Virus events	Send an alert email message when the FortiMail unit detects a virus.

See also

Configuring alert email

Configuring alert recipients

Microsoft 365, Exchange and Google Workspace threat remediation

Microsoft 365, Exchange 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.

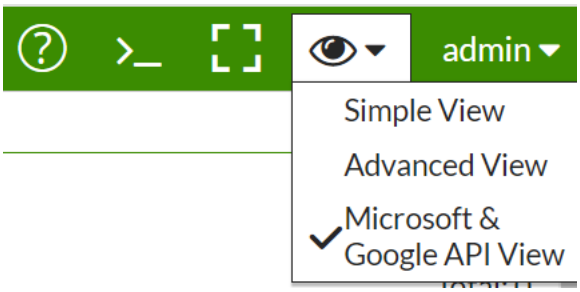
You can also conduct on-demand search and scan of email messages already delivered to the user's inbox. Once scanned, you can decide what to do with the infected or spam email. You can also manually apply actions directly to the email messages you specify.

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:

- A valid CA-signed certificate
- The FortiMail unit must be reachable by hostname (not IP address)

Note that Microsoft and Google API management settings are available from the *View* dropdown menu in the top right corner of the GUI.



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 560.
2. Create antivirus, antispam, content, DLP, and action profiles to be used to scan the email. See Configuring profiles on page 565.
3. Conduct real-time scans or scheduled scans and searches for email according to your criteria. See Configuring scanning policies on page 562.
4. View the history, antivirus, and antispam logs. See Monitoring log messages on page 566.

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

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.

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.

To create a Microsoft 365 account

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 562.
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

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 562.
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*, *Continue*, and then *Done*.
8. Go to *IAM & Admin* > *Service Accounts*. Select *Keys* of the new account. 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 562.
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.

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 unit, 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 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
Enable	Enter a descriptive name.
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, entering the type's settings as required.
Recipient	Define the recipient type, entering 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.

4. Click *Create*.
   For full configuration and procedural details, see Real-time scanning of Microsoft 365 email in FortiMail.

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.
Mailbox	Select to scan **All** mailboxes, or specify specific mailboxes to scan.
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.
Mailbox	Select to search **All** mailboxes, or specify specific mailboxes to search.
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 565.

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 204.
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 461.
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***: Send a copy to FortiMail system quarantine folder, and move the email message from the user's inbox to the Deleted Items folder on Microsoft 365 or Google Workspace. If desired, the user can view the deleted email by clicking Recover

GUI item	Description
	Deleted Items. • ***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 113.

Managing firmware and configuration

Fortinet periodically releases FortiMail firmware updates to include enhancements and address issues. After you have registered your FortiMail unit, FortiMail firmware is available for download at http://support.fortinet.com/.

Installing new firmware can overwrite antivirus and antispam packages using the versions of the packages that were current at the time that the firmware image was built. To avoid repeat updates, update the firmware **before** updating your FortiGuard Antivirus and FortiGuard Antispam packages.

New firmware can also introduce new features which you must configure for the first time.

If you are upgrading, it is especially important to note that the upgrade process may require a specific path. Very old versions of the firmware may not be supported by the configuration upgrade scripts that are used by the newest firmware. As a result, you may need to upgrade to an intermediate version of the firmware first, **before** upgrading to your intended version. Upgrade paths are described in the Release Notes.

Before upgrading the firmware of the FortiMail unit, for the most current upgrade information, review the Release Notes for the new firmware version.

Release Notes are available from http://support.fortinet.com/ when downloading the firmware image file.

Release Notes may contain late-breaking information that was not available at the time this Administration Guide was prepared.

In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.

Before you can download firmware updates for your FortiMail unit, you must first register your FortiMail unit with Fortinet Technical Support. For details, go to http://support.fortinet.com/ or contact Fortinet Technical Support.

This section includes:

Testing firmware before installing it

You can test a new firmware image by temporarily running it from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiMail unit.

To test a new firmware image

1. Connect your management computer to the FortiMail console port using a RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiMail unit. Requires login as “admin” or an administrator with read and write privileges to the system configuration.
3. Connect port1 of the FortiMail unit directly or to the same subnet as a TFTP server.
4. Copy the new firmware image file to the root directory of the TFTP server.
5. Verify that the TFTP server is currently running, and that the FortiMail unit can reach the TFTP server.
   To use the FortiMail CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where `192.168.1.168` is the IP address of the TFTP server.
6. Enter the following command to restart the FortiMail unit:
   ```
   execute reboot
   ```
7. As the FortiMail units starts, a series of system startup messages are displayed.
   ```
   Press any key to display configuration menu........
   ```
8. Immediately press a key to interrupt the system startup.

You have only three seconds to press a key. If you do not press a key soon enough, the FortiMail unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,I,Q,or H:
```

9. Type `G` to get the firmware image from the TFTP server.
   The following message appears:
   ```
   Enter TFTP server address [192.168.1.168]:
   ```
10. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    ```
    Enter Local Address [192.168.1.188]:
    ```
11. Type a temporary IP address that can be used by the FortiMail unit to connect to the TFTP server.
    The following message appears:
    ```
    Enter File Name [image.out]:
    ```
12. Type the firmware image file name and press Enter.
    The FortiMail unit downloads the firmware image file from the TFTP server and displays a message similar to the following:
    ```
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
    ```
13. Type `R`.
    The FortiMail image is loaded into memory and uses the current configuration, **without** saving the new firmware image to disk.
14. To verify that the new firmware image has been loaded, log in to the CLI and type:
    ```
    get system status
    ```

15. Test the new firmware image.
    - If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure Installing firmware on page 569.
    - If the new firmware image does **not** operate successfully, reboot the FortiMail unit to discard the temporary firmware and resume operation using the existing firmware.

See also

Backup and restore

Installing firmware

Installing firmware

You can use either the GUI or the CLI to upgrade or downgrade the firmware of the FortiMail unit.

Only the super admin accounts with the "super_admin_prof" access profile can perform firmware upgrades/downgrades through the GUI.

Firmware changes are either:

- an upgrade to a newer version
- a downgrade to an earlier version

To determine if you are upgrading or reverting your firmware image, examine the firmware version number. For example, if your current firmware version is `FortiMail-400 3.00,build288,080327`, changing to `FortiMail-400 3.00,build266,071209`, an earlier build number and date, indicates that you are reverting.

Reverting to an earlier version may cause the FortiMail unit to remove parts of the configuration that are not valid for that earlier version. In some cases, you may lose all mail data and configurations.

No matter if you are upgrading or downgrading, it is always a good practice to back up the configuration and mail data.

To install firmware using the GUI

1. Log in to the Fortinet Technical Support web site, https://support.fortinet.com/.
2. Download the firmware image file to your management computer.
3. Log in to the GUI as the super admin.
4. In the advanced mode of the GUI, install firmware in one of two ways:
    - Go to *Dashboard* > *Status*, and in the System Information area, in the Firmware version row, click *Update*. Click Browse to locate the firmware and then click Submit.
    - Go to *System* > *Maintenance* > *Configuration*, under *Restore Firmware*, check *Local PC*, and click *Browse* to locate the firmware. Then click *Restore*.

    Your web browser uploads the firmware file to the FortiMail unit. The FortiMail unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiMail unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiMail unit or restore the configuration file.

5. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all changes.
6. To verify that the firmware was successfully installed, log in to the GUI and go to *Dashboard* > *Status*. Text appearing in the Firmware version row indicates the currently installed firmware version.

To install firmware using the CLI

1. Log in to the Fortinet Technical Support web site, https://support.fortinet.com/.
2. Download the firmware image file to your management computer.
3. Connect your management computer to the FortiMail console port using a RJ-45 to DB-9 serial cable or a null-modem cable.
4. Initiate a connection from your management computer to the CLI of the FortiMail unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
5. Connect port1 of the FortiMail unit directly or to the same subnet as a TFTP server.
6. Copy the new firmware image file to the root directory of the TFTP server.
7. Verify that the TFTP server is currently running, and that the FortiMail unit can reach the TFTP server.
   To use the FortiMail CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where `192.168.1.168` is the IP address of the TFTP server.
8. Enter the following command to download the firmware image from the TFTP server to the FortiMail unit:
   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```
   where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:
   ```
   execute restore image tftp image.out 192.168.1.168
   ```
   One of the following message appears:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
   or:
   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```
9. Type `y`.
   The FortiMail unit downloads the firmware image file from the TFTP server. The FortiMail unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
   If you are downgrading the firmware to a previous version, the FortiMail unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiMail unit or restore the configuration file.
10. If you also use the GUI, clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all tab, button, and other changes.
11. To verify that the firmware was successfully installed, log in to the CLI and type:
    ```
    get system status
    ```
12. If you have downgraded the firmware version, reconnect to the FortiMail unit using its default IP address for port1, 192.168.1.99, and restore the configuration file. For details, see Reconnecting to the FortiMail unit on page 571 and Restoring the configuration on page 572.
    If you have upgraded the firmware version, to verify the conversion of the configuration file, see Verifying the

configuration on page 574. If the upgrade is unsuccessful, you can downgrade the firmware to a previous version.

13. Update the FortiGuard Antivirus definitions.

Installing firmware replaces the current antivirus definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your FortiGuard Antivirus definitions are up-to-date.

See also

System maintenance on page 267

Reconnecting to the FortiMail unit

Restoring the configuration

Verifying the configuration

Reconnecting to the FortiMail unit

After downgrading to a previous firmware version, the FortiMail unit reverts to default settings for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiMail GUI and/or CLI.

Use either of the following procedures if the FortiMail unit has been reset to a default configuration and you need to reconnect to the GUI.

If your FortiMail unit has not been reset to its default configuration, but you cannot connect to the GUI or CLI, you can restore the firmware, resetting the FortiMail unit to its default configuration in order to reconnect using the default network interface IP address. For more information, see Clean installing firmware on page 574.

To reconnect using the LCD panel

This procedure requires a FortiMail model whose hardware includes a front LCD panel.

1. Press Enter to display the Main Menu.
2. Press Enter to display the interface list.
3. Use the up or down arrows to highlight the network interface that is connected to your management computer, and press Enter.
4. Press Enter for IP Address.
5. Use the up and down arrows to increase or decrease each number of each IP address digit. Press Enter to go to the next IP address digit or press Esc to move to the previous digit.
6. After selecting the last IP address digit, press Enter to save the IP address.
7. Repeat steps Press Enter for IP Address. on page 5714 to Reconnecting to the FortiMail unit on page 5716 to enter the netmask address for the network interface.
8. After selecting the last netmask address digit, press Enter to save the netmask address.
9. Press Esc to return to the Main Menu.

The network interface's IP address and netmask is saved. You can now reconnect to either the GUI or CLI through that network interface using. For information on restoring the configuration, see Restoring the configuration on page 572.

To reconnect using the CLI

1. Connect your management computer to the FortiMail console port using a RJ-45 to DB-9 serial cable or a null-modem cable.
2. Start HyperTerminal, enter a name for the connection and click OK.
3. Configure HyperTerminal to connect directly to the communications (COM) port on your computer and click OK.
4. Select the following port settings and click OK:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Press Enter to connect to the FortiMail CLI.
   The login prompt appears.
6. Type `admin` and press Enter twice.
   The following prompt appears:
   ```
   Welcome!
   ```
7. Enter the following command:
   ```
   config system interface
      edit <interface_str>
         set ip <ip&netmask>
   end
   ```
   where:
   - `<interface_str>` is the name of the network interface, such as `port1`
   - `<ip$netmask>` is the IP address/netmask of the network interface, such as 192.168.1.10/24
8. Enter the following command:
   ```
   config system interface
      edit <interface_str>
         set allowaccess {https | http | ssh | snmp | ping | telnet}
   end
   ```
   The network interface's IP address and netmask is saved. You can now reconnect to either the GUI or CLI through that network interface. For information on restoring the configuration, see Restoring the configuration on page 572.

See also

Restoring the configuration

Restoring the configuration

After upgrading or downgrading, you may need to restore a backup copy of the configuration file from your local PC using either the GUI or CLI.

If you have just downgraded or restored the firmware of the FortiMail unit, restoring the configuration file can be used to reconfigure the FortiMail unit from its default settings.

You can also migrate the configuration from one unit to another same or higher model unit, as long as they run the same firmware version.

To restore the configuration file using the GUI

1. Clear your browser's cache. If your browser is currently displaying the GUI, also refresh the page.
2. Log in to the GUI.
3. In the advanced management mode, go to *System* > *Maintenance* > *Configuration*.
4. Click *Restore Configuration* to locate and select the configuration file that you want to restore, then click *Restore*. The FortiMail unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
5. After restoring the configuration file, verify that the settings have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 574.

To restore the configuration file using the CLI

The following procedure restores only the core configuration file, which does not include items such as the Bayesian databases, dictionary database, and other items. To restore backups of those items, use the GUI.

1. Initiate a connection from your management computer to the CLI of the FortiMail unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
2. Connect a network interface of the FortiMail unit directly or to the same subnet as a TFTP server.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Verify that the TFTP server is currently running, and that the FortiMail unit can reach the TFTP server.
   To use the FortiMail CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where `192.168.1.168` is the IP address of the TFTP server.
5. Enter the following command:
   ```
   execute restore config tftp <file_name> <tftp_ipv4>
   ```
   The following message appears:
   ```
   This operation will overwrite the current settings!
        (The current admin password will be preserved.)
        Do you want to continue? (y/n)
   ```
6. Enter `y`.
   The FortiMail unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
7. After restoring the configuration file, verify that the settings have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 574.

See also

Backup and restore

Verifying the configuration

Installing firmware

Clean installing firmware

Verifying the configuration

After installing a new firmware file, you should verify that the configuration has been successfully converted to the format required by the new firmware and that no configuration data has been lost.

In addition to verifying successful conversion, verifying the configuration also provides familiarity with new and changed features.

To verify the configuration upgrade

1. Clear your browser's cache.
2. Log in to the GUI using the `admin` administrator account.
   Other administrator accounts may not have sufficient privileges to completely review the configuration.
3. Review the configuration and compare it with your configuration backup to verify that the configuration has been correctly converted.

See also

System maintenance on page 267

Restoring the configuration

Installing firmware

Clean installing firmware

Clean installing the firmware can be useful if:

- you are unable to connect to the FortiMail unit using the GUI or the CLI
- you want to install firmware **without** preserving any existing configuration
- a firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware).

Unlike upgrading or downgrading firmware, clean installing firmware re-images the boot device, including the signatures that were current at the time that the firmware image file was created. Also, a clean install can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. **A clean install cannot be done through a network connection.**

Back up your configuration before beginning this procedure, if possible. A clean install resets the configuration, including the IP addresses of network interfaces. For information on reconnecting to a FortiMail unit whose network interface configuration has been reset, see Reconnecting to the FortiMail unit on page 571.

If you are reverting to a previous FortiMail version, you might not be able to restore your previous configuration from the backup configuration file.

To clean install the firmware

1. Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.
2. Connect your management computer to the FortiMail console port using a RJ-45 to DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiMail unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Connect port1 of the FortiMail unit directly to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. Verify that the TFTP server is currently running, and that the FortiMail unit can reach the TFTP server.
   To use the FortiMail CLI to verify connectivity, if it is responsive, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where `192.168.1.168` is the IP address of the TFTP server.
7. Enter the following command to restart the FortiMail unit:
   ```
   execute reboot
   ```
   or power off and then power on the FortiMail unit.
8. As the FortiMail units starts, a series of system startup messages are displayed.
   ```
   Press any key to display configuration menu.....
   ```
9. Immediately press a key to interrupt the system startup.

You have only three seconds to press a key. If you do not press a key soon enough, the FortiMail unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,I,Q,or H:
```

10. If the firmware version requires that you first format the boot device before installing firmware, type `F` (format boot device) before continuing.
11. Type `G` to get the firmware image from the TFTP server.
    The following message appears:
    ```
    Enter TFTP server address [192.168.1.168]:
    ```
12. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    ```
    Enter Local Address [192.168.1.188]:
    ```
13. Type a temporary IP address that can be used by the FortiMail unit to connect to the TFTP server.
    The following message appears:
    ```
    Enter File Name [image.out]:
    ```

14. Type the firmware image file name and press Enter.
    The FortiMail unit downloads the firmware image file from the TFTP server and displays a message similar to the following:
    ```
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
    ```
15. Type `D`.
    The FortiMail unit downloads the firmware image file from the TFTP server. The FortiMail unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
    The FortiMail unit reverts the configuration to default values for that version of the firmware.
16. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all tab, button, and other changes.
17. To verify that the firmware was successfully installed, log in to the CLI and type:
    ```
    get system status
    ```
    The firmware version number appears.
18. Either reconfigure the FortiMail unit or restore the configuration file from a backup. For details, see Restoring the configuration on page 572.
19. Update the attack definitions.

Installing firmware replaces the current FortiGuard Antivirus definitions with the definitions included with the firmware release you are installing. After you install new firmware, update the antivirus definitions.

See also

Backup and restore

Restoring the configuration

Installing firmware

Upgrading firmware on HA units

If you are installing or upgrading firmware to a high availability (HA) group, install firmware on the secondary unit/units before installing firmware on the primary unit.

To ensure HA works properly, the primary unit and the secondary units must be running the same firmware build. Therefore, if only the secondary units are upgraded, the primary unit may not be able to detect the secondary units anymore.

Similar to upgrading the firmware of a standalone FortiMail unit, normal email processing is temporarily interrupted while firmware is being installed on the primary unit, but, if the HA group is active-passive, it is **not** interrupted while firmware is being installed on secondary units.

Installing firmware on an active-passive HA group does not necessarily trigger a failover. Before a firmware installation, the primary unit signals the secondary unit that a firmware upgrade is taking place. This causes the HA daemon operating on the secondary unit to pause its monitoring of the primary unit for a short time. When the firmware installation is complete, the primary unit signals the secondary unit to resume HA heartbeat monitoring. If the secondary unit has not received this signal after a few minutes, the secondary unit resumes HA heartbeat monitoring anyway, and, if the primary

unit has failed during the firmware installation, the HA group fails over to the secondary unit, which becomes the new primary unit.

To upgrade firmware on an active-passive HA pair

1. Back up configuration on both the primary and secondary units by going to *System* > *Maintenance* > *Configuration*.
2. Upgrade the firmware on the secondary unit according to the upgrade path specified in the release notes.
   The reboot event of the secondary unit will be logged in the primary unit's HA logs. For details, see Failover scenario 3: System reboot or reload of the secondary unit on page 248.
3. Upgrade the firmware on the primary unit.
   The primary unit will send a command to the secondary unit to wait for the reboot, so that the secondary unit will not take over the primary role during the primary unit's reboot. For details, see Failover scenario 2: System reboot or reload of the primary unit on page 247.

   Optionally, you can manually force a failover to the secondary unit before upgrading the primary unit. But this will cause some unnecessary data synchronization. Therefore, it is recommended to upgrade the primary unit directly during your maintenance window.
4. Verify the traffic flow on the primary unit.

To upgrade firmware on an active-active HA cluster

1. Back up configuration on each unit.
2. Upgrade the firmware on the secondary units one by one according to the upgrade path specified in the release notes.
3. Lastly, upgrade the firmware on the primary unit.
4. Verify the traffic flow on the cluster.

Best practices and fine tuning

This section is a collection of guidelines to ensure the most secure and reliable operation of FortiMail units.

These same guidelines can be found alongside their related setting throughout this Administration Guide. To provide a convenient checklist, these guidelines are also listed here.

This section includes:

General security tuning

The following is a general list of techniques and strategies to improve the security of your FortiMail device.

- Install the FortiMail unit in a secure location, such as a locked room with restricted access. Prohibiting access to the unit will increase the security of the device since unauthorized users can disrupt your entire network through unintentional and intentional interventions
- Always remember to upgrade the firmware to the latest version.
- Do not allow administration access on the external interface and use internal access methods such as IPsec VPN or SSL VPN. If you have to have remote access and cannot use IPsec or SSL VPN, only allow HTTPS and SSH and use secure access methods such as trusted hosts and Two-factor authentication.
- Make sure to establish trusted hosts for administrators to limit what computers an administrator can log in to the unit from. Identifying a trusted house will make the unit only accept the administrator's login from the configured IP address or subnet.
- Change the default administrative port to a non-standard port.
- Register with support services to activate the warranty on your device.
- To avoid the possibility of an administrator walking away from the management computer and leaving it exposed, you can add an automatic idle time-out. If the GUI is not used for a specified amount of time, the unit automatically logs the administrator out.
- Enable automatic clock synchronization to facilitate auditing and consistency between expiry dates used in expiration of certificates and security protocols.
- Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if "p4ssw0rd" is used as a password, it can be cracked. Create a safer password policy that administrators must follow to facilitate a safer connection.
- Set a lockout duration for when an administrator enters an incorrect password a specified number of times, using the CLI command `set admin-lockout-duration` and `set admin-lockout-threshold` under `config system global`.

System security tuning

- Enable administrative access only to the network interfaces (located in *System* > *Network* > *Interface*) through which legitimate FortiMail administrators will connect.
- Restrict administrative access to trusted hosts/networks (located in *System* > *Administrator* > *Administrator*) from which legitimate FortiMail administrators will connect.
- Create additional system- and domain-level administrators with limited permissions for less-demanding management tasks.
- Administrator passwords should be at least six characters long, use both numbers and letters, and be changed regularly. Administrator passwords can be changed by going to *System* > *Administrator* > *Administrator* and selecting the *Edit* icon for the login to be modified.
- If your FortiMail unit has an LCD panel, restrict access to the control buttons and LCD by requiring a personal identification number (PIN, located in *System* > *Configuration* > *Option*).
- Do not increase the administrator idle time-out (located in *System* > *Configuration* > *Option*) from the default of five minutes.
- Verify that the system time and time zone (located in *System* > *Configuration* > *Time*) are correct. Many features, including FortiGuard updates, SSL connections, log timestamps and scheduled reports, rely on a correct system time.

Network topology tuning

The FortiMail unit can be bypassed in a complex network environment if the network is not carefully planned and deployed.

To ensure maximum safety:

- Configure routers and firewalls to send all SMTP traffic to or through the FortiMail unit for scanning.
- If the FortiMail unit will operate in gateway mode, on public DNS servers, modify the MX records for each protected domain to contain only a single MX record entry that refers to the FortiMail unit. Spammers can easily determine the lowest priority mail server (highest preference number in MX record) and deliver spam to it, instead of the FortiMail unit, in an attempt to avoid spam defenses.
- If the FortiMail unit will operate in transparent mode, deploy it directly in front of your protected email servers so that all email can be scanned.
- If the FortiMail unit will operate in transparent mode, do not connect two ports to the same VLAN on a switch or to the same hub. Some Layer 2 switches become unstable when they detect the same media access control (MAC) address originating on more than one switch interface or from more than one VLAN.

High availability (HA) tuning

- Isolate HA interface connections from your overall network. Heartbeat and synchronization packets contain sensitive configuration information and can consume considerable network bandwidth. For an active-passive or a active-active HA group consisting of only two FortiMail units, directly connect the HA interfaces using a crossover cable. For a active-active HA group consisting of more than two FortiMail units, connect the HA interfaces to a switch and do not connect this switch to your overall network.

- Use FortiMail active-passive HA to provide failover protection so that if your primary FortiMail unit fails, the backup FortiMail unit can continue processing email with only a minor interruption to your email traffic.
- Use active-active HA if you want to create a mail server farm for a large organization. You can also install a FortiMail active-active HA group behind a load balancer. The load balancer can balance the mail processing load to all FortiMail units in the active-active HA group, improving mail processing capacity.
- Maintain the HA heartbeat connection between HA members. If HA heartbeat communication is interrupted and no remote services are detected, HA synchronization is disrupted and, for active-passive HA groups, the backup unit will assume that the primary unit has failed and become the new primary unit.
- License all FortiMail units in the HA group for the FortiGuard Antispam and FortiGuard Antivirus services. If you only license the primary unit in an active-passive HA group, after a failover the backup unit cannot connect to the FortiGuard Antispam service. Also, antivirus engine and antivirus definition versions are not synchronized between the primary and backup units.
- Configure HA to synchronize the system mail directory and the user home directory so that no email messages in these directories are lost when a failover occurs.
- Do not synchronize/back up the MTA spool directories. Because the content of the MTA spool directories is very dynamic, synchronizing MTA spool directories between FortiMail units may not be effective and may use a lot of bandwidth. In addition, it is usually not necessary because, if the former primary unit can restart, the MTA spool directories will synchronize after a failover. For details, see Using high availability (HA) on page 223.
- Store mail data on a NAS server while operating an HA group. For example, backing up your NAS server regularly can help prevent loss of FortiMail mail data. Also, if your FortiMail unit experiences a temporary failure you can still access the mail data on the NAS server.
- If you are using a NAS server, disable mail data synchronization. If mail data synchronization is enabled for a FortiMail active-passive HA group that is using a NAS server for remote storage of mail data, both the primary and backup units store the mail data to the NAS server, resulting in duplicate traffic. Disable mail data synchronization to conserve system resources and network bandwidth.
- Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. These alert messages may aid in quick discovery and diagnosis of network problems. SNMP can be configured in *System* > *Configuration* > *SNMP*. Syslog output can be configured in *Log & Report* > *Log Setting* > *Remote*. Email alerts can be configured in *Log & Report* > *Alert Email*.
- If you configure an HA virtual IP in active-passive mode, configure one IP address but both host names in your DNS records.

SMTP connectivity tuning

- Configure a fully qualified domain name (FQDN) that is different than that of your protected email server (gateway mode and transparent mode). The FortiMail unit's domain name will be used by many FortiMail features such as quarantine, spam reports, Bayesian database training, alerts, and DSN email. The FQDN is formed by prepending the host name to the local domain name, both of which are configured in *System* > *Mail Setting* > *Mail Server Settings*.
- Use a different host name for each FortiMail unit when managing multiple FortiMail units of the same model or when configuring an HA cluster. The host name is set in *System* > *Mail Setting* > *Mail Server Settings*.
- If the FortiMail unit is used as an outbound relay (gateway mode and server mode only) or if remote email users will view their per-recipient quarantines, the FortiMail unit's FQDN must be globally DNS-resolvable. External SMTP servers require that A records and reverse DNS records be configured on public DNS servers for both forward and reverse lookup of the FQDN and its IP address.
- Configure the public DNS records for each of your protected domains with only one MX record that routes incoming email through the FortiMail unit (gateway mode). With only one MX record, spammers cannot bypass the FortiMail unit by using lower-priority mail gateways.

- If the FortiMail unit is operating in transparent mode, SMTP clients are configured for authentication, and you have disabled the *Use client-specified SMTP Server to send email* option for SMTP proxies (located in *System* > *Mail Setting* > *Proxies*), you must configure and apply an authentication profile (such as *Profile* > *Authentication*). Without the authentication profile, authentication with the FortiMail unit will fail. Additionally, you must configure an access control rule (located in *Policy* > *Access Control* > *Receiving*) to allow relay to external domains. The SMTP client uses the FortiMail to relay, instead of a protected mail server or an external mail server.

Antispam tuning

- **If the spam catch rate is low, see Troubleshoot antispam issues on page 594 for fine tuning instructions.**
- **Use block and safe lists with caution.** They are simple and efficient tools for fighting spam and enhancing performance. They can also cause false positives and false negatives if not used properly, however. For example, a safe list entry *.edu would allow all mail from the .edu top level domain to bypass the FortiMail unit's antispam scans.
- **Do not safelist protected domains.** Because safe lists bypass antispam scans, email with spoofed sender addresses in the protected domains could bypass antispam features.
- To prevent directory harvest attacks (DHA), use a combination of recipient verification and sender reputation.
  DHA is a common method used by spammers. It utilizes recipient verification in an attempt to determine an email server's valid email addresses so that they can be added to a spam database.

  If *Recipient Address Verification* (accessed through *Domain & User* > *Domain* > *Domain*) is enabled, each recipient address will be verified with the protected email server. For email destined for invalid recipient addresses, the FortiMail unit will return `User Unknown` messages to the SMTP client. However, spammers will utilize this response to guess and learn valid recipient addresses.

  To prevent this, enable *Enable sender reputation* in session profiles (located in *Profile* > *Session* > *Session*). Sender reputation weighs each SMTP client's IP address and assigns them a score. If the SMTP client sends several email messages to unknown recipients, the sender's reputation score is increased significantly. When the sender reputation score exceeds the threshold, the SMTP client's SMTP sessions are terminated at connection level.
- To prevent delivery status notification (DSN) spam, enable bounce verification.
  Spammers may sometimes use the 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 prevent this, enable bounce address tagging and verification (located in *Security* > *Bounce Verification* > *Setting*) and configure it with an active key. In addition, disable both the *Bypass bounce verification* option (located in *Domain & User* > *Domain* > *Domain*) and the *Bypass bounce verification check* option (located in *Profile* > *Session* > *Session*). It is also recommended to select *Use antispam profile settings* for the *Bounce verification action option* (located in *Security* > *Bounce Verification* > *Setting*). Finally, verify that all email, both incoming and outgoing, is routed 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.

Policy tuning

- Disable or delete policies and policy settings with care. Any changes made to policies take effect immediately.
- Arrange policies in the policy list from most specific at the top to more general at the bottom. Policy matches are checked from the top of the list, downward. For example, a very general policy matches all connection attempts. When you create exceptions to a general policy, you must add them to the policy list above the general policy.
- Verify all SMTP traffic has a matching policy. **If traffic does not match a policy, it is allowed**. If you're certain all desired traffic is allowed by existing policies, add an IP policy to the bottom of the IP policy list to reject all remaining connections and thereby tighten security.
  To do this, create a new IP policy. Enter `0.0.0.0/0` as the IP address to match, and select Reject connections with this match. Finally, move this policy to the bottom of the IP policy list. With this policy in place, the FortiMail unit's default behavior of allowing traffic with no policy matches is effectively reversed. Traffic with no other matches will now be denied by this final policy.
- Users can authenticate with the FortiMail unit using SMTP, POP3, IMAP, LDAP, or RADIUS servers. For users to authenticate successfully, you must create and apply an authentication profile (accessed from *Profile* > *LDAP* > *LDAP*, or *Profile* > *Authentication* or *Profile* > *Authentication* > *RADIUS*).
- Addresses specified in an IP-based policy should be as specific as possible. Use subnets or specific IP addresses for more granular control. Use a 32-bit subnet mask (that is, 255.255.255.255) when creating a single host address. The IP setting `0.0.0.0/0` matches all hosts.

System maintenance tips

- Before upgrading or downgrading the firmware, always perform a complete backup, including the configuration file and other related data such as the Bayesian database, dictionary, and block and safe lists.
- Upgrade to the latest available firmware. After downloading the firmware file from Fortinet Technical Support (https://support.fortinet.com/), back up the configuration and other data, then go to *Dashboard* > *Status*, and, in the *Firmware Version* row, select the *Update* link.
- Configure the FortiMail unit to accept scheduled updates of antivirus and attack definitions. FortiGuard updates are configured in *System* > *FortiGuard* > *AntiVirus*.
- Before a FortiMail unit can receive FortiGuard Antivirus and/or FortiGuard Antispam updates, it needs to connect to the FortiGuard Distribution Network (FDN). FDN connection status can be checked in *System* > *FortiGuard* > *Licensed Feature*.
- Allow the FortiMail unit access to a valid DNS server. DNS services are required for many FortiMail features, including scheduled updates and FortiGuard Antispam rating queries. The DNS server used by the FortiMail unit is configured in *System* > *Network* > *DNS*.

Performance tuning

- Configure *Recipient Address Verification* (located in *Domain & User* > *Domain* > *Domain*) with an SMTP or LDAP server. This is especially important when quarantining is enabled because of the potentially large amount of quarantined mail for invalid recipients.

Microsoft Exchange server's user verification feature is disabled by default.

Alternatively, enable *Automatic Removal of Invalid Quarantine Accounts* (located in *Domain & User* > *Domain* > *Domain*) to delete invalid user quarantine directories daily at a configured time.

If quarantining is enabled and neither of these features are enabled, performance will suffer and could potentially cause the FortiMail unit to refuse SMTP connections if subject to extremely heavy mail traffic.

- Enable greylisting (located in *Profile* > *AntiSpam* > *AntiSpam*) to reject many spam delivery attempts before more resource-intensive antispam scans are used to identify spam.
- Apply spam throttling features by creating an IP-based policy (located in *Policy* > *IP Policy* > *IP Policy*) with a session profile (located in *Profile* > *Session* > *Session*). Sender reputation, session limiting, and error handling are particularly useful.
- To reduce latency associated with DNS queries, use a DNS server on your local network.
- If logs are stored on the FortiMail unit, set logging rotation size (located in *Log & Report* > *Log Setting* > *Local*) to between 10 MB and 20 MB, and set the event logging level to warning or greater. Delete or back up old logs regularly to free storage space.
- Regularly delete or backup old reports to reduce the number of reports on the local disk.
- Regularly delete old and unwanted mail queue entries and quarantined mail.
- Schedule resource-intensive and non-time-critical tasks, such as report generation and delivery of deferred oversize messages, to low-traffic periods.
- Disable resource-intensive scans, such as the heuristic scan (located in *Profile* > *AntiSpam* > *AntiSpam*), when spam capture rate is otherwise satisfactory.
- Consider enabling the *Max message size to scan* and *Bypass scan on SMTP authentication* in the *Scan Conditions* section of antispam profiles (located in *Profile* > *AntiSpam* > *AntiSpam*).

Back up logs and mail before formatting the hard disks. Formatting log disks deletes all log entries. Formatting mail disks with the `execute formatmaildisk` CLI command will result in the loss of all locally stored mail; `execute formatmaildisk_backup` will preserve it. These operations require a reboot when complete. For more information, see the FortiMail CLI Reference.

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 on page 578.

This section contains the following topics:

Establish a system baseline

Before you can clearly define an abnormal operation, you need to know what the normal operating status is. You can create a repository of this baseline information by keeping logs, and by regularly running information gathering commands and saving the output. When there is a problem, this regular operation data helps you determine what has changed.

It is a good idea to back up the FortiMail unit's configuration regularly. If you accidently change something, the backup can help you restore normal operation quickly and easily. Backups also can aid in troubleshooting.

Define the problem

Before you can solve a problem, you need to understand it. Often this step can be the longest in this process. Before starting to troubleshoot a problem, answer these questions:

- Where and when did the problem occur?
- Has it ever worked before?
  If the unit never worked properly, you may not want to spend time troubleshooting something that could well be defective.
- Where does the problem lie?
  Be specific. Do not assume the problem being experienced is the actual problem. First determine if the FortiMail unit's problem lies elsewhere before starting to troubleshoot the unit.
- Is it a connectivity issue? Can your FortiMail unit communicate with your network and the Internet? Is there connection to a DNS server?
- Is there more than one thing not working?
  Make a list.
- Is it partly working? If so, what parts are working?
  Make a list.
- Can the problem be reproduced at will or is it intermittent?
  An intermittent problem can be difficult to troubleshoot due to the difficulty reproducing the issue.
- Are the servers covered by the policy working? Has a policy been disabled?
  Check the status of the protected servers.
- Is your system overloaded?
  View the System Resource on the dashboard.
- What has changed?
  Do not assume that nothing has changed in the network. Use the FortiMail event log to see if something changed in the configuration. If something did change, see what the effect is when you roll back the change.
- After determining the scope of the problem and isolating it, what servers does if affect?

Once the problem is defined, you can search for a solution and then create a troubleshooting plan to solve it.

Search for a known solution

You can save time and effort during the troubleshooting process by checking if other FortiMail administrators experienced a similar problem before. First check within your organization. Next, access the Fortinet online resources that provide valuable information about FortiMail technical issues.

Technical documentation

FortiMail administration guides, quickstart guides, and other technical documents are available online at:

http://docs.fortinet.com

Also check the release notes for your FortiMail unit.

Knowledge Base

The Fortinet Knowledge Base includes a variety of articles, white papers, and other documentation providing technical insight into a range of Fortinet products at:

http://kb.fortinet.com

Fortinet technical discussion forums

Administrators can exchange experiences and tips related to their Fortinet products through an online technical forum at:

http://support.fortinet.com/forum

Fortinet training services online campus

The Fortinet Online Campus hosts a collection of tutorials and training materials which can help increase your knowledge of the Fortinet products at:

http://campus.training.fortinet.com

Create a troubleshooting plan

Once you fully define the problem or problems, begin creating a troubleshooting plan. The plan should list all possible causes of the problems that you can think of, and how to test for each cause.

The plan will act as a checklist so that you know what you have tried and what is left to check. The checklist is helpful if more than one person will be troubleshooting: without a written plan, people can become easily confused and steps skipped. Also, if you have to pass the problem-solving to someone else, providing a detailed list of what data you gathered and what solutions you tried demonstrates professionalism.

Be ready to add steps to your plan as needed. After you are part way through, you may discover that you overlooked some tests, or a test you performed discovered new information. This is normal.

Check your access

Make sure your administrator account has the permissions you need to run all diagnostic tests and to make configuration changes. Also, you may need access to other networking equipment such as switches, routers, and servers to help you test. If you do not normally have access to this equipment, contact your network administrator for assistance.

Gather system information

Your FortiMail unit provides many features to aid in troubleshooting and performance monitoring.

Use the GUI's dashboard and the CLI commands to define the scope and details of your problem. Keep track of the information you gather. Fortinet customer support may request it if you contact them for assistance.

In the advanced management mode of the GUI, go to *Monitor* to view the system information and all other mail delivery information. For details, see Monitoring the system on page 113.

You can also use the CLI diagnose commands to troubleshoot both the hardware and firmware issues. For details, see the diagnose command chapter in the FortiMail CLI Reference.

Before using a `diagnose debug` command, make sure to enable the debug feature by entering:

```
diagnose debug enable
```

Check port assignments

There are 65535 port numbers available for each of the IPv4 TCP and UDP stacks that applications can use when communicating with each other. If someone recently changed a FortiMail or network port, that may be part of your problem.

In addition, some ports may be assigned to other Fortinet or third-party devices on your network.

Many UDP and TCP port numbers have internationally recognized IANA port assignments and are commonly associated with specific applications or protocols. FortiMail default port numbers usually follow those port number assignments. See also Appendix C: Port Numbers on page 611.

Troubleshoot hardware issues

Problem

Event log shows RAID errors regarding a degraded array event on multiple HD dev. `(ref./dev/md2 and /dev/md3)`

Solution

You may have a hard drive device problem. For example, one of the RAID disks may not be functioning properly. Check the RAID status (see Configuring RAID on page 217).

Troubleshoot GUI and CLI connection issues

Problem

An administrator account can connect to the advanced mode of the GUI, but not to the basic mode nor to the CLI.

Solution

Set the administrator account's Domain to System. Domain administrators, also known as tiered administrators, cannot access the CLI or the basic mode of the GUI. For more information, see FortiMail operation modes on page 33.

If you require the ability to restrict the account to specific areas of the GUI, consider using access profiles instead. For details, see Configuring administrator profiles on page 170.

Problem

An administrator account's password has been misplaced, or needs to be changed but no one with the existing password is available.

Solution

Administrators with physical access to a FortiMail unit can use a console cable and the maintainer administrator account to log into the CLI. The maintainer account allows you to log into a FortiMail unit if you have lost all administrator passwords.

The admin maintainer account feature is enabled using the following CLI command:

```
config system global
   set admin-maintainer enable
end
```

Once logged into the FortiMail unit with the maintainer account, you can reset the passwords of super-admin profile accounts, or enter the `execute factoryreset` command to return the FortiMail unit to its default configuration.

For full configuration and procedural details, see Resetting a lost administrator password.

Problem

Administrators cannot log in to the GUI or the CLI.

Solution

Check the following solutions.

Use correct admin name and password combination

This may be obvious, but it should be the first thing to check.

Allow access for interface is not enabled

Each FortiMail interface has a set of administrator access protocols — HTTP, HTTPS, SSH, TELNET, PING, and SNMP. These are the methods an administrator can use to connect to FortiMail; any or all can be disabled on any interface.

For security purposes, you should only enable access that is required. If you open access for troubleshooting, remember to disable it afterwards. Failure to do so will leave a gap in your security that hackers might exploit.

To enable administrator access on the dmz interface

1. Log on as administrator.
2. Go to *System* > *Network* > *Interface*.
3. Select the interface and click *Edit*.
4. Under *Access*, select the protocols you want to use to access the interface.
5. Click OK.
6. Repeat for each interface where administrative access is required.

Trusted hosts for admin account will not allow current IP

A trusted host is a secure location where an administrator logs in. For example, on a secure network an administrator can to log in from an internal subnet but not from the Internet.

If an external administrator login is required, a secure VPN tunnel can be established with a set IP address or range of addresses that are entered as a trusted host address.

Trusted host login issues occur when an administrator attempts to log in from an IP address that is not included in the trusted host list.

To verify trusted host login issues

1. Record the IP address where the administrator is attempting to log in to the FortiMail unit.
2. Log in to the GUI and go to *System* > *Administrator* > *Administrator*.
3. Select the administrator account in question and click the Edit icon.
4. Compare the list of trusted hosts to the problem IP address. If there is a match, the problem is not due to trusted hosts.
5. If there is no match and the new address is valid (secure), add it to the list of trusted hosts.
6. Select OK.

If the problem was due to trusted hosts, the administrator can now log in.

Accept low encryption in browsers

If you are connecting to FortiMail-VM with a trial license or to a LENC version of FortiMail, you may ***not*** be able to see the logon page due to an SSL cipher error during the connection. In this case, you must configure your browser to accept low encryption.

For example, in Mozilla Firefox, if you receive this error message:

```
ssl_error_no_cypher_overlap
```

you may need to enter `about:config` in the URL bar, then set

```
security.ssl3.rsa.rc4_40_md5 to true.
```

Troubleshoot FortiGuard connection issues

Problem

The FortiMail unit cannot connect to the FDN servers to use FortiGuard Antivirus and/or FortiGuard Antispam services.

Solution

FortiGuard Antivirus and FortiGuard Antispam subscription services use multiple types of connections with the FortiGuard Distribution Network (FDN).

For all FortiGuard connection types, you must:

- Register your FortiMail unit with the Fortinet Technical Support web site, https://support.fortinet.com/.
- Get a trial or purchased service contract for FortiGuard Antispam and/or FortiGuard Antivirus, and apply it to your FortiMail unit. If you have multiple FortiMail units operating in high availability (HA) together, all of them must have a service contract. You can view service contracts applied to each of your registered FortiMail units by visiting the Fortinet Technical Support web site:

  https://support.fortinet.com/
- Configure your FortiMail unit to connect with a DNS server that can resolve the domain names of FortiGuard servers. For more information, see Configuring DNS on page 161.
- Configure your FortiMail unit with at least one route so that the FortiMail unit can connect to the Internet. For more information, see Configuring static routes on page 161.

To verify DNS resolution of the FortiGuard Antispam service, enter:

```
execute nslookup name service.fortiguard.net
```

To verify DNS resolution of the FortiGuard antivirus service, enter:

```
execute nslookup name fds1.fortinet.com
```

To verify network connectivity, enter:

```
execute traceroute <address_ipv4>
```

where `<address_ipv4>` is one of the FortiGuard servers.

If those tests succeed, then also examine requirements specific to the type of communication that is failing:

scheduled updates (FortiGuard Antivirus and FortiGuard Antispam)	• Configure the system time of the FortiMail unit, including its time zone. For more information, see Configuring the time and date on page 171. • Intermediary firewall devices must allow the FortiMail unit to use HTTPS on TCP port 443 to connect to the FDN. • If your FortiMail unit connects to the Internet through a proxy, use the CLI command `set system autoupdate tunneling` to enable the FortiMail unit to connect to the FDN through the proxy. For more information, see the FortiMail CLI Reference. • You might need to override the FortiGuard server to which the FortiMail unit is connecting, and connect to one other than the default server for your time zone.
rating queries (FortiGuard Antispam)	• Intermediary firewall devices must allow the FortiMail unit to use UDP port 53 to connect to the FDN.

If you suspect that a device on your network is interfering with connectivity, you can analyze traffic and verify that the FortiMail unit is sending and receiving traffic on the required port numbers. Use the CLI command `diagnose sniffer` to perform packet capture. If traffic is being corrupted or interrupted, you may need to perform packet capture at additional points on your network to locate the source of the interruption.

Troubleshoot MTA issues

Problem

SMTP clients receive the message `550 5.7.1 Relay access denied`.

Solution

This indicates rejection due to lack of relay permission.

- For incoming connections, relay will be allowed automatically unless explicitly rejected through the access control list (see Configuring access control receiving policies on page 337).
- For outgoing connections, relay will be allowed only if explicitly granted by authentication (see Controlling email based on IP addresses on page 348) or by the access control list (see Configuring access control receiving policies on page 337). If authentication is required, verify that the SMTP client is configured to authenticate.

If you receive a 5.7.1 error message that does **not** mention relay access, and sender reputation or endpoint reputation is enabled, verify that the SMTP client has not exceeded the reputation score threshold for rejection.

Problem

The FortiMail unit is bypassed.

Solution

FortiMail units can be physically bypassed in a complex network environment if the network is not carefully planned and deployed. Bypassing can occur if SMTP traffic is not correctly routed by intermediary NAT devices such as routers and firewalls.

If your FortiMail unit will be performing antispam scans on outgoing email, all outgoing email must be routed through the FortiMail unit. If your email users and protected servers are configured to relay outgoing mail through another MTA such as that of your ISP, the FortiMail unit will be bypassed for outgoing email.

Spammers can easily determine the lowest priority mail server (highest preference number in the DNS MX record) and deliver spam through that lower-priority MX in an attempt to avoid more effective spam defenses.

To ensure that spammers cannot bypass the FortiMail unit

1. Configure routers and firewalls to route SMTP traffic to the FortiMail unit for scanning.
2. If the FortiMail unit is operating in gateway mode, modify the DNS server for each protected domain to keep only one single MX record which refers to the FortiMail unit.

3. Verify that all possible connections have a matching policy. If no policy matches, the connection will be allowed but will not be scanned (to prevent this, you can add a policy to the bottom of the IP policy list that rejects all connections that have not matched any other policy).
4. Verify that you have selected an antispam profile in each policy, and have enabled antispam scans.

Problem

Both antispam and antivirus scans are bypassed.

Solution

If email is not physically bypassing the FortiMail unit, but is not undergoing both antispam and antivirus scans, verify that access control rules are not too permissive. Also verify that a policy exists to match those connections, and that you have selected antispam and antivirus profiles in the policy. Scans will not be performed if no policy exists to match the connection.

Problem

Antispam scans are bypassed, but antivirus scans are not.

Solution

If antivirus scans occur, but antispam scans do not, verify that safe lists are not too permissive and that you have not safelisted senders in the protected domains. Safelist entries cause the FortiMail unit to omit antispam scans.

Additionally, verify that either the *Bypass scan on SMTP authentication* option is disabled, or confirm that authenticated SMTP clients have not been compromised and are not a source of spam.

Problem

Recipient verification through SMTP fails.

Solution

If you have enabled the Recipient Address Verification option with a protected domain's SMTP server, but recipient verification fails, possible causes include:

- The SMTP server is not available.
- The network connection is not reliable between the FortiMail unit and the SMTP server.
- The server is a Microsoft Exchange server and SMTP recipient verification is not enabled and configured.

When the SMTP server is unavailable for recipient verification, the FortiMail unit returns the 451 SMTP reply code. The email would remain in the sending queue of the sending MTA for the next retry.

Problem

SMTP clients receive the message `451 Try again later`.

Solution

There are several situations in which the FortiMail unit could return the `451 Try again later` SMTP reply code to an SMTP client. Below are some common causes.

- The greylist routine has encountered an unknown sender or the greylist entry has expired for the existing sender and recipient pair. This is an expected behavior, and, for legitimate email, will resolve itself when the SMTP client retries its delivery later during the greylist window.
- Recipient verification is enabled and the FortiMail unit is unable to connect to the recipient verification server. There should be some related entries in the antispam log, such as `Verify <user@example.com> Failed, return TEMPFAIL`. If this occurs, verify that the server is correctly configured to support recipient verification, and that connectivity with the recipient verification server has not been interrupted.

Problem

The FortiMail unit replies with a temporary failure SMTP reply code, and the event log shows `Milter (fas_milter): timeout before data read`.

Solution

The timeout is caused by the FortiMail unit not responding within four minutes.

Slow or unresponsive DNS server response for DNSBL and SURBL scans can cause the FortiMail unit's antispam scans to be unable to complete before the timeout. When this occurs, the FortiMail unit will report a temporary failure. In most cases, the sending MTA will retry delivery later. If this problem is persistent, verify connectivity with your DNSBL and SURBL servers, and consider providing private DNSBL/SURBL servers on your local network.

Problem

The event log shows `Milter (mailfilterd): timeout before data read, where=eom`.

Solution

This may be caused by the following reason:

If an email message contains a shortened URL that redirects to another URL, the FortiMail unit is able to send a request to the shortened URL to get the redirected URL and scan it against the FortiGuard AntiSpam database. By default, this function is enabled. To use it, you need to open your HTTP port to allow the FortiMail unit to send requests for scanning the redirected URL.

This also means, if the upstreaming device (firewall, router, etc.) does not allow HTTP traffic from the FortiMail unit, FortiMail's HTTP request to FortiGuard servers will get timeout.

To solve this problem

- Allow HTTP/HTTPS outbound traffic from the FortiMail unit on the upstreaming device.

or

- Run the following CLI commands on FortiMail to disable the feature:

```
config system fortiguard antispam
  set uri-redirect-lookup disable
end
```

Problem

When recipient verification is enabled on the Microsoft Exchange server, all email is rejected.

Solution

By default, Microsoft Exchange servers will not verify the recipient. With an Microsoft Exchange server as the MTA, it is recommended to configure the FortiMail to use LDAP to do recipient verification using the Microsoft Active Directory service. Alternatively, you can configure Microsoft Exchange to enable SMTP recipient verification.

To configure recipient verification on a Microsoft Exchange server

1. Open the Microsoft Exchange system manager and go to Global settings > Message Delivery > Properties.
2. Enable Recipient Filtering.
3. Click Filter recipients who are not in the Directory.
4. Go to Administrative Groups > First Administrative Group > Servers > [your server] > SMTP > the default SMTP virtual server > Properties.
5. Click Advanced.
6. Click Edit.
7. Click Apply Recipient Filter.
8. Click OK.

To test the configuration, open a Telnet connection to port 25 of your Microsoft Exchange server.

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 with caution. For example, a safe list entry *.edu would allow all email from all domains in the .edu top level domain to bypass antispam scans.
- Do not safelist protected domains. Because safe lists bypass antispam scans, email with spoofed sender addresses in the protected domains could bypass antispam features.
- 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 497).
2. Next, disable both the *Bypass bounce verification* option (see Configuring protected domains on page 280) and the *Bypass bounce verification chec*k option (see Configuring session profiles on page 361).
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 497.

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 528) 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.

Troubleshoot HA issues

Problem

Active-passive HA cluster does not switch to the secondary unit after a failure.

Solution

If an individual service has failed that does not disrupt the HA heartbeat, an active-passive HA cluster may not fail over. For example, it is possible that one or more services (such as SMTP, IMAP, POP3, web access, or a hard drive or network interface) could fail on the primary unit without affecting the HA heartbeat.

To cause failover when an individual service fails, configure service monitoring (see Service Monitor section on page 237) on both the primary unit and secondary unit.

See also

Monitoring HA status

Service Monitor section

Problem

Mail queues do not appear on the HA secondary unit.

Solution

In order to display queue content in the secondary unit, mail data must be synchronized from the primary unit. If the *Backup MTA queue directories* option is disabled, mail queues will not be synchronized. You can enable MTA spool synchronization to view the mail queues from either the secondary or primary unit.

Synchronization of MTA spool directories can result in decreased performance, and may not let you to view all email in the mail queues, as mail queue content can change more rapidly than synchronization occurs.

Troubleshoot resource issues

Problem

The FortiMail unit is suffering from sluggish or stalled performance.

Solution

Use the CLI to view a list of the most system-intensive processes. This may show processes that are hogging resources. For example:

```
diagnose system top 10
```

The above command generates a report of processes every 10 seconds. The report provides the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI window until you enter `q` (quit).

Troubleshoot bootup issues

This section addresses problems you may experience in rare cases when powering on your FortiMail unit. If you continue to have problems, please contact customer support for assistance.

It is rare that units experience any of the symptoms listed here. Fortinet hardware is reliable with a long expected operation life.

When you cannot connect to the FortiMail unit through the network using CLI or the GUI, connect a PC directly to the FortiMail unit's management console using a serial connection (the cable varies with the FortiMail model. See the model's quickstart guide for details).

Open a terminal emulation interface, such as HyperTerminal, to act as the console. The issues covered in this section all refer to various potential bootup issues.

Once you have a direct console connection to the FortiMail unit, work through the following steps and keep a copy of the console's output messages. If you have multiple problems, go the problem closest to the top of the list first, and work your way down.

1. Do you see the boot options menu
2. Do you have problems with the console text
3. Do you have visible power problems
4. You have a suspected defective FortiMail unit

Do you see the boot options menu

1. Do you see the boot options menu?
   - If no, ensure your serial communication parameters are set to `no flow control`, check that the correct baud rate is correctly set (usually 9600, data bits 8, parity none, stop bits 1), and reboot the FortiMail unit by powering off and on.
     - If that fixes your problem, you are done.
     - If it does not fix your problem, go to Do you have visible power problems.

Do you have problems with the console text

1. Do you see any console messages?
   - If no, go to Do you have visible power problems.
   - If yes, continue.
2. Are there console messages but text is garbled on the screen?
   - If yes, ensure your console communication settings are correct for your unit (such as, baud rate 9600, data bits 8, parity none, stop bits 1). Check the FortiMail QuickStart Guide for settings specific to your model.
     - If that fixes the problem, you are done.
3. Do the console messages stop before the prompt: `Press Any Key to Download Boot Image`?
   - If yes, go to You have a suspected defective FortiMail unit.
   - If no, follow the console instruction `Press any key to Download Boot Image` and go to the next step.
4. When pressing a key, do you see one of the following messages?

   ```
   [G] Get Firmware image from TFTP server
   [F] Format boot device
   [B] Boot with backup firmware and act as default
   [Q] Quit menu and continue to boot with default firmware
   [H] Display this list of options
   ```

   - If yes, go to You have a suspected defective FortiMail unit.
   - If no, ensure you serial communication parameters are set to `no flow control`, check that the correct baud rate is set.

     To find the unit's current baud rate using CLI, enter these commands:

     ```
     config system console
     get
     ```

Change settings if needed and reboot the FortiMail unit by powering off and on.

5. Did the reboot fix the problem?
   - If that fixes your problem, you are done.
   - If that does not fix your problem, go to You have a suspected defective FortiMail unit.

Do you have visible power problems

1. Is there any LED on the FortiMail unit?
   - If no, ensure power is on. If that fixes the problem you are done. If not, continue.
   - If yes, continue.
2. Do you have an external power adapter?
   - If no, go to You have a suspected defective FortiMail unit.
   - If yes, try replacing the power adapter.
3. Is the power supply defective?
   - If no, go to You have a suspected defective FortiMail unit.
   - If yes, replace the power supply and begin the tests again at Do you see the boot options menu.

You have a suspected defective FortiMail unit

If you followed the previous steps and determined there is a good chance your unit is defective, contact Fortinet customer support.

Troubleshoot installation issues

For troubleshooting tips and tools related to FortiMail installation and setup, see Testing the installation on page 95.

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 firmware version
   - 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

For bootup problems:

- provide all console messages and output
- if you suspect a hard disk issue, provide your evidence

2. Document the problem and the steps you took to define the problem.
3. Open a support ticket.

For details on using the Fortinet support portal and providing the best information, see the Knowledge Base article, "Fortinet Support Portal for Product Registration, Contract Registration, Ticket Management, and Account Management" at:

http://kb.fortinet.com/

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 508. If you have enabled it (see Configuring the Bayesian training control accounts on page 514 and Accept training messages from user on page 389)**,**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 377.

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 473, Configuring protected domains on page 280, and Using quarantine reports on page 604). 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 354 and Configuring authentication profiles on page 420.

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 C: Port Numbers on page 611), 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 377) 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 473)
- the quarantine control email addresses (see Configuring the quarantine control options on page 480)

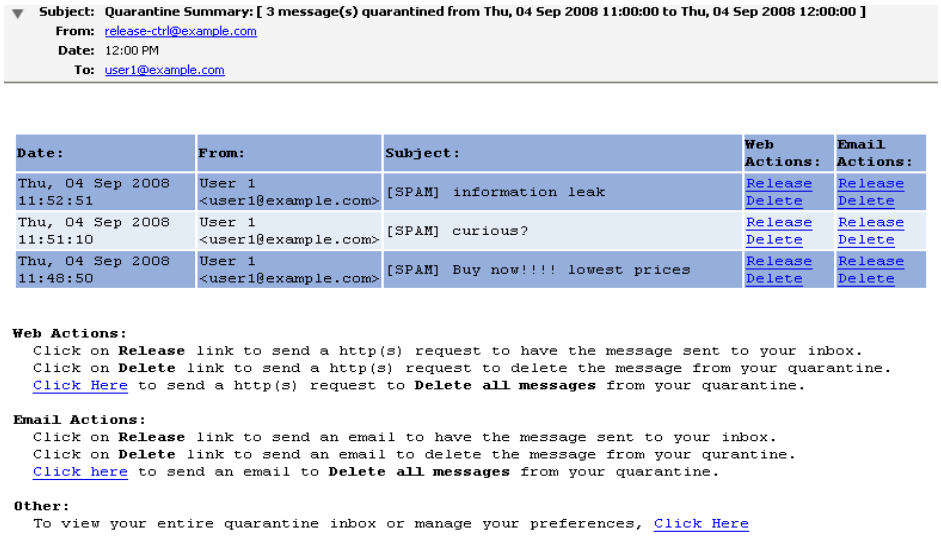
When email is added to their personal quarantine, email users will periodically receive an email similar to one of the samples below.

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: 1184166681.16BFAj510009380000@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 337.
- Create an authentication profile to authenticate the users. For details, see Configuring authentication profiles on page 420.
- Enable SMTP authentication in the incoming recipient-based policy. For details, see Controlling email based on sender and recipient addresses on page 354.

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 A: 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 B: Maximum Values

Each FortiMail platform, including the VM platforms, has hard-coded limits for the maximum number of objects that can be configured for various features. They may not be practical for every situation, especially when other features are used to their maximum, and are not a promise of performance.

There is no warning message when a limit is reached, but FortiMail will not allow you to add more.

To view the maximum values of all FortiMail models, see FortiMail Maximum Values.

Appendix C: 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 611
- Outgoing port numbers on page 612

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 163. If traffic capture is enabled, then the FortiMail unit listens on port numbers that are specified by the filter. See Traffic capture on page 277.

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)
161	UDP	• FortiManager	SNMPquery
25	TCP	• Email servers,	• Email relay/proxy/server (SMTP)

Default Port Number	IP Protocol	Source IP address	Purpose
		relays	• Spam sample submission by email users
465	TCP	• Email users	• 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	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
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)
9443	UDP		(Deprecated) FortiGuard Antivirus push
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 615) • 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

Default Port Number	IP Protocol	Destination IP Address	Purpose
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	HA centralized monitoring
6688	TCP		HA centralized monitoring
20000	UDP and TCP		HA heartbeat signal (base port)
20001	TCP		HA synchronization control
20002	TCP		HA file synchronization
20003	TCP		HA data synchronization
20004	TCP		HA checksum synchronization
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
443	TCP	• FortiSandbox	URL scan (HTTPS)
514	TCP		File scan (OFTPS)
443	TCP	• FortiManager	Registration, configuration backup/pull, and firmware pull
162	UDP		Event traps (SNMP)
514	UDP and TCP	• FortiAnalyzer • Syslog	Logging
80 or 443	TCP	• Dynamic DNS servers	Dynamic DNS (HTTP or HTTPS)
80	TCP	• Web servers	Resolution of tiny URLs into the redirect target URL

Default Port Number	IP Protocol	Destination IP Address	Purpose
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 securewf.fortiguard.net (United States only)
- service.fortiguard.net (global) or usservice.fortiguard.net (United States only)

Appendix D: 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`, `exampleccom`, 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 617.

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 617.

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 617.

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`.

Regular Expression	Matches and Non-Matches
`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.  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
```

Appendix E: Working with TLS/SSL

This appendix describes how to use the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocols on the FortiMail unit, including information on how TLS/SSL works, how it is supported on the FortiMail unit, and some troubleshooting tips.

This section contains the following topics:

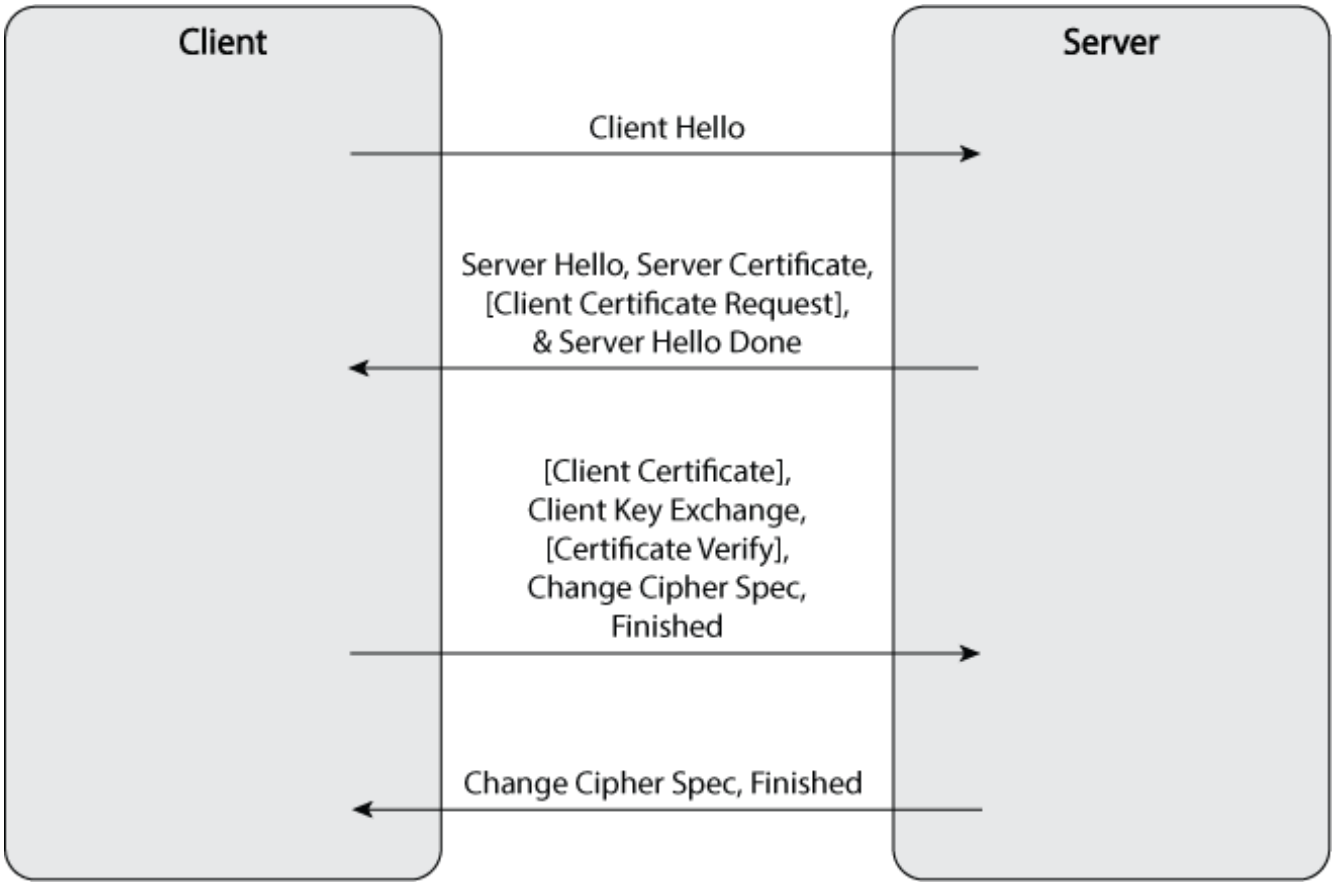
About TLS/SSL

TLS and its predecessor SSL are cryptographic protocols that provide communication security over the Internet. They secure network connections above the Transport Layer by using symmetric cryptography for privacy and a keyed message authentication code for message integrity.

How TLS/SSL works

TLS/SSL uses asymmetric encryption algorithm for authentication and deriving the session key and symmetric algorithm to encrypt the data for its speed. For the user data to go through the encryption tunnel, a TLS handshake must take place to authenticate the peer and generate the common session key for data encryption. The diagram below describes how TLS negotiation works at the high level:

Client-server TLS negotiation workflow



Client Hello

Client Hello is the first message sent by the client to the server in the TLS/SSL session setup sequence. It typically contains the ciphers and extensions supported by the client.

Server Hello, Server Certificate, [Client Certificate Request] and Server Hello Done

In response to Client Hello, the server sends back the following messages:

- Server Hello: Contains the cipher the server picked from the list provided by the client based on its preference.
- Server Certificate: Contains the server's certificate and its CA if configured so.
- [Client Certificate Request]: Optionally, the server can request the client certificate for authentication, which usually is not used.
- Server Hello Done: Concludes the server-client handshake.

[Client Certificate], Client Key Exchange, [Certificate Verify], Change Cipher Spec, Finished

In response to Server Hello, Server Certificate, [Client Certificate Request] and Server Hello Done, the client sends back the following messages:

- [Client Certificate Request], [Certificate Verify]: If the server requests the client certificate, the client will send its own certificate and a Certificate Verify message which is a signature over the previous handshake message using its certificate related private key.
- Client Key Exchange: Usually contains a pre-master key which is encrypted using the server's public key obtained from its certificate.
- Change Cipher Spec: A message to notify the server about the start of data authentication and encryption.
- Finished: A message encrypted with the new key is sent to determine if the server is able to decrypt the message and the negotiation was successful.

Change Cipher Spec, Finished

In response to [Client Certificate], Client Key Exchange, [Certificate Verify], Change Cipher Spec, Finished, the server sends back a Change Cipher Spec to confirm the start of data authentication and encryption. The server also sends its own Finished message encrypted using the common session key. If the client can read this message then the negotiation is successfully completed.

From now on, all the communication between the client and server is encrypted.

The "client" and "server" described above are roles in a specific session. The same device may change roles in different sessions. For example, when the FortiMail unit receives email from either a client or another sending MTA, the FortiMail unit acts as the TLS server. When the FortiMail unit relays email to the next hop receiving MTA, it acts as a TLS client. Nonetheless, some applications always act as a TLS client or server, but not both. For example, a web browser always acts as a TLS client and a web server always acts as a TLS server.

FortiMail support of TLS/SSL

By default, the FortiMail unit supports TLS/SSL in two slightly different ways:

- **SMTPS**
  SMTPS is also called SMTP over SSL. It runs on a different port than the regular email port (465 by default). To connect with SMTPS, the client needs to start the TLS handshake directly at the very beginning.
- **STARTTLS**
  STARTTLS is a command that runs on a regular email service port, 25 by default. If the server supports STARTTLS, this command shows up in the welcome banner and the client runs it to establish a TLS session to protect all subsequent communication. If the server does not support this feature, it will not advertise the STARTTLS command and the client will use clear text communication. The STARTTLS command is more flexible than SMTPS.

Although this document mainly covers STARTTLS, most is applicable to SMTPS.

FortiMail TLS behavior in both directions of mail flow

FortiMail may be either receiving or delivering email. TLS behavior varies by direction.

- **Mail receiving**

  By default both SMTPS and STARTTLS are supported when the FortiMail unit receives messages. Whether the email will be encrypted with TLS/SSL depends on the mail client or sending MTA. The TLS support can be turned on or off globally by going to *System* > *Mail Setting* > *Mail Server Settings*.

  If you deselect the *SMTP over SSL/TLS* option, STARTTLS will not be advertised to the client and the SMTPS port (465) will not be listening. As a result, the FortiMail unit will not accept emails through TLS/SSL.
- **Mail delivering**

  There is no global setting to control how TLS is used when the FortiMail unit delivers emails to the next hop receiving MTA. By default, it uses STARTTLS "preferred" option which means:
  - If the receiving MTA supports STARTTLS, the FortiMail unit will use TLS and transmit emails in the protected session.
  - If the receiving MTA does not advertise STARTTLS, the FortiMail unit will use clear text SMTP session to transmit emails.
  - If the receiving MTA supports STARTTLS, but the TLS session does not succeed, the FortiMail unit will fall back to the clear text SMTP session to retransmit emails after the **third** failed attempt.

TLS profile

The default behavior of FortiMail TLS/SSL support may not meet your specific requirements. In order to add more flexibility to the TLS/SSL support, the FortiMail unit supports TLS profiles. This document uses FortiMail v4.1 as an example.

TLS profiles allow you to selectively disable or enable TLS for specific email recipient patterns, IP subnets, and so on. A common use of TLS profiles is to enforce TLS transport to a specific domain and verify the certificate of the receiving servers.

To configure a TLS profile, go to *Profile* > *Security* > *TLS*.

The *TLS level* option has these choices:

None	Disables TLS and the FortiMail unit does not accept STARTTLS command from the client in receiving direction or does not start TLS in the delivering direction (even if STARTTLS is advertised by the receiving MTA), depending on which direction the TLS profile is applied.
Preferred	This is the default behavior. Whether TLS is used depends on the other party of the session.
Edit	Select to change settings for the widget. This option appears only on the *CLI Console* widget.
Secure	Enforces both TLS encryption and certificate validation. Failure of server certificate validation will fail mail delivery.

The *Action on failure* option has these choices:

Temporarily Fail	If a TLS session cannot be established, the FortiMail unit will fail temporarily and retry later. No DSN will be bounced back.
Fail	If a TLS session cannot be established, the FortiMail unit will fail the mail delivery immediately and a DSN will be bounced back to notify the sender about the failure.

Example

This example shows how to enforce TLS on a specific domain and verify the validity of the receiving server certificate.

Scenario

All emails to `example.mil` must be encrypted with TLS and the FortiMail unit needs to verify the certificate of the receiving server to defend against email server spoofing or man-in-the-middle attack. If the certificate validation fails, the FortiMail unit will not deliver emails to that server, `example.mil`.

To verify the certificate of the receiving server and apply the TLS profile

1. Import the server CA certificate.
   Add the certificate of the CA that issued the server certificate to the FortiMail unit. If more than one level of CAs was used, import all intermediate and root CA certificates to the FortiMail unit. Any missing CA certificate will break the chain of trust and then certificate validation will fail.
2. Create a TLS profile.
   Select *Secure* for *TLS level*. Find the CA from the drop down list after enabling *Check CA issuer*. If the certificate subject also needs to be verified, select *Check certificate subject* and configure the substring that is contained in the server certificate. Minimum encryption strength can be configured if needed. A failure of any checks enabled in the profile will fail the TLS session and email delivery to the destination domain.
3. Create delivery policy and apply the profile.
   Apply the newly created TLS profile in the delivery policy by going to *Policy* > *Access Control* > *Delivery*.

Now all email from the FortiMail unit to `example.mil` will be delivered through TLS and the server certificate will be verified. If the certificate validation does not succeed, the FortiMail unit will not deliver email to `example.mil`.

Troubleshooting FortiMail TLS issues

This section describes some FortiMail TLS issues and their solutions and contains the following topics:

Common error messages

There are two most commonly seen error messages on the FortiMail unit or other email systems: `verify=CAFail` and `CAFail`.

verify=CAFail

This error message appears when the remote certificate is not issued by a trusted CA or the CA certificate is not available for verification. Usually this error is not fatal and the encryption can be applied without any problems. The only issue is that the communication is susceptible to man-in-the-middle or server-spoofing attacks. However, if there is a TLS profile with *Secure* level enabled in a delivery rule, the connection will fail if the remote certificate is validated by the FortiMail unit.

If you are not concerned with email server-spoofing or man-in-the-middle attacks, you can just ignore this error message.

To fix this issue, either:

- Configure the remote server to send all the CA certificates together with its server certificate during the TLS/SSL handshake. This can be achieved by copying and pasting all the CA certificates into the server certificate file, assuming that they are all in PEM format.
  In many cases, this is not possible. For example, the remote server belongs to another organization. Therefore, you can only fix this problem on the FortiMail unit, as described in the following option.
- Import the certificate of root CA and all intermediate CAs that issued the server certificate to the FortiMail unit, so that the FortiMail unit can validate the server certificate all the way to the root CA. For information on how to get CA certificates, see Useful tools on page 625.

CAFail

This error message may appear on the external email server talking to the FortiMail unit. This is because that the FortiMail CA certificate is not available to external server for verification. In early versions of the FortiMail firmware, the system does not send out all CA certificates even though they are imported onto the FortiMail unit. This issue was fixed in release 4.1.1 (build 232).

To fix this issue

1. Upgrade your FortiMail firmware to release 4.1.1 build 232 or later.
2. Import the certificates of the root CA and all intermediate CAs that issued the FortiMail certificate in effect.

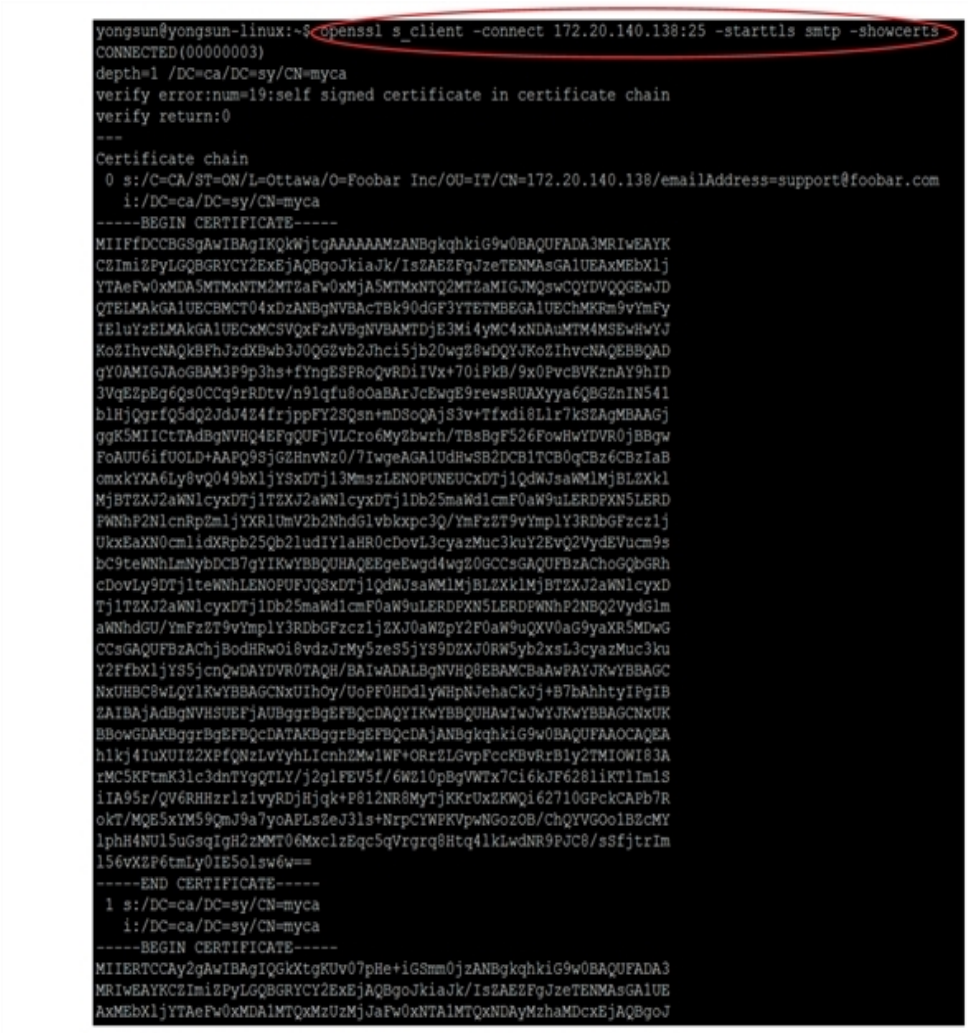
Useful tools

OpenSSL is useful for troubleshooting and testing TLS/SSL related issues. You can use `openssl` to get the certificate of the CA that issued the remote server certificate by typing the following syntax at a command-line prompt:

```
openssl s_client -connect server-ip:port -starttls smtp -showcerts
```

The following is an example of the tool output:

Sample Openssl tool output

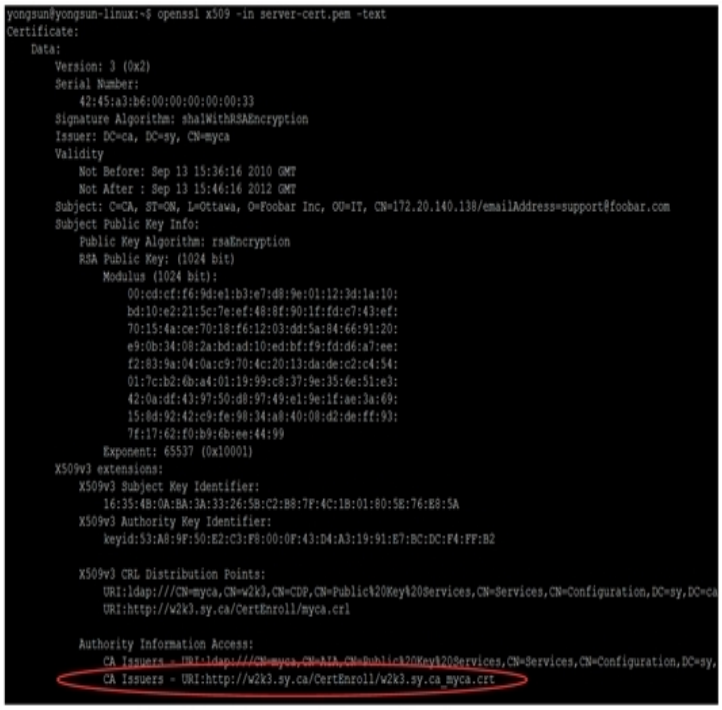


Note: The certificate is displayed in Base64 format (PEM) in the output. If the server CA certificate is also displayed in the output, the FortiMail unit should be able to validate the server certificate. However, in many cases the CA certificate is not sent by the remote server. You can just copy the certificate from the command output starting from "----Begin certificate----" and ending with "----end certificate-----" and store it in a file such as `server-cert.pem`. Then the certificate can be read with Openssl using the following command:

```
openssl x509 -in server-cert.pem -text
```

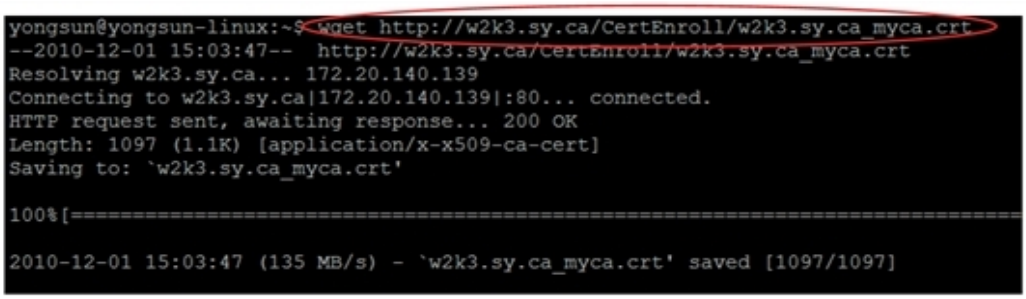
The following is a sample output of this command:

Sample openssl command output



Within the certificate, there is a section called `Authority Information Access (AIA)` that contains a URL to the CA certificate. Download the certificate from the URL identified and import it into the FortiMail unit. If there is more than one level of CA, you can repeat the process until you get the root CA certificate. Then import all the intermediate CA and root CA certificates into the FortiMail unit.

Importing the CA certificate



The FortiMail unit only supports certificates in PEM format. If the CA certificates you downloaded are in DER (binary) format, you need to convert them with Openssl using the following command:

`openssl x509 -in my-ca.crt -inform DER -out myca.pem -outform PEM`

Appendix F: PKI Authentication

This appendix describes how to configure Public key infrastructure (PKI) authentication on FortiMail. Included is information used to create a customized template to request certificates for use with FortiMail, install CA certificates, install client certificates, and configure the FortiMail unit to use PKI authentication.

This appendix provides one specific example of configuring PKI authentication on FortiMail. Other methods and tools can be used to accomplish the same result.

The information in this appendix is intended only as an example. Local operating procedure might vary. For generic FortiMail PKI configuration procedures, see Configuring PKI authentication on page 304.

Introduction to PKI authentication

PKI authentication is the methodology used to verify the identity of a user by checking the validity of a certificate that is bound to a specific user identity.

PKI authentication is an alternative to traditional password based authentication. The traditional method is based on "what you know" - a password used for authentication. PKI authentication is based on "what you have" - a private key related to the certificate bound to the user.

A common weakness of traditional password based authentication is the vulnerability to password guessing or brute force attack. PKI authentication is more resilient to this type of attack, hence PKI provides a stronger authentication mechanism.

In cryptography, PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). PKI authentication relies on two factors:

- Chain of trust. If the Root CA is trusted, then all certificates issued by the Root CA are trusted, as are all certificates issued by any intermediate CA that is trusted by the Root CA.
- Public key encryption algorithm. The data encrypted by public key can only be decrypted by private key. This is the basis for asymmetric data encryption. Similarly, the data encrypted by private key can be decrypted by the public key. This is usually used for digital signature. The private key is only available to a specific individual, while its related public key is embedded in the certificate signed by a CA.

PKI authentication can be implemented on FortiMail for administrators and email users. The FortiMail operation mode determines what these users can access using PKI authentication. The following table describes the impact of operation mode on each FortiMail user type.

Access types and FortiMail operation mode

Access type	FortiMail operation mode	Description
Administrative	**Server** **Gateway** **Transparent**	Administrators use PKI authentication to perform FortiMail management and administration functions, regardless of the FortiMail operation mode.
Email users	**Server**	Email users use PKI authentication to access regular email and quarantined email that is hosted on a FortiMail unit when operating in server mode.
Quarantined (spam) email only	**Gateway** **Transparent**	Email users use PKI authentication to access quarantined email (spam) contained in a bulk folder that is hosted on a FortiMail unit when operating in gateway or transparent mode.

FortiMail PKI architecture

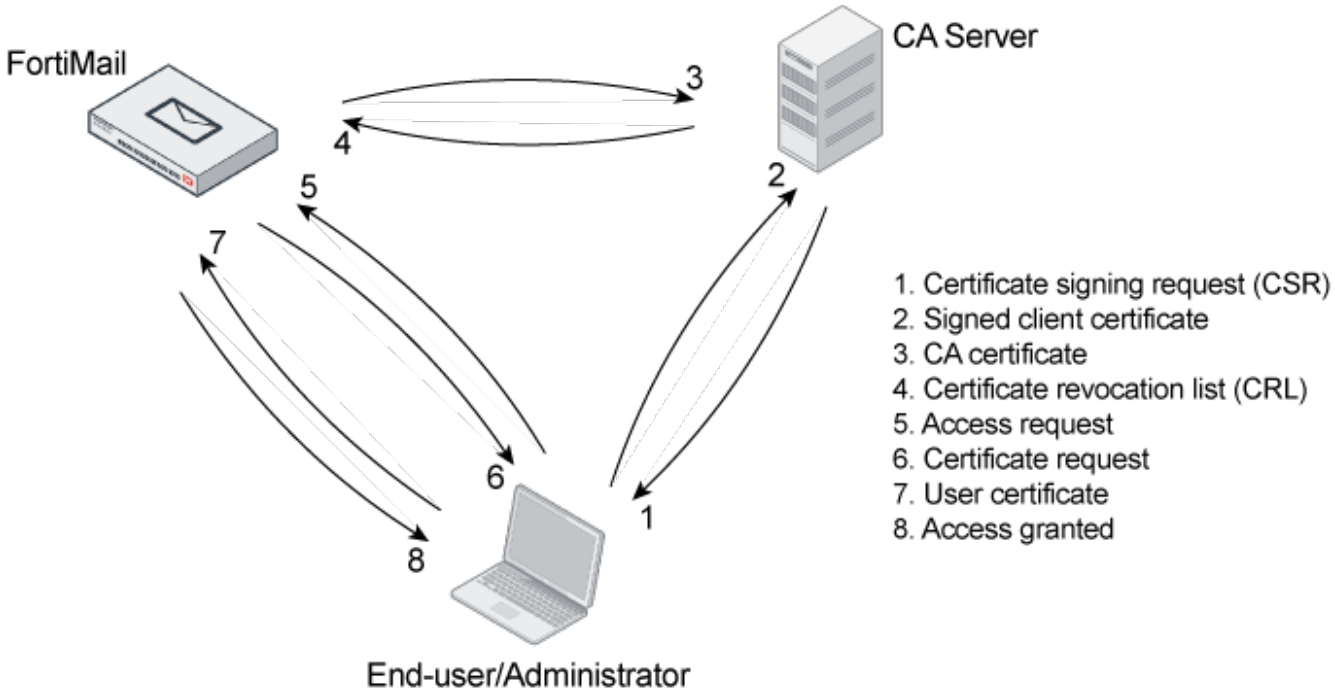
The FortiMail PKI architecture ensures that users present the necessary certificates before communication between the user and FortiMail starts. The two parties exchange certificates and verify the following:

- the certificate is issued by a trusted CA
- the claimed identity matches the one in the certificate
- the certificate has not expired
- the certificate type/usage matches the intended usage in the certificate

The diagram below illustrates a typical FortiMail PKI architecture.

PKI supports standards for Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). Those standards are beyond the scope of this document. For more information on those standards, see RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

FortiMail PKI architecture



Configuring PKI authentication on FortiMail

This section provides an example process for configuring PKI authentication on FortiMail.

The process described in this section is an example of one specific method for configuring PKI authentication on FortiMail. This process is not intended to replace the generic FortiMail PKI configuration procedures provided in other parts of this Administration Guide, or local operating practices.

The procedures in this document are intended for FortiMail administrators responsible for requesting, generating and delivering signed certificates on behalf of all end-users to enable PKI authentication on FortiMail.

Before you begin

When PKI authentication is configured and enabled, client certificates enable the administrator to access the GUI and the end-user to access webmail. This section includes procedures to create server certificates to enable the FortiMail unit to communicate with other devices using PKI authentication (that is, an SMTP server), create and distribute client certificates, and to configure and enable PKI authentication on the FortiMail unit for the users.

This document assumes that you have configured your CA server and are running your own local certification authority (CA). Generating certificates through a commercial CA is not included in this document.

The tasks involved in configuring PKI authentication on FortiMail require a thorough understanding of public-key cryptography, security certificates and certification processes.

The procedures in this document use tools such as Microsoft Management Console (MMC) and the Microsoft Certificate Service (MSCS) to generate certificates for PKI authentication on FortiMail. These tools enable the administrator to create customized client certificates on behalf of all end-users.

Once a client certificate is generated, the administrator must export and transmit that client certificate to the appropriate end-user, and instruct the end-user how to import the client certificate into their browser.

All client certificates and related private keys (usually saved in PKCS12 format) must be stored securely to prevent unauthorized use of the private key and client certificate.

PKI configuration work flow

Example PKI configuration work flow on page 632 is a work flow diagram that shows an example method for requesting, generating and delivering client certificates to FortiMail end-users and administrators, and for configuring the FortiMail unit for PKI authentication. The procedures cover PKI authentication requirements for FortiMail server, transparent and gateway operation modes. Each block in the work flow diagram is supported by a detailed procedure to complete the task.

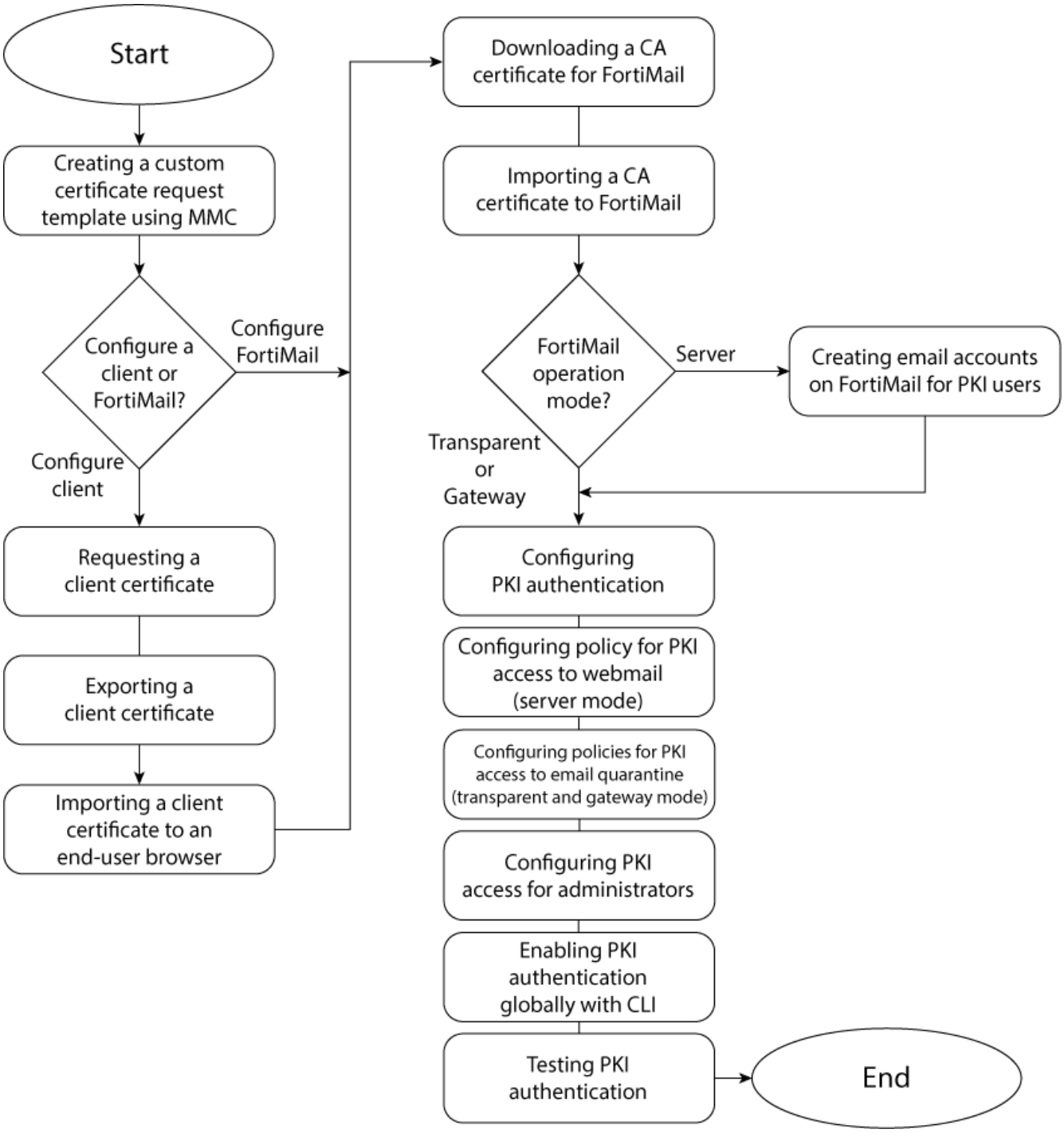
Perform the tasks in the order specified by the work flow diagram.

Prerequisites

Ensure that you have completed the following before performing any PKI configuration tasks:

- Read Before you begin on page 630.
- Installed Windows Server 2003, Enterprise Edition.
- Configured a Windows Server 2003 server as a stand-alone certification authority (CA).
- Have access to Microsoft Internet Explorer version 7 or higher.
- Installed Microsoft Certificate Services (MSCS) with web enrollment on the CA server.

Example PKI configuration work flow



Creating a custom certificate request template using MMC

Use this procedure to create a custom certificate request template using the Microsoft Management Console (MMC).

MMC comes with a variety of certificate templates. However, none of those templates are designed to meet the specific needs of FortiMail. A custom certificate template includes all information required by the FortiMail certification authority (CA) server to establish the identity of the client and create trusts for the secure exchange of information.

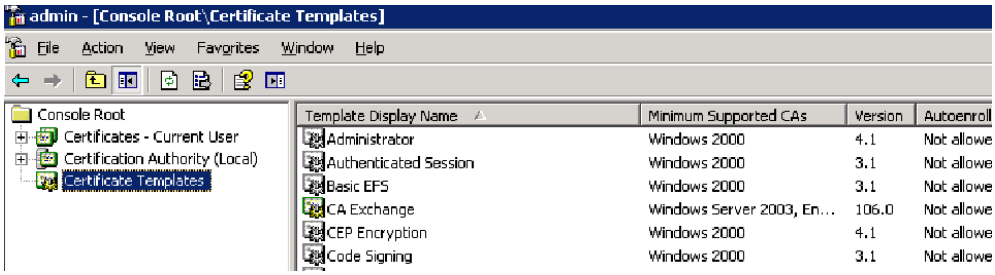
The custom certificate request template removes ambiguity and enables administrators to create certificate signature requests (CSR) specifically for FortiMail clients (that is, email users and administrators).

The custom certificate template is created using the MMC Certificate Template snap-in.

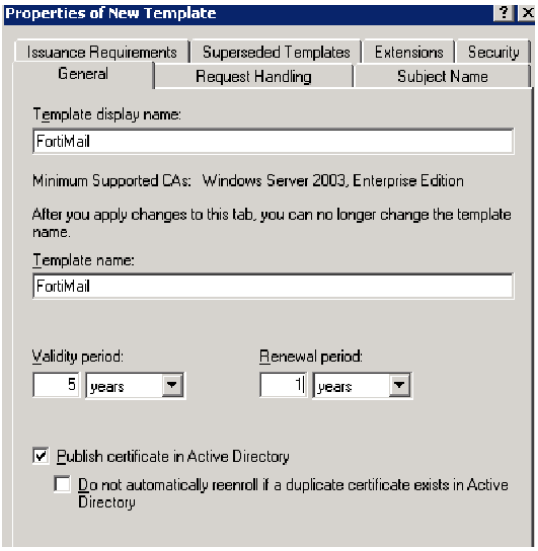
Before you begin this procedure, refer to Prerequisites on page 631.

To create a custom certificate template

1. Log in to the local certificate authority (CA) server and start MMC (on the Start Menu, click Run, type MMC, and then click OK).
2. In the Console Root folder, add the Certificate Template and Certificate Authority snap-ins.

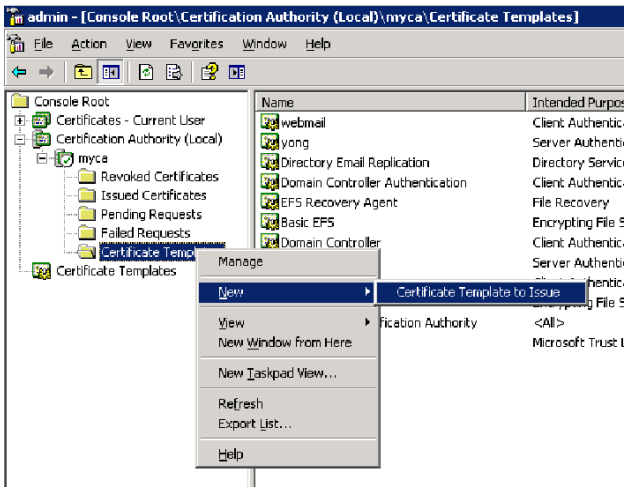


3. Select the Certificate Templates snap-in from the Console Root folder.
4. In the right pane, right-click User in the Template Display Name column and select Duplicate Template from the dropdown menu.
   The Properties of New Template window appears.



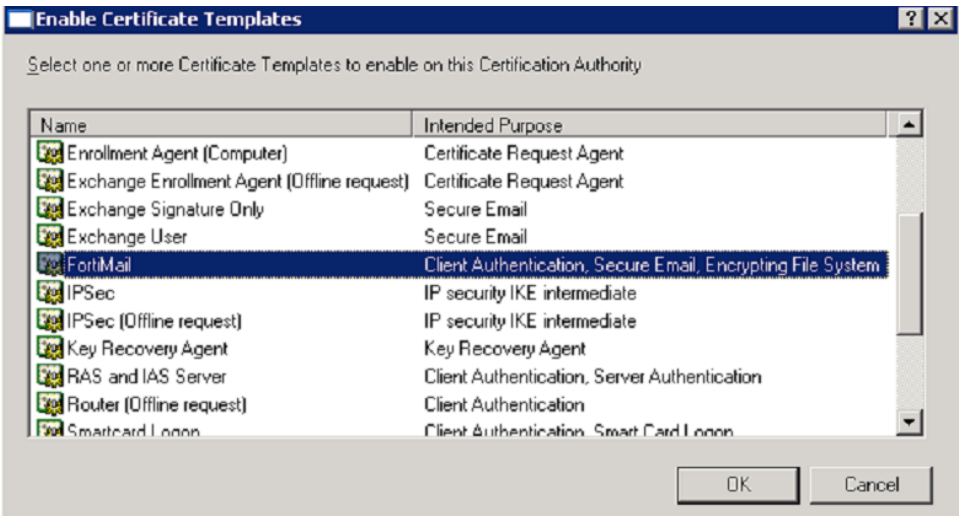
5. On the General tab, fill in the template name, validity period and renewal period according to your specific requirements.
6. On the Request Handling tab, select Signature and encryption in the Purpose field.
7. On the Subject Name tab, select Supply in the request. A subject name must be supplied in the request because the default subject name does not work with FortiMail.
8. On the Security tab, select Administrator and select (check) Allow as the Enroll Permission for Administrator.

9. On the Extensions tab, select Application Policies and verify that Client Authentication appears in Description of Application Policies.
10. On the Superseded Templates tab, select User in the Certificate templates area. This is the template that will be used as a base for the new template.
11. Leave the remainder of the settings on the Properties of New Template window as their default values and click OK. The new template is created and stored on the local certificate authority (CA) server.
12. Select the Certificate Authority snap-in from the Console Root folder.
13. Right-click Certificate Template and select New > Certificate Template to Issue.



The Enable Certificate Templates window appears.

14. Select the new template created in step On the General tab, fill in the template name, validity period and renewal period according to your specific requirements. on page 633 and click OK.



The new custom template is now installed on the local certificate authority (CA).

15. Once the custom template installed, you can proceed to Requesting a client certificate on page 635 to create client certificates, or Downloading a CA certificate for FortiMail on page 641 to configure FortiMail.

Requesting a client certificate

Use this procedure to request a client certificate using the Microsoft Certificate Services (MSCS) web enrollment tool.

A client certificate is a digitally-signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key.

Certificates are generally used to establish identity and create trusts for the secure exchange of information. Therefore, certification authorities (CAs) can issue certificates to people, such as FortiMail end-users, and to devices, such as the FortiMail unit itself when acting as a client of an SMTP mail server.

The entity that receives the certificate is the **subject** of the certificate. The issuer and signer of the certificate is a certification authority (CA).

Typically, certificates contain the following information:

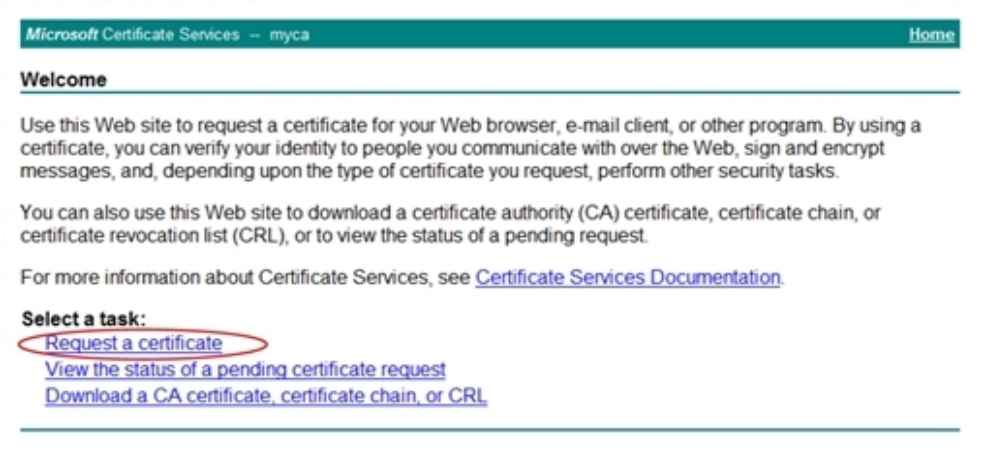
- The subject's public key value.
- The subject's identifier information, such as the name and e-mail address.
- The validity period (the length of time that the certificate is considered valid).
- Issuer identifier information.
- The digital signature of the issuer, which attests to the validity of the binding between the subject's public key and the subject's identifier information.

Every certificate contains Valid From and Valid To dates, which set the boundaries of the validity period. Once a certificate's validity period has passed, a new certificate must be requested by the subject of the now-expired certificate.

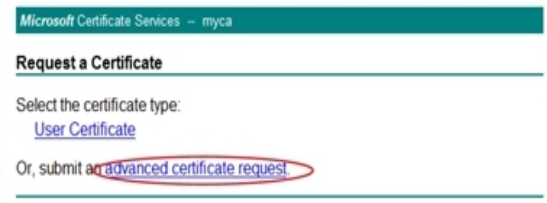
This document assumes all certificates are requested by the administrator on behalf of end-users. Certificate creation by individual end-users is beyond the scope of this document. If end users are permitted to create their own certificates, refer to the documentation accompanying the tools used by the end-user to create their own certificates.

To create a client certificate

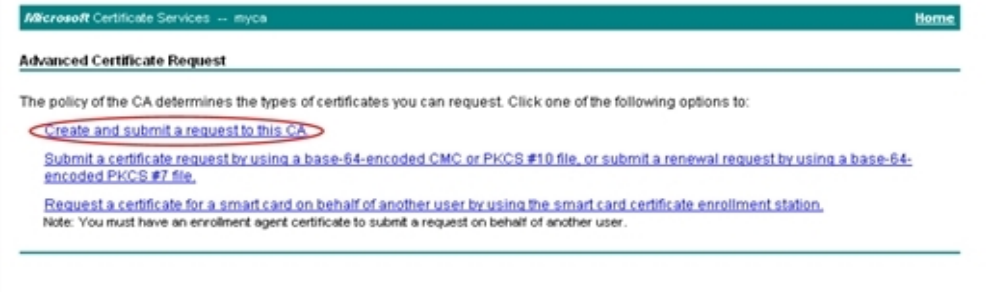
1. Open your web browser and enter the following in the address bar:
   `http://<ip_of_your_ms_ca_server>/certsrv/`
   Where `<ip_of_your_ms_ca_server>` is the IP address of the Windows 2003 Server that hosts the local Certification Authority (CA).
2. Log in to the CA server as administrator.
   The Microsoft Certificate Services home page for your local CA appears.



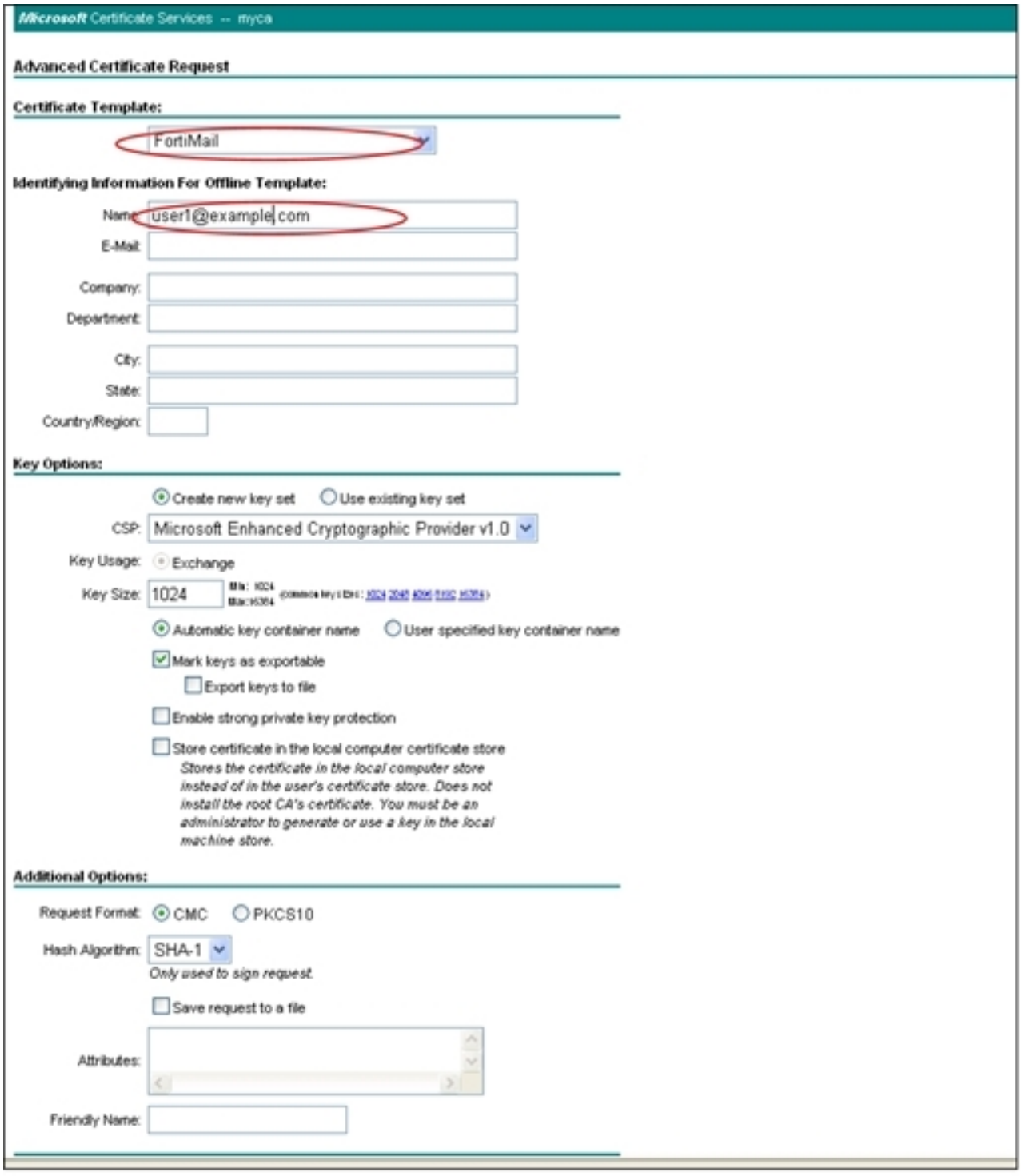
3. Select the Request a certificate link.
   The Request a Certificate page appears.



4. Click the Advanced certificate request link.
   The Advanced Certificate Request page appears.



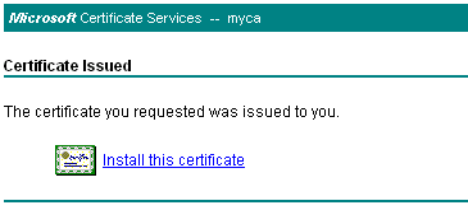
5. Click Create and Submit a request to this CA link.
   The Certificate Request Template appears.



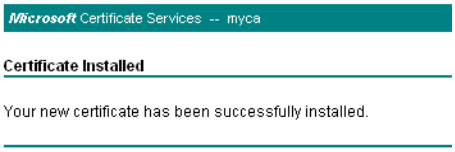
6. In the Certificate Template dropdown list, select the new template created in Creating a custom certificate request template using MMC on page 632.
7. Fill in the Name field with the **email address** of the end-user (subject) on behalf of which the client certificate request is being made.

For the purposes of FortiMail, the Name field must exactly match the **email address** of the end-user recorded in the FortiMail unit. For more information, see Creating email accounts on FortiMail for PKI users on page 643.
If desired, the full name of the user can be entered in the Friendly Name field.

8. Click Submit to send a certificate signature request (CSR) to the CA server on behalf of the end-user.
9. If a message appears, warning you that the Website is requesting a new certification on your behalf, click Yes to proceed.
   Once the CA server completes processing the request, the Certificate Issued window appears.



10. Click the Install this certificate link to load the certificate into the certificate store on your browser.
11. If a message appears, warning you that the web site is adding one or more certificates to your computer, click Yes to proceed.
    The Certificate Installed window appears.



    The client certificate is now stored in certificate store on your browser. The certificate is stored with the name specified in steps Fill in the Name field with the email address of the end-user (subject) on behalf of which the client certificate request is being made. on page 637.
12. Return to the Microsoft Certificate Services (MSCS) home page for your local CA and repeat steps Select the Request a certificate link. on page 636 through If a message appears, warning you that the web site is adding one or more certificates to your computer, click Yes to proceed. on page 638 for each end-user that will communicate with FortiMail using PKI authentication.
13. Proceed to Exporting a client certificate on page 638 to export and transmit the client certificate to the end-user.

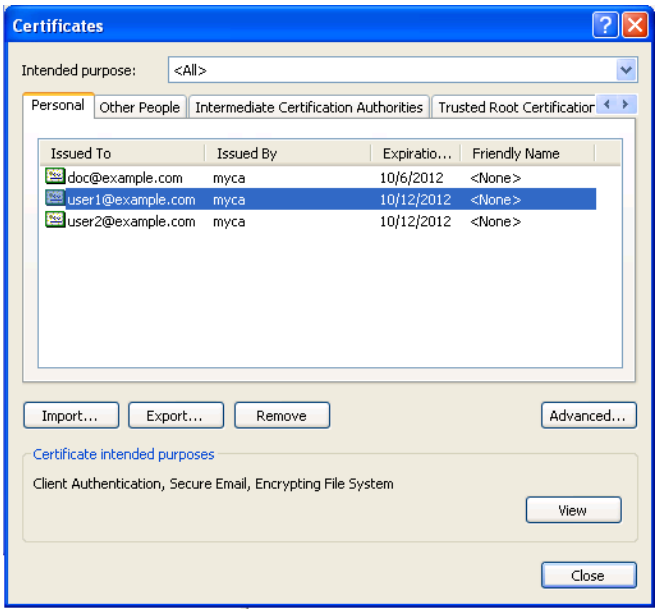
Exporting a client certificate

Use this procedure to export and transmit a client certificate created in Requesting a client certificate on page 635 to the appropriate end-user.

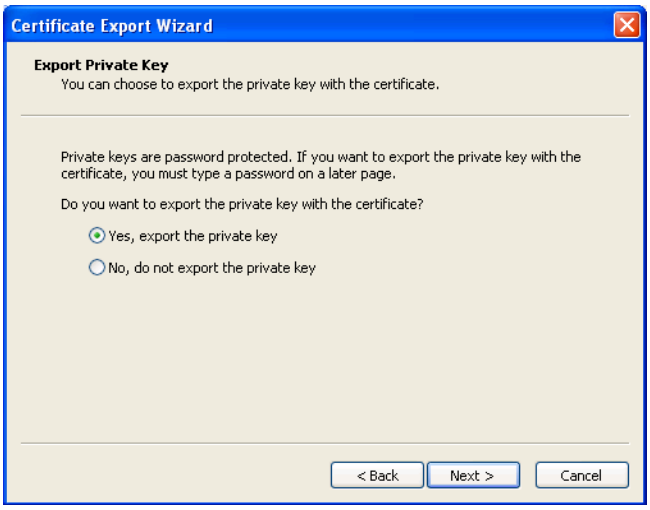
The client certificate must reside in the certificate store of the end-user computer before the end-user can connect to the FortiMail unit using PKI authentication.

To export and transmit the client certificate

1. Open your browser, and select Tools > Internet Options > Content > Certificates.
   The Certificates window appears.
2. Select the Personal tab to display a list of the client certificates created in Requesting a client certificate on page 635.



3. Select a client certificate from the list and click Export to export the certificate.
   The Certificate Export Wizard welcome page appears.
4. Click Next to continue from the Certificate Export welcome page.
   The Export Private Key window appears.



You must export the private key at the same time as the certificate. The private key is associated with a specific end-user, and contains information used by the certification authority to authenticate the end-user. Private keys must be password protected, and must be securely transmitted to end-users.

5. Select Yes, export the private key and select Next.
   The Export File Format window appears.
6. Select Personal Information Exchange - PKCS #12 (.PFX) as the file format.
7. Select Enable strong protection for the password and select Next.
   The Password selection window appears.

8. Enter and confirm a password for the certificate and select Next.
   The File name window appears.
9. Enter a unique file name for the certificate and browse to the location where you want to save the exported certificate and private key.

   For clarity, a consistent naming convention should be used for client certificate names, email account names, PKI user names and recipient base policy names. This will help associate specific users with the various components of PKI authentication.

10. When Completing Certificate Export Wizard appears, click Finish to export the certificate and private key to the location specified in step Enter a unique file name for the certificate and browse to the location where you want to save the exported certificate and private key. on page 640.
    The certificate and private key are exported to the specified location as a single file with a .pfx extension.
11. Transmit the certificate .pfx file to the end-user, along with instructions on what the user has to do to install the certificate on their web browser.
12. Proceed to Importing a client certificate to an end-user browser on page 640 to import the certificate .pfx file on the end-user browser.

Importing a client certificate to an end-user browser

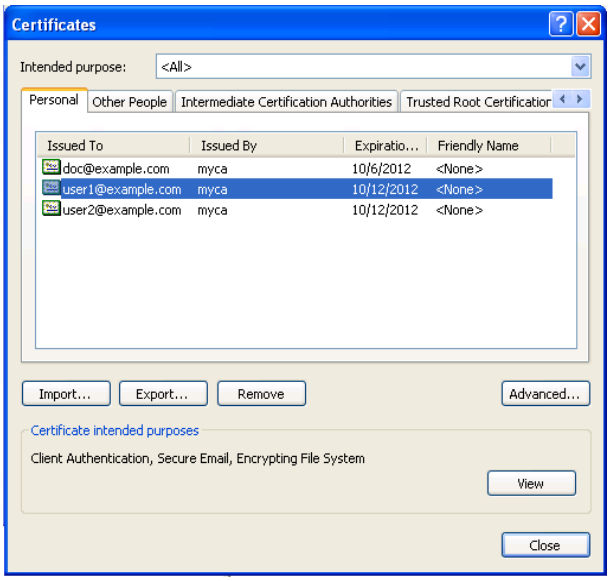
Use this procedure to import the client certificate into the end-user browser. The certificate is transmitted from the administrator in a .pfx file, using the procedure Exporting a client certificate on page 638.

The following is a generic procedure for importing a certificate into a browser. You must provide the end-user with specific instructions for importing the certificate according to browser type/version and local operating procedures.

To import a client certificate into Internet Explorer

1. Retrieve the .pfx file that was transmitted to the end-user from the administrator and store the file in a folder that is accessible from the end-user computer.

2. Open an IE browser on the end-user computer, and select Tools > Internet Options > Content > Certificates and select the Personal tab.
   The Certificates window appears.



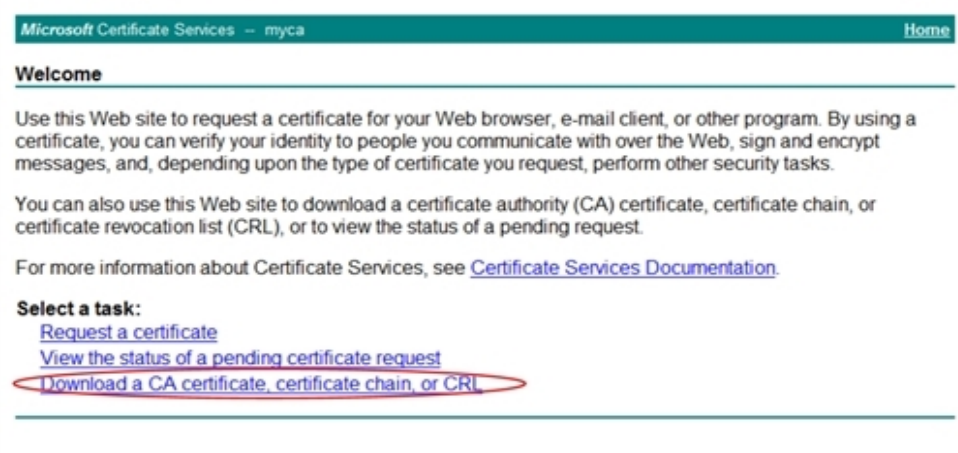
3. Open the Personal tab and select Import.
   The Certificate Import Wizard welcome page appears.
4. Click Next to continue from the Certificate Import welcome page.
   The File to Import window appears.
5. Select Browse and ensure that the Files of type is set to Personal Information Exchange (*.pfx, *.p12), or All Files (*.*), or whatever file format was used to export the certificate in Exporting a client certificate on page 638.
6. Browse to the location on the end-user computer where the .pfx file is stored, select the certificate file and select Open.
7. The path to the certificate location appears in the File to Import window. Select Next.
   The Password window appears.
8. Type the password supplied by the administrator that is used to retrieve the private key and select Next.
   The Certificate Store window appears.
9. Select the Place all certificates in the following store button, browse to the Personal Certificate Store and select Next.
10. When Completing Certificate Import Wizard appears, click Finish to import the certificate and private key to the location specified in step Select the Place all certificates in the following store button, browse to the Personal Certificate Store and select Next. on page 641.
    The certificate and private key are now imported to the Personal certificate store in the end-user browser. The browser is now has the appropriate client certificate for PKI authentication on the FortiMail unit.
11. Proceed to Creating email accounts on FortiMail for PKI users on page 643.

Downloading a CA certificate for FortiMail

Use this procedure to download a CA certificate from your CA server to your local certificate store. The CA certificate will then be imported to FortiMail and used as part of the client authentication process when end-users connect to FortiMail.

To download a CA certificate

1. Open your web browser and enter the following in the address bar:
   `http://<ip_of_your_ms_ca_server>/certsrv/`
   Where `<ip_of_your_ms_ca_server>` is the IP address of the Windows 2003 Server that hosts the local Certification Authority (CA).
2. Log in to the CA server as administrator.
   The Microsoft Certificate Services (MSCS) home page for your local CA appears.



3. Select the Download CA certificate link.
   The Download a CA Certificate page appears.

4. Select Base64 as the CA certificate encoding method.
5. Click Download CA certificate and choose a location to save the CA certificate.
6. Proceed to Importing a CA certificate to FortiMail on page 642 to import the CA certificate into the FortiMail unit.

Importing a CA certificate to FortiMail

Use this procedure to import a CA certificate that was downloaded in Downloading a CA certificate for FortiMail on page 641.

Use the FortiMail GUI and the following procedure to import the CA certificate.

1. From *System* > *Certificate* > *CA Certificate*, select the Import button.

Creating email accounts on FortiMail for PKI users

An email account must exist on the FortiMail unit for each PKI user. End-users cannot be authenticated using PKI if their email accounts do not exist on FortiMail, even if they have the required client certificate installed in their browsers.

The FortiMail operation mode determines whether end user email accounts are created automatically by FortiMail (transparent and gateway modes) or whether the end-user accounts need to be created manually on FortiMail (server mode).

If the FortiMail units is operating in server mode, see Configuring local user accounts (server mode only) on page 297 to manually create end-user email accounts.

If the FortiMail unit is operating in gateway or transparent mode, the FortiMail unit can be configured to store quarantined (spam) email. In this configuration, email accounts are created automatically on the FortiMail unit when it receives quarantined email. The quarantined email is stored in a bulk folder on the FortiMail unit. The email user can review, delete or release their quarantined email. For more information, see Managing the quarantines on page 120.

Once the email accounts are created on FortiMail, proceed to Configuring PKI authentication on page 304.

A PKI user can be either an individual email user, all email users associated with a specific domain, or a FortiMail administrator.

If PKI authentication is used for email users and for FortiMail administrators, ensure that unique PKI users are created for the administrator accounts, and those PKI users are associated with the appropriate administrator accounts. For more information, see Configuring PKI access for administrators on page 645.

Failure to create unique PKI users for administrators could result in email user access to administrator functions.

Once the PKI user is created on FortiMail, proceed to Configuring policy for PKI access to webmail (server mode) on page 643.

Configuring policy for PKI access to webmail (server mode)

Use this procedure to configure a recipient based policy for email access using PKI authentication.

This procedure applies only if the FortiMail unit is operating in **server** mode. In server mode, PKI users can access all email, including quarantine email, stored on the FortiMail unit.

If the FortiMail unit is operating in transparent or gateway mode, see Configuring policies for PKI access to email quarantine (transparent and gateway mode) on page 644.

1. Ensure that the CA certificate has been imported to the FortiMail unit. For more information, see Importing a CA certificate to FortiMail on page 642.
2. Create a PKI user for each webmail user that requires access to regular email residing on the FortiMail unit (server mode). For more information, see Configuring PKI authentication on page 304.

3. From *Policy* > *Recipient Policy*, select New to create a new recipient based policy, or Edit to change an existing policy. For more information on recipient base policies, see Controlling email based on sender and recipient addresses on page 354.
4. In the recipient based policy, expand Advanced Setting and configure the following:
   - Ensure the Enable PKI authentication for webmail access is enabled.
   - If desired, select a PKI user name from the dropdown list.

   Ensure the PKI user is appropriate for the selected recipient. Choosing the wrong PKI user could result in email user access to administrator functions. For more information, see Configuring PKI authentication on page 304.

   - Ensure Certificate validation is mandatory is enabled. This will enforce PKI authentication for the specified PKI user.
5. Repeat steps From Policy > Recipient Policy, select New to create a new recipient based policy, or Edit to change an existing policy. For more information on recipient base policies, see Controlling email based on sender and recipient addresses on page 353. on page 644 and In the recipient based policy, expand Advanced Setting and configure the following: on page 644 for each webmail PKI user.
6. If there are quarantine email PKI users to add, proceed to Configuring policies for PKI access to email quarantine (transparent and gateway mode) on page 644. Otherwise, proceed to Configuring PKI access for administrators on page 645.

Configuring policies for PKI access to email quarantine (transparent and gateway mode)

Use this procedure to configure a recipient-based policy for quarantine (spam) email access using PKI authentication.

This procedure applies only if the FortiMail unit is operating in **gateway or transparent** modes. In gateway or transparent mode, the FortiMail unit can be configured to store regular email on an SMTP server and quarantine email in a bulk folder on the FortiMail unit. From the end-user perspective, connection to the regular email folders and bulk (quarantine) email folder is seamless, but the folders actually reside on two separate servers.

For more information on storing quarantine email on FortiMail, see Managing the quarantines on page 120.

To configure access to email quarantine using PKI

1. Ensure that the CA certificate has been imported to the FortiMail unit. For more information, see Importing a CA certificate to FortiMail on page 642.
2. Create a PKI user for each email user that requires access to quarantine email. For more information, see Configuring PKI authentication on page 304.
3. From *Policy* > *Recipient Policy*, select New to create a new recipient based policy for quarantined email or Edit to change an existing policy. For more information on recipient base policies, see Controlling email based on sender and recipient addresses on page 354.
4. Expand Advanced Setting and configure the following:
   - Ensure the Enable PKI authentication for webmail access is enabled.
   - If desired, select a PKI user name from the dropdown list.

   Ensure the PKI user is appropriate for the selected recipient. Choosing the wrong PKI user could result in email user access to administrator functions.

- Ensure Certificate validation is mandatory is enabled. This will enforce PKI authentication for the specified PKI user.

5. Repeat steps From Policy > Recipient Policy, select New to create a new recipient based policy for quarantined email or Edit to change an existing policy. For more information on recipient base policies, see Controlling email based on sender and recipient addresses on page 353. on page 644 and Expand Advanced Setting and configure the following: on page 644 for each PKI user that requires access to quarantine email.
6. Proceed to Configuring PKI access for administrators on page 645

Configuring PKI access for administrators

Use this procedure to configure PKI authentication for administrative access to the FortiMail unit. This procedure applies only to administrators, and can be used if the FortiMail unit is operating **server, transparent or gateway** mode.

1. Ensure that the CA certificate has been imported to the FortiMail unit. For more information, see Importing a CA certificate to FortiMail on page 642.
2. Create a PKI user for each administrator that requires to access FortiMail administrative functions. For more information, see Configuring PKI authentication on page 304.
3. From System > Administrator, select an existing administrator or create a new administrator account for which PKI authentication will be used. For more information, see Configuring administrator accounts and access profiles on page 165.
4. In the Administer window, configure the following:
   - Select PKI from the Auth type dropdown list.
   - Select the appropriate PKI user name from the PKI user dropdown list.
5. Repeat steps From System > Administrator, select an existing administrator or create a new administrator account for which PKI authentication will be used. For more information, see Configuring administrator accounts and access profiles on page 165. on page 645 and In the Administer window, configure the following: on page 645 for each administrative PKI user.
6. Return to the Enabling PKI authentication globally with CLI on page 645.

Enabling PKI authentication globally with CLI

Use this procedure to enable PKI authentication globally. PKI authentication is enabled globally using the command line interface (CLI). Using CLI ensure that PKI authentication is enabled for all domains.

For more information on CLI commands, see the FortiMail CLI Reference.

To enable PKI authentication with CLI

1. Open a CLI session on the FortiMail unit.
2. Enter the following CLI commands:

```
config system global
   set pki-mode enable
end
```

PKI authentication is now enabled for all designated users (email and administrator) and domains.

From this point forward, when email users access their webmail, or when administrators connect to the FortiMail unit, they will be prompted to confirm their client certificate when connecting to FortiMail.

Proceed to Testing PKI authentication on page 646 to validate that PKI authentication is working properly.

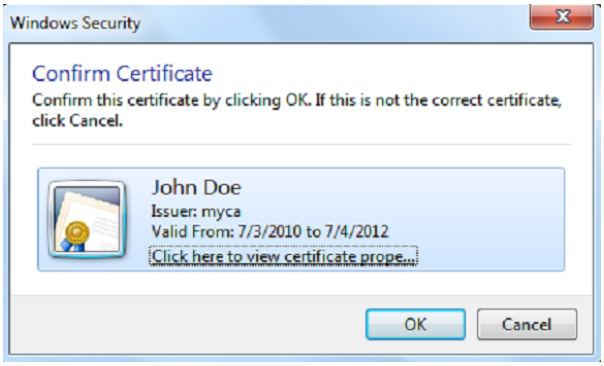
Testing PKI authentication

Comment: Procedure is based on original Webmail PKI Tech Note, Appendix steps 7.

Use this procedure to test whether PKI authentication is working properly.

To test PKI authentication

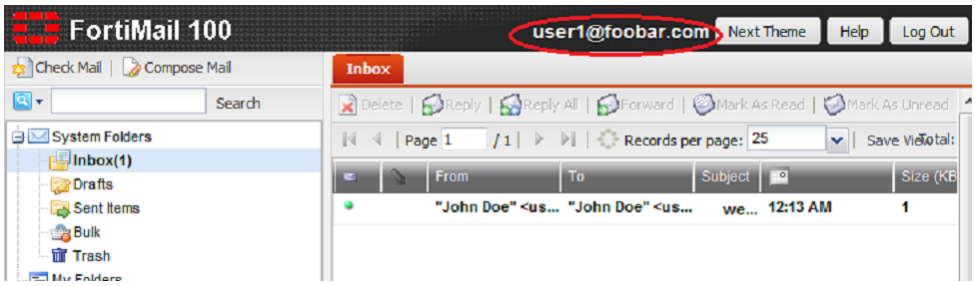
1. From a client browser that has been configured for PKI authentication, enter the URL of the webmail server.
2. Verify that a Confirm Certificate prompt appears.



3. If the Confirm Certificate prompt appears, select OK and go to step The user is automatically logged on. The FortiMail webmail account and all appropriate folder appear in their browser. on page 646.
   If the certificate confirmation prompt does not appears, it might be because the FortiMail HHTP server has not yet loaded the new settings. Enter the following CLI command to manually enforce a reload of the configuration.

   ```
   execute reload
   ```

4. Return to step From a client browser that has been configured for PKI authentication, enter the URL of the webmail server. on page 646 and try the URL again.
5. The user is automatically logged on. The FortiMail webmail account and all appropriate folder appear in their browser.



This confirms that the certificate bound to the end-user browser is valid, and that PKI authentication is working properly.

All users and administrators configured for PKI authentication can now log in to FortiMail without password.

www.fortinet.com