FortiMail Administration Guide

Version 6.0.6

FortiMail 6.0.6 Administration Guide

August 7, 2019

2nd Edition

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of contents

Concepts and workflow 6
- Email protocols 6
- Client-server connections in SMTP 8
- The role of DNS in email delivery 9
- How FortiMail processes email 12
- FortiMail operation modes 24
- FortiMail high availability modes 24
- FortiMail management methods 25

Setting up the system 26
- Connecting to the Web UI or CLI 26
- Choosing the operation mode 34
- Running the Quick Start Wizard 39
- Connecting to FortiGuard services 44
- Gateway mode deployment 46
- Transparent mode deployment 72
- Server mode deployment 94
- Testing the installation 114
- Backing up the configuration 126

Using the dashboard 128
- Viewing the dashboard 128
- Using the CLI Console 128

Using FortiView 129
- Viewing mail statistics 129
- View threat statistics 129
- Viewing top user statistics 129
- Viewing current IP sessions 130

Monitoring the system 131
- Viewing log messages 131
- Managing the quarantines 137
- Managing the mail queue 144
- Viewing the greylist statuses 147
- Viewing sender, authentication and endpoint reputation 151
- Managing archived email 156
- Viewing generated reports 158

Configuring system settings 160
- Configuring network settings 160

Configuring administrator accounts and access profiles 179
Configuring system time, options, and other system options 185
Configuring mail settings 195
Customizing GUI, replacement messages and email templates 218
Configuring RAID 230
Using high availability (HA) 236
Managing certificates 275
Using FortiSandbox antivirus inspection 285
Configuring FortiGuard services 287
System maintenance 295

Configuring domains and users 307

Configuring protected domains 307
Managing users 325
Configuring user aliases 337
Configuring address mappings 339
Configuring IBE users 341
Managing the address book (server mode only) 346
Sharing calendars and address books (server mode only) 351
Migrating email from other mail servers (server mode only) 356

Configuring policies 359

What is a policy? 359
How to use policies 360
Controlling SMTP access and delivery 362
Controlling email based on IP addresses 375
Controlling email based on sender and recipient addresses 381

Configuring profiles 389

Configuring session profiles 389
Configuring antispam profiles and antispam action profiles 407
Configuring antivirus profiles and antivirus action profiles 425
Configuring content profiles and content action profiles 430
Configuring resource profiles 443
Workflow to enable and configure authentication of email users 445
Configuring authentication profiles 446
Configuring LDAP profiles 450
Configuring dictionary profiles 479
Configuring security profiles 483
Configuring IP pools 488
Configuring email and IP groups 490
Configuring notification profiles 491

Configuring security settings ... **493**
Configuring authentication reputation ... 493
Configuring email quarantines and quarantine reports ... 494
Configuring the block lists and safe lists ... 504
Configuring greylisting ... 512
Configuring the URL exempt list ... 523
Configuring bounce verification and tagging ... 523
Configuring endpoint reputation ... 527
Training and maintaining the Bayesian databases ... 531
Adding file signatures ... 540
Configuring action profile preferences ... 541
Configuring adult image analysis ... 541
Configuring encryption settings ... **543**
Configuring IBE encryption ... 543
Configuring certificate bindings ... 547
Configuring data loss prevention ... **551**
DLP configuration workflow ... 551
Defining the sensitive data ... 551
Configuring DLP rules ... 553
Configuring DLP profiles ... 553
Archiving email ... **555**
Email archiving workflow ... 555
Configuring email archiving accounts ... 555
Configuring email archiving policies ... 559
Configuring email archiving exemptions ... 560
Logs, reports and alerts ... **562**
About FortiMail logging ... 562
Configuring logging ... 569
Configuring report profiles and generating reports ... 572
Configuring alert email ... 575
Installing firmware ... **578**
Testing firmware before installing it ... 578
Installing firmware ... 580
Clean installing firmware ... 585
Upgrading firmware on HA units ... 587
Best practices and fine tuning ... **589**
General security tuning ... 589
System security tuning ... 590
Network topology tuning ... 590
High availability (HA) tuning ... 591

SMTP connectivity tuning ... 592
Antispam tuning ... 592
Policy tuning ... 593
System maintenance tips ... 594
Performance tuning ... 594
Troubleshooting ... 596
Establish a system baseline ... 596
Define the problem ... 597
Search for a known solution ... 597
Create a troubleshooting plan ... 598
Gather system information ... 598
Troubleshoot hardware issues ... 599
Troubleshoot GUI and CLI connection issues ... 599
Troubleshoot FortiGuard connection issues ... 600
Troubleshoot MTA issues ... 602
Troubleshoot antispam issues ... 605
Troubleshoot HA issues ... 607
Troubleshoot resource issues ... 608
Troubleshoot bootup issues ... 608
Troubleshoot installation issues ... 610
Contact Fortinet customer support for assistance ... 610
Setup for email users ... 612
Training Bayesian databases ... 612
Managing tagged spam ... 613
Accessing the personal quarantine and webmail ... 613
Sending email from an email client (gateway and transparent mode) ... 616
Appendix A: Supported RFCs ... 618
Appendix B: Maximum Values ... 621
Appendix C: Port Numbers ... 622
Appendix D: Regular expressions ... 623
Special characters with regular expressions and wild cards ... 623
Case sensitivity ... 623
Modifiers ... 623
Word boundary ... 624
Syntax ... 624
Examples ... 625
Appendix E: Working with TLS/SSL ... 626
About TLS/SSL ... 626
How TLS/SSL works ... 626
FortiMail support of TLS/SSL ... 628

Troubleshooting FortiMail TLS issues 630
Appendix F: PKI Authentication 634
Introduction to PKI authentication 634
FortiMail PKI architecture 635
Configuring PKI authentication on FortiMail 636
Index 654

Concepts and 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.

This section includes:

- Email protocols
- Client-server connections in SMTP
- The role of DNS in email delivery
- How FortiMail processes email
- FortiMail operation modes
- FortiMail high availability modes
- FortiMail management methods

Email protocols

There are multiple prevalent standard email protocols:

- SMTP
- POP3
- IMAP
- HTTP and HTTPS

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 8.

SMTP communications typically occur on TCP port number 25.

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, multipart 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.

POP3 communications typically occur on TCP port number 110.

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, but may use POP3 when operating in server mode, when an email user retrieves their email.

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.

IMAP communications typically occur on TCP port number 143.

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 strictly for the transport of email, are often used by webmail applications to view email that is stored remotely.

HTTP communications typically occur on TCP port number 80; HTTPS communications typically occur on TCP port number 443.

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.

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.

In order to deliver email, unless the email is incoming and the email server has no domain name and is accessed by IP address only, MTAs must query a DNS server for the MX record and the corresponding A record. For more information, see "The role of DNS in email delivery" on page 9.

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 vs email directionality

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

- **Incoming vs outgoing SMTP connections**

  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.

Figure 1: Incoming versus outgoing SMTP connections

- **Incoming vs 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.

The role of DNS 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 FortiMail high availability (HA) instead. For details, see "FortiMail high availability modes" on page 24.

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

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 359. For information about profiles, see "Configuring profiles" on page 389.

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

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 email that is incoming to or outbound from protected domains.

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 307.

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. For information on configuring the SMTP greeting, see "Configuring protected domains" on page 307.

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 rules" on page 363.

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 307.

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 "Customizing replacement messages" on page 218.

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 227.

Advanced delivery features

Processing email takes time. That can cause delays that result in client and server timeouts. 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)

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 389 and "Configuring security settings" on page 493.

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 16.

Table 1: FortiMail antispam technique highlights

Greylist scanning	See "Configuring greylisting" on page 512.
DNSBL scanning	In addition to supporting Fortinet's FortiGuard Antispam DNSBL service, the FortiMail unit supports third-party DNS Blocklist servers. See "Configuring SURBL options" on page 414.
SURBL scanning	In addition to supporting Fortinet's FortiGuard Antispam SURBL service, the FortiMail unit supports third-party Spam URI Realtime Block Lists servers. See "Configuring SURBL options" on page 414.
Bayesian scanning	See "Training the Bayesian databases" on page 533.
Heuristic scanning	See "Configuring heuristic options" on page 413.
Image spam scanning	See "Configuring image spam options" on page 417.
PDF scanning	See "Configuring scan conditions" on page 419.
Block/safe lists	• For information on global block/safe lists, see "Configuring the global block and safe list" on page 506. • For information on domain-wide block/safe lists, see "Configuring the per-domain block lists and safe lists" on page 508. • For information on personal block/safe lists, see "Configuring the personal block lists and safe lists" on page 510. • For information on session block/safe lists, see "Click the arrow to expand Lists." on page 404.
Banned word scanning	See "Configuring banned word options" on page 415.
Safe list word scanning	See "Configuring safelist word options" on page 416.
Sender reputation	See "Viewing sender reputation statuses" on page 151.

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 (URI) contained in the message body – commonly known as Spam URI Realtime 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 URIs (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 (URI) 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 in the following sequence, from the top of the table towards the bottom. Disabled scans are skipped. Note that is this only a general sequence and the actions are taken 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 non-antispam functions 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.

The PDF file type scan does not appear in this table. When enabled, the PDF file type converts the first page of any PDF attachments into to a format 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 below.

Table 2: Execution sequence of antispam techniques

Check	Check Involves	Action If Positive	Action If Negative
Client initiates communication with the FortiMail unit			

Table 2: Execution sequence of antispam techniques

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 the “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			
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.

Table 2: Execution sequence of antispam techniques

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.
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.
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.
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.

Table 2: Execution sequence of antispam techniques

Access control rules	Client IP address, envelope sender and recipient (`MAIL FROM:` and `RCPT TO:`)	If the combination of client IP, the domain/email address of the sender, and the domain/email of the recipient matches an access control rule (*Policy* > *Access Control* > *Receive*), the FortiMail unit performs the action selected in the access control rule, which is one of the following: • *Safe*: Accept and relay the email, skipping all subsequent antispam checks, ***except greylisting***, **only if** the recipient belongs to a protected domain or the sender is authenticated. • *Safe & Relay*: Accept and relay the email, skipping all subsequent antispam checks. • *RELAY*: Accept and relay the email if it passes subsequent antispam checks. ***Do not apply greylisting.*** • *REJECT*: Reject the email and return SMTP reply code 550 to the client. • *DISCARD*: Accept the email, but silently delete it instead of delivering it. Neither the sender nor the recipient are notified of the deletion.	If a matching access control rule does not exist, and if the recipient is a member of a protected domain, the default action is *RELAY*; if the recipient is not a member of a protected domain, the default action is *REJECT*. For more information, see "Configuring access control rules" on page 363.
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 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.

Table 2: Execution sequence of antispam techniques

Recipient verification	Envelope recipient (`RCPT TO:`)	If the recipient is unknown, reject the message.	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.
DATA command received from SMTP client			
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.

Table 2: Execution sequence of antispam techniques

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			
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.	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.

Table 2: Execution sequence of antispam techniques

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.
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 analysis	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 URI 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.

Table 2: Execution sequence of antispam techniques

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.
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 or quarantined.

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 or quarantined.

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.

FortiMail high availability modes

FortiMail units can be configured to operate in high availability (HA) clusters. FortiMail HA has two modes: active-passive and config-only.

- **Active-passive HA**: Two FortiMail units operate as an HA cluster, synchronizing both configuration and data, providing failover protection.
- **Config-only HA**: Up to 25 FortiMail units use an identical configuration, but do not synchronize data, and therefore operate as independent FortiMail units.

Fortinet recommends HA to achieve uninterrupted service.

For more information on HA, see “Using high availability (HA)” on page 236.

FortiMail management methods

After you install the FortiMail unit, you can configure and manage it with either of:

- the web-based manager
- and/or the 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 179.

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 186.

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

Basic mode versus advanced mode

The web UI enables you to configure the FortiMail unit by connecting to the FortiMail unit through a web browser. The web UI 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 pre-defined 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 web UI 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 web UI.

Setting up the system

These instructions in this chapter will guide you to the point where you have a simple, verifiably working installation. From there, you can begin to use optional features and fine-tune your configuration.

FortiMail initial setup involves the following steps:

- Connecting to the Web UI or CLI
- Choosing the operation mode
- Running the Quick Start Wizard
- Connecting to FortiGuard services
- Gateway mode deployment
- Transparent mode deployment
- Server mode deployment
- Testing the installation
- Backing up the configuration

Connecting to the Web UI or CLI

To configure, maintain, and administer the FortiMail unit, you need to connect to it. There are three methods for these tasks:

- using the web UI, a graphical user interface (GUI), from within a current web browser (see "Connecting to the FortiMail web UI for the first time")
- using the 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 28)
- using the 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 33).

Connecting to the FortiMail web UI for the first time

To use the web UI for the initial configuration, you must have:

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

Table 3: Default settings for connecting to the web UI

Network Interface	port1
URL	https://192.168.1.99/admin

Table 3: Default settings for connecting to the web UI

Administrator Account	admin
Password	(none)

To connect to the web UI

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

   For example, in Microsoft Windows 7, from the Windows Start menu, go to *Control Panel* > *Network and Sharing Center* > *Change Adapter Settings* > *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 URLhttps://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 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`.

   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 web UI appears.

To log out from the web UI

- Click the *Log Out* button at the upper right corner of the web UI.

Connecting to the FortiMail CLI for the first time

For the initial configuration, you can access the CLI from your management computer using either of these two ways:

- **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.

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.

Before you can access the CLI through the network, you usually must enable SSH and/or Telnet on the network interface through which you will access the CLI.

This section includes:

- Local console connection and initial configuration
- Enabling access to the CLI through the network (SSH or Telnet)
- Connecting to the CLI using SSH
- Connecting to the CLI using Telnet
- Logging out from the CLI console

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
- the RJ-45-to-DB-9 or null modem cable included in your FortiMail package
- 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 null modem or RJ-45-to-DB-9 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 the following text, followed by a command line prompt:

   `Welcome!`

Initial configurations with CLI

Once you've physically connected your computer to the FortiMail unit, you can configure the basic FortiMail system settings through the CLI. For more information on other CLI commands, see the FortiMail CLI Guide.

To change the admin password:

```
config system admin
    edit <admin_name>
        set password <new_password>
end
```

To change the operation mode:

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

To configure the interface IP address:

```
config system interface
    edit <interface_name>
          set <ip_address>
end
```

To configure the system route/gateway:

```
config system route
    edit <route_int>
        set destination <destination_ip4mask>
        set gateway <gateway_ipv4>
        set interface <interface_name>
end
```

To configure the DNS servers:

```
config system dns
    set primary <ipv4_address>
    set secondary <ipv4_ address>
end
```

To configure the NTP time synchronization:

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

To configure the SNMP v3 user settings:

```
config system snmp user
    edit <user_name>
        set query-status {enable | disable}
        set query-port <port_number>
        set security-level {authnopriv | authpriv | no authnopriv}
        set auth-proto {sha1 | md5}
        set aut-pwd <password>
        set status {enable | disable}
        set trap-status {enable | disable}
        set trapevent {cpu | deferred-queue | ha | ip-change | logdisk
         | mem | raid | remote-storage | spam | system | virus}
        set trapport-local <port_number>
        set trapport-remote <port_number>
    config host
        edit <host_no>
          set ip <class_ip>
    end
end
```

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

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.

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.

You can do this using either:

- a local console connection (see the following procedure)
- the web-based manager

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as PuTTY
- the RJ-45-to-DB-9 or null modem cable included in your FortiMail package
- a network cable
- prior configuration of the operating mode, network interface, and static route

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.
3. Using a local console connection, connect and log into the CLI. For details, see "Local console connection and initial configuration" on page 28.
4. Enter the following commands:

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

where:

- `<interface_str>` is the name of the network interface associated with the physical network port, such as `port1`
- `{aggregator http https ping ssh telnet webservice}` 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, and Telnet, and allow only HTTPS, ICMP ECHO (ping), and SSH administrative access on `port1`:

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

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

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 32 or "Connecting to the CLI using Telnet" on page 33.

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 or not you have enabled FIPS-CC mode, but generally include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a FortiMail network interface configured to accept SSH connections (see "Enabling access to the CLI through the network (SSH or Telnet)" on page 30)
- 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 30)
- 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

No matter how you connect to the FortiMail CLI console (direct console connection, SSH, or Telnet), to exit the console, enter the *Exit* command.

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:

- IP addresses and netmasks for each of the network interfaces
- the default gateway
- the 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 web UI to complete additional setup. To continue, see "Connecting to the FortiMail web UI for the first time" on page 26.

Choosing the operation mode

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

FortiMail units can run in one of three operation modes: gateway mode, transparent mode, or server mode. Requirements of each operation mode vary.

Table 4: 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.

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
- Characteristics of gateway mode
- Characteristics of transparent mode
- Characteristics of server mode
- Changing the operation mode

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 combatting 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.

Figure 2: 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 46.

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.

Figure 3: 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 72.

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.

Figure 4: 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 94.

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 web UI. (See "Connecting to the FortiMail web UI for the first time".)
2. In the *System Information* widget on the dashboard, select either *Gateway*, *Server*, or *Transparent* from the *Operation mode* drop-down 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 web UI appears.

Do not change the operation mode once you have committed resources to configuring FortiMail. Changing the operation mode resets most configurations 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 al settings configured by the Quick Start Wizard can also be configured through the standard and advanced modes of the web UI, 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 web UI.

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
- Step 1: Time Settings
- Step 2: Network Settings
- Step 3: Local Host Settings
- Step 4: Edit Administrator Password
- Step 5: Operation Mode
- Step 6: Domain Configuration
- Step 7: Policy Settings
- Step 8: Reviewing and saving the configuration
- Continuing the installation

Starting the wizard

Open the web UI in a browser.

In either standard mode or advanced mode, select *Wizard* from the dropdown list in the top right corner of the web UI.

Select *OK* when prompted to continue. The first page of the wizard appears in a new window over the web UI. You cannot access the web UI 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, and if the FortiMail unit uses the same domain name as your mail server, it may become difficult to distinguish email messages that originate from the FortiMail unit.

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 web UI, 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 usually 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 83.

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 46 (gateway mode) or "Configuring DNS records" on page 94 (transparent mode).
SMTP server (gateway mode only)	Enter the fully qualified domain name (FQDN) or IP address of the primary SMTP server for this protected domain, then also configure *Port*. 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. The default SMTP port number is 25.
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*.

None of the settings you made on the wizard take effect until you click *OK* on the final page.

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 236
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 44.
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 114.

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 web UI.
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.

   Figure 5: DNS error when resolving the FortiGuard Antispam domain name

   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.

Figure 6: Connection error when verifying FortiGuard Antispam rating query connectivity

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 46, "Transparent mode deployment" on page 72, or "Server mode deployment" on page 94.)

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 and Report* > *Log Settings* > *Local Log Settings* in the advanced mode of the web UI. 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.
```

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 use push updates or manually initiate updates as alternatives or in conjunction with scheduled updates. If protection from the latest viral threats is a high priority, you could configure both scheduled updates and push updates, using scheduled updates as a failover method to increase the likelihood that the FortiMail unit will still periodically retrieve updates if connectivity is interrupted during a push notification. While using ***only*** scheduled updates could potentially leave your network vulnerable to a new virus, it minimizes short disruptions to antivirus scans that can occur if the FortiMail unit applies push updates during peak volume times.

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

To configure scheduled updates

1. Go to *System* > *FortiGuard* > *AntiVirus* in the advanced mode of the web UI.

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
- 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 "The role of DNS in email delivery" on page 9.

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

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 modes" on page 24.

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 web UI 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 you configured *Web release host name/IP* (located in *AntiSpam* > *Quarantine* > *Quarantine Report* in the advanced mode of the web UI).

See the following:

- 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%40examp
     le.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM2N
     TkjRSxVMzoyLA%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 web UI, 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%40exa
     mple.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM
     2NTkjRSxVMzoyLA%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 48, 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 web UI 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.

Figure 7: 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 illustrated in Figure 7 on page 49, and the *Use MX Record* option is enabled, Table 6 on page 75 illustrates differences between the public and private DNS servers for the authoritative DNS records of example.com.

Table 5: 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 web UI.

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.

Figure 8: 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 39 and "Configuring DNS records" on page 46.

Configuring the firewall

With the FortiMail unit behind a FortiGate unit, you must configure firewall policies to allow traffic between the internal network and the Internet.

To create the required policies, complete the following:

- Configuring the firewall address
- Configuring the service groups
- Configuring the virtual IPs
- Configuring the firewall policies

The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall address

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.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following and then click *OK*.

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `172.16.1.5`.
Interface	Select *internal*.

Configuring the service groups

In order to create firewall policies that govern only email and FortiMail-related traffic, you must first create groups of services that define protocols and port numbers used in that traffic.

Because FortiGuard-related services for FortiMail units are not predefined, you must define them before you can create a service group that contains those services.

For more information on protocols and port numbers used by FortiMail units, see Fortinet Communication Ports and Protocols at http://docs.fortinet.com.

To add a custom service for FortiGuard Antivirus push updates

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following and then click *OK*:

Name		Enter a name to identify the custom service entry, such as `FortiMail_antivirus_push_updates`.
Protocol Type		Select *TCP/UDP*.
Protocol		Select *UDP*.
Destination Port		
	Low	Enter `9443`.
	High	Enter `9443`.

To add a custom service for FortiGuard Antispam rating queries

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following and then click *OK*.

Name		Enter a name to identify the custom service entry, such as `FortiMail_antispam_rating_queries`.
Protocol Type		Select *TCP/UDP*.
Protocol		Select *UDP*.
Destination Port		
	Low	Enter `8889`.
	High	Enter `8889`.

To add a service group for incoming FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_incoming_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, and your custom service for FortiGuard Antivirus push updates, *FortiMail_antivirus_push_updates*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for outgoing FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_outgoing_services`.
5. In the *Available Services* area, select *DNS*, *NTP*, *HTTPS*, *SMTP*, and your custom service for FortiGuard Antispam rating queries, *FortiMail_antispam_rating_queries*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for email user traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `POS_IMAP_services`.
5. In the *Available Services* area, select *POP3* and *IMAP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the virtual IPs

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 private IP address of the FortiMail unit by creating a virtual IP 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.

To add virtual IPs, the FortiGate unit must be operating in NAT mode.

To add a virtual IP for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following and then click *OK*.

Name	Enter a name to identify the virtual IP entry, such as `FortiMail_VIP`.
External Interface	Select *wan1*.
Type	Select *Static NAT.*
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `172.16.1.5`.

To add a virtual IP for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following and then click *OK*.

Name	Enter a name to identify the virtual IP entry, such as `protected_email_server_VIP`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `172.16.1.10`.

Configuring the firewall policies

First, create a firewall policy that allows 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.

Second, create a firewall policy that allows outgoing email and other FortiMail connections from the FortiMail unit to the Internet.

Last, create a firewall policy that allows 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.

To add the Internet-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following and then click *OK*.

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *internal*.
Destination Address Name	Select *FortiMail_VIP*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_incoming_services*.
Action	Select *ACCEPT*.

To add the FortiMail-to-Internet policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *all*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_outgoing_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the Internet-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following and then click *OK*.

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *internal*.
Destination Address Name	Select *protected_email_server_VIP*.
Schedule	Select *ALWAYS*.
Service	Select *PO3_IMAP_services*.
Action	Select *ACCEPT*.

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 114.

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.

Figure 9: 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 39 and "Configuring DNS records" on page 46.

Configuring the firewall

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 traffic:

- 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

To create the required policies, complete the following:

- Configuring the firewall addresses
- Configuring the service groups
- Configuring the virtual IPs
- Configuring the firewall policies

The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall addresses

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.

To add a firewall address for local email users

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `local_email_users_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `172.16.1.0/24`.
Interface	Select *internal*.

5. Select *OK*.

To add a firewall address for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `protected_email_server_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `192.168.1.10/32`.
Interface	Select *dmz*.

5. Select *OK*.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `10.10.10.5/32`.
Interface	Select *wan1*.

5. Select *OK*.

Configuring the service groups

In order to create firewall policies that governs email and FortiMail-related traffic, you must first create service groups that contain services that define protocols and port numbers used in that traffic.

To add a service group for internal email user and protected server traffic to the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `SMTP_quar_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, and *SMTP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for POP3 and IMAP traffic to the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.

4. In *Group Name*, enter a name to identify the service group entry, such as `P03_IMAP_services`.
5. In the *Available Services* area, select *POP3* and *IMAP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the virtual IPs

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.

To add virtual IPs, the FortiGate unit must be operating in NAT mode.

To add a wan1 virtual IP for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `protected_email_server_VIP_wan1`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `192.168.1.10`.

5. Select *OK*.

To add an internal virtual IP for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `protected_email_server_VIP_internal`.
External Interface	Select *internal*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `172.16.1.2`.
Mapped IP Address/Range	Enter `192.168.1.10`.

5. Select *OK*.

Configuring the firewall policies

Create the following firewall policies:

- Allow SMTP connections from the protected email server to the FortiMail unit.
- Allow SMTP_quar_services from the local email users to the FortiMail unit.
- allow SMTP connections that are received at the wan1 virtual IP address from the FortiMail unit, then apply a static NAT when forwarding the traffic to the private network IP address of the protected email server.
- Allow PO3_IMAP_services that are received at the internal virtual IP address, then apply a static NAT when forwarding the traffic to the private network IP address of the protected email server.
- Allow PO3_IMAP_services that are received at the wan1 virtual IP address, then apply a static NAT when forwarding the traffic to the private network IP address of the protected email server.

To add the email-server-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *dmz*.
Source Address Name	Select *protected_email_server_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *FortiMail_address*.
Schedule	Select *ALWAYS*.

Service	Select *SMTP*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the local-users-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *local_email_users_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *FortiMail_address*.
Schedule	Select *ALWAYS*.
Service	Select *SMTP_quar_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the FortiMail-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *protected_email_server_VIP_wan1*.
Schedule	Select *ALWAYS*.
Service	Select *SMTP*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the local-users-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *local_email_users_address*.
Destination Interface/zone	Select *internal*.
Destination Address Name	Select *protected_email_server_VIP_internal*.
Schedule	Select *ALWAYS*.
Service	Select *PO3_IMAP_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the remote-users-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *dmz*.
Destination Address Name	Select *protected_email_server_VIP_wan1*.
Schedule	Select *ALWAYS*.
Service	Select *PO3_IMAP_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

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 114.

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.

Figure 10: 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 39 and "Configuring DNS records" on page 46.

Configuring the firewall

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

To create the required policies, complete the following:

- Configuring the firewall addresses
- Configuring the service groups
- Configuring the virtual IPs
- Configuring the firewall policies

The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall addresses

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.

To add a firewall address for local email users

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `local_email_users_address`.
Type	Select *Subnet/IP Range*.

Subnet /IP Range	Enter `172.16.1.0/24`.
Interface	Select *internal*.

5. Select *OK*.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `192.168.1.5/32`.
Interface	Select *dmz*.

5. Select *OK*.

Configuring the service groups

In order to create firewall policies that govern only email and FortiMail-related traffic, you must first create groups of services that define protocols and port numbers used in that traffic.

Because FortiGuard-related services for FortiMail units are not predefined, you must define them before you can create a service group that contains those services.

For more information on protocols and port numbers used by FortiMail units, see Fortinet Communication Ports and Protocols at http://docs.fortinet.com.

To add a custom service for FortiGuard Antivirus push updates

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name	Enter a name to identify the custom service entry, such as `FortiMail_antivirus_push_updates`.
Protocol Type	Select *TCP/UDP*.
Protocol	Select *UDP*.
Destination Port	

Low	Enter 9443.
High	Enter 9443.

5. Select *OK*.

To add a custom service for FortiGuard Antispam rating queries

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name	Enter a name to identify the custom service entry, such as `FortiMail_antispam_rating_queries`.
Protocol Type	Select *TCP/UDP*.
Protocol	Select *UDP*.
Destination Port	
Low	Enter 8889.
High	Enter 8889.

5. Select *OK*.

To add a service group for remote incoming FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_incoming_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, and your custom service for FortiGuard Antivirus push updates, *FortiMail_antivirus_push_updates*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for outgoing FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_outgoing_services`.
5. In the *Available Services* area, select *DNS*, *NTP*, *HTTPS*, *SMTP*, and your custom service for FortiGuard Antispam rating queries, *FortiMail_antispam_rating_queries*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for internal email user traffic to the FortiMail unit

1. Access FortiGate.

2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `SMTP_quar_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, and *SMTP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for POP3 and IMAP traffic to the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `PO3_IMAP_services`.
5. In the *Available Services* area, select *POP3* and *IMAP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the virtual IPs

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

To add virtual IPs, the FortiGate unit must be operating in NAT mode.

To add a wan1 virtual IP for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `FortiMail_VIP_wan1`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.

External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `192.168.1.5`.

5. Select *OK*.

To add a wan1 virtual IP for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `protected_email_server_VIP_wan1`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `172.16.1.10`.

5. Select *OK*.

To add a internal virtual IP for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `FortiMail_VIP_internal`.
External Interface	Select *internal*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `172.16.1.2`.
Mapped IP Address/Range	Enter `192.168.1.5`.

5. Select *OK*.

To add a dmz virtual IP for the protected email server

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `protected_email_server_VIP_dmz`.
External Interface	Select *dmz*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `192.168.1.2`.
Mapped IP Address/Range	Enter `172.16.1.10`.

5. Select *OK*.

Configuring the firewall policies

Create the following firewall policies:

- Allow SMTP_quar_services that are received at the internal virtual IP address, then apply a static NAT when forwarding the traffic to the private network IP address of the FortiMail unit.
- Allow FortiMail_incoming_services that are received at the wan1 virtual IP address that maps to the FortiMail unit, then apply a static NAT when forwarding the traffic to the private network IP address of the FortiMail unit.
- Allow FortiMail_outgoing_services from the FortiMail unit to the Internet.
- Allow SMTP traffic that is received at the DMZ virtual IP address, then apply a static NAT when forwarding the traffic to the private network IP address of the protected email server.
- Allow PO3_IMAP_services that are received at the wan1 virtual IP address that maps to the protected email server, then apply a static NAT when forwarding the traffic to the private network IP address of the protected email server.

To add the internal-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *internal_address*.
Destination Interface/zone	Select *dmz*.

Destination Address Name	Select *FortiMail_VIP_internal*.
Schedule	Select *ALWAYS*.
Service	Select *SMTP_quar_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the Internet-to-FortiMail unit policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *dmz*.
Destination Address Name	Select *FortiMail_VIP_wan1*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_incoming_services*.
Action	Select *ACCEPT*.

5. Select *OK*.

To add the FortiMail-to-Internet policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *dmz*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *all*.
Schedule	Select *ALWAYS*.

Service	Select *FortiMail_outgoing_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the FortiMail-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *dmz*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *internal*.
Destination Address Name	Select *protected_email_server_VIP_dmz*.
Schedule	Select *ALWAYS*.
Service	Select *SMTP*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the remote-users-to-email-server policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *internal*.
Destination Address Name	Select *protected_email_server_VIP_wan1*.
Schedule	Select *ALWAYS*.
Service	Select *PO3_IMAP_services*.
Action	Select *ACCEPT*.

5. Select *OK*.

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 114.

Transparent mode deployment

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

- Configuring DNS records
- Example 1: FortiMail unit in front of an email server
- Example 2: FortiMail unit in front of an email hub
- Example 3: FortiMail unit for an ISP or carrier

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 usually 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 "The role of DNS in email delivery" on page 9.

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 web UI 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 *AntiSpam* > *Quarantine* > *Quarantine Report* in the advanced mode of the web UI) 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%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM2NTkjRSxVMzoyLA%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 web UI, 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%40exa
     mple.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM
     2NTkjRSxVMzoyLA%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 48, 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 web UI 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

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

Figure 11: Public and private DNS servers (transparent mode)

In some situations, a private DNS server may be required. If:

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

you should 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 Figure 7 on page 49, and the *Use MX record* option is enabled, Table 6 on page 75 illustrates differences between the public and private DNS servers for the authoritative DNS records of example.com.

Table 6: 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 web UI.

Example 1: FortiMail unit in front of an email server

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

This example assumes that the FortiMail unit is protecting a single 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 88.

Figure 12: 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 39.

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	
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. **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. **Note:** This function does not take effect if the email is sent from protected domains to protected domains.
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*.
2. In the *Session* column for an IP-based policy, select the name of the session profile to edit the profile.

   A dialog appears.
3. Configure the following:

Connection Settings	
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 unit. Disable to replace the 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.

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

For information on determining directionality, see "Connection directionality vs email directionality" on page 8.

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*.
2. Edit SMTP proxy settings on both Port 1 and Port 2:

Port 1	
Incoming connections	*Drop*
Outgoing connections	*Pass through*
Local connections	*Allow*
Port 2	
Incoming connections	*Proxy*
Outgoing connections	*Drop*
Local connections	*Disallow*

If *Use client-specified SMTP server to send email* is disabled under *System* > *Mail Settings* > *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 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 114.

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.

Figure 13: 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 39.

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*.
2. In the row corresponding to the protected domain, select *Edit*.
3. Configure the following:

Transparent Mode Options	
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. **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. **Note:** This function does not take effect if the email is sent from protected domains to protected domains.
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*.
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 Settings	
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 unit. Disable to replace the 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 vs email directionality" on page 8.

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* in the advanced mode of the web UI.
2. Edit SMTP proxy settings on both Port 1 and Port 2:

Port 1	
Incoming connections	*Drop*
Outgoing connections	*Pass through*
Local connections	*Allow*
Port 2	
Incoming connections	*Proxy*
Outgoing connections	*Drop*
Local connections	*Disallow*

Testing the installation

Basic configuration is now complete, and the installation may be tested. For testing instructions, see "Testing the installation" on page 114.

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 a config-only 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.)

Figure 14: 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.

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 39.

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 web UI. For instructions on how to connect to the CLI, see "Connecting to the Web UI or CLI" on page 26.
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 web UI, 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 web UI 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 on port2 to edit it.
3. Select *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. 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* in the advanced mode of the web UI.
2. Select *New*.
3. In *Profile Name*, type a name for the session profile, such as `external_session_profile`.
4. Configure the following:

Connection Settings	
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 unit.
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 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.
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 Settings	
Prevent encryption of the session (transparent mode only)	Enable to block `STARTTLS`/MD5 commands so that email connections cannot be TLS-encrypted.
Unauthenticated Session Settings	
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* in the advanced mode of the web UI.
2. Select *New*.
3. In *Profile Name*, type a name for the session profile, such as `internal_session_profile`.
4. Configure the following:

Connection Settings	
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 unit.
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.

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 Settings	
Prevent encryption of the session (transparent mode only)	Enable to block `STARTTLS`/MD5 commands so that email connections cannot be TLS-encrypted.
Unauthenticated Session Settings	
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* in the advanced mode of the web UI.

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* in the advanced mode of the web UI.
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 vs email directionality" on page 8.

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 Settings* > *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 Settings* > *Proxies* in the advanced mode of the web UI.
2. Enable *Use client-specified SMTP server to send email.*
3. Go to *System* > *Network*.
4. Edit SMTP proxy settings on both port 2 and port 3:

Port 2	
Incoming connections	*Drop*
Outgoing connections	*Proxy*
Local connections	*Disallow*
Port 3	
Incoming connections	*Drop*
Outgoing connections	*Proxy*
Local connections	*Disallow*

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, you use a FortiGate unit as the router/firewall, you can go to *Router* > *Policy Route* to 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 http://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 114.

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 "The role of DNS in email delivery" on page 9.

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 modes" on page 24.

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 web UI 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 *AntiSpam* > *Quarantine* > *Quarantine Report* in the advanced mode of the web UI) 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

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%40examp
     le.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM2N
     TkjRSxVMzoyLA%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 web UI, 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%40exa
     mple.com%3AMTIyMDUzOTQzOC43NDJfNjc0MzE1LkZvcnRpTWFpbC00MDAsI0YjUyM
     2NTkjRSxVMzoyLA%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 48, 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 web UI 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.

Figure 15: 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 web UI.

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".

Figure 16: 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 39 and "Configuring DNS records" on page 94.

Configuring the firewall

With the FortiMail unit behind a FortiGate unit, you must configure policies to allow traffic:

- from the Internet to the FortiMail unit
- from the FortiMail unit to the Internet

To create the required policies, complete the following:

- Configuring the firewall address
- Configuring the service groups
- Configuring the virtual IPs
- Configuring the firewall policies

The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall address

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.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `172.16.1.5`.
Interface	Select *internal*.

5. Select *OK*.

Configuring the service groups

In order to create firewall policies that govern only FortiMail-related traffic, you must first create groups of services that define protocols and port numbers used in that traffic.

Because FortiGuard-related services for FortiMail units are not predefined, you must define them before you can create a service group that contains those services.

For more information on protocols and port numbers used by FortiMail units, see the Fortinet Knowledge Center article FortiMail Traffic Types and TCP/UDP Ports.

To add a custom service for FortiGuard Antivirus push updates

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name	Enter a name to identify the custom service entry, such as `FortiMail_antivirus_push_updates`.
Protocol Type	Select *TCP/UDP*.
Protocol	Select *UDP*.
Destination Port	

	Low	Enter 9443.
	High	Enter 9443.

5. Select *OK*.

To add a custom service for FortiGuard Antispam rating queries

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name		Enter a name to identify the custom service entry, such as `FortiMail_antispam_rating_queries`.
Protocol Type		Select *TCP/UDP*.
Protocol		Select *UDP*.
Destination Port		
	Low	Enter 8889.
	High	Enter 8889.

5. Select *OK*.

To add a service group for incoming FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_incoming_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, *POP3*, *IMAP*, and your custom service for FortiGuard Antivirus push updates, *FortiMail_antivirus_push_updates*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

To add a service group for outgoing FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_outgoing_services`.
5. In the *Available Services* area, select *DNS*, *NTP*, *HTTPS*, *SMTP*, and your custom service for FortiGuard Antispam rating queries, *FortiMail_antispam_rating_queries*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the virtual IPs

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.

To add virtual IPs, the FortiGate unit must be operating in NAT mode.

To add a virtual IP for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `FortiMail_VIP`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `172.16.1.5`.

5. Select *OK*.

Configuring the firewall policies

First, create a firewall policy that allows 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.

Second, create a firewall policy that allows outgoing email and other connections from the FortiMail unit to the Internet.

To add the Internet-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.

Destination Interface/zone	Select *internal*.
Destination Address Name	Select *FortiMail_VIP*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_incoming_services*.
Action	Select *ACCEPT*.

5. Select *OK*.

To add the FortiMail-to-Internet policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *all*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_outgoing_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

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

1. Go to *Domain & User* > *User* > *User*. (The *User* tab appears only when FortiMail operates in server mode.)
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 114.

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".

Figure 17: 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 39 and "Configuring DNS records" on page 94.

Configuring the firewall

With the FortiMail unit in front of a FortiGate unit which is between the FortiMail unit and local email users, you must configure a policy to allow from local email users to the FortiMail unit.

To create the required policies, complete the following:

- Configuring the firewall addresses
- Configuring the service group
- Configuring the firewall policy

The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall addresses

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.

To add a firewall address for local email users

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `local_email_users_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `172.16.1.0/24`.
Interface	Select *internal*.

5. Select *OK*.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Addres***s**.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `10.10.10.5/32`.
Interface	Select *wan1*.

5. Select *OK*.

Configuring the service group

In order to create a firewall policy that governs only FortiMail-related traffic, you must first a create service group that contains services that define protocols and port numbers used in that traffic.

To add a service group for email user traffic to the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `local_email_users_services`.

5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, *POP3*, and *IMAP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the firewall policy

Create a firewall policy that allows outgoing email and other FortiMail connections from the local email users to the FortiMail unit.

To add the internal-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *local_email_users_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *FortiMail_address*.
Schedule	Select *ALWAYS*.
Service	Select *local_email_users_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

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

1. Go to *Domain & User* > *User* > *User*. (The *User* tab appears only when FortiMail operates in server mode.)
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 114.

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".

Figure 18: 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 39 and "Configuring DNS records" on page 94.

Configuring the firewall

With the FortiMail unit located in the DMZ of a FortiGate unit which is between the FortiMail unit and local email users, you must configure policies to allow traffic:

- from local email users to the FortiMail unit
- from the FortiMail unit to the Internet
- from the Internet to the FortiMail unit

To create the required policies, complete the following:

- Configuring the firewall addresses
- Configuring the service groups
- Configuring the virtual IPs
- Configuring the firewall policies

Note: The following procedures use a FortiGate unit running FortiOS v3.0 MR7. If you are using a different firewall appliance, consult the appliance's documentation for completing similar configurations.

Configuring the firewall addresses

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.

To add a firewall address for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Address* > *Address*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `FortiMail_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `192.168.1.5`.
Interface	Select *dmz*.

5. Select *OK*.

To add a firewall address for local email users

1. Go to *Firewall* > *Address* > *Address*.
2. Select *Create New*.
3. Complete the following:

Name	Enter a name to identify the firewall address entry, such as `local_email_users_address`.
Type	Select *Subnet/IP Range*.
Subnet /IP Range	Enter `172.168.1.0/24`.
Interface	Select *internal*.

4. Select *OK*.

Configuring the service groups

In order to create firewall policies that govern only FortiMail-related traffic, you must first create groups of services that define protocols and port numbers used in that traffic.

Because FortiGuard-related services for FortiMail units are not predefined, you must define them before you can create a service group that contains those services.

For more information on protocols and port numbers used by FortiMail units, see the Fortinet Knowledge Center article FortiMail Traffic Types and TCP/UDP Ports.

To add a custom service for FortiGuard Antivirus push updates

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name		Enter a name to identify the custom service entry, such as `FortiMail_antivirus_push_updates`.
Protocol Type		Select *TCP/UDP*.
Protocol		Select *UDP*.
Destination Port		
	Low	Enter `9443`.
	High	Enter `9443`.

5. Select *OK*.

To add a custom service for FortiGuard Antispam rating queries

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Custom*.
3. Select *Create New*.
4. Configure the following:

Name		Enter a name to identify the custom service entry, such as `FortiMail_antispam_rating_queries`.
Protocol Type		Select *TCP/UDP*.
Protocol		Select *UDP*.
Destination Port		
	Low	Enter `8889`.
	High	Enter `8889`.

5. Select *OK*.

To add a service group for incoming FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_incoming_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, *POP3*, *IMAP*, and your custom service for FortiGuard Antivirus push updates, *FortiMail_antivirus_push_updates*, then select the right arrow to move them to the Members area.
6. Select *OK*.

To add a service group for outgoing FortiMail traffic

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `FortiMail_outgoing_services`.
5. In the Available Services area, select DNS, NTP, HTTPS, SMTP, and your custom service for FortiGuard Antispam rating queries, FortiMail_antispam_rating_queries, then select the right arrow to move them to the Members area.
6. Select *OK*.

To add a service group for email user traffic to the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Service* > *Group*.
3. Select *Create New*.
4. In *Group Name*, enter a name to identify the service group entry, such as `local_email_users_services`.
5. In the *Available Services* area, select *HTTP*, *HTTPS*, *SMTP*, *POP3*, and *IMAP*, then select the right arrow to move them to the *Members* area.
6. Select *OK*.

Configuring the virtual IPs

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.

To add a wan1 virtual IP for the FortiMail unit

1. Access FortiGate.
2. Go to *Firewall* > *Virtual IP* > *Virtual IP*.
3. Select *Create New*.
4. Complete the following:

Name	Enter a name to identify the virtual IP entry, such as `FortiMail_VIP_wan1`.
External Interface	Select *wan1*.
Type	Select *Static NAT*.
External IP Address/Range	Enter `10.10.10.1`.
Mapped IP Address/Range	Enter `192.168.1.5`.

5. Select *OK*.

Configuring the firewall policies

First, create a firewall policy that allows 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.

Second, create a firewall policy that allows outgoing email and other FortiMail connections from the FortiMail unit to the Internet.

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

To add the Internet-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *wan1*.
Source Address Name	Select *all*.
Destination Interface/zone	Select *dmz*.
Destination Address Name	Select *FortiMail_VIP_wan1*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_incoming_services*.
Action	Select *ACCEPT*.

5. Select *OK*.

To add the FortiMail-to-Internet policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.

3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *dmz*.
Source Address Name	Select *FortiMail_address*.
Destination Interface/zone	Select *wan1*.
Destination Address Name	Select *all*.
Schedule	Select *ALWAYS*.
Service	Select *FortiMail_outgoing_services*.
Action	Select *ACCEPT*.

5. Select *NAT*.
6. Select *OK*.

To add the internal-to-FortiMail policy

1. Access FortiGate.
2. Go to *Firewall* > *Policy* > *Policy*.
3. Select *Create New*.
4. Complete the following:

Source Interface/zone	Select *internal*.
Source Address Name	Select *local_email_users_address*.
Destination Interface/zone	Select *dmz*.
Destination Address Name	Select *FortiMail_address*.
Schedule	Select *ALWAYS*.
Service	Select *local_email_users_services*.
Action	Select *ACCEPT*.

5. Select *OK*.

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

1. Go to *Domain & User* > *User* > *User*. (The *User* tab appears only when FortiMail operates in server mode.)
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 114.

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.

Figure 19: Connection test paths (gateway mode)

Figure 20: Connection test paths (transparent mode)

Figure 21: 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 117.

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.

Table 7: Some 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, 25 (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
- `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 and 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 web UI.

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* > *Sender Reputation* > *Display*, respectively.

If these menu paths are not available, first select *Advanced* >> to switch to the advanced mode of the web UI.

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.

If these menu paths are not available, first select *Advanced* >> to switch to the advanced mode of the web UI.

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* > *Network* > *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 545fwl-/Z_T^EU[_B[T_
0x0040 4559 6b6a 776b 646e 776c 6b6a 772b 646eEYkjwkdnwlkjw+dn
0x0050 776c 6b6a 776b 646e 776c 6b6a 776b 86a9wlkjwkdnwlkjwk..
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 (http://www.wireshark.org/).

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 Perl interpreter
- 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:

   `diag 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 drop-down 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 2019.07.25 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 XP, go to *Start* > *Run* and enter `cmd`.
On Windows 7, click the Start (Windows logo) menu to open it, 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

Figure 22: 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.

Figure 23: 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 web UI

1. Log in to the web UI 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 web UI, 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`:

   ```
   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
- Using the CLI Console

Viewing the dashboard

Dashboard > *Status* displays first after you log in to the web UI. 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.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view the dashboard, go to *Dashboard* > *Status*.

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.

Using the CLI Console

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

You can click the Open in New Window button to move the CLI Console into a pop-up window that you can resize and reposition.

For more information about CLI 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
- View threat statistics
- Viewing top user statistics
- Viewing current IP sessions

Viewing mail statistics

The *FortiView* > *Mail Statistics* > *By Count* tab contains summaries of the number of email messages in each time period that the FortiMail unit detected viruses, spam, or neither.

The *FortiView* > *Mail Statistics* > *By Size* tab contains summaries by the file sizes of email messages in each time period that the FortiMail unit detected viruses, spam, or neither.

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

For email ***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 use the *Mail Statistics* tab, first configure your FortiMail unit to detect spam and/or viruses. For more information, see "Configuring profiles" on page 389 and "Configuring policies" on page 359.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

View threat statistics

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

Viewing top user statistics

The *FortiView* > *Top User Statistics* tab displays the top email senders and recipients, top virus sender and recipients, and top spam senders and recipients.

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

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

Viewing current IP sessions

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

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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.

This section includes:

- Viewing log messages
- Managing the quarantines
- Managing the mail queue
- Viewing the greylist statuses
- Viewing sender, authentication and endpoint reputation
- Managing archived email
- Viewing generated reports

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.

You can also view history log messages from the *History Log* widget in *Monitor* > *Log* > *History*.

Logs stored remotely cannot be viewed from the web UI of the FortiMail unit. If you require the ability to view logs from the web UI, also enable local storage. For details, see "Configuring logging to the hard disk" on page 569.

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 543.

  For more information on log types, see "FortiMail log types" on page 564.

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 rolled log file whose time might range from `2008-05-08 11:59:36 Thu` to `2008-05-29 10:44:02 Thu`.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view the list of log files and their contents

1. Go to *Monitor* > *Log*.
2. 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* for a log file that can be viewed with a plain text editor such as Microsoft Notepad. • *CSV Format* for 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. 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 135.
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.

3. 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 135.
- 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 137.

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, 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 135.

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 Columns.*
4. Turn on/off 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 on a log message, a context menu appears.

Figure 24: Using the right-click menus on log reports

Right-click pop-up menus

Table 8: 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 to Table	Select to export the selected log messages to a table format. A new tab named *Exported Table* appears, displaying the exported information. The table format allows you to copy the information and paste it elsewhere.

Table 8: Log report right-click menu options

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 137.
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 137.
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 137.
Release Quarantined Message	When viewing quarantine logs on the *History* tab, select one or multiple log entries of the "Quarantine to Review" or "Quarantine" messages, then from the right-click popup menu, select the Release Quarantined Message option to release the selected message/messages. For details about quarantined email, see "Managing the quarantines" on page 137.

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. Enter your search criteria by configuring one or more of the following:

GUI item	Description
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.
From	Enter all or part of the sender's email address as it appears in the log message. This option does not appear for event log searches.
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.
Log ID	Enter all or part of the log ID in the log message.
Client name (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 565.
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 565.
Match condition	• *Contain*: searches for the exact match. • *Wildcard*: supports wildcards in the entered search criteria.
Time	Select the time span of log messages to include in the search results. 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 specify the current date, and also specify the size of the span of time (10 days and 8 hours) before that date.

5. Click *Apply*.

   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.

Cross-searching log messages

Since different types of log files record different events/activities, the same SMTP session (with one or more email messages sent during the session) or the same email message may be logged in different types of log files. For example, if the FortiMail units detects a virus in an email messages, this event will be logged in the following types of log files:

- History log: because the history log records the metadata of all sent and undelivered email messages.
- AntiVirus log: because a virus is detected. The antivirus log has more descriptions of the virus than the history log does.
- Event log: because the FortiMail system'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.

The cross-search searches log files recorded five minutes before and after the log entry (this design is for performance purpose). Therefore, the search may cover multiple log files but may not cover all the related log files if any log files 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:
   - **Cross Search (Session)** 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.
   - **Cross Search (Message)** to 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.

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 two 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 138.

- 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 141.

To quarantine spam and/or email with prohibited content, you must select a quarantine action in an antispam profile or content profile. For details, see "Configuring antispam profiles and antispam action profiles" on page 407 and "Configuring content profiles and content action profiles" on page 430.

All FortiMail models can be configured to remotely store their quarantined email messages in a centralized quarantine hosted on a high end FortiMail model (FortiMail VM02, FortiMail 400E series and above).

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 web UI).

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 web UI, 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 138. For information on configuring the schedule and recipients of the quarantine report, see "Configuring global quarantine report settings" on page 495.

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 action profiles" on page 422 and "Configuring content profiles" on page 430.

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 139.

To reduce the amount of hard disk space consumed by quarantined mail, regularly release or delete the contents of each recipient's quarantine.

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 501.

To access this part of the web UI, your administrator account's access profile must have *Read-Write* permission to the *Quarantine* category. For details, see "About administrator account permissions and domains" on page 179.

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 the amount of hard disk space consumed by quarantined mail, regularly release or delete the contents of each recipient's quarantine.

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 501.

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 496. 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 307 for quarantine report settings that are domain-specific, or "Configuring global quarantine report settings" on page 495 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 503.

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 445.
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 329, 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" 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 action profiles" on page 422 and/or "Configuring content action profiles" on page 439.
8. Select the antispam and/or content profiles in incoming recipient-based policies. If you configured a resource profile in step 6, 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 381.
9. Either email users or FortiMail administrators can manage email in the per-recipient quarantines. For details, see "Managing the personal quarantines" on page 138 and "Releasing and deleting email via quarantine reports" on page 501.

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.

   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.

5. Click *Create* 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 502.

To reduce the amount of hard disk space consumed by the system quarantine, regularly release or delete items from the system quarantine.

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 427, "Configuring antispam action profiles" on page 422 and "Configuring content action profiles" on page 439.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Quarantine* category

For details, see "About administrator account permissions and domains" on page 179.

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:
   - **Content** -- these are the email messages caught by content profiles.
   - **Virus** -- these are the email messages caught by antivirus profiles.
   - **Bulk** -- these are the email messages caught by antispam profiles.

GUI item	Description
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.
Mailbox	Lists the current mailbox, which is named *Inbox*. 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 502. To view email messages quarantined in that mailbox, double-click its row. For more information, see "Managing the system quarantine" on page 141.
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 502.

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	User 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 143.
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.
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 140.

Managing the mail queue

The FortiMail unit prioritizes the mail queue into two types:

- 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 another two 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 keep resending invalid email (for example, email destined to an invalid MTA).

After the undelivered email remains in the deferred queue for five minutes, the mail appears under *Monitor* > *Mail Queue* > *Mail Queue*. This also means that email staying in the deferred queue for less than five minutes does not appear on the *Mail Queue* tab.

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 146.

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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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

To reduce the amount of hard disk space consumed by quarantined mail, regularly release or delete the contents of each recipient's quarantine.

Table 9: Managing the deferred mail queue

GUI item	Description
View (button)	Select a message and click *View* to see its contents.
Delete (button)	Click to deleted the selected item.

Table 9: Managing the deferred mail queue

GUI item	Description
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*: Displays all email in the regular mail queue. After three failed delivery retries, the mail will be moved to the Default-slow mail queue. • *Incoming*: Only displays the delayed incoming emai that meets the following criteria: 1. The mail must be destined to both protected and unprotected domains; 2. The mail must have triggered different actions in regard to different domains, for example, inserting disclaimer for outgoing email and tagging the subjects for incoming email. If the incoming email action is triggered, the mail will be moved to the Incoming mail queue. If both the outgoing email action and incoming email action are triggered, the mail will be moved to both the Incoming and Outgoing mail queues. After three failed delivery retries, the mail will be moved to the Incoming-slow mail queue. • *Outgoing*: Only displays the delayed outgoing emai that meets the following criteria: 1. The mail must be destined to both protected and unprotected domains; 2. The mail must have triggered different actions in regard to different domains, for example, inserting disclaimer for outgoing email and taking no action for incoming email is considered to be different actions for different domains. If the outgoing email action is triggered, the mail will be moved to the Outgoing mail queque. If both the outgoing email action and incoming email action are triggered, the mail will be moved to both the Incoming and Outgoing mail queues. After three failed delivery retries, the mail will be moved to the Outgoing-slow mail queue. • *IBE*: Only displays the IBE email in the regular mail queue. For information about IBE email, see "Configuring IBE encryption" on page 543. After three failed delivery retries, the mail will be moved to the IBE-slow mail queue. • *Default-slow*: Displays all email in the slow mail queue. • *Incoming-slow*: Displays the incoming email in the slow mail queue. • *Outgoing-slow*: Displays the outgoing email in the slow mail queue. • *IBE-slow*: Displays the IBE email in the slow mail queue. • *Thresholded-queue*: Displays the email throttled by delivery control policies (see "Configuring delivery control policies" on page 374). 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.
Session ID	Lists the `Session-Id:` message header of the email.
Envelope From	Lists the sender (`MAIL FROM:`) of the email.

Table 9: Managing the deferred mail queue

GUI item	Description
Envelope To	Lists the recipient (`RCPT TO:`) of the email.
Subject	Lists the email subjects.
Reason	Lists the reasons why the email has been deferred, such as DNS lookup failure or refused connections.
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 (configuragle with CLI command `config system fortiguard antispam set outbreak-protection-period`) if the enabled FortiGuard antispam check (block IP and/or URI 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 (configuragle 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 "Managing antivirus profiles" on page 425). 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. For more information about FortiSandbox, please visit Fortinet's web site at http://www.fortinet.com.

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 messages from `"postmaster"` 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, you can:
• 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 312.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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

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 513.

To use greylisting, you must enable the greylist scan in the antispam profile. For more information, see "Managing antispam profiles" on page 407.

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 381, and "Controlling email based on IP addresses" on page 375), ***or*** if the matching access control rule's *Action* is *RELAY* (see "Order of execution" on page 16).

You can configure the initial delay associated with greylisting, and manually exempt senders. For details, see "Configuring the grey list TTL and initial delay" on page 517 and "Manually exempting senders from greylisting" on page 519.

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 150.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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

Table 10: 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 149.
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.
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.

Table 10: Viewing the list of pending and individual greylist entries

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 grey list TTL and initial delay" on page 517. • *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 150. *N/A* appears if the greylisting period has already elapsed.
Expire	Lists the time and date when the entry will expire. The greylist entry's expiry time is determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings` (for details, see the FortiMail CLI Reference). The default initial expiry time is 4 hours. If the initial expiry time elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. • TTL: Between the entry's PASSTHROUGH time and initial expiry time, if the entry is hit again (the sender retries to send the message again), the entry's expiry time will be reset by adding the TTL value (time to live) to the message's "Received" time. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. For information on configuring the TTL, see "Configuring the grey list TTL and initial delay" on page 517.

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 148. For more information on consolidation requirements, see "Automatic greylist entries" on page 516.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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

Table 11: 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.
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 grey list TTL and initial delay" on page 517.

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

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

For more information on enabling sender reputation and configuring the score thresholds, see "Configuring sender reputation options" on page 391.

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

Table 12: 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 153.
IP	The IP address of the SMTP client.
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 391.
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* > *Sender Reputation* > *Display*.
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 the *Display* tab to refresh its view.

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 493.

To view the authentication reputation statuses

1. Go to Monitor > Reputation > Authentication Reputation
2. If Authentication Reputation is set to *Enable*, this page displays the following information:

GUI item	Description
Blocked IP	Lists the blocked IP addresses.
Access	Lists the access type: CLI, Mail, or Web. For details see "Configuring authentication reputation" on page 493.
Expiry Time	Displays when the blocking period will end. The blocking period is configurable under *Security* > *Authentication Reputation* > *Settings*. For details see "Configuring authentication reputation" on page 493.

3. If it is set to *Monitor only*, this page displays the following information:

GUI item	Description
IP	Lists the IP addresses with login failures.
Score	Displays the reputation scores. An IP/score in red color means that the IP address would have been blocked if the reputation setting was set to *Enable* instead of *Monitor only*.

Viewing endpoint reputation statuses

Go to *Monitor* > *Endpoint Reputation* > *Auto Blocklist* 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 527.

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 531. 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 389.

You can alternatively blocklist MSISDNs/subscriber IDs manually. For more information, see "Manually blocklisting endpoints" on page 529.

You can exempt MSISDNs/subscriber IDs from automatic blocklisting. For more information, see "Exempting endpoints from endpoint reputation" on page 530.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Block/Safe List* category

For details, see "About administrator account permissions and domains" on page 179.

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

Table 13: Auto Blocklist tab

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 155.
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 *Auto Blocklist* tab based on the MSISDN, subscriber ID, or other sender identifier.

To filter the endpoint block list entries

1. Go to *Monitor* > *Endpoint Reputation* > *Auto Blocklist*.

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*.
Case Sensitive	Enable for case-sensitive filtering.
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.

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 the *Auto Blocklist* tab to refresh its view.

Managing archived email

You can archive email according to criteria you specify. For details, see "Email archiving workflow" on page 555.

You can view and search archived email through the web UI. 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 533.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 555.
3. From the *Archive Folder* drop-down 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 157.
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 555.
3. From the *Archive Folder* drop-down 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 555.
3. From the *Archive Folder* drop-down 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 generated reports

The *Report* tab displays the list of reports generated from the report profiles. You can delete, view, and/or download generated reports.

FortiMail units can generate reports automatically, according to the schedule that you configure in the report profile, or manually, when you select a report profile and click *Generate*. For more information, see "Configuring report profiles and generating reports" on page 572.

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

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and generate reports

1. Go to *Monitor* > *Report* > *Report*.

GUI item	Description
Delete (button)	Click to delete the selected item.
Download (button)	Click to create a PDF version of the report.
Report File Name	Lists the name of the generated report, and the date and time at which it was generated. For example, `Report 1-2008-03-31-2112` is a report named Report 1, generated on March 31, 2008 at 9:12 PM. 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.
Last Access Time	Lists the date and time when the FortiMail unit completed the generated report.
Size	Lists the file size of the report in HTML format, in bytes.

2. 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*.
3. 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, mark the check box in the row corresponding to the report, such as `treportprofile-2011-06-27-1039`, then click *Download* and select *Download HTML*. Your browser downloads a file with an archive (.tgz.gz) file extension to your management computer. To view the report, first extract the report files from the archive, then open the HTML files in your web browser.
   - Each *Query Selection* in the report becomes a separate HTML file. You can view the report as individual HTML files. 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 `Spam_Recipient.html`. The report appears in a new browser window.

Configuring system settings

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

This section includes:

- Configuring network settings
- Configuring administrator accounts and access profiles
- Configuring system time, options, and other system options
- Configuring mail settings
- Customizing GUI, replacement messages and email templates
- Configuring RAID
- Using high availability (HA)
- Managing certificates
- Using FortiSandbox antivirus inspection
- Configuring FortiGuard services
- System maintenance

Configuring network settings

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

This section includes:

- About IPv6 Support
- About the management IP
- About FortiMail logical interfaces
- Configuring the network interfaces
- Configuring link status monitoring
- Configuring static routes
- Configuring DNS
- Configuring dynamic DNS
- Configuring port forwarding
- Scanning SMTP traffic redirected from FortiGate
- Using the traffic capture

About IPv6 Support

IP version 6 (IPv6) handles issues that weren't around decades ago when IPv4 was created such as running out of IP addresses, fair distributing 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 them to any needs.

IPv6 has 128-bit addresses compared to IPv4's 32-bit addresses, effectively eliminating address exhaustion. This new very large address space will likely reduce 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, an upgrade that may take a while to complete and will force IPv6 and IPv4 to work side-by-side during the transition period.

Starting from 4.3 release, FortiMail supports the following IPv6 features:

- Network interface
- Network routing
- High Availability
- DNS
- Admin 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 pool (starting from 4.3.3 release)

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 169.

Unless you configured an override server IP address, FortiMail units uses 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 289.

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

About FortiMail logical interfaces

In addition to the FortiMail physical 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.

Virtual LANs (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 163.

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 the *System* > *Network* > *Interface* page. You cannot configure the interface anymore.

For information about adding redundant interfaces, see "Configuring the network interfaces" on page 163.

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'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 163.

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 subinterfaces, redundant interfaces, and loopback interfaces. For more information, see "About FortiMail logical interfaces" on page 162, and "Editing network interfaces" on page 164.

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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 161.
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see "About FortiMail logical interfaces" on page 162.
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. See "Editing network interfaces" on page 164 for information on bridged networks in transparent mode.

GUI item	Description
IP/Netmask	Displays the IP address and netmask of the network interface. If the FortiMail unit is in transparent mode, *IP/Netmask* may alternatively display *bridging*. This means that "Do not associate with management IP" on page 169 has been disabled, and the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, *IP* and *Netmask* may alternatively display *bridged (isolated)* while the effective HA operating mode is *slave* and therefore the network interface is currently disconnected from the network, or *bridging (waiting for recovery)* while the effective HA operating mode is *failed* and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity. For more information, see "Effective Operating Mode" on page 246 and "Virtual IP address" on page 258.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface. For more information about IPv6 support, see "About IPv6 Support" on page 160.
Access	Displays the administrative access and webmail access services that are enabled on the network interface, such as HTTPS for the web UI.
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 164.

Editing network interfaces

You can edit FortiMail's 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 182.

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 162.
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.
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	
Manual	Select to enter a static IP address, then enter the IP address and netmask for the network interface.

GUI item	Description
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 DNS 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	

GUI item	Description
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 web-based manager, webmail, and per-recipient quarantine through this network interface. • *HTTP*: Enable to allow HTTP connections to the web-based manager, 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 495. • *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 163. • *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 182.
Web access	Enable the GUI access type that this network interface should accept. • *Admin*: Enable to allow access the admin 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: POP3, POP3S, IMAP, or IMAPS.
MTU	

GUI item	Description
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.

4. 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 162.
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.
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	

GUI item	Description
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 164. 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 169 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 web-based manager, webmail, and per-recipient quarantine through this network interface. • *HTTP*: Enable to allow HTTP connections to the web-based manager, 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 495. • *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 163. • *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 182.
MTU	

GUI item	Description
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 STMP relay, see “Click Create.” on page 358. **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 359.

GUI item	Description
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 359. **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 twice" on page 213.
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 359. **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 twice" on page 213.
Local connections	elect 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*.

   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".

Configuring link status monitoring

Link status monitoring enables the FortiMail unit to track the status of its 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 Propegate 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 Settings* popup window, specify the ports you want to propagate the status to by moving the ports from the left box to the right box.
7. Click *OK* to confirm your selections and return to the Link Status screen.

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.

When you add a static route through the web UI, the FortiMail unit evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiMail unit adds the static route.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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.

   A dialog appears.

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.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

Configuring dynamic DNS

The *System* > *Network* > *DDNS* tab lets you configure the FortiMail unit to use a dynamic DNS (DDNS) service.

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

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and configure dynamic DNS accounts

1. Go to *System* > *Network* > *DDNS*.

GUI item	Description
Server	Displays the name of your DDNS service provider.
User Name	Displays your user name for the DDNS service provider.
Host/Domain Name	A public host name or fully qualified domain name (FQDN) that should resolve to the public IP address of the FortiMail unit. Its public DNS records 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" on page 196 and "Local domain name" on page 197, which could be valid only for your internal network.
Update Time	Displays the interval in hours that the FortiMail unit waits between contacts to the DDNS service provider.

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*.

   A dialog appears.

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" on page 176 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. The tab returns to the list of dynamic DNS accounts, which should now include your new account.
5. Double-click the row corresponding to the new DDNS account.

   The *Host/Domain Name Setting* area is now visible.
6. In the *Host/Domain Name Setting* area, click *Create New*, or, to modify an existing host/domain name, select its row and click *Edit*.

   A dialog appears.

7. 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 fully qualified domain name (FQDN) whose records the DDNS provider should update.
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" on page 176. This option is the most common choice. To configure the interval of DDNS IP detection queries, see "Update time" on page 175. **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*

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

FortiMail port forwarding allows remote computers, for example, computers on the Internet, to connect to a specific computer or service within a private local area network (LAN). Port Forwarding is useful when FortiMail is deployed as a gateway and you want external users to access an internal server via FortiMail.

For example, FortiMail port1 is connected to the Internet and its IP address 192.168.37.4, port 7000, is mapped to 10.10.10.42, port 8000, on a private network. Attempts to communicate with 192.168.37.4, port 7000, from the Internet are translated and sent to 10.10.10.42, port 8000, by the FortiMail unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4, port 7000, rather than the 10.10.10.42 network behind the FortiMail unit.

To view and configure port forwarding rules

1. Go to *System* > *Network* > *Port Forwarding*.

GUI item	Description
ID	Displays the ID number assigned by the FortiMail unit.
Protocol	Displays the type of protocol.
Host IP	Displays the mapped IP address.
Host Port	Displays the assigned port number on the host computer.
Destination IP	Displays the IP address being mapped to the host.
Destination Port	Displays the assigned port number of the destination computer.

2. Select *New* to configure a new forwarding rule or double-click a rule to modify it.

   A dialog appears.
3. In *Protocol*, specify the protocol that the rule will apply to: *TCP, UDP,* or *Both*.
4. In *Host IP* and *Port*, enter the IP address and port number that will be mapped. In most cases, they are the IP address and port of the receiving FortiMail interface. In the above example, they are 192.168.37.4 and 7000.
5. In *Destination IP* and *Port*, enter the IP address and port number that will be mapped to. In most cases, they are the IP address and port of the system behind the FortiMail unit. In the above example, they are 10.10.10.42 and 8000.
6. 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.
Tunnel ID	Enter the WCCP tunnel ID assigned by FortiGate.
Local IP	Enter the IP address of the FortiMail interface that communicates with FortiGate.
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.

Using the 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* > *Network* > *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*.

Configuring administrator accounts and access profiles

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

This topic includes:

- About administrator account permissions and domains
- Configuring administrator accounts
- Configuring admin 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 web UI.

Access profiles and domain assignments together control which commands and areas an administrator account can access. ***Permissions result from an interaction of the two.***

The domain to which an administrator is assigned is one of:

- System

  The administrator can access areas regardless of whether an item pertains to the FortiMail unit itself or to a protected domain. Every administrator's permissions are restricted only by their access profile.
- a protected 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 or 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 web UI. (For more information on the display modes of the GUI, see "Basic mode versus advanced mode" on page 25.)

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 domain administrators' access profiles.

Table 14: Areas of the GUI that domain administrators cannot access

Monitor ***except*** for the *Personal quarantine* tab
System ***except*** for the *Administrator* tab

Table 14: Areas of the GUI that domain administrators cannot access

Domain & User ***except*** for the domain, its subdomains, associated domains, and user preference.
Policy > *Access Control* > *Receive* *Policy* > *Access Control* > *Delivery*
Profile > *Authentication*
Security ***except*** for *Security* > *Bayesian* > *User and Security* > *Block/Safe List*
Email Archiving
Log & Report

Access profiles assign either read, read/write, or no access to each area of the FortiMail software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an administrator access profile, see "Configuring admin profiles" on page 184.

About the "admin" account

Unlike other administrator accounts whose access profile is *super_admin_prof* and domain 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

In previous FortiMail releases (older than v5.1), when you add remote RADIUS or LDAP accounts to FortiMail for account authentication purpose, you must add them one by one on FortiMail. Starting from FortiMail v5.1, you can use the wildcard to add RADIUS accounts all at once. Starting from v5.2, you can also use the wildcard for LDAP accounts.

To achieve this, you can enable the preconfigured "remote_wildcard" account and specify which RADIUS or LDAP profile to use. Then every account on the RADIUS or LDAP server will be able to log on to FortiMail.

To add all accounts on a RADIUS or LDAP server to FortiMail

1. Go to *System* > *Administrator* > *Administrator*.
2. Double click the built-in "remote_wildcard" account.
3. Configure the following and click *OK*.

GUI item	Description
Enable	Select it to enable the wildcard account.
Administrator	The default name is remote_wildcard and it is not editable.

GUI item	Description
Domain	Select *System* for the entire FortiMail unit or the name of a protected domain, such as example.com, to which this administrator account will be assigned. For more information on protected domain assignments, see "About administrator account permissions and domains" on page 179. ***Note*:** If *Domain* is a protected domain, the administrator cannot use the CLI, or the basic mode of the web UI. ***Note***: If you enable domain override in the RADIUS profile, this setting will be overwritten by the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing protected domain. For details, see "Configuring authentication profiles" on page 446.
Access profile	Select the name of an access 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 admin profiles" on page 184. ***Note***: If you enable remote access override in the RADIUS profile, this access profile will be overwritten by the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing access profile. For details, see "Configuring authentication profiles" on page 446.
Authentication type	Select RADIUS or LDAP. And then select the RADIUS or LDAP profile. For details, see "Configuring authentication profiles" on page 446.
Trusted hosts	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`. **Note:** For additional security, restrict all trusted host entries to administrative hosts on your trusted private network. **Note:** For information on restricting administrative access protocols that can be used by these hosts, see "Editing network interfaces" on page 164.
Language	Select this administrator account's preference for the display language of the web UI. This setting overwrites the default language configured under System Customization > Appearance. See "Customizing the GUI appearance" on page 227.
Theme	Select this administrator account's preference for the display theme.\ This setting overwrites the default theme configured under System Customization > Appearance. See "Customizing the GUI appearance" on page 227.

Configuring administrator accounts

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

By default, FortiMail units have a single administrator account, `admin`. For more granular control over administrative access, you can create additional administrator accounts that are restricted to a specific protected domain and with restricted permissions. For more information, see "About administrator account permissions and domains" on page 179.

Depending on the type of administrators logging on to FortiMail, this list may not display all administrator accounts.

- For the super `admin` user, all administrators will be displayed.
- For administrators with super_admin_prof access profile, all administrators except for the super `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 more information on the system quarantine administrator account, see "Configuring the system quarantine setting" on page 502.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Others* category.

For details, see "About administrator account permissions and domains" on page 179.

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.

   A dialog appears.
3. Configure the following and then click *Create*:

GUI item	Description
Enable	Select it to enable the new account. If disabled, the account will not be able to 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.
Domain	Select *System for* the entire FortiMail unit or the name of a protected domain, such as example.com, to which this administrator account will be assigned. For more information on protected domain assignments, see "About administrator account permissions and domains" on page 179. **Note:** If *Domain* is a protected domain, the administrator cannot use the CLI, or the basic mode of the web UI.

GUI item	Description
Admin profile	Select the name of an admin 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 admin profiles" on page 184.
Authentication type	Select the local or remote type of authentication that the administrator will use: • *Local* • *RADIUS* • *PKI* • *LDAP* **Note:** RADIUS, LDAP and PKI authentication require that you first configure a RADIUS authentication profile, LDAP authentication profile, or PKI user. For more information, see "Configuring authentication profiles" on page 446 and "Configuring PKI authentication" on page 332.
Password	If you select Local as the authentication type, enter a secure password for this administrator account. The password can contain any character except spaces. This field does not appear if authentication type is not *Local* or *RADIUS+Local*.
Confirm password	Enter this account's password again to confirm it. This field does not appear if authentication type is not *Local* or *RADIUS+Local*.
LDAP profile	If you choose to use *LDAP* authentication, select an LDAP profile you want to use.
RADIUS profile	If you choose to use *RADIUS* or *RADIUS + Local* authentication, select a RADIUS profile you want to use.
PKI profile	If you choose to use PKI authentication, select a PKI profile you want to use.
Trusted hosts	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`. **Note:** For additional security, restrict all trusted host entries to administrative hosts on your trusted private network. **Note:** For information on restricting administrative access protocols that can be used by these hosts, see "Editing network interfaces" on page 164.

GUI item	Description
Language	Select this administrator account's preference for the display language of the web UI. This setting overwrites the default language configured under System Customization > Appearance. See "Customizing the GUI appearance" on page 227.
Theme	Select this administrator account's preference for the display theme.\ This setting overwrites the default theme configured under System Customization > Appearance. See "Customizing the GUI appearance" on page 227.

Configuring admin profiles

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

Admin profiles, in conjunction with the domain to which an administrator account is assigned, govern which areas of the web UI and CLI that an administrator can access, and whether or not they have the permissions necessary to change the configuration or otherwise modify items in each area.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see About administrator account permissions and domains.

To view and configure administrator accounts

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

GUI item	Description
Name	Displays the name of the administrator access profile.
(Green dot in column heading.)	Indicates whether or not the profile is being used in one or more administrator accounts. If so, a red dot appears in this column, and the profile cannot be deleted. **Note:** The access profile named *super_admin_prof* is always used by the `admin` administrator account, and cannot be deleted. In this case, a grey dot indicates only that the profile is not being used by any other administrator account.

2. Either click *New* to add an account or double-click an access profile to modify it.

   A dialog appears.
3. In *Profile Name*, enter the name for this access profile.

4. In the *Access Control* table, for each access control option, select the permissions to be granted to administrator accounts associated with this access profile. For details, see About administrator account permissions and domains.

   For 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.

Starting from 6.0.4 release, administrators with Read Only privileges to System Quarantine, Personal Quarantine, Archive, and Mail Queque categories cannot view emal contents anymore. Only administrators with Read-Write privileges can view email contents.

Configuring system time, options, and other system options

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

This topic includes:

- Configuring the time and date
- Configuring system options
- Configuring SNMP queries and traps

Configuring the time and date

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.

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

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

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 ports on the interfaces

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and 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. **Note:** For better security, use a low idle timeout value.
LCD Panel (models with LCD panels)	
PIN Protection	Enable to require administrators to first 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. **Caution:** For better security, always configure an LCD PIN; otherwise, anyone with physical access can reconfigure the unit.
Login Disclaimer Settings	The disclaimer message appears when an administrator or user logs in to the FortiMail unit web-based manager, the FortiMail Webmail, or the FortiMail unit to view the IBE encrypted email.
Login disclaimer	You can use the default disclaimer text or customize it.
Reset To Default (button)	If you have customized the disclaimer text but want to use the default text, select this button.

GUI item	Description
Apply to login page	*Admin*: Select to display the disclaimer message when the administrator logs in to the FortiMail unit web-based manager. *Webmail*: Select to display the disclaimer message when the user logs into the FortiMail Webmail. *IBE*: Select to display the disclaimer message when the user logs into the FortiMail unit to view the IBE encrypted email.
Password Policy	Displays the password policy for administrators, FortiMail Webmail users, and IBE encrypted email users.
Enable	Select to enable the password policy.
Minimum password length	Set the minimum acceptable length (8) for passwords.
Password must contain	Select any of the following special character types to require in a password. Each selected type must occur at least once in the password. *Uppercase letters* — A, B, C, ... Z *Lowercase letters* — a, b, c, ... z *Number* — 0 ... 9 *Non alphanumeric character* — punctuation marks, @,#, ... %
Apply password policy to	Select where to apply the password policy: *Administrators* — Apply to administrator passwords. If any password does not conform to the policy, require that administrator to change the password at the next login. *Local mail users* — Apply to FortiMail webmail users' passwords. If any password does not conform to the policy, require that user to change the password at the next login. *IBE users* — Apply to the passwords of the users who access the FortiMail unit to view IBE encrypted email. If any password does not conform to the policy, require that user to change the password at the next login.
Administration Ports	Specify the TCP ports for administrative access on all interfaces. Default port numbers: • HTTP: 80 • HTTPS: 443 • SSH: 22 • TELNET: 23

Configuring SNMP queries and traps

Go to *System* > *Configuration* > *SNMP* to configure SNMP to monitor FortiMail system events and thresholds, or a high availability (HA) cluster for failover messages.

You can also use SNMP to monitor some models which have monitored power supplies and RAID controllers. 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.

To monitor FortiMail system information and receive FortiMail traps, you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager. RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see "FortiMail MIBs" on page 192. For information on HA-specific MIB and trap MIB fields, see "Getting HA information using SNMP" on page 243.

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.

The FortiMail SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Before you can use its SNMP queries, you must enable SNMP access on the network interfaces that SNMP managers will use to access the FortiMail unit. For more information, see "Editing network interfaces" on page 164.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

This section includes:

- Configuring an SNMP threshold
- Configuring an SNMP v1 and v2c community
- Configuring an SNMP v3 user

Configuring an SNMP threshold

Configure under what circumstances an event is triggered.

To set SNMP thresholds

1. Go *System* > *Configuration* > *SNMP.*
2. Click the plus sign to expand the *SNMP Threshold* area.
3. Configure the following:

GUI item	Description
SNMP agent enable	Enable to activate the FortiMail SNMP agent. This must be enabled to accept queries from SNMP managers or send traps from the FortiMail unit.
Description	Enter a descriptive name for the FortiMail unit.
Location	Enter the location of the FortiMail unit.
Contact	Enter administrator contact information.
SNMP Threshold	To change a value in the four editable columns, select the value in any row. It becomes editable. Change the value and click outside of the field. A red triangle appears in the field's corner and remains until you click *Apply*.

GUI item	Description
Trap Type	Displays the type of trap, such as *CPU Usage*.
Trigger	You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.
Threshold	Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one, an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period.
Sample Period(s)	Sets the time period in seconds during which the FortiMail unit SNMP agent counts the number of triggers that occurred. This value should ***not*** be less than the *Sample Freq(s)* value.
Sample Freq(s)	Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the *Sample Period(s)* value.
Community	Displays the list of SNMP communities (for SNMP v1 and v2c) added to the FortiMail configuration. For information on configuring a community, see either "Configuring an SNMP v1 and v2c community" or "Configuring an SNMP v3 user" on page 191.
Name	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
Status	A green check mark icon indicates that the community is enabled.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.
User	Displays the list of SNMP v3 users added to the FortiMail configuration. For information on configuring a v3 user, see "Configuring an SNMP v3 user" on page 191.
Name	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
Status	A green check mark icon indicates that the user is enabled.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.
Security level	Displays the security level.

Configuring an SNMP v1 and v2c community

An SNMP community is a grouping of equipment for SNMP-based network administration purposes. You can add up to three SNMP communities so that SNMP managers can connect to

the FortiMail unit to view system information and receive SNMP traps. You can configure each community differently for SNMP traps and to monitor different events. You can add the IP addresses of up to eight SNMP managers to each community.

To configure an SNMP community

1. Go to *System* > *Configuration* > *SNMP*.
2. Under *Community*, click *New* to add a community or select a community and click *Edit*.

   The *SNMP Community* page appears.
3. Configure the following:

GUI item	Description
Name	Enter a name to identify the SNMP community. If you are editing an existing community, you cannot change the name. You can add up to 16 communities.
Enable	Enable to send traps to and allow queries from the community's SNMP managers.
Community Hosts	Lists SNMP managers that can use the settings in this SNMP community to monitor the FortiMail unit. Click *Create* to create a new entry. You can add up to 16 hosts.
IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP community.
Delete (button)	Click to remove this SNMP manager.
Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.
Queries	Enter the *Port* number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiMail unit. Mark the *Enable* check box to activate queries for each SNMP version.
Traps	Enter the *Local Port* and *Remote Port* numbers (162 local, 162 remote by default) that the FortiMail unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Enable traps for each SNMP version that the SNMP managers use.
SNMP Event	Enable each SNMP event for which the FortiMail unit should send traps to the SNMP managers in this community. ***Note***: Since FortiMail checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiMail checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

Configuring an SNMP v3 user

SNMP v3 adds more security by using authentication and privacy encryption. You can specify an SNMP v3 user on FortiMail so that SNMP managers can connect to the FortiMail unit to view system information and receive SNMP traps.

To configure an SNMP v3 user

1. Go to *System* > *Configuration* > *SNMP*.
2. Under *Users*, click *New* to add a user or select a user and click *Edit*.

   The *SNMPv3 User* page appears.

   You can add up to 16 users.
3. Configure the following:

GUI item	Description
User name	Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
Enable	Enable to send traps to and allow queries from the user's SNMP managers.
Security level	Choose one of the three security levels: • *No authentication, no privacy*: This option is similar to SNMP v1 and v2. • *Authentication, no privacy*: This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiMail. You must also specify the authentication protocol (either SHA1 or MD5). • *Authentication, privacy*: This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiMail must match.
Authentication Protocol	For *Security level*, if you select either *Authentication* option, you must specify the authentication protocol and password. Both the authentication protocol and password on the SNMP manager and FortiMail must match.
Privacy protocol	For *Security level*, if you select *Privacy,* you must specify the encryption protocol and password. Both the encryption protocol and password on the SNMP manager and FortiMail must match.
Notification Hosts	Lists the SNMP managers that FortiMail will send traps to. Click *Create* to create a new entry. You can add up to 16 host.
IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP user.
Delete (button)	Click to remove this SNMP manager.
Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.

GUI item	Description
Queries	Enter the *Port* number (161 by default) that the SNMP managers use for SNMP v3 queries to receive configuration information from the FortiMail unit. Select the *Enable* check box to activate queries.
Traps	Enter the *Local Port* and *Remote Port* numbers (162 local, 162 remote by default) that the FortiMail unit uses to send SNMP v3 traps to the SNMP managers. Select the *Enable* check box to activate traps.
SNMP Event	Enable each SNMP event for which the FortiMail unit should send traps to the SNMP managers. ***Note***: Since FortiMail checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiMail checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

FortiMail MIBs

The FortiMail SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiMail unit configuration.

The FortiMail MIBs are listed in the following table. You can obtain these MIB files from Fortinet technical support. To communicate with the SNMP agent, you must compile these MIBs into your SNMP manager.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

Table 15: FortiMail MIBs

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 “MIB fields” on page 193.
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 “FortiMail traps” on page 192.

FortiMail traps

The FortiMail unit’s SNMP agent can send traps to SNMP managers that you have added to SNMP communities. To receive traps, you must load and compile the FortMail trap MIB into the SNMP manager.

All traps sent 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.
fmlTrapArchiveEvent	Trap sent when remote archive event occurs.
fmlTrapIpChange	Trap sent when the IP address of the specified interface has been changed.

MIB fields

The Fortinet MIB contains fields reporting current FortiMail unit status information. The tables below list the names of the MIB fields and describe the status information available for each. You can view more details about the information available from all Fortinet MIB fields by compiling the MIB file into your SNMP manager and browsing the MIB fields.

Table 16: MIB fields

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.
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	HA event type ID.
fmlHAUnitIp	Unit IP address where the event occurs.
fmlHAEventReason	The reason for the HA event.
fmlArchiveServerIp	IP address of the remote Archive Server.
fmlArchiveFilename	Archive mail file name.

Table 17: 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.

Table 18: System session MIB fields

MIB field	Description
fmIIpSessTable	FortiMail IP sessions table.
fmIIpSessEntry	Particular IP session information.
fmIIpSessIndex	An index value that uniquely identifies an IP session.
fmIIpSessProto	The protocol of the connection.
fmIIpSessFromAddr	The session source IP address,
fmIIpSessFromPort	The session source port number.
fmIIpSessToAddr	The session destination IP address.
fmIIpSessToPort	The session destination port number.
fmIIpSessExp	Time (in seconds) until the session expires.

Table 19: Mail options MIB fields

MIB field	Description
fmIMailOptionsDeferQueue	The current number of deferred email messages.

Configuring mail settings

Go to *System* > *Mail Settings* to configure assorted settings that apply to the SMTP server and webmail server that are built into the FortiMail unit.

This section includes:

- Configuring mail server settings
- Configuring SMTP relay hosts
- Configuring global disclaimers
- Configuring disclaimer exclusion list
- Selecting the mail data storage location
- Configuring proxies (transparent mode only)

Configuring mail server settings

Use the mail server settings to configure SMTP server/relay settings of the *System* domain, which is located on the local host (that is, your FortiMail unit).

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure local SMTP server settings

1. Go to *System* > *Mail Settings* > *Mail Server Settings*.

   A multisection page appears.

2. Configure the following sections as needed:

- "Configuring local host settings" on page 196
- "Configuring DSN options" on page 198
- "Configuring mail queue setting" on page 198
- "Configuring outgoing email options" on page 199
- "Configuring deferred message delivery" on page 200
- "Configuring domain check options" on page 200

Configuring local host settings

Provide the name and SMTP information for the FortiMail server itself.

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" on page 196 and `example.com` is the "Local domain name" on page 197. **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 575.

GUI item	Description
Local domain name	Enter the local domain name to which the FortiMail unit belongs. 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" on page 196 and `example.com` is the "Local domain name" on page 197. **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/delete for the per-recipient quarantines may fail. **Note:** The "Local domain name" on page 197 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 qurantine 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.
SMTP server port number	Enter the port number on which the FortiMail unit's SMTP server will listen for SMTP connections. The default port number is 25.
SMTP over SSL/TLS	Enable to allow SSL- and 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 receive SMTPS connections. However, it does ***not*** require them. To enforce client use of SMTPS, see "Configuring access control rules" on page 363.
SMTPS server port number	Enter the port number on which the FortiMail unit's built-in MTA listens for secure SMTP connections. The default port number is 465. This option is unavailable if SMTP over SSL/TLS is disabled.
SMTP MSA service	Enable 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.

GUI item	Description
SMTP MSA port number	Enter the TCP port number on which the FortiMail unit listens for email clients to submit email for delivery. The default port number is 587.
POP3 server port number	Enter the port number on which the FortiMail unit's POP3 server will listen for POP3 connections. The default port number is 110. This option is available only if the FortiMail unit is operating in server mode.
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.
Webmail access	Enable to redirect HTTP webmail access to HTTPS.

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 144 and "Managing undeliverable mail" on page 146.

GUI item	Description
DSN (NDR) email generation	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.
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 mail queue setting

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 144 and "Managing undeliverable mail" on page 146.

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 199.
Time interval for retry	Select the number of minutes between delivery retries for email messages in the deferred and spam mail queues.
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 201.

GUI item	Description
Deliver to relay host	Select a relay that you configured in "Configuring SMTP relay hosts" on page 201.
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.

GUI item	Description
Delivery Failure Handling	When email delivery fails, you can choose to use the mail queue settings ("Configuring mail queue setting" on page 198) 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 • Network failure -- connection • Network failure -- other • Temporary failure from remote MTA (4XX reply code) • Permanent failure from remote MTA (5XX reply code)

Configuring deferred message delivery

You can choose to defer delivery of two types of email to conserve bandwidth and improve performance of the mail server:

- large email messages
- lower priority email from certain senders, for example, marketing campaign email and mass mailing

Oversized message delivery can be resource-intensive. 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 oversize email messages.
- In *Stop delivering messages at*, select the hour and minute of the day at which to stop delivering oversize email messages.

To configure the size limit or senders of deferred email, see "Configuring content profiles" on page 430.

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 465), 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" on page 201. 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, the verification is successful, and: • If "Automatically create domain association for verified domain" on page 201 is ***enabled***, the FortiMail unit automatically adds the unknown domain as a domain associated of the protected domain selected in *Internal domain to hold association*. • If "Automatically create domain association for verified domain" on page 201 is ***disabled***, and the LDAP domain name lookup of the unknown domain name is successful, the FortiMail unit routes the email to the IP address resolved for the domain name during the lookup. Because the domain is not formally defined as a protected domain, the email is considered to be outgoing, and outgoing recipient-based policies are used to scan the email. For more information, see "Controlling email based on sender and recipient addresses" on page 381.
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" on page 201 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 465. For more information about domain association, see "Domain Association" on page 318. 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 465) returned its own parent domain, that parent domain is used. This option is available only if "Automatically create domain association for verified domain" on page 201 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 199), 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 210.

Server relay is ignored if the FortiMail unit is operating in transparent mode, and "Use client-specified SMTP server to send email" on page 217 (for outgoing connections) or "Use this domain's SMTP server to deliver the mail" on page 314 (for incoming connections containing outgoing email messages) is enabled.

.

Server relay is ignored for email that matches an antispam or content profile where you have enabled "Deliver to alternate host" on page 429.

To configure STMP relays

1. Go to *System* > *Mail Settings* > *Relay Host List*. You can configure a maximum of 5 relays.
2. Click *New*.
3. Configure the following:

GUI item	**Description**
Name	Enter a descriptive name for this relay host.
Relay type	A relay host can be any of the following three types: • Host: specify the domain name or IP address of the relay. • MX Record: specify the domain name for the record for FortiMail to query. • IP Group: select an IP group. For details about IP groups, see "Configuring IP groups" on page 491.
Port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).

GUI item	**Description**
Use SMTPS	Enable to initiate SSL- and 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)

Configuring global disclaimers

The *System* > *Mail Settings* > *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 360.

If "Allow per-domain settings" on page 204 is enabled, you can configure disclaimer messages that are specific to each protected domain. For more information, see "Disclaimer for a domain" on page 320.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure disclaimer messages

1. Go to *System* > *Mail Settings* > *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 320.
Outgoing (or Incoming)	
Insert new 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.
Insert disclaimer at	Select to insert the disclaimer at the end or start of the email and click *Edit* to author a disclaimer. This disclaimer can be in HTML or text. The maximum length is 1024 characters.
Enable disclaimer exclusion list	If you do not want to insert disclaimers to the email messages from certain senders or to certain recipients, you can enable this option. For details about disclaimer exclusion list, see "Configuring disclaimer exclusion list" on page 204.

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 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 203), you can enable the exclusion list.

To create a disclaimer exclusion list

1. Go to *System* > *Mail Settings* > *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 and/or recipient pattern. For example, for sender pattern, if you add *@example.com, all messages from example.com users will be exempted from disclaimer insertion.
4. Click *Create*.

Selecting the mail data storage location

The *System* > *Mail Settings* > *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 the HA mode and group" on page 250.

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. For information about backing up mail data, see "Configuring mailbox backups" on page 302.

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 2003 R2 /Windows 2008 Service for NFS

If you do not need consolidated storage for the mail queue and email user inboxes, the higher FortiMail models (FortiMail VM02/400C series and above) 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.

FortiMail VM02, VM04, 400C, 400E, and 1000D models can host a maximum of 10 clients and FortiMail VM08/2000E and above models can host up to 20 clients. Any FortiMail model can be a client.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure mail data storage

1. Go to *System* > *Mail Settings* > *Storage*.
2. Configure the following:

GUI item	Description
NAS section	
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.
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.

GUI item	Description

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 TCP port number on which the NFS server listens for connections.
	  • *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*: the user name of the FortiMail unit's account on the iSCSI server.
	  • *Password*: the password of the FortiMail unit's account on the iSCSI server.
	  • *Hostname/IP address*: the IP address or fully qualified domain name (FQDN) of the iSCSI server.
	  • *Port*: the TCP port number on which the iSCSI server listens for connections.
	  • *Encryption key*: the 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*: 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).
	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.

GUI item	Description
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 section	
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. • *Name*: Enter a name to identify this client to the quarantine server. This value must match the name of the client as it is configured on the quarantine server. Otherwise, the connection will fail. • *Host*: Enter the IP address of the FortiMail unit that is acting as a centralized quarantine server.
Centralized IBE section	
Disabled	Select to store IBE encrypted email on the FortiMail unit's local disk or RAID.

GUI item	Description
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 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 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 Settings* > *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 307 and "Configuring session profiles" on page 389.

This section contains the following topics:

- About the transparent mode proxies
- Use client-specified SMTP server to send email

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.

- Incoming versus outgoing SMTP connections
- Transparency of the proxies and built-in MTA
- Avoiding scanning email twice
- Relaying using FortiMail's built-in MTA versus unprotected SMTP servers

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" on page 217 (for outgoing connections), or
- "Use this domain's SMTP server to deliver the mail" on page 314 (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, 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.

Table 20: Mail routing in transparent mode

Destination IP of connection	RCPT TO:	Configuration	Result

Table 20: Mail routing in transparent mode

SMTP Server (incoming connection)	A protected domain (incoming email)	N/A		Built-in MTA establishes session with SMTP Server
	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 131.

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" on page 308 field.
- Outgoing connections

  The destination IP address does ***not*** match any protected domain's "SMTP Server" on page 308 field.

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.

Figure 25: 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. It is possible that an incoming connection could contain an outgoing email message, and vice versa.

For example, in Figure 25 on page 212, 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.

For information on the concept of incoming versus outgoing at the application layer, see "Inbound versus outbound email" on page 360.

When the FortiMail unit is operating in transparent mode, directionality correlates with which proxy will be used, if any.

For example, in Figure 25 on page 212, 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" on page 308 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" on page 217, 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 314, 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 213.

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 390 option in each session profile
- select "Hide the transparent box" on page 313 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 217 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.

Avoiding scanning email twice

Depending on your network topology, in transparent mode, you may need to verify that the FortiMail unit is not scanning the same email twice.

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" on page 308). 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" on page 308 is configured with the IP address of an internal mail relay.

Table 21 on page 214 shows the configuration options that result in correct mail routing for this desired scenario. Figure 26 on page 214 shows the mail routing that would result from this configuration, in this topology.

Figure 26: Avoiding scanning email twice: Example 1 topology

Table 21: Avoiding scanning email twice: Example 1 configuration

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" on page 308	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" on page 308 is configured with the IP address of an internal mail relay.

Remote MUAs' outgoing email must not be routed through the internal mail relays.

Table 22 on page 216 shows the configuration options that result in correct mail routing for this desired scenario. Figure 27 on page 215 shows the mail routing that would result from this configuration, in this topology.

Figure 27: Avoiding scanning email twice: Example 2 topology

Table 22: Avoiding scanning email twice: Example 2 configuration

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" on page 308	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
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" on page 308 field 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 171 from external MTAs and "Outgoing connections" on page 171 (from remote MUAs) on port 2. (If we wanted to block remote MUAs only, we could simply select *Drop* for "Outgoing connections" on page 171 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 217, ***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. The 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.

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 Figure 25 on page 212.)

- 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 217 (for outgoing connections) and "Use this domain's SMTP server to deliver the mail" on page 314 (for incoming connections containing outgoing email messages).

Use client-specified SMTP server to send email

In FortiMail transparent mode, go to *System* > *Mail Settings* > *Proxies* 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 201, 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 210.

If this option is enabled, consider also enabling "Prevent open relaying" on page 401. 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 488.

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 375.

Customizing GUI, replacement messages and email templates

This section contains the following topics:

- Customizing replacement messages
- Customizing email templates
- Customizing the GUI appearance

Customizing replacement messages

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

When the FortiMail unit detects a virus in an email attachment, it replaces the attachment with a message that provides information about the virus and source of the email.

All the disclaimers, replacement 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.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

Viewing the replacement messages list

To view the replacement message list, go to *System* > *Customization* > *Custom Message.*

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

You can reword existing messages or create new ones.

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. For descriptions of the default replacement message variables, see "Default replacement message variables" on page 220.

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

To customize text replacement messages

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 replacement message.

   Some messages include a *Subject* and *From* area. You can edit their content too and add variables.
4. There is a limit of 4000 characters for each replacement message.
5. If custom variables exist, you can add them to the text. To do so:
   - Select *Insert Variables*. 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 Variables* link does not appear. Some message types include predefined variables. You can create variables. See "Creating variables" on page 219.
6. 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 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 replacement 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 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. Click *Insert Variables* to include any other existing variables, if needed. For example, you may enter
     The file %%FILE%% is infected with the virus %%VIRUS%%, and has been deleted
     where %%FILE%% is the file name and %%VIRUS%% provides the virus name.

     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*.

Table 23: Default replacement message variables

Variable	Description	Found under
%%FILE%%	The name of the file that is infected with a virus.	System > Customization > Custom Message > Replacement > Virus message
%%VIRUS%%	The name of the virus that has infected the file.	
%%FILE%%	The name of the file that was removed from the email.	System > Customization > Custom Message > Replacement > Suspicious message
%%EMAIL_ID%%	The ID that FortiMail assigns to the 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
%%ORIG_ENVELOPE_FROM%%	The original envelope sender address (MAIL FROM) 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.	

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%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 503.	
%%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.	

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%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 503.	
%%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
%%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.	

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%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_URI%%	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.	
%%URI_HELP%%	The Help link in the notification about secure email.	
%%FIRST_NAME%%	The first name of the notification recipient.	

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%LINK_URI%%	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.	
%%URI_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
%%SEMAIL_SUBJECT%%	The subject of the notification.	
%%URI_HELP%%	The Help link in the notification about secure email.	
%%LINK_URI%%	The link in the notification that you can click to open the secure message.	
%%URI_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

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%URI_ABOUT%%	The About link in the notification about secure email.	System > Customization > Custom Email Template > Secure message > Secure message notification - Push
%%SEMAIL_SUBJECT%%	The subject of the notification.	
%%URI_HELP%%	The Help link in the notification about secure email.	
%%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.	

Table 23: Default replacement message variables (continued)

Variable	Description	Found under
%%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.	

Customizing email templates

The FortiMail unit may send out notification email in the following cases:

- To send out quarantine reports (see "Configuring email quarantines and quarantine reports" on page 494)
- To send out IBE-related email (see "FortiMail IBE configuration workflow" on page 544)
- To repackage virus-infected email with new email body (see "Configuring antivirus action profiles" on page 427)
- To send out notification email to any mail recipient for any FortiMail actions (see "Configuring notification profiles" on page 491)

FortiMail allows you to customize the email templates for all the above mentioned email/report types.

To customize email templates

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

     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 you 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 web-based manager, per-recipient quarantine, and webmail pages 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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 web UI.
Product icon	Select *Change* to upload an icon that will be used as the favicon of the FortiMail web UI. The default icon is the Fortinet company icon.
Custom top logo	Select *Change* to upload a graphic that will appear at the top of all pages in the web UI. 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 at a later time.

GUI item	Description
Default language	Select the default language for the display of the web-based manager and the login page. You can configure a separate language preference for each administrator account. For details, see "Configuring administrator accounts" on page 182.
Default theme	Select the default display theme (red, green, blue, and light blue) for the display of the web-based manager and the login page. You can configure a separate theme preference for each administrator account. For details, see "Configuring administrator accounts" on page 182.
Webmail Portal	
Webmail login	Enter a word or phrase that will appears on top of the webmail login page, such as Webmail Login.
Login user name hint	Enter a hint for the user name, such as Your Email Address. This hint will appear as a mouse-over display on the login name field.
Login page	Select one of the following options: • *Default/Built-in*: uses the default login page. • *Customize*: edits the default page to create your own login page. • *3rd Party/Single Sign On*: uses 3rd party SSO for webmail login authentication. Currently FortiMail supports SAML SSO and Google G-Suite. Click *Edit* to import the IDP metadata and enter other required SSO information.
Allow user to change theme	If selected, the webmail users will be able to customize the theme by themselves.
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 a graphic 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 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 at a later time.

GUI item	Description
Default language	Select the language in which webmail pages will be displayed. By default, the FortiMail unit will use the same language as the web UI. For web UI language settings, see "Configuring system options" on page 186.
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 229. • *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

1. Go to *System* > *Customization* > *Appearance*.
2. Click the arrow to expand *Webmail interface*.
3. Underneath the list of language customizations, in *Language name in English*, enter the name for the new language using English and US-ASCII encoding, such as `Welsh`.
4. In *Language name*, enter the name for the language using its own characters and UTF-8 encoding.
5. Click *Create*.

   The new language appears at the bottom of the webmail languages list.
6. Select the new language's row.
7. Click *Download* and select *Download login page resource file* from the pop-up menu.
8. Click *Download* again and select *Download webmail resource file*.

   Your web browser downloads both files.
9. Open both files in an XML editor or plain text editor that supports UTF-8 encoding.
10. For each `value` in the resource files, 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.

11. Save both files.
12. Return to the web UI.
13. Select the new language's row.
14. Click *Upload* and select *Upload login page resource file* from the pop-up menu. Choose the login page resource file that you translated, then click *OK*.
15. Click *Upload* again and select *Upload webmail resource file* from the pop-up menu. Choose the login page resource file that you translated, then click *OK*.
16. 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.

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 for FortiMail models with software RAID controllers" on page 231 or "Configuring RAID on FortiMail models with hardware RAID controllers" on page 233.

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 562, and "Configuring alert email" on page 575.

If your FortiMail model does not support RAID, the tab in the *RAID* menu displays the message, `RAID is not available on this system.`

About RAID levels

Supported RAID levels vary by FortiMail model.

FortiMail 400B, 400C, and 5002B 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.

FortiMail 1000D, 2000B, 3000C, 3000D and 4000A models use hardware RAID controllers that require that the log disk and mail disk use the same RAID level.

FortiMail 100C, 200D, and 5001A 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 235.

The following tables describe RAID levels supported by each FortiMail model.

Table 24: 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
7 or more	10, 10 + hot spares, 50, 50 + hot spares	50 + hot spares

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 for FortiMail models with software RAID controllers

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 230.

GUI item	Description
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. After replacing the disk, add it to a RAID unit, then click *Re-scan*.

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 295.

2. In the *Level* column, click the row corresponding to the RAID device whose RAID level you want to change.

   The *Level* field changes to a drop-down menu.
3. Select RAID level 0 or 1.
4. Click *Apply*.

   A warning message appears.
5. Click *Yes* to confirm the change.

Configuring RAID on FortiMail models with hardware RAID controllers

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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 230.
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.
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 230. To change the RAID level, use *Set RAID level*.

GUI item	Description
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.
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. This option is not available on FortiMail-2000B/3000C models.
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. 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 295.

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*.

   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 web UI from its drive bay on the FortiMail unit.

   On a FortiMail-2000A or FortiMail-4000A, press in the tab, then pull the drive handle to remove the dive. On a FortiMail-2000B or FortiMail-3000C, press the button to eject the drive.

   To locate the correct hard disk to remove on a FortiMail-2000A, refer to the following diagram.

Drive 1 (p0)	Drive 4 (p3)
Drive 2 (p1)	Drive 5 (p4)
Drive 3 (p2)	Drive 6 (p5)

   To locate the correct hard disk to remove on a FortiMail-2000B or 3000C, refer to the following diagram.

Drive 1 (p0)	Drive 3 (p2)	Drive 5 (p4)
Drive 2 (p1)	Drive 4 (p3)	Drive 6 (p5)

To locate the correct hard disk to remove on a FortiMail-4000A, look for the failed disk. (Disk drive locations vary by the RAID controller model.)

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.

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 in order to increase processing capacity or availability.

For the general procedure of how to enable and configure HA, see "How to use HA" on page 244.

This section contains the following topics:

- About high availability
- About the heartbeat and synchronization
- About logging, alert email and SNMP in HA
- How to use HA
- Monitoring the HA status
- Configuring the HA mode and group
- Configuring service-based failover
- Example: Failover scenarios
- Example: Active-passive HA group in gateway mode

About high availability

FortiMail units can operate in one of two HA modes, active-passive or config-only.

Table 25: Comparison of HA modes

Active-passive HA	**Config-only HA**
2 FortiMail units in the HA group	2-25 FortiMail units in the HA group
Typically deployed behind a switch	Typically deployed behind a load balancer
Both configuration* and data synchronized	Only configuration* synchronized
Only primary unit processes email	All units process email

Table 25: Comparison of HA modes

No data loss when hardware fails	Data loss when hardware fails
Failover protection, but no increased processing capacity	**Increased processing capacity, but no failover protection**

* For exceptions to synchronized configuration items, see "Configuration settings that are not synchronized" on page 240.

Figure 28: Active-passive HA group operating in gateway mode

Figure 29: Config-only HA group operating in gateway mode

If the config-only HA group is installed behind a load balancer, the load balancer stops sending email to failed FortiMail units. All sessions being processed by the failed FortiMail unit must be restarted and will be re-directed by the load balancer to other FortiMail units in the config-only HA group.

You can mix different FortiMail models in the same HA group. However, all units in the HA group must have the same firmware version.

When mixing FortiMail models, the HA group is limited by the capacity and configuration limits of the least powerful model.

Communications between HA cluster members occur through the heartbeat and synchronization connection. For details, see "About the heartbeat and synchronization" on page 238.

To configure FortiMail units operating in HA mode, you usually connect only to the primary unit (*master*). The primary unit's configuration is almost entirely synchronized to secondary units (*slave*), so that changes made to the primary unit are propagated to the secondary units.

Exceptions to this rule include connecting to a secondary unit in order to view log messages recorded about the secondary unit itself on its own hard disk, and connecting to a secondary unit to configure settings that are not synchronized. For details, see "Configuration settings that are not synchronized" on page 240.

To use FortiGuard Antivirus or FortiGuard Antispam with HA, license all FortiMail units in the cluster. If you license only the primary unit in an active-passive HA group, after a failover, the secondary unit cannot connect to the FortiGuard Antispam service. For FortiMail units in a config-only HA group, only the licensed unit can use the subscription services.

For instructions of how to enable and configure HA, see "How to use HA" on page 244.

About the heartbeat and synchronization

Heartbeat and synchronization traffic consists of TCP packets transmitted between the FortiMail units in the HA group through the primary and secondary heartbeat interfaces.

Service monitoring traffic can also, for short periods, be used as a heartbeat. For details, see "Remote services as heartbeat" on page 254.

Heartbeat and synchronization traffic has three primary functions:

- to monitor the responsiveness of the HA group members
- to synchronize configuration changes from the primary unit to the secondary units

  For exceptions to synchronized configuration items, see "Configuration settings that are not synchronized" on page 240.
- to synchronize mail data from the primary unit to the secondary unit (active-passive only)

  Mail data consists of the FortiMail system mail directory, user home directories, and mail queue.

FortiGuard Antispam packages and FortiGuard Antivirus engines and definitions are not synchronized between primary and secondary units.

When the primary unit's configuration changes, it immediately synchronizes the change to the secondary unit (or, in a config-only HA group, to the peer units) through the primary heartbeat interface. If this fails, or if you have inadvertently de-synchronized the secondary unit's configuration, you can manually initiate synchronization. For details, see "Start configuration sync" on page 247. You can also use the CLI command `diagnose system ha sync` on either the primary unit or the secondary unit to manually synchronize the configuration. For details, see the *FortiMail CLI Reference*.

During normal operation, the secondary unit expects to constantly receive heartbeat traffic from the primary unit. Loss of the heartbeat signal interrupts the HA group, and, if it is active-passive in style, generally triggers a failover. For details, see "Failover scenario 1: Temporary failure of the primary unit" on page 261.

Exceptions include system restarts and the `execute reload` CLI command. In case of a system reboot or reload of the primary unit, the primary unit signals 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 262.

Periodically, the secondary unit checks with the primary unit to see if there are any configuration changes on the primary unit. If there are configuration changes, the secondary unit will pull the configuration changes from the primary unit, generate a new configuration, and reload the new configuration. In this case, both the primary and secondary units send alert email. For details, see "Failover scenario 3: System reboot or reload of the secondary unit" on page 263.

Behavior varies by your HA mode when the heartbeat fails:

- Active-passive HA

  A new primary unit is elected: the secondary unit becomes the new primary unit and assumes the duty of processing of email. During the failover, no mail data or configuration changes are lost, but some in-progress email deliveries may be interrupted. These interrupted deliveries may need to be restarted, but most email clients and servers can gracefully handle this. Additional failover behaviors may be configured. For details, see "On failure" on page 252.

Maintain the heartbeat connection. 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 simultaneously. For details on correcting this, see "Restore to configured operating mode" on page 248.

- Config-only HA

  Each secondary unit continues to operate normally. However, with no primary unit, changes to the configuration are no longer synchronized. You must manually configure one of the secondary units to operate as the primary unit, synchronizing its changes to the remaining secondary units.

For failover examples and steps required to restore normal operation of the HA group in each case, see "Example: Failover scenarios" on page 260.

HA default ports and protocols

The following default ports are used for HA heartbeat and synchronization. In case you have a firewall in between the primary and secondary units, make sure the following ports are allowed in your firewall policies:

UDP/20000	Base port for HA heartbeat signal
UDP/20001	Synchronization control
TCP/20002	File synchronization
TCP/20003	Data synchronization
TCP/20004	Checksum synchronization
TCP/25	HA service monitoring - remote SMTP
TCP/80	HA service monitoring - remote HTTP
TCP/110	HA service monitoring - remote POP3
TCP/143	HA service monitoring - remote IMAP

Configuration settings that are not synchronized

All configuration settings on the primary unit are synchronized to the secondary unit, except the following:

Table 26: HA settings not synchronized

Operation mode	You must set the operation mode (gateway, transparent, or server) of each HA group member before configuring HA.
Host name	The host name distinguishes members of the cluster. For details, see "Host name" on page 196.
Static route	Static routes are not synchronized because the HA units may be in different networks (see "Configuring static routes" on page 173).
Interface configuration (gateway and server mode only)	Each FortiMail unit in the HA group must be configured with different network interface settings for connectivity purposes. For details, see "Configuring the network interfaces" on page 163. Exceptions include some active-passive HA settings which affect the interface configuration for failover purposes. These settings are synchronized. For details, see "Virtual IP Address" on page 272.

Table 26: HA settings not synchronized

Management IP address (transparent mode only)	Each FortiMail unit in the HA group should be configured with different management IP addresses for connectivity purposes. For details, see "About the management IP" on page 161.
SNMP system information	Each FortiMail unit in the HA group will have its own SNMP system information, including the *Description*, *Location*, and *Contact*. For details, see "Configuring the network interfaces" on page 163.
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.
Main HA configuration	The main HA configuration, which includes the HA mode of operation (such as *master* or *slave*), is not synchronized because this configuration must be different on the primary and secondary units. For details, see "Configuring the HA mode and group" on page 250.
HA Daemon configuration	The following HA daemon settings are not synchronized: • *Shared password* • *Backup mail data directories* • *Backup MTA queue directories* You must add the shared HA password to each unit in the HA group. All units in the HA group must use the same shared password to identify the group. Since the mail data and MTA queue backup settings are not synchronized, to use this feature, you must enable it on both the master and slave units. For information about now to enable this feature, see "Configuring the backup options" on page 252. Synchronized HA daemon options that are active-passive HA settings affect how often the secondary unit tests the primary unit and how the secondary unit synchronizes configuration and mail data. Because HA daemon settings on the secondary unit control how the HA daemon operates, in a functioning HA group you would change the HA daemon configuration on the secondary unit to change how the HA daemon operates. The HA daemon settings on the primary unit do not affect the operation of the HA daemon.
HA service monitoring configuration	In active-passive HA, the HA service monitoring configuration is not synchronized. The remote service monitoring configuration on the secondary unit controls how the secondary unit checks the operation of the primary unit. The local services configuration on the primary unit controls how the primary unit tests the operation of the primary unit. For details, see "Configuring service-based failover" on page 258. **Note:** You might want to have a different service monitoring configuration on the primary and secondary units. For example, after a failover you may not want service monitoring to operate until you have fixed the problems that caused the failover and have restarted normal operation of the HA group.

Table 26: HA settings not synchronized

Product name and icon	The product names and icons under *System* > *Customization* > *Appearance* are not synchronized. All other appearance settings are synchronized.
Config-only HA	In config-only HA, the following settings are not synchronized: • the local domain name • default certificate • iSCSI initiator name • iSCSI ID for remote storage • SNMP settings • IP pools (see "Configuring IP pools" on page 488) • the quarantine report host name (see "Web release host name/IP" on page 496) • IBE settings of base URL, Help content URL, and About content URL • Centralized quarantine client IP address • Centralized IBE client IP address • Starting from 5.4.0 release, all system, domain, and user level block/safe lists are synchronized. Before 5.4.0 release, user-level block/safe lists are not synchronized. But system and domain-level block/safe lists are synchronized. Before v5.0.2 release, domain-level block/safe lists are not automatically synchronized either.

Synchronization of MTA queue directories after a failover

During normal operation, email messages are in one of three states:

- being received or sent by the primary unit
- waiting to be delivered in the mail queue
- stored on the primary unit's mail data directories (email quarantines, email archives, and email inboxes of server mode)

When normal operation of an active-passive HA group is interrupted and a failover 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.

You usually should configure HA to synchronize the stored mail data to prevent loss of email messages, but you usually will ***not*** want to regularly synchronize the mail queue. This is because, to prevent loss of email messages in the failed primary unit, FortiMail units in active-passive HA use the following failover mechanism:

If the failed primary unit effective HA operating mode is *failed*, a sequence similar to the following occurs automatically when the problem that caused the failure is corrected.

1. The secondary unit detects the failure of the primary unit, and becomes the new primary unit.

2. The former primary unit restarts, detects the new primary unit, and becomes a secondary unit.

You may have to manually restart the 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, as long as 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 in these directories will not be synchronized at the exact moment a failover occurs.

About logging, alert email and SNMP in HA

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. For details on configuring logging and viewing log messages, see "Logs, reports and alerts" on page 562.

To distinguish alert email from each member of the HA cluster, configure a different host name for each member. For details, see "Host name" on page 196.

To use SNMP, configure each cluster member separately and enable HA events for the community. If you enable SNMP for all units, they can all send SNMP traps. Additionally, you can use an SNMP server to monitor the primary and secondary units for HA settings, such as the HA configured and effective mode of operation. For details on SNMP, see "Configuring the network interfaces" on page 163.

To aid in quick discovery and diagnosis of network problems, consider configuring SNMP, Syslog, and/or alert email to monitor the HA cluster for failover messages.

Getting HA information using SNMP

You can use an SNMP manager to get information about how FortiMail HA is operating. The FortiMail MIB (fortimail.mib) and the FortiMail trap MIB (fortimail.trap.mib) include the HA fields listed below.

Table 27: FortiMail MIB fields

MIB Field	Description
	fortimail.mib
fmlHAEventId	Provides the ID of the most recent HA event.
fmlHAUnitIp	Provides the IP address of the port1 interface of the FortiMail unit on which an HA event occurred.
fmlHAEventReason	Provides the description of the reason for the HA event.
fmlHAMode	Provides the HA configured mode of operation that you configured the FortiMail unit to operate in; one of operation *master* (primary unit) or *slave* (secondary unit).
fmlHAEffectiveMode	Provides the effective HA mode of operation (applies to active-passive HA only), either as the primary unit or as the secondary unit. The effective HA mode of operation matches the configured mode of operation unless a failure has occurred.
	fortimail.trap.mib
fmlTrapHAEvent	Provides the FortiMail HA trap that is sent when an HA event occurs. This trap includes the contents of the `fmlSysSerial`, `fmlHAEventId`, `fmlHAUnitIp`, and `fmlHAEventReason` MIB fields.

How to use HA

In general, to enable and configure HA, you should perform the following:

1. If the HA cluster will use FortiGuard Antivirus and/or FortiGuard Antispam services, license all FortiMail units in the HA group for the FortiGuard Antispam and FortiGuard Antivirus services, and register them with the Fortinet Technical Support web site, https://support.fortinet.com/.
2. Physically connect the FortiMail units that will be members of the HA cluster.

   You must connect at least one of their network interfaces for heartbeat and synchronization traffic between members of the cluster. For reliability reasons, Fortinet recommends that you connect both a primary and a secondary heartbeat interface, and that they be connected directly or through a dedicated switch that is not connected to your overall network.
3. For config-only clusters, configure each member of the cluster to store mail data on a NAS server that supports NFS connections. (Active-passive groups may also use a NAS server, but do not require it.) For details, see "Selecting the mail data storage location" on page 204.
4. On each member of the cluster:
   - Enable the HA mode that you want to use (either active-passive or config-only) and select whether the individual member will act as a primary unit or secondary unit within the cluster. For information about the differences between the HA modes, see "About high availability" on page 236.
   - Configure the local IP addresses of the primary and secondary heartbeat and synchronization network interfaces.
   - For active-passive clusters, configure the behavior on failover, and how the network interfaces should be configured for whichever FortiMail unit is currently acting as the primary unit. Additionally, if the FortiMail units store mail data on a NAS, disable mail data synchronization between members.
   - For config-only clusters, if the FortiMail unit is a primary unit, configure the IP addresses of its secondary units; if the FortiMail unit is a secondary unit, configure the IP address of its primary unit.

   For details, see "Configuring the HA mode and group" on page 250.

5. If the HA cluster is active-passive and you want to trigger failover when hardware or a service fails, even if the heartbeat connection is still functioning, configure service monitoring. For details, see "Configuring service-based failover" on page 258.
6. Monitor the status of each cluster member. For details, see "Monitoring the HA status" on page 245. To monitor HA events through log messages and/or alert email, you must first enable logging of HA activity events. For details, see "Logs, reports and alerts" on page 562.

Monitoring the HA status

The *Status* tab in the *High Availability* submenu shows the configured HA mode of operation of a FortiMail unit in an HA group. You can also manually initiate synchronization and reset the HA mode of operation. A reset may be required if a FortiMail unit's effective HA mode of operation differs from its configured HA mode of operation, such as after a failover when a configured primary unit is currently acting as a secondary unit.

For FortiMail units operating as secondary units, the *Status* tab also lets you view the status and schedule of the HA synchronization daemon.

Appearance of the *Status* tab varies by:

- whether the HA group is active-passive or config-only
- whether the FortiMail unit is configured as a primary unit or secondary unit
- whether a failover has occurred (active-passive only)

If HA is disabled, this tab displays:

HA mode is currently disabled

Before you can use the *Status* tab, you must first enable and configure HA. For details, see "Configuring the HA mode and group" on page 250.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view the HA mode of operation status, go *System* > *High Availability* > *Status*.

Table 28: Viewing HA status

GUI item		Description
Mode Status		
	Configured Operating Mode	Displays the HA operating mode that you configured, either: • *master*: Configured to be the primary unit of an active-passive group. • *slave*: Configured to be the secondary unit of an active-passive group. • *config master*: Configured to be the primary unit of a config-only group. • *config slave*: Configured to be a secondary unit of a config-only group. For information on configuring the HA operating mode, see "Mode of operation" on page 251. After a failure, the FortiMail unit may not be acting in its configured HA operating mode. For details, see "Effective Operating Mode" on page 246.
	Effective Operating Mode	Displays the mode that the unit is currently operating in, either: • *master*: Acting as primary unit. • *slave*: Acting as secondary unit. • *off*: For primary units, this indicates that service/interface monitoring has detected a failure and has taken the primary unit offline, triggering failover. For secondary units, this indicates that synchronization has failed once; a subsequent failure will trigger failover. For details, see "On failure" on page 252 and "Restart the HA system" on page 248. • *failed*: Service/network interface monitoring has detected a failure and the diagnostic connection is currently determining whether the problem has been corrected or failover is required. For details, see "On failure" on page 252. The configured HA operating mode matches the effective operating mode unless a failure has occurred. For example, after a failover, a FortiMail unit configured to operate as a secondary unit could be acting as a primary unit. For explanations of combinations of configured and effective HA modes of operation, see "Monitoring the HA status" on page 245. For information on restoring the FortiMail unit to an effective HA operating mode that matches the configured operating mode, see "Restore to configured operating mode" on page 248. This option appears only if the FortiMail unit is a member of an active-passive HA group.

Table 28: Viewing HA status

GUI item	Description
Daemon Status	
Monitor	Displays the time at which the secondary unit's HA daemon will check to make sure that the primary unit is operating correctly, and, if monitoring has detected a failure, the number of times that a failure has occurred. Monitoring occurs through the heartbeat link between the primary and secondary units. If the heartbeat link becomes disconnected, the next time the secondary unit checks for the primary unit, the primary unit will not respond. If the maximum number of consecutive failures is reached, and no secondary heartbeat or remote service monitoring heartbeat is available, the secondary unit will change its effective HA operating mode to become the new primary unit. For details, see "HA base port" on page 254. This option appears only for secondary units in active-passive HA groups.
Configuration	Displays the time at which the secondary unit's HA daemon will synchronize the FortiMail configuration from the primary unit to the secondary unit. The message `slave unit is currently synchronizing` appears when the HA daemon is synchronizing the configuration. For information on items that are not synchronized, see "Configuration settings that are not synchronized" on page 240. This option appears only for secondary units in active-passive HA groups.
Data	Displays the time at which the secondary unit HA daemon will synchronize mail data from the primary unit to the secondary unit. The message `slave unit is currently synchronizing` appears when the HA daemon is synchronizing data. For details, see "Backup mail data directories" on page 253 and "Backup MTA queue directories" on page 253. This option appears only for secondary units in active-passive HA groups.
Start configuration sync	Click to manually initiate synchronization of the configurations. For information on items that are not synchronized, see "Configuration settings that are not synchronized" on page 240.

Table 28: Viewing HA status

GUI item	Description
Restore to configured operating mode	Click to reset the FortiMail unit to an effective HA operating mode that matches the FortiMail unit's configured operating mode. For example, for a configured primary unit whose effective HA operating mode is now *slave*, after correcting the cause of the failover, you might click this option on the primary unit to restore the configured primary unit to active duty, and restore the secondary unit to its slave role. This option appears only if the FortiMail unit is a member of an active-passive HA group. **Note:** Before selecting this option, if the effective HA operating mode changed due to failover, you should resolve any issues that caused the failover.
Switch to SLAVE mode	Click to manually switch the effective HA operating mode of the primary unit so that it becomes a secondary unit. This option appears only if the FortiMail unit is currently operating as a primary unit.
Restart the HA system	Click to restart HA processes after they have been halted due to detection of a failure by service monitoring. For details, see "On failure" on page 252, "Configuring service-based failover" on page 258, and "Restarting the HA processes on a stopped primary unit" on page 249. This option appears only if the FortiMail unit is configured to operate as the primary unit (*master*), but its effective HA operating mode is *off*.

Table 29: Combinations of configured and effective HA modes of operation

Configured operating mode	Effective operating mode	Description
master	master	Normal for the primary unit of an active-passive HA group.
slave	slave	Normal for the secondary unit of an active-passive HA group.
master	off	The primary unit has experienced a failure, or the FortiMail unit is in the process of switching to operating in HA mode. HA processes and email processing are stopped.

Table 29: Combinations of configured and effective HA modes of operation

Configured operating mode	Effective operating mode	Description
slave	off	The secondary unit has detected a failure, or the FortiMail unit is in the process of switching to operating in HA mode. After the secondary unit starts up and connects with the primary unit to form an HA group, the first configuration synchronization may fail in special circumstances. To prevent both the secondary and primary units from simultaneously acting as primary units, the effective HA mode of operation becomes *off*. If subsequent synchronization fails, the secondary unit's effective HA mode of operation becomes *master*.
master	failed	The remote service monitoring or local network interface monitoring on the primary unit has detected a failure, and will attempt to connect to the other FortiMail unit. If the problem that caused the failure has been corrected, the effective HA mode of operation switches from *failed* to *slave*, or to match the configured HA mode of operation, depending on the *On failure* setting. Additionally, f the HA group is operating in transparent mode, and if the effective HA mode of operation changes to *failed*, the network interface IP/netmask on the secondary unit displays *bridging (waiting for recovery)*. For details, see "Configuring the network interfaces" on page 163.
master	slave	The primary unit has experienced a failure but then returned to operation. When the failure occurred, the unit configured to be the secondary unit became the primary unit. When the unit configured to be the primary unit restarted, it detected the new primary unit and so switched to operating as the secondary unit.
slave	master	The secondary unit has detected that the FortiMail unit configured to be the primary unit failed. When the failure occurred, the unit configured to be the secondary unit became the primary unit.
config master	N/A	Normal for the primary unit of a config-only HA group.
config slave	N/A	Normal for the secondary unit of a config-only HA group.

Restarting the HA processes on a stopped primary unit

If you configured service monitoring on an active-passive HA group (see "Configuring service-based failover" on page 258) and either the primary unit or the secondary unit detects a service failure on the primary unit, the primary unit changes its effective HA mode of operation to *off*, stops processing email, and halts all of its HA processes.

After resolving the problem that caused the failure, you can use the following steps to restart the HA processes on the primary unit.

In this example, resolving this problem could be as simple as reconnecting the cable to the port2 network interface. Once the problem is resolved, use the following steps to restart the stopped primary unit.

To restart a stopped primary unit

1. Log in to the web-based manager of the primary unit.
2. Go to *System* > *High Availability* > *Status*.
3. Select *click HERE to restart the HA system*.

   The primary unit restarts and rejoins the HA group.

If a failover has occurred due to processes being stopped on the primary unit, and the secondary unit is currently acting as the primary unit, you can restore the primary and secondary units to acting in their configured roles. For details, see "Restore to configured operating mode" on page 248.

Configuring the HA mode and group

The *Configuration* tab in the *System* > *High Availability* submenu lets you configure the high availability (HA) options, including:

- enabling HA
- selecting whether the HA group is active-passive or config-only in style (for information on the differences, see Table 25 on page 236)
- whether this individual FortiMail unit will act as a primary unit or a secondary unit in the cluster
- network interfaces that will be used for heartbeat and synchronization
- service monitor

For an explanation of active-passive and config-only, see "About high availability" on page 236.

HA settings, with the exception of *Virtual IP Address* settings, are not synchronized and must be configured separately on each primary and secondary unit.

You must maintain the physical link between the heartbeat and synchronization network interfaces. These connections enable cluster members to detect the responsiveness of other members, and to synchronize data. If they are interrupted, normal operation will be interrupted and, for active-passive HA groups, a failover will occur. For more information on heartbeat and synchronization, see "About the heartbeat and synchronization" on page 238.

For an active-passive HA group, or a config-only HA group consisting of only two FortiMail units, directly connect the heartbeat network interfaces using a crossover Ethernet cable. For a config-only HA group consisting of more than two FortiMail units, connect the heartbeat network interfaces through a switch, and do not connect this switch to your overall network.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure HA options

1. Go to *System* > *High Availability* > *Configuration*.

   The appearance of sections and the options in them options vary greatly with your choice in the *Mode of operation* drop-down-list.

2. Configure the following sections, as applicable:

- "Configuring the primary HA options" on page 251
- "Configuring the master configuration IP" on page 252
- "Configuring the backup options" on page 252
- "Configuring the advanced options" on page 253
- "Configuring the slave system options" on page 254
- "Storing mail data on a NAS server" on page 255
- "Configuring interface monitoring" on page 255
- "Configuring service-based failover" on page 258

3. Click *Apply*.

Configuring the primary HA options

Go to *System* > *High Availability* > *Configuration* and click the arrow to expand the *HA configuration* section, if needed. The options presented vary greatly depending on your choice in the *Mode of operation* drop-down-list.

Table 30: HA main options

GUI item	Description
Mode of operation	Enables or disables HA, selects active-passive or config-only HA, and selects the initial configured role this FortiMail unit in the HA group. • *off*: The FortiMail unit is not operating in HA mode. • *master*: The FortiMail unit is the primary unit in an active-passive HA group. • *slave*: The FortiMail unit is the secondary unit in an active-passive HA group. • *config master*: The FortiMail unit is the primary unit in a config-only HA group. • *config slave*: The FortiMail unit is a secondary unit in a config-only HA group. **Caution:** For config-only 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. For details on configuring NAS, see "Storing mail data on a NAS server" on page 255 and "Selecting the mail data storage location" on page 204

Table 30: HA main options

GUI item	Description
On failure	Select one of the following behaviors of the primary unit when it detects a failure, such as on a power failure or from service/interface monitoring. • *switch off:* Do not process email or join the HA group until you manually select the effective operating mode (see "Restart the HA system" on page 248 and "Restore to configured operating mode" on page 248). • *wait for recovery then restore original role*: On recovery, the failed primary unit's effective HA mode of operation resumes its configured master role. This also means that the secondary unit needs to give back the master role to the primary unit. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent. • *wait for recovery then restore slave role*: On recovery, the failed primary unit's effective HA mode of operation becomes *slave*, and the secondary unit continue to assume the *master* role. The primary unit then synchronizes the content of its MTA queue directories with the current master unit. The new master unit can then deliver email that existed in the former primary unit's MTA queue at the time of the failover. For information on manually restoring the FortiMail unit to acting in its configured HA mode of operation, see "Restore to configured operating mode" on page 248. In most cases, you should select the *wait for recovery then restore slave role* option. This option appears only if "Mode of operation" on page 251 is *master*.
Shared password	Enter an HA password for the HA group. You must configure the same *Shared password* value on both the primary and secondary units.

Configuring the master configuration IP

If you are configuring the unit as the secondary unit in a config-only group, go to *System* > *High Availability* > *Configuration* to configure the master IP address.

In the *Master IP address* field, enter the IP of the primary heartbeat network interface of the primary unit. The secondary unit synchronizes only with this primary unit's IP address.

Configuring the backup options

Go to *System* > *High Availability* > *Configuration* to configure backup options, which appear only when the mode of operation is *master* or *slave*.

Because the backup settings are not synchronized, to use this feature, you must enable it on both the master and slave units.

Table 31: HA backup options

GUI item	Description
Backup mail data directories	Synchronize system quarantine, email archives, email users' mailboxes (server mode only), preferences, and per-recipient quarantines. Unless the HA cluster stores its mail data on a NAS server, you should configure the HA cluster to synchronize mail directories. If mail data changes frequently, you can manually initiate a data synchronization when significant changes are complete. For details, see "Start configuration sync" on page 247.
Backup MTA queue directories	Synchronize the mail queue of the FortiMail unit. For more information on the mail queue, see "Managing the mail queue" on page 144. **Caution:** 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. **Note:** 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 242.

Configuring the advanced options

Go to *System* > *High Availability* > *Configuration* to configure the advanced options. For config-only groups, just the *HA base port* option appears.

Table 32: HA advanced options

GUI item	Description
HA base port	Enter the first of four TCP port numbers that will be used for: • the heartbeat signal • synchronization control • data synchronization • configuration synchronization **Note:** For active-passive groups, in addition to configuring the heartbeat, you can configure service monitoring. For details, see "Configuring service-based failover" on page 258. **Note:** In addition to automatic immediate and periodic configuration synchronization, you can also manually initiate synchronization. For details, see "Start configuration sync" on page 247.
Heartbeat lost threshold	Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the secondary unit assumes the role of the primary unit. The heartbeat will continue to check for availability once per second. To prevent premature failover when the primary unit is simply experiencing very heavy load, configure a total threshold of three (3) seconds or more to allow the secondary unit enough time to confirm unresponsiveness by sending additional heartbeat signals. **Note:** If the failure detection time is too short, the secondary unit may falsely detect a failure when during periods of high load. **Caution:** If the failure detection time is too long the primary unit could fail and a delay in detecting the failure could mean that email is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover.
Remote services as heartbeat	Enable to use remote service monitoring as a secondary HA heartbeat. If enabled and both the primary and secondary heartbeat links fail or become disconnected, if remote service monitoring still detects that the primary unit is available, a failover will not occur. **Note:** The remote service check is only applicable for temporary heartbeat link fails. If the HA process restarts due to system reboot or HA daemon reboot, physical heartbeat connections will be checked first. If the physical connections are not found, the remote service monitoring does not take effect anymore. **Note:** Using remote services as heartbeat provides HA heartbeat only, not synchronization. To avoid synchronization problems, you should not use remote service monitoring as a heartbeat for extended periods. This feature is intended only as a temporary heartbeat solution that operates until you reestablish a normal primary or secondary heartbeat link.

Configuring the slave system options

This section appears only when the mode of operations is set to *config master* under *System > High Availability > Configuration.*

Table 33: HA peer options

GUI item	Description
Slave IP address	Double-click in order to modify, then enter the IP address of the primary network interface on that secondary unit.
Create	Click to add a secondary unit to the list of *Peer systems*, then double-click its *IP address*. The primary unit synchronizes only with secondary units in the list of *Peer systems*.
Delete	Click the row corresponding to a peer IP address, then click this button to remove that secondary unit from the HA group.

Storing mail data on a NAS server

For FortiMail units operating in server mode as a config-only HA group, you ***must*** store mail data on a NAS server instead of locally. If mail data is stored locally, email users' messages and other mail data could be scattered across multiple FortiMail units.

Even if your FortiMail units are not operating in server mode with config-only HA, however, storing mail data on a NAS server may have a number of benefits for your organization. For example, backing up your NAS server regularly can help prevent loss of mail data. Also, if your FortiMail unit experiences a temporary failure, 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 config-only HA groups using a network attached storage (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 a 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 details, see "Backup mail data directories" on page 253.

For instructions on storing mail data on a NAS server, see "Selecting the mail data storage location" on page 204.

Configuring interface monitoring

In active-passive HA mode, Interface monitor checks the local interfaces on the primary unit. If a malfunctioning interface is detected, a failover will be triggered.

To configure interface monitoring

1. Go to *System* > *High Availability* > *Configuration*.
2. Select master or slave as the mode of operation.

3. Expand the Interface area, if required.
4. Click on the port/interface name to configure the interface. For details, see "Configuring the network interfaces" on page 163.

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 groups)
- *Master configuration* (for secondary units in config-only groups)

Peer systems (for the primary unit on config-only groups)

5. Select a row in the table and click Edit to configure the following HA settings on the interface.

GUI item	Description
Port	Displays the interface name you're configuring.
Enable port monitor	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.

GUI item	Description
Heartbeat status	Specify if this interface will be used for HA heartbeat and synchronization. • Disable Do not use this interface for HA heartbeat and synchronization. • Primary Select the primary network interface for heartbeat and synchronization traffic. For more information, see "About the heartbeat and synchronization" on page 238. This network interface must be connected directly or through a switch to the *Primary heartbeat* network interface of other members in the HA group. • Secondary Select the secondary network interface for heartbeat and synchronization traffic. For more information, see "About the heartbeat and synchronization" on page 238. The secondary heartbeat interface is the backup heartbeat link between the units in the HA group. If the primary heartbeat link is functioning, the secondary heartbeat link is used for the HA heartbeat. If the primary heartbeat link fails, the secondary link is used for the HA heartbeat and for HA synchronization. This network interface must be connected directly or through a switch to the *Secondary heartbeat* network interfaces of other members in the HA group. **Caution**: Using the same network interface for both HA synchronization/heartbeat traffic and other network traffic could result in issues with heartbeat and synchronization during times of high traffic load, and is not recommended. **Note**: In general, you should isolate the network interfaces that are used for heartbeat traffic from your overall network. Heartbeat and synchronization packets contain sensitive configuration information, are latency-sensitive, and can consume considerable network bandwidth.
Peer IP address	Enter the IP address of the matching heartbeat network interface of the other member of the HA group. For example, if you are configuring the primary unit's primary heartbeat network interface, enter the IP address of the secondary unit's primary heartbeat network interface. Similarly, for the secondary heartbeat network interface, enter the IP address of the other unit's secondary heartbeat network interface. For information about configuration synchronization and what is not synchronized, see "About the heartbeat and synchronization" on page 238. This option appears only for active-passive HA.
Peer IPv6 address	Enter the peer IPv6 address in the active-passive HA group. For IPv6 support, see "About IPv6 Support" on page 160.

GUI item	Description
Virtual IP action	Select whether and how to configure the IP addresses and netmasks of the FortiMail unit whose effective HA mode of operation is currently *master*. For example, a primary unit might be configured to receive email traffic through *port1* and receive heartbeat and synchronization traffic through *port5* and *port6*. In that case, you would configure the primary unit to set the IP addresses or add virtual IP addresses for *port1* of the secondary unit on failover in order to mimic that of the primary unit. • *Ignore*: Do not change the network interface configuration on failover, and do not monitor. For details on service monitoring for network interfaces, see "Configuring the network interfaces" on page 163. • *Set*: Add the specified virtual IP address and netmask to the network interface on failover. Normally, you will configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. Both originating and reply traffic uses the virtual IP address. This option results in the network interface having two IP Addresses: the actual ***and*** the virtual. For examples, see "Example: Active-passive HA group in gateway mode" on page 267. In v3.0 MR2 and older releases, the behavior is different -- the originating traffic uses the actual IP address, instead of the virtual IP address. • *Bridge:* Include the network interface in the Layer 2 bridge. While the effective HA mode of operation is *slave*, the interface is deactivated and cannot process traffic, preventing Layer 2 loops. Then, when the effective HA mode of operation becomes *master*, the interface is activated again and can process traffic. This option appears only if the FortiMail unit is operating in transparent mode. This option is not available for Port1 and the ports not in the bridge group. For information on configuring bridging network interfaces, see "Editing network interfaces" on page 164. **Note:** Settings in this section are synchronizable. Configure the primary unit, then synchronize it to the secondary unit. For details, see "Start configuration sync" on page 247.
Virtual IP address	Enter the virtual IPv4 address for this interface.
Virtual IPv6 address	Enter the virtual IPv6 address for this interface. For IPv6 support, see "About IPv6 Support" on page 160.

Configuring service-based failover

Go to *System* > *High Availability* > *Configuration* to configure remote service monitoring, local network interface monitoring, and local hard drive monitoring.

Service monitoring is not available for config-only HA groups.

HA service monitoring settings are not synchronized and must be configured separately on each primary and secondary unit.

With remote service monitoring, the secondary unit confirms that it can connect to the primary unit over the network using SMTP service, POP service (POP3), and Web service (HTTP) connections. If you configure the HA pair in server mode, the IMAP service can also be checked.

With local network interface monitoring and local hard drive monitoring, the primary unit monitors its own network interfaces and hard drives.

If service monitoring detects a failure, the effective HA operating mode of the primary unit switches to *off* or *failed* (depending on the *On failure* setting) and, if configured, the FortiMail units send HA event alert email, record HA event log messages, and send HA event SNMP traps.A failover then occurs, and the effective HA operating mode of the secondary unit switches to *master*. For information on the *On failure* option, see "Configuring the HA mode and group" on page 250. For information on the effective HA operating mode, see "Monitoring the HA status" on page 245.

Remote service monitoring can be effective to configure in addition to, or sometimes as a backup alternative to, the heartbeat. While the heartbeat tests for the general responsiveness of the primary unit, it does not test for the failure of individual services which email users may be using such as POP3 or webmail. The heartbeat also does not monitor for the failure of network interfaces through which non-heartbeat traffic occurs. In this way, configuring remote service monitoring provides more specific failover monitoring. Additionally, if the heartbeat link is briefly disconnected, enabling HA services monitoring can prevent a false failover by acting as a temporary secondary heartbeat. For information on treating service monitoring as a secondary heartbeat, see "Remote services as heartbeat" on page 254.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure service monitoring

1. Go to *System* > *High Availability* > *Configuration*.
2. Select master or slave as the mode of operation.
3. Expand the service monitor area, if required.
4. Select a row in the table and click *Edit* to configure it.
5. For Remote SMTP, Remote IMAP, Remote POP, and Remote HTTP services, configure the following:

GUI item	Description
Enable	Select to enable connection responsiveness tests for SMTP.
Name	Displays the service name.
Remote IP	Enter the peer IP address.
Port	Enter the port number of the peer SMTP service.
Timeout	Enter the timeout period for one connection test.
Interval	Enter the frequency of the tests.
Retries	Enter the number of consecutively failed tests that are allowed before the primary unit is deemed unresponsive and a failover occurs.

6. For interface monitoring and local hard drive monitoring, configure the following:

GUI item	Description
Enable	Enable local hard drive monitoring to check if the local hard drive is still accessible, or if the mail data disk is almost full. If the hard disk is not responsive, or if the mail data disk is 95 percent full, a failover will occur. Interface monitoring is enabled when you configure interface monitoring. See "Configuring interface monitoring" on page 255. Network interface monitoring tests all active network interfaces whose: • *Virtual IP action* setting is ***not*** *Ignore* • *Configuring interface monitoring* setting is enabled For details, see "Configuring interface monitoring" on page 255 and "Virtual IP action" on page 258.
Interval	Enter the frequency of the test.
Retries	Specify the number of consecutively failed tests that are allowed before the local interface or hard drive is deemed unresponsive and a failover occurs.

Example: Failover scenarios

This section describes basic FortiMail active-passive HA failover scenarios. For each scenario, refer to the HA group shown in the following figure. To simplify the descriptions of these scenarios, the following abbreviations are used:

- P1 is the configured primary unit.
- S2 is the configured secondary unit.

Figure 30: Example active-passive HA group

This section contains the following HA failover scenarios:

This topic includes:

- Failover scenario 1: Temporary failure of the primary unit
- Failover scenario 2: System reboot or reload of the primary unit
- Failover scenario 3: System reboot or reload of the secondary unit
- Failover scenario 4: System shutdown of the secondary unit
- Failover scenario 5: Primary heartbeat link fails
- Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure)

Failover scenario 1: Temporary failure of the primary unit

In this scenario, the primary unit (P1) fails because of a software failure 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.

Here is what happens during this process:

1. The FortiMail HA group is operating normally.
2. The power is accidentally disconnected from P1.
3. S2's primary heartbeat test detects that P1 has failed.

   How soon this happens depends on the HA daemon configuration of S2.
4. The effective HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'MASTER heartbeat disappeared'
   The state changed from 'SLAVE' to 'MASTER'

6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from temporary failure of the primary unit

After P1 recovers from the hardware failure, what happens next to the HA group depends on P1's HA *On failure* settings under *System* > *High Availability* > *Configuration*.

Figure 31:HA On Failure settings

- *switch off*

  P1 will not process email or join the HA group until you manually select the effective HA operating mode (see "Restart the HA system" on page 248 and "Restore to configured operating mode" on page 248).

- *wait for recovery then restore original role*

  On recovery, P1's effective HA operating mode resumes its configured master role. This also means that S2 needs to give back the master role to P1. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent.

  In the case, the S2 will send out another alert email similar to the following:

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'SLAVE asks us to switch roles (recovery after a restart)
  The state changed from 'MASTER' to 'SLAVE'

  After recovery, P1 also sends out an alert email similar to the following:

  This is the HA machine at 172.16.5.10.

  The following critical event was detected
  The system was shutdown!

- *wait for recovery then restore slave role*

  On recovery, P1's effective HA operating mode becomes *slave*, and S2 continues to assume the *master* role. P1 then synchronizes the content of its MTA queue directories with the current master unit, S2. S2 can then deliver email that existed in P1's MTA queue directory at the time of the failover. For information on manually restoring the FortiMail unit to acting in its configured HA mode of operation, see "Restore to configured operating mode" on page 248.

Failover scenario 2: System reboot or reload of the primary unit

If you need to reboot or reload (not shut down) P1 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload <httpd...>`, or by clicking the *Restart* button under *Monitor* > *System Status* > *Status* on the GUI:

- P1 will send a holdoff command to S2 so that S2 will not take over the master role during P1's reboot.
- P1 will also send out an alert email similar to the following:

  This is the HA machine at 172.16.5.10.

The following critical event was detected
The system is rebooting (or reloading)!

- S2 will hold off checking the services and heartbeat with P1. Note that S2 will only hold off for about 15 minutes. In case P1 never boots up, S2 will take over the master role.
- S2 will send out an alert email, indicating that S2 received the holdoff command from P1.

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer rebooting (or reloading)'
  The state changed from 'SLAVE' to 'HOLD_OFF'

After P1 is up again:

- P1 will send another command to S2 and ask S2 to change its state from holdoff to slave and resume monitoring P1's services and heartbeat.
- S2 will send out an alert email, indicating that S2 received instruction commands from P1.

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer command appeared'
  The state changed from 'HOLD_OFF' to 'SLAVE'
- S2 logs the event in the HA logs.

Failover scenario 3: System reboot or reload of the secondary unit

If you need to reboot or reload (not shut down) S2 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload <httpd...>`, or by clicking the *Restart* button under *Dashboard* > *Status* on the GUI, the behavior of P1 and S2 is as follows:

For FortiMail v4.1 and newer releases:

- P1 will send out an alert email similar to the following, informing the administrator of the heartbeat loss with S2.

  This is the HA machine at 172.16.5.10.

  The following event has occurred
  'ha: SLAVE heartbeat disappeared'
- S2 will send out an alert email similar to the following:

  This is the HA machine at 172.16.5.11.

  The following critical event was detected
  The system is rebooting (or reloading)!
- P1 will also log this event in the HA logs.

For FortiMail v4.0 releases:

- P1 will not send out the alert email.
- P1 will log the event in the HA logs.

Failover scenario 4: System shutdown of the secondary unit

If you shut down S2:

- No alert email is sent out from either P1 or S2.
- P1 will log this event in the HA logs.

Failover scenario 5: 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 secondary unit (S2) changes to operating as a primary unit, and ***both*** FortiMail units are acting as primary units.

Two primary units connected to the same network may cause 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 web-based manager of S2 to restore its effective HA operating mode to *slave* (secondary unit).

1. The FortiMail HA group is operating normally.
2. The heartbeat link Ethernet cable is accidently 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 HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'MASTER heartbeat disappeared'
   The state changed from 'SLAVE' to 'MASTER'
6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from a heartbeat link failure

Because the hardware failure is not permanent (that is, the failure of the heartbeat link was caused by a disconnected cable, not a failed port on one of the FortiMail units), you may want to return both FortiMail units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect the primary heartbeat interface by reconnecting the heartbeat link Ethernet cable.

   Even though the effective HA operating mode of S2 is *master*, S2 continues to attempt to find the other primary unit. When the heartbeat link is reconnected, S2 finds P1 and determines that P1 is also operating as a primary unit. So S2 sends a heartbeat signal to notify P1 to stop operating as a primary unit. The effective HA operating mode 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 172.16.5.10

   The following event has occurred

   'SLAVE asks us to switch roles (user requested takeover)'

   The state changed from 'MASTER' to 'OFF'

3. P1 records event log messages (among others) indicating that P1 is switching to *off* mode.

   The configured HA mode of operation of P1 is *master* and the effective HA operating mode of P1 is *off*.

   The configured HA mode of operation of S2 is *slave* and the effective HA operating mode of S2 is *master*.

   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 web-based manager of P1, go to *System* > *High Availability* > *Status*.
5. Check for synchronization messages.

   Do not proceed to the next step until P1 has synchronized with S2.
6. Connect to the web-based manager of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.

   The HA group should return to normal operation. P1 records the event log message (among others) indicating that S2 asked P1 to return to operating as the primary unit.
7. P1 and S2 synchronize their MTA queue directories. All email in these directories can now be delivered by P1.

Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure)

Depending on your network configuration, the network connection between the primary and secondary units can fail for a number of reasons. In the network configuration shown in Figure 30 on page 260, the connection between port1 of primary unit (P1) and port1 of the secondary unit (S2) can fail if a network cable is disconnected or if the switch between P1 and S2 fails.

A more complex network configuration could include a number of network devices between the primary and secondary unit's non-heartbeat network interfaces. In any configuration, remote service monitoring can only detect a communication failure. Remote service monitoring cannot determine where the failure occurred or the reason for the failure.

In this scenario, remote service monitoring has been configured to make sure that S2 can connect to P1. The *On failure* setting located in the HA main configuration section is *wait for recovery then restore slave role*. For information on the *On failure* setting, see "On failure" on page 252. For information about remote service monitoring, see "Configuring service-based failover" on page 258.

The failure occurs when power to the switch that connects the P1 and S2 port1 interfaces is disconnected. Remote service monitoring detects the failure of the network connection between the primary and secondary units. Because of the *On failure* setting, P1 changes its effective HA operating mode to *failed*.

When the failure is corrected, P1 detects the correction because while operating in failed mode P1 has been attempting to connect to S2 using the port1 interface. When P1 can connect to S2, the effective HA operating mode of P1 changes to *slave* and the mail data on P1 will be synchronized to S2. S2 can now deliver this mail. The HA group continues to operate in this manner until an administrator resets the effective HA modes of operation of the FortiMail units.

1. The FortiMail HA group is operating normally.
2. The power cable for the switch between P1 and S2 is accidently disconnected.
3. S2's remote service monitoring cannot connect to the primary unit.

   How soon this happens depends on the remote service monitoring configuration of S2.
4. Through the HA heartbeat link, S2 signals P1 to stop operating as the primary unit.
5. The effective HA operating mode of P1 changes to *failed*.

6. The effective HA operating mode of S2 changes to *master*.
7. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

   This is the HA machine at 172.16.5.11.

   The following event has occurred
   ‘MASTER remote service disappeared’
   The state changed from ‘SLAVE’ to ‘MASTER’
8. S2 logs the event (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
9. P1 sends an alert email similar to the following, indicating that P1 has stopped operating in HA mode.

   This is the HA machine at 172.16.5.10.

   The following event has occurred
   'SLAVE asks us to switch roles (user requested takeover)'

   The state changed from 'MASTER' to 'FAILED'
10. P1 records the following log messages (among others) indicating that P1 is switching to *Failed* mode.

Recovering from a network connection failure

Because the network connection failure was not caused by failure of either FortiMail unit, you may want to return both FortiMail units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect power to the switch.

   Because the effective HA operating mode of P1 is *failed*, P1 is using remote service monitoring to attempt to connect to S2 through the switch.
2. When the switch resumes operating, P1 successfully connects to S2.

   P1 has determined the S2 can connect to the network and process email.
3. The effective HA operating mode of P1 switches to *slave*.
4. P1 logs the event.
5. P1 sends an alert email similar to the following, indicating that P1 is switching its effective HA operating mode to *slave*.

   This is the HA machine at 172.16.5.10.

   The following event has occurred
   'SLAVE asks us to switch roles (user requested takeover)'

   The state changed from 'FAILED' to 'SLAVE'
6. P1 synchronizes the content of its MTA queue directories to S2. S2 can now deliver all email in these directories.

   The HA group can continue to operate with S2 as the primary unit and P1 as the secondary unit. However, you can use the following steps to restore each unit to its configured HA mode of operation.
7. Connect to the web-based manager of P1 and go to *System* > *High Availability* > *Status*.
8. Check for synchronization messages.

   Do not proceed to the next step until P1 has synchronized with S2.

9. Connect to the web-based manager of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.
10. Connect to the web-based manager of P1, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.

    P1 should return to operating as the primary unit and S2 should return to operating as the secondary unit.
11. P1 and S2 synchronize their MTA queue directories again. P1 can now deliver all email in these directories.

Example: Active-passive HA group in gateway mode

In this example, two FortiMail-400 units are configured to operate in gateway mode as an active-passive HA group.

The procedures in this example describe HA configuration necessary to achieve this scenario. Before beginning, verify that both of the FortiMail units are already:

- physically connected according to Figure 32 on page 268
- operating in gateway mode
- configured with the IP addresses for their *port3* and *port1* network interfaces according to Figure 32 on page 268, with the exception of the HA virtual IP address that will be configured in this example (for details, see "Editing network interfaces" on page 164)
- allowing HTTPS administrative access through their *port1* network interfaces according to Figure 32 on page 268

Figure 32: Virtual IP address for HA failover

The active-passive HA group is located on a private network with email users and the protected email server. All are behind a FortiGate unit which separates the private network from the Internet. The DNS server, remote email users, and external SMTP servers are located on the Internet.

For both FortiMail units:

port1	• connected to a switch which is connected only to the computer that the FortiMail administrator uses to manage the HA group • administrative access occurs through this port
port3	• connected to a switch which is connected to the private network and, indirectly, the Internet • email connections occur through this port
port6	• connected directly to each other using a crossover cable • heartbeat and synchronization occurs through this port

The secondary unit will become the new primary unit when a failover occurs. In order for it to receive the connections formerly destined for the failed primary unit, the new primary unit must adopt the failed primary unit's IP address. You will configure an HA virtual IP address on *port3* for this purpose.

While the configured primary unit is functional, the HA virtual IP address is associated with its *port3* network interface, which receives email connections. After a failover, the HA virtual IP address becomes associated with the new primary unit's *port3*. As a result, after a failover, the new primary unit (originally the secondary unit) will then receive and process the email connections.

This example contains the following topics:

- About standalone versus HA deployment
- Configuring the DNS and firewall settings
- Configuring the primary unit for HA operation
- Configuring the secondary unit for HA operation
- Administering an HA group

About standalone versus HA deployment

If you plan to convert a standalone FortiMail unit to a member of an HA group, first understand the changes you need to make for HA deployment shown in Figure 32 on page 268 in the context of its similarities and differences with a standalone deployment.

Examine the network interface configuration of a standalone FortiMail-400 unit in the following table.

Table 34: Example standalone network interface configuration

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; the target of your email DNS A records. (No administrative access.)
port5	Default	Not connected.
port6	Default	Not connected.

Similarly, for the HA group, DNS A records should target the IP address of the *port3* interface of the primary FortiMail-400 unit. Additionally, administrators should administer each FortiMail unit in the HA group by connecting to the IP address of each FortiMail unit's *port1*.

If a failover occurs, the network must be able to direct traffic to *port3* of the secondary unit ***without*** reconfiguring the DNS A record target. The secondary unit must cleanly and automatically substitute for the primary unit, as if they were a single, standalone unit.

Unlike the configuration of the standalone unit, for the HA group to accomplish that substitution, all email connections must use an IP address that transfers between the primary unit and the secondary unit according to which one's effective HA operating mode is currently *master*. This transferable IP address can be accomplished by configuring the HA group to either:

- set the IP address of the current primary unit's network interface
- add a virtual IP address to the current primary unit's network interface

In this example, the HA group uses the method of adding a virtual IP address. Email connections will not use the actual IP address of *port3*. Instead, all email connections will use only the virtual IP address 172.16.1.2, which is used by *port3* of whichever FortiMail unit's

effective HA operating mode is currently *master*. During normal HA group operation, this IP address resides on the primary unit. Conversely, after a failover occurs, this IP address resides on the former secondary unit (now the current primary unit).

Also unlike the configuration of the standalone unit, both *port5* and *port6* are configured for each member of the HA group. The primary unit's *port5* is directly connected using a crossover cable to the secondary unit's *port5*; the primary unit's *port6* is directly connected to the secondary unit's *port6*. These links are used solely for heartbeat and synchronization traffic between members of the HA group.

For comparison with the standalone unit, examine the network configuration of the primary unit in the following table.

Table 35: Example primary unit HA network interface configuration

Interface	IP/Netmask	Virtual IP address		Description
		Setting	IP address	
port1	192.168.1.5	Ignore		Administrative connections to this FortiMail unit. (Because the IP address does not follow the FortiMail unit whose effective mode is currently *master*, connections to this IP address are specific to this physical unit. Administrators can still connect to this FortiMail unit after failover, which may be useful for diagnostic purposes.)
port2, port4	Default	Ignore		Not connected.
port3	172.16.1.5	Set	172.16.1.2	Email connections to the FortiMail unit; the target of your email DNS MX and A records. Connections should ***not*** be destined for the actual IP address, but instead the virtual IP address (172.16.1.2) which follows the FortiMail unit whose effective HA operating mode is *master*. No administrative access.
port5	10.0.1.2	Ignore		Secondary heartbeat and synchronization interface.
port6	10.0.0.2	Ignore		Primary heartbeat and synchronization interface.

Because the "Virtual IP action" on page 258 settings are synchronized between the primary and secondary units, you do not need to configure them separately on the secondary unit. However, you must configure the secondary unit with other settings listed in Table 36.

Table 36: Example secondary unit HA network interface configuration

Interface	IP/Netmask	Virtual IP Address		Description
		Setting	IP address	
port1	192.168.1.6	(synchronized from primary unit)	(synchronized from primary unit)	Administrative connections to this FortiMail unit. (Because the IP address does not follow the FortiMail unit whose effective mode is currently *master*, connections to this IP address are specific to this physical unit. Administrators can connect to this FortiMail unit even when it is currently the secondary unit, which may be useful for HA configuration and log viewing.)
port2, port4	Default	(synchronized from primary unit)	(synchronized from primary unit)	Not connected.
port3	172.16.1.6	(synchronized from primary unit)	(synchronized from primary unit)	Connections should ***not*** be destined for the actual IP address, but instead the virtual IP address (172.16.1.2) which follows the FortiMail unit whose effective HA operating mode is *master*. As a result, no connections should be destined for this network interface until a failover occurs, causing the secondary unit to become the new primary unit. No administrative access.
port5	10.0.1.4	(synchronized from primary unit)	(synchronized from primary unit)	Secondary heartbeat and synchronization interface.
port6	10.0.0.4	(synchronized from primary unit)	(synchronized from primary unit)	Primary heartbeat and synchronization interface.

Configuring the DNS and firewall settings

In the example shown in Figure 32 on page 268, SMTP clients will connect to the virtual IP address of the primary unit. For SMTP clients on the Internet, this connection occurs through the public network virtual IP on the FortiGate unit, whose policies allow the connections and route them to the virtual IP on the current primary unit.

Because the FortiMail HA group is installed behind a firewall performing NAT, the DNS server hosting records for the domain example.com must be configured to reflect the public IP address of the FortiGate unit, rather than the private network IP address of the HA group.

The DNS server has been configured with:

- an MX record to indicate that the FortiMail unit is the email gateway for example.com
- an A record to resolve fortimail.example.com into the FortiGate unit's public IP address
- a reverse DNS record to enable external email servers to resolve the public IP address of the FortiGate unit into the domain name of the FortiMail unit

Configuring the primary unit for HA operation

The following procedure describes how to prepare a FortiMail unit for HA operation as the primary unit according to Figure 32 on page 268.

Before beginning this procedure, verify that you have completed the required preparations described in "Example: Active-passive HA group in gateway mode" on page 267.

To configure the primary unit for HA operation

1. Connect to the web-based manager of the primary unit at https://192.168.1.5/admin.
2. Go to *System* > *Network.*
3. Configure port 6 to 10.0.0.2/255.255.255.0 and port 6 to 10.0.1.2/255.255.255.0.
4. Go to *System* > *High Availability* > *Configuration*.
5. Configure the following:

HA Configuration section	**.**
Mode of operation	master
On failure	wait for recovery then assume slave role
Shared password	change_me
Backup options section	See "Configuring the backup options".
Backup mail data directories	enabled
Backup MTA queue directories	disabled
Advanced options section	See "Configuring the advanced options".
HA base port	2000
Heartbeat lost threshold	15 seconds
Remote services as heartbeat	disabled
Interface section	See "Configuring interface monitoring".
Interface	port6
Enable port monitor	Enabled
Heartbeat status	Primary
Peer IP address	10.0.0.4
Interface	port5
Enable port monitor	Enabled
Heartbeat status	Secondary
Peer IP address	10.0.1.4
Virtual IP Address	

port1	Ignore
port2	Ignore
port3	Set 172.16.1.2/255.255.255.0
port4	Ignore
port5	Ignore
port6	Ignore

6. Click *Apply*.

   The FortiMail unit switches to active-passive HA mode, and, after determining that there is no other primary unit, sets its effective HA operating mode to *master*. The virtual IP 172.16.1.2 is added to *port3*; if not already complete, configure DNS records and firewalls to route email traffic to this virtual IP address, ***not*** the actual IP address of the *port3* network interface.

7. To confirm that the FortiMail unit is acting as the primary unit, go to *System* > *High Availability* > *Status* and compare the *Configured Operating Mode* and *Effective Operating Mode*. Both should be *master*.

   If the effective HA operating mode is ***not*** *master*, the FortiMail unit is ***not*** acting as the primary unit. Determine the cause of the failover, then restore the effective operating mode 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 Figure 32 on page 268.

Before beginning this procedure, verify that you have completed the required preparations described in "Example: Active-passive HA group in gateway mode" on page 267. Also verify that you configured the primary unit as described in "Configuring the primary unit for HA operation" on page 272.

To configure the secondary unit for HA operation

1. Connect to the web-based manager of the secondary unit at https://192.168.1.6/admin.
2. Go to *System* > *Network.*
3. Configure port 6 to 10.0.0.4/255.255.255.0 and port 6 to 10.0.1.4/255.255.255.0.
4. Go to *System* > *High Availability* > *Configuration*.
5. Configure the following:

Main Configuration section	See "Configuring the primary HA options"
Mode of operation	slave
On failure	wait for recovery then restore slave role
Shared password	change_me
Backup options section	See "Configuring the backup options".
Backup mail data directories	enabled

Backup MTA queue directories	disabled
Advanced options section	See “Configuring the advanced options”.
HA base port	2000
Heartbeat lost threshold	15 seconds
Remote services as heartbeat	disabled
Interface section	See “Configuring interface monitoring”.
Interface	port6
Heartbeat status	primary
Peer IP address	10.0.0.2
Interface	port5
Heartbeat status	secondary
Peer IP address	10.0.1.2
Virtual IP Address	(Configuration of the ports will be synchronized with the primary unit, and are therefore not required to be configured on the secondary unit.)
port1	Ignore
port2	Ignore
port3	Set 172.16.1.2/255.255.255.0
port4	Ignore
port5	Ignore
port6	Ignore

6. Click *Apply*.

   The FortiMail unit switches to active-passive HA mode, and, after determining that the primary unit is available, sets its effective HA operating mode to *slave*.

7. Go to *System* > *High Availability* > *Status*.

8. Select *click HERE to start a configuration/data sync*.

   The secondary unit synchronizes its configuration with the primary unit, including “Virtual IP action” on page 258 settings that configure the HA virtual IP that the secondary unit will adopt on failover.

9. To confirm that the FortiMail unit is acting as the secondary unit, go to *System* > *High Availability* > *Status* and compare the *Configured Operating Mode* and *Effective Operating Mode*. Both should be *slave*.

   If the effective HA operating mode is ***not*** *slave*, the FortiMail unit is ***not*** acting as the secondary unit. Determine the cause of the failover, then restore the effective operating mode to that matching its configured HA mode of operation.

If the heartbeat interfaces are not connected, the secondary unit cannot connect to the primary unit, and so the secondary unit will operate as though the primary unit has failed and will switch its effective HA operating mode to *master*.

When both primary unit and the secondary unit are operating in their configured mode, configuration of the active-passive HA group is complete. For information on managing both members of the HA group, see "Administering an HA group" on page 275.

Administering an HA group

In most cases, you will an HA group by connecting to the primary unit as if it were a standalone unit.

Table 37: Management tasks performed on each HA group member

Connect to...	For...
Primary unit (192.168.1.5)	• synchronized configuration items, such as antispam settings • primary unit HA management tasks, such as viewing its effective HA operating mode and configuring its "Mode of operation" on page 251 and *"Shared password" on page 252* • viewing the log messages of the primary unit
Secondary unit (192.168.1.6)	• secondary unit HA management tasks, such as viewing its effective HA operating mode and configuring its "Mode of operation" on page 251 and *"Shared password" on page 252* • viewing the log messages of the secondary unit

If the initial configuration synchronization fails, such as if it is disrupted or the network cable is loose, you should manually trigger synchronization after changing the configuration of the primary unit. For information on manually triggering configuration synchronization, see "Start configuration sync" on page 247.

Some parts of the configuration are not synchronized, and must be configured separately on each member of the HA group. For details, see "Configuration settings that are not synchronized" on page 240.

Managing certificates

This section explains how to manage X.509 security certificates using the FortiMail web UI. Using the *Certificate* submenu, you can generate certificate requests, install signed certificates,

import CA root certificates and certificate revocation lists, and back up and restore installed certificates and private keys.

FortiMail uses certificates for PKI authentication in secure connections. PKI authentication is the process of determining if a remote host can be trusted with access to network resources. To establish its trustworthiness, the remote host must provide an acceptable authentication certificate by obtaining a certificate from a certification authority (CA).

You can manage the following types of certificates on FortiMail:

Table 38: Certificate types

Certificate type	Usage
CA certificates	FortiMail uses CA certificates to authenticate the PKI users, including administrators and web mail users. For details, see "Configuring PKI authentication" on page 332 and "Managing certificate authority certificates" on page 283.
Server certificates	FortiMail must present its local server certificate for the following secure connections: • the web UI (HTTPS connections only) • webmail (HTTPS connections only) • secure email, such as SMTPS, IMAPS, and POP3S For details, see "Managing local certificates" on page 276.
Personal certificates	Mail users' personal certificates are used for S/MIME encryption. For details, see "Configuring certificate bindings" on page 547.

This section contains the following topics:

- Managing local certificates
- Managing certificate authority certificates
- Managing the certificate revocation list
- Managing OCSP server certificates

Managing local certificates

System > *Certificate* > *Local Certificate* displays both the signed server certificates and unsigned certificate requests.

On this tab, you can also generate certificate signing requests and import signed certificates in order to install them for local use by the FortiMail unit.

FortiMail units require a local server certificate that it can present when clients request secure connections, including:

- the web UI (HTTPS connections only)
- webmail (HTTPS connections only)
- secure email, such as SMTPS, IMAPS, and POP3S

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view local certificates

1. Go to *System* > *Certificate* > *Local Certificate*.

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 278.
Download (button)	Click the row of a certificate file or certificate request file in order to select it, then click this button and select either: • *Download*: 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 280. • *Download PKCS12 File*: Download a PKCS #12 (.p12) file. For details, see "Downloading a PKCS #12 certificate" on page 282.
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 the "default."
Import (button)	Click to import a signed certificate for local use. For more information, see "Importing a certificate" on page 281.
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 "Obtaining and installing a local certificate" on page 278.

Obtaining and installing a local certificate

There are two methods to obtain and install a local certificate:

- If you already have a signed server certificate (a backup certificate, a certificate exported from other devices, and so on), you can import the certificate into FortiMail. For details, see "Importing a certificate" on page 281.
- Generate a certificate signing request on the FortiMail unit, get the request signed by a CA ,and import the signed certificate into FortiMail.

For the second method, follow these steps:

- Generating a certificate signing request
- Downloading a certificate signing request
- Submitting a certificate request to your CA for signing
- Importing a certificate

Generating a certificate signing request

You can generate a certificate request 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).

For other related steps, see "Obtaining and installing a local certificate" on page 278.

To generate a certificate request

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.

GUI item	Description
ID type	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. 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 web UI 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 163 and "Configuring dynamic DNS" on page 174. 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.

GUI item		Description
	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. This option cannot be changed, but appears in order to indicate that only RSA is currently supported.
Key size		Select a security key size of *1024 Bit*, *1536 Bit* or *2048 Bit*. Larger keys are slower to generate, but provide better security.

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 280.

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 "Obtaining and installing a local certificate" on page 278.

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 "Obtaining and installing a local certificate" on page 278.

To submit a certificate request

1. Using the web browser on the management computer, browse 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.
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 281.

Importing a certificate

You can upload Base64-encoded certificates in either privacy-enhanced email (PEM) or public key cryptography standard #12 (PKCS #12) format from your management computer to the FortiMail unit.

DER encoding is not supported in FortiMail version 4.0 GA and MR1 releases.

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 generated on the FortiMail unit and 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 "Obtaining and installing a local certificate" on page 278.

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. From *Type*, 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 "Obtaining and installing a local certificate" on page 278.
   - *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 file	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. This option appears only when *Type* is *PKCS12 certificate* or *Certificate*.

Downloading a PKCS #12 certificate

You can export certificates from the FortiMail unit to a PKCS #12 file for secure download and import to another platform, or for backup purposes.

To download a PKCS #12 file

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click the row that corresponds to the certificate in order to select it.
3. Click *Download*, then select *Download PKCS12 File* on the pop-up menu.

   A dialog appears.
4. In *Password* and *Confirm password*, enter the password that will be used to encrypt the exported certificate file. The password must be at least four characters long.
5. Click *Download*.
6. If your browser prompts you for a location to save the file, select a location.

   Your web browser downloads the PKCS #12 (.p12) file. For information on importing a PKCS #12 file, see "Importing a certificate" on page 281.

Managing certificate authority certificates

Go to *System* > *Certificates* > *CA Certificate* to view and import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

CA certificates are required by connections that use transport layer security (TLS), and by S/MIME encryption. For more information, see "Configuring TLS security profiles" on page 483 and "Configuring certificate bindings" on page 547. 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 332.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view a the list of CA certificates, go to *System* > *Certificate* > *CA Certificate*.

Table 39: Managing CA certificates

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.

Managing the certificate revocation list

The *Certificate Revocation List* tab lets you view and import certificate revocation lists.

To ensure that your FortiMail unit validates only valid (not revoked) certificates, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses. For more information, see "Managing OCSP server certificates" on page 284.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view remote certificates, go to *System* > *Certificate* > *Certificate Revocation List*.

Table 40: Managing certificate revocation lists

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.

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, rather than by importing certificate revocation lists (CRL). For information about importing CRLs, see "Managing the certificate revocation list" on page 283.

Remote certificates are required if you enable OCSP for PKI users. For more information, see "Configuring PKI authentication" on page 332.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view a the list of remote certificates, go to *System* > *Certificate* > *Remote*.

Table 41: Managing OCSP server certificates

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).

Table 41: Managing OCSP server certificates

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.

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 "Managing antivirus profiles" on page 425). 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 afterwards.

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 cloud service, see "FortiCloud service" on page 286.
Server name/IP	Enter the FortiSandbox host name or IP address. The port to use is 514. If you have a firewall in between FortiMail and FortiSandbox, make this port is allowed.
Notification email	This is the email address that FortiSandbox will use to send out notifications and reports. If you want to receive such email, enter your email address. For details, see the FortiSandbox documentation.
Statistics interval	Specify how long FortiMail should wait to retrieve some high level statistics from FortiSandbox. The default interval is 5 minutes. The statistics include how many malwares 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.
File Scan Settings	

GUI item	Description
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.
URI Scan Settings	
Enable	Enable to scan the URIs to determine if they are malicious or phishing sites. ***Note***: If you do not want to send any URIs to FortiSandbox, you can do so by adding them to the URL exempt list. For details, see "Configuring the URL exempt list" on page 523.
Email selection	Specify to scan URIs in all email or the suspicious email only. Suspicious email messages are those received during spam outbreaks.
URI selection	Specify to scan all URIs or the unrated URIs only. The unrated URIs are the URIs that are tagged as unrated by the FortiGuard antispam service.
Upload URI 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 URIs to FortiSandbox for scanning. Choosing not to upload those URIs may help improving the FortiSandbox performance.
Number of URIs per email	Specify how many URIs will be scanned in one email message.

FortiCloud service

FortiCloud service, or FortiSandbox cloud service, allows you to use the FortiSandbox antivirus service without owning your own FortiSandbox appliances.

To use the FortiCloud service

1. Go to *Dashboard* > *Status*.
2. Under *License Information*, click *Activate* besides *FortiCloud*.
3. In the popup dialog box, select *Create Account* and enter the required information; if you have already created an account, select *Login* and enter the required information. 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)*.
4. Go to *System* > *FortiSandbox* > *FortiSandbox* and select *Cloud* for *FortiSanbox type* in the *FortiSandbox Setting*. Also configure other scan settings (see "Using FortiSandbox antivirus inspection" on page 285).

5. 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.

6. 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.

Figure 33: License information after upgrading from older releases

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

Configuring FortiGuard services

FortiMail uses Fortinet FortiGuard antivirus, antispam, and URI protection services.

Go to *System* > *FortiGuard* > *License* to view 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 support two kinds of automatic update mechanisms:

- scheduled updates, by which the FortiMail unit periodically polls the FDN to determine if there are any available updates
- push updates, by which the FDN notifies FortiMail units when updates become available

You may want to configure both scheduled and push updates. In this way, if the network experiences temporary problems such as connectivity issues that interfere with either method, the other method may still provide your FortiMail unit with updated protection. You can alternatively manually update the FortiMail unit by uploading an update file by going to *Dashboard* > *Status* and click *Update* under *Licence Information*.

For FortiGuard Antispam and FortiGuard Antivirus update connectivity requirements and troubleshooting information, see "Troubleshoot FortiGuard connection issues" on page 600.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

Verifying connectivity with FortiGuard services

If you subscribe to FortiGuard Antivirus and/or FortiGuard Antispam services, your FortiMail unit needs to connect to the FortiGuard Distribution Network (FDN) in order to verify its license and use the services.

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

FortiMail units use multiple connection types with the FDN. To completely verify connectivity, you should test each connection type by performing both of the following procedures.

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.

Before performing the following 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. For more information, see the FortiMail CLI Reference.

If the FortiMail unit connects to the Internet/FDN servers through a proxy, FortiMail can only get updates for the antivirus engine, antivirus signatures, and heuristic antispam rules from the FDN server. FortiMail cannot connect to the FDN server to perform realtime FortiGuard antispam queries through the proxy. In this case, you can only use a FortiManager unit locally as the override server.

To verify scheduled update connectivity

1. Go to *System* > *FortiGuard* > *Update*.
2. If you want your FortiMail unit to connect to a specific FDN other than the default for its time zone, enable *Use override server address*, enter the fully qualified domain name (FQDN) or IP address of the FDN.

If you want to use a FortiManager unit as the override server, enter the FortiManager IP address and port number (8890), such as 192.168.1.1:8890.

On the FortiManager side, use the following CLI command to enable FortiMail support. The default setting is disable.

```
config fmupdate support-pre-fgt43
  set status enable
end
```

3. Click *Apply*.
4. Click *Refresh*.

   A dialog appears, notifying you that the process could take a few minutes.
5. Click *OK*.

The FortiMail unit tests the connection to the FDN and, if any, the override server. Time required varies by the speed of the FortiMail unit's network connection, and the number of timeouts that occur before the connection attempt is successful or the FortiMail unit determines that it cannot connect. When the connection test completes, the page refreshes. Test results are as follows:

- *Available*: The FortiMail unit successfully connected to the FDN or override server.
- *Unavailable*: The FortiMail unit ***could not*** connect to the FDN or override server, and cannot download updates from it. For CLI commands that may assist you in troubleshooting, see "To configure the FortiGuard antispam options" on page 292.

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 antivirus definitions.

You can use push updates or manually initiate updates as alternatives or in conjunction with scheduled updates. If protection from the latest viral threats is a high priority, you could configure both scheduled updates and push updates, using scheduled updates as a failover method to increase the likelihood that the FortiMail unit always retrieves periodic updates if connectivity is interrupted during a push notification. While using ***only*** scheduled updates could potentially leave your network vulnerable to a new virus, it minimizes short disruptions to antivirus scans that can occur if the FortiMail unit applies push updates during peak volume times.

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. For details, see "Verifying connectivity with FortiGuard services" on page 288.

To configure FortiGuard antivirus options

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

Use override server address	Enable to override the default FDN server to which the FortiMail unit connects for updates, then enter the IP address of the override public or private FDN server.

Allow push update	Enable to allow the FortiMail unit to accept push notifications (UDP 9443). If the FortiMail unit is behind a NAT device, you may also need to enable and configure *Use override push IP*. Push notifications only notify the FortiMail unit that an update is available. They do not transmit the update itself. After receiving a push notification, the FortiMail unit then initiates a separate TCP 443 connection, similar to scheduled updates, in order to the FDN to download the update.
Use override push IP	Enable to override the IP address and default port number to which the FDN sends push notifications. • When enabled, the FortiMail unit notifies the FDN to send push updates to the IP address and port number that you enter (for example, a virtual IP/port forward on a NAT device that will forward push notifications to the FortiMail unit). • When disabled, the FortiMail unit notifies the FDN to send push updates to the FortiMail unit's IP address, using the default port number (UDP 9443). This is useful only if the FortiMail unit has a public network IP address. This option is available only if *Allow push update* is enabled.
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 you specify Enable with Defer in the above field, specify 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.
	• Extended: Some high-end FortiMail models support the usage of an extended virus database, which contains viruses that are not active any more.
	• 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.
	To use the extended and extreme virus databases, you must enable them with the following CLI command:
	`config system fortiguard antivirus`
	`  set virus-db {default | extended | extreme}`
	`end`

Scheduled update	Enable to perform updates according to a schedule, then select one of the following as the frequency of update requests. When the FortiMail unit requests an update at the scheduled time, results appear in *Last Update Status*. • *Every*: Select to request to update once every 1 to 23 hours, then select the number of hours between each update request. • *Daily*: Select to request to update once a day, then select the hour of the day to check for updates. • *Weekly*: Select to request to update once a week, then select the day of the week, the hour, and the minute of the day to check for updates. If you select *00* minutes, the update request occurs at a randomly determined time within the selected hour.

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. For details, see "Verifying connectivity with FortiGuard services" on page 288.

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 562.

Configuring FortiGuard antispam service

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

To configure the FortiGuard antispam options

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. Verify that the *Enable service* is enabled. Also specify the FortiGuard server port (the default number is 53).
3. Specify a spam outbreak protection level. Higher level means more strict filtering. 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 URI filter) returns no result (see "Configuring FortiGuard options" on page 411). 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.
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. Click *Apply*.

Manually querying FortiGuard antispam service

For testing or any other purposes, you may want to manually query the FortiGuard antispam service by entering an IP address, URI, or a Hash value of an email message.

To query FortiGuard antispam service

1. Go to *System* > *FortiGuard* > *License.*
2. Enter an IP, URI or hash value of an email message.
3. Click *Query*.

   If the query is successful, the *Query result* field will display if the IP/URI is spam or unknown (not spam).

   If the query is unsuccessful, the *Query result* field will display *No response*. In this case, you can use the following tips to troubleshoot the issue.

   If the FortiMail unit can reach the DNS server, but cannot successfully resolve the domain name of the FDN, a message appears notifying you that a DNS error occurred.

Figure 34: DNS error when resolving the FortiGuard Antispam domain name

4. Verify that the DNS servers contain A records to resolve `service.fortiguard.net` and other FDN servers. To try to obtain additional insight into the cause of the query failure, manually perform 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 has expired, a message appears notifying you that a connection error occurred.

   Figure 35: Connection error when verifying FortiGuard Antispam connectivity

5. Verify that:
   - this is no proxy in between FortiMail and the FDN server.
   - 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 (located in *System* > *Network* > *DNS*) and to the FDN servers
   - firewalls between the FortiMail unit and the Internet or override server allow FortiGuard Antispam rating query traffic.

     The default port number for FortiGuard antispam query is UDP port 53 in v4.0. Prior to v4.0, the port number was 8889.
6. To try to obtain additional insight into the point of the connection failure, trace 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* option.

   You can use the antispam log to monitor for subsequent query connectivity interruptions. When sending email through the FortiMail unit that matches a policy and profile where the *FortiGuard* option is enabled, if the FortiMail cannot connect to the FDN and/or its license is not valid, and if Information-level logging is enabled, the FortiMail unit records a log message in the antispam log (located in *Monitor* > *Log* > *AntiSpam*) whose *Log Id* field is `0300023472` and whose *Message* field is:

   ```
   FortiGuard-Antispam: No Answer from server.
   ```
7. 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 FortiGuard URI click protection service

When configuring the content profiles (see "Configuring content disarm and reconstruction" on page 433), you can choose what to do with the URIs contained in the email messages: either remove them or leave them.

However, if the URIs are not removed, there is a chance that email users may click and follow them. To protect users from harmful or spam URIs, such as phishing or advertising web sites, FortiMail uses FortiGuard URI filter service (see "Configuring a FortiGuard URI filter profile" on page 412) and FortiSandbox to scan the URIs after the users click the URIs. Depending on the

inspection results from FortiGuard and FortiSandbox, you can decide if you would allow the users to access the URIs or block them.

To configure FortiGuard URI click protection settings

1. Go to *System* > *FortiGuard* > *URI Protection* and configure the following:

GUI item		Description
URI Rewrite		FortiMail must rewrite URIs to ensure that the URIs will be directed to FortiMail first when users click the URIs.
	Category	Specify what URI categories will be rewritten.
	Base URL	Enter prefix “https://” and the FortiMail FQDN or IP address. Note that without the prefix, the URL will not work. The rewritten URI will be in this format: https://company.com/fmlurlsvc/?fewReq/baseValue&url=originalUrlEscaped. Using the originalUrlEscaped part, you can get the original URL with the help of a URL decoding web site, such as https://www.urldecoder.org.
URI Click Handling		When users click the URIs in the email messages, you can choose to block or allow their access.
	Category	Choose the URI category for the below action.
	Action	Specify either to *Block* or *Allow with Confirmation* for the above URI category.
	FortiSandbox Scan	For all other URI categories not specified above, you can choose to send them to FortiSandbox (see “Using FortiSandbox antivirus inspection” on page 285) for further scanning. **Enable**: Toggle to enable or disable FortiSandbox scan. **Action**: *Allow with Confirmation* means to allow access with warning; *Block* means to block access; and *Submit only* means to allow access while sending the URIs for scanning. **Timeout action**: When the URIs are sent to FortiSandbox for scanning, it may take a while to get the results back. You should specify how long you want to wait for the results before you take Block, Allow, or Allow with Confirmation actions. **Timeout**: Specify how long (in seconds) you want to wait for FortiSandbox scan results before you take Block, Allow, or Allow with Confirmation actions.
URI Removal		You can also choose to remove the URIs in the specified category.
	Category	Specify the URI category to remove the URIs.

System maintenance

The *Maintenance* menu contains features for use during scheduled maintenance: updates, backups, restoration, and centralized administration.

The *Maintenance* menu also lets you install firmware using one of the possible methods. For information on this and other installation methods and preparation, see "Installing firmware" on page 578.

This section includes:

- Backup and restore
- Using the traffic capture
- Configuring FortiGuard services

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 web UI and webmail

To access those parts of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read-Write* permission to ***all*** categories

For details, see "About administrator account permissions and domains" on page 179.

In addition, although they are not part of the configuration, you may want to back up the following data:

- email archives
- log files
- generated report files
- mailboxes

To back up the configuration file

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 204.

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*.

Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see "Restoring the configuration" on page 583.

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 informatoin and login credentials.
   - Click *Apply*.

To back up the Bayesian databases

1. Go to *System* > *Maintenance* > *Database Maintenance*.
2. Click *Backup Bayesian database*.

   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 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* > *Contacts*.
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 web UI and webmail UI

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 archivesGo 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 156 and "Configuring email archiving accounts" on page 555.

6. Continue using the instructions in "Configuring mailbox backups" on page 302.

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 295.

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

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*.

Restoring the configuration

In the *Restore Configuration* area under *System* > *Maintenance* > *Configuration*, you can restore the backup FortiMail configuration from your local PC, For details, see "Restoring the configuration" on page 583.

Restoring 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 580.

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 204), mail data cannot be backed up.

This section contains the following topics:

- Viewing the mailbox backup/restoration status
- Configuring mailbox backups
- Restoring mailboxes from backups

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

Table 42: 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 web UI automatically refreshes its display of this tab.
Refresh (button)	Click to manually refresh the tab's display.
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 302.

Table 42: Backing up and restoring mailboxes from *System* > *Maintenance* > *Mail Data*

GUI item		Description
	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 "Configuring mailbox backups" on page 302. • *RESTORING:* The FortiMail unit is currently restoring a backup copy of the mailboxes from the backup media configured in "Configuring mailbox backups" on page 302. • *STOPPING*: You have cancelled 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) in "Configuring mailbox backups" on page 302. • *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) in "Configuring mailbox backups" on page 302. 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 "Configuring mailbox backups" on page 302 and configured the restoration item correctly in "Restoring mailboxes from backups" on page 304. **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.

Table 42: Backing up and restoring mailboxes from *System* > *Maintenance* > *Mail Data*

GUI item		Description
	Percentage Complete	Indicates the percentage of bytes of data transferred to or from the backup media so far. 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 "Configuring mailbox backups" on page 302 and configured the restoration item correctly in "Restoring mailboxes from backups" on page 304.
	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 "Configuring mailbox backups" on page 302. 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 302. This link does not appear if a backup or restoration is currently in progress.

Table 42: Backing up and restoring mailboxes from *System* > *Maintenance* > *Mail Data*

GUI item	Description
Click here to format backup device	If you use a USB device for backup, use 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, use 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.

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. For information about selecting a storage device, see "Selecting the mail data storage location" on page 204.

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 298.

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.

GUI item		Description
Schedule		The *Schedule* options are disabled if *Protocol* is *External USB (auto detect)*.
	Day	Select either: • *None*: Disable scheduled backups. • *A day of the week*: Enable scheduled backups, and select which day of the week that the FortiMail unit will automatically back up email users' mailboxes to the backup media. Also configure *Hour*. 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. 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 298.
	Hour	Select which time on the day that you selected in *Day* that the FortiMail unit will automatically back up email users' mailboxes to the backup media. 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. This option is not available if *Day* is *None*.
Device		
	Protocol	Select one of the following types of backup media: • *NFS*: A network file system (NFS) server. • *SMB/Windows Server:* A 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 298, 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 with the device chosen.	

GUI item		Description
	Username	Enter the user name of the FortiMail unit's account on the backup server.
	Domain	If you choose SMB/Windows Server as the backup media AND if the account name has a domain part, you must enter the domain name as well.
	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 TCP 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. FortiMail v5.0 release supports both forward slash (/) and backslash (\) in the path name, while FortiMail v4.0 release only supports forward slash (/).
	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).

Restoring mailboxes from backups

The *Restore Options* area of the *Mail Data* tab lets you selectively restore email users' mailboxes from mailbox backups.

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 "Configuring mailbox backups" on page 302.

To configure restoration

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) 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 another FQDN or the FQDN of another FortiMail unit. Usually, you should enter an FQDN of this FortiMail unit, but you may enter the FQDN of another FortiMail unit if you want to import that FortiMail unit's mailbox backup. For example, assume you are upgrading to a FortiMail-2000 from a FortiMail-400 and have used a USB disk to store a backup of the mailboxes of the FortiMail-400, whose FQDN was fortimail.example.com. Configure the FortiMail-2000 to also use the USB disk as backup media. Then import the FortiMail-400's mailbox backup to the FortiMail-2000 by entering `fortimail.example.com` in this field for the FortiMail-2000.
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 drop-down list. If you want to restore only the mailbox of a specific email user within this protected domain, also configure *For this user*.

GUI item	Description
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 302. 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. **Note**: To restore from a specific full and incremental version of backup, you can use the CLI command "`execute backup-restore old-restore <full_int> <increments_int> domain <domain_str> user <user_str>`". **Caution:** Back up mailboxes before selecting this button. Restoring mailboxes overwrites all mailboxes that currently exist.

3. To manually initiate restoration of mail data, click *Restore*.

Downloading a trace file

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

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* > *Maintenance* > *Configuration*.
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.

This section includes:

- Configuring protected domains
- Configuring local user accounts (server mode only)
- Configuring user aliases
- Configuring address mappings
- Configuring IBE users
- Managing the address book (server mode only)
- Sharing calendars and address books (server mode only)
- Migrating email from other mail servers (server mode only)

Configuring protected domains

The *Domains* tab displays the list of 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

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.

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 318.

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

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

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 488.

To view and 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 one of the methods by which 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" on page 308 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.

GUI item	Description
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 318.

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. 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" on page 309. 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" on page 309 is enabled.

GUI item	Description
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" on page 311 and "Fallback SMTP server" on page 311. • *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" on page 311. • *IP Group:* Configure the connection to rotate among one or ***many*** protected SMTP servers for load balancing. Also configure the IP "IP group" on page 311. • *LDAP Domain Mail Host*: Query the LDAP server for the FQDN or IP address of the SMTP server. Also configure the *LDAP Profile* (see "Configuring LDAP profiles" on page 450). **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 reason, DNS lookups are skipped in gateway and server mode unless the sending domain is blank.

GUI item	Description
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" on page 311 and "Use SMTPS" on page 312. 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 360 and "Avoiding scanning email twice" on page 213. This field appears only if "Relay type" on page 310 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" on page 310 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" on page 310 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" on page 310 is *LDAP Domain Mail Host*.
Port	Enter the port number on which the SMTP server listens. If you enable "Use SMTPS" on page 312, "Port" on page 311 automatically changes to the default port number for SMTPS, but can still be customized. Displays the default SMTP port number is 25; the default SMTPS port number is 465. This field appears only if "Relay type" on page 310 is *Host*, *IP Group* or *LDAP Domain Mail Host*.
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" on page 310 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 450), 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.

GUI item	Description
Use SMTPS	Enable to use SMTPS for connections originating from or destined for this protected server. This field appears only if "Relay type" on page 310 is *Host*, *IP Group* or *LDAP Domain Mail Host*.
Relay Authentication	To test relay authentication, enable it and enter an email user name/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 EHLO, sender (MAIL FROM), and recipient (RCPT TO) information. Click *Test*. The test results will be dispalyed. **Note:** STARTTLS is not supported for relay host testing.

4. Configure the following sections as needed:
   - 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 multisection 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.
Use 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 TCP 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.
Use 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 450.

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:

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):

GUI item	Description

	`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" on page 380 in the IP-based policy, this option supsersedes the "Hide this box from the mail server" on page 390 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 201, 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 210. **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 *Use SMTP server* or *Use 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.

If you have also enabled *Recipient Address Verification (see* "Configuring recipient address verification" on page 312), 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.
Use SMTP server	Query the SMTP server to verify that the recipient address is an email user account that actually exists.
Use 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 450.

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.
1. Expand the *LDAP Options* section.
2. Configure the following:

GUI item	Description
LDAP 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. For more information, see "Configuring LDAP profiles" on page 450.

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 450.
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 450.

Configuring advanced settings

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

- Quarantine Report Setting
- Domain Association
- DKIM Setting
- Disclaimer for a domain
- Sender address rate control
- Other advanced 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.

Starting from FortiMail 4.1, domain-wide quarantine report settings are independent from the system-wide quarantine report settings.
However, in older releases, domain-wide quarantine report settings are a subset of the system-wide quarantine report settings. For example, if the system settings for schedule include only Monday and Thursday, when you are setting the schedule for the quarantine reports of the protected domain, you can select either Monday or Thursday.

For information on system-wide quarantine report settings and quarantine reports in general, see "Configuring global quarantine report settings" on page 495 and "Customizing GUI, replacement messages and email templates" on page 218.

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 Settings*.
4. Click to expand *Quarantine Report Setting*.
5. Configure the following:

GUI item		Description
Send to		
	Original recipient	Enable to send the quarantine report to all recipients. For more information, see "Managing the personal quarantines" on page 138.
	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 454. 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
Schedule		Click the arrow to expand the options.
	Setting	Select the schedule to use when sending quarantine reports. • *Use system settings*: Use the system-wide quarantine report schedule. For more information, see "Configuring global quarantine report settings" on page 495. • *Use domain settings*: Use a quarantine report schedule that is specific to this protected domain. Also configure "These Hours" on page 317 and "These Days" on page 317.
	These Hours	Select which hours to send the quarantine report for this protected domain. This option is available only when "Setting" on page 317 is *Use domain settings*.
	These Days	Select which days to send the quarantine report for this protected domain. This option is available only when "Setting" on page 317 is *Use domain settings*.
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.

This section does not appear in server mode.

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.

Associated domains do not re-use DKIM keys and signing settings. Domain keys are by nature tied to the exact protected domain only, and cannot be used for any other protected domain, including associated domains.

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

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 Settings*, 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 Setting

The *DKIM Setting* section appears when configuring an existing protected domain; that is, it does not appear when configuring a ***new*** domain. It lets you create domain keys for this protected domain.

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 389.

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.

After you generate the key pair by creating a domain key selector, 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+y
     DvGbfndyHZuVQdSHhwdKAdsfiyOa03iPniCfQEbuM0d+4/AoPyTXHHPFBBnChMMHkW
     gHYlRDm5UMjrH5J1zDT5OyFxUEur+NtfS6LF29Te+6vSS+D3asfZ85V6WJDHSI9JV0
     504uwDeOOh/aewIDAQAB"
```

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 a domain key pair

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Double-click to modify an existing protected domain.

Because information from the protected domain is used to generate the key pair, you cannot create DKIM keys while initially creating the protected domain.

3. Click to expand *Advanced Settings*.
4. Click to expand *DKIM Setting*.
5. In the text box to the left of *Create*, enter a selector to use for the DKIM key, such as `example_com2`.
6. 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, 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.

7. Click to select the domain key, then click *Download*.

   Your web browser downloads the plain text file which contains the exported DNS record (.dkim) file.

8. 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.

9. 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.

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 217.

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 Settings*.
4. Click to expand *Disclaimer*.

You cannot configure the domain disclaimer unless the *Allow per-domain settings* option is enabled on the *System* > *Mail Settings* > *Disclaimer* tab.

5. Configure the following:

GUI item	Description
Disclaimer	
Setting	Select which type of disclaimer message to append. • *Disable*: Do not append disclaimer messages. • *Use system settings*: Append the system-wide disclaimer messages. For more information, see "Configuring global disclaimers" on page 203. • *Use domain settings*: Append the disclaimer messages configured specifically for this protected domain. Also configure the per-domain disclaimer messages in *For Incoming Messages* and *For Outgoing Messages*. This option is available only if you have enabled per-domain disclaimer messages. For more information, see "Configuring global disclaimers" on page 203.
Disclaimer in incoming message header	Enable to use append a disclaimer message to the message header of incoming messages that is specific to this protected domain, then enter the disclaimer message. The maximum length is 256 characters. This option is available only if "Setting" on page 321 is *Use domain settings*.
Disclaimer in incoming message body	Enable to use append a disclaimer message to the message body of incoming messages that is specific to this protected domain, then enter the disclaimer message. The maximum length is 1024 characters. This option is available only if "Setting" on page 321 is *Use domain settings*.
Disclaimer in outgoing message header	Enable to use append a disclaimer message to the message header of outgoing messages that is specific to this protected domain, then enter the disclaimer message. The maximum length is 256 characters. This option is available only if "Setting" on page 321 is *Use domain settings*.
Disclaimer in outgoing message body	Enable to use append a disclaimer message to the message body of outgoing messages that is specific to this protected domain, then enter the disclaimer message. The maximum length is 1024 characters. This option is available only if "Setting" on page 321 is *Use domain settings*.

Sender address rate control

For users under this domain, you can rate control how much they 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 Settings*.

4. Click to expand *Sender Address Rate Control.*
5. For email users under this domain, you can configure the following rate control settings:
   - 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 sender 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 491).

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 307.

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 Settings* section.
4. Click to expand the *Other* section.
5. Configure the following:

GUI item	Description
Webmail language	Select either to use the default system language or a different language that the FortiMail unit will use to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same language as the web UI. For more information, see "Customizing the GUI appearance" on page 227.
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 > Scan Options). 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*, you can also set the message size limit. Here is how the two settings work together: • For outgoing email, only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. The smaller size will be used.

SMTP greeting (EHLO/HELO) Name (As Client)	Select how the FortiMail unit will identify itself during the `HELO` or `EHLO` greeting when delivering mail to the protected SMTP server as a client. • *Use this domain name*: The FortiMail unit will identify itself using the domain name for this protected domain. If the FortiMail unit will handle internal email messages (those for which both the sender and recipient addresses in the envelope contain the domain name of the protected domain), to use this option, you must also configure your protected SMTP server to use its host name for SMTP greetings. Failure to do this will result in dropped SMTP sessions, as both the FortiMail unit and the protected SMTP server will be using the same domain name when greeting each other. • *Use system host name*: The FortiMail unit will identify itself using its own host name. • *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. By default, the FortiMail unit uses the domain name of the protected domain. 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* ***Note***: IP pools are skipped for email delivery between protected domains. 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 313 or "Use client-specified SMTP server to send email" on page 217, you cannot use IP pools. For more information on IP pools, see "Configuring IP pools" on page 488.

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 You can alternatively remove this header from any matching email using session profiles. For details, see "Remove received header" on page 403.
Use global Bayesian database	Enable to use the global Bayesian database instead of the Bayesian database for this protected domain. If you do not need the Bayesian database to be specific to the protected domain, you may want to use the global Bayesian database instead in order to simplify database maintenance and training. Disable to use the per-domain Bayesian database. **Note:** Train the global or per-domain Bayesian database before using it. If you do not train it first, Bayesian scan results may be unreliable. For more information on Bayesian database types and how to train them, see "Types of Bayesian databases" on page 532 and "Training the Bayesian databases" on page 533.
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 523.

Domain level service settings (server mode only)

If you are a 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 307.

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 Settings*.
4. Configure the following under *Service Settings*:

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 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 356.

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.

This section includes:

- Configuring local user accounts (server mode only)
- Configuring user preferences
- Configuring PKI authentication

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 web UI 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 612.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

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

GUI item	Description
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as *Inbox, Drafts and Sent*. You can check the size of each mailbox, and empty or delete mailboxes as required. The *SecureMail* mailbox contains the secured email for the user. The *Bulk* mailbox contains spam quarantined by the FortiMail unit. Click *Back* to return to the *Users* tab.
Export .CSV (button)	Click to download a backup of the email users list in comma-separated value (CSV) file format. The user passwords are encoded for security. **Caution:** Most of the email user accounts data, such as mailboxes and preferences, is not included in the .csv file. For information on performing a complete backup, see "Backup and restore" on page 295.
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 328. 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 307. You may also want to back up the existing email user accounts. For details, see "Backup and restore" on page 295.
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 450.
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`. 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 307.

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 drop-down 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 in "Configuring user authentication options" on page 456.

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* is enabled. For details, see "Workflow to enable and configure authentication of email users" on page 445 and "Configuring resource profiles" on page 443.

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 359.

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 (non-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.)

   Figure 36: 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 web-based manager. For more information, see "Configuring LDAP profiles" on page 450.

6. Click *OK*.

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 443.

To empty a mailbox folder

1. Go to *Domain & User* > *User* > *U*ser.
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*.

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 web UI. Email users can modify their own preferences by logging in to the FortiMail webmail or email quarantine.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

To view and manage existing user preferences

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

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 drop-down menu with preference management options. Two options apply just to selected users: • *Clear SafeList for Selected Users* • *Clear BlockList for Selected Users* Other options apply to all users in the selected domain: • *Clear SafeList for All Domain Users* • *Clear BlockList for 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	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 227.

GUI item	Description
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 "Configuring the personal block lists and safe lists" on page 510.
Block List	The icon in this column indicates whether or not a personal block list currently exists for this email user. Hover the mouse pointer over the list icon to determine its status: • *New*: A personal block list does not exist for this email user. • *Edit:* A personal block list exists for this email user. Click the icon to open a dialog where you can configure, back up, or restore the personal block list. Block lists include sender IP addresses, domain names, and email addresses that the email user wants to block **Note:** System-level lists take precedence over domain-level lists while domain-level lists take precedence over personal-level lists. For more information on safe lists and block lists, see "Configuring the personal block lists and safe lists" on page 510.
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. 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.

GUI item	Description
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 "Configuring the personal block lists and safe lists" on page 510) 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.

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.

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 web UI (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 634.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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 333 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 283.

GUI item	Description
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 335 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 450. • 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.
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 283. If you select *None*, you ***must*** configure "Subject" on page 335.
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. If you do not configure "Subject" on page 335, you ***must*** configure "CA" on page 335.
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 335 and "Query field" on page 336. **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 drop-down 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 450. This option is available only if "LDAP query" on page 335 is enabled.

GUI item	Description	
	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 335 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" on page 336, "Remote certificate" on page 336, and "Unavailable action" on page 336.	
	URL	Displays the URL of the OCSP server. This option is available only if "OCSP" on page 336 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 284. This option is available only if "OCSP" on page 336 is enabled.
	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" on page 336 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 332.
3. In the web UI, import the CA certificate into the FortiMail unit. For more information, see "Managing certificate authority certificates" on page 283.
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 179.

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 381.

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.

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 450.

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Others* category.

For details, see "About administrator account permissions and domains" on page 179.

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.

   A dialog appears. Its features vary with the operation mode.
3. 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.*
4. If the FortiMail unit is operating in gateway or transparent mode, do the following:
   - Select the name of its protected domain from the drop-down 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*.
5. 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 users* 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 *Members* 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 *Members* area.
   - To remove members from the alias, select one or more email addresses in the *Members* area, then click <- arrow. The email addresses are removed from the *Members* area. Local email addresses return to the *Available users* area.
6. Click *Create* or *OK.*

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. They do not translate many email addresses into a single email address.

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. This 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.

Table 43: Match evaluation and rewrite behavior for email address mappings

Order of evaluation	Match condition	If yes...	Rewrite to...

Table 43: Match evaluation and rewrite behavior for email address mappings

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 with 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 450.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Others* category.

For details, see "About administrator account permissions and domains" on page 179.

To view and configure a 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.

GUI item	Description
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 Table 43 on page 339.
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 Table 43 on page 339. 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.

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 vice versa), this substitution will fail.

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 configure secure questions for forgotten passwords and IBE domains. For details about how to use IBE service, see "FortiMail IBE configuration workflow" on page 544.

This section contains the following topics:

- Configuring active users
- Configuring expired users
- Configuring security questions
- Configuring IBE authentication

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 345.
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.

GUI item	Description
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 changes 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 345.
Last Access	Displays the time stamp when: • the FortiMail unit sends a notification (*Pre-registered* status) • the mail recipient registers on the FortiMail unit (*Activated* status) • a mail user changes the password (*Password reset* status) • a mail recipient, who belongs to an IBE domain, authenticates on the FortiMail unit (*LDAP* status)

Configuring expired users

Depending on the configuration of *User registration expiry time* and *User inactivity expiry time* in the IBE service, if email recipients fail to register or authenticate on the FortiMail unit, or fail to access the FortiMail unit after registration for a certain period of time, they become expired users. For more information about IBE service configuration, see "Configuring IBE encryption" on page 543.

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.
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 345.

GUI item	Description
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 and last name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Status	Displays the expired user's status.
Last Access	Displays the time stamp when the user was last active.

Configuring security questions

There are several predefined security questions available to present to mail recipients when they register on the FortiMail unit. You can add questions.

To view the security questions, go to *Domain & User* > *IBE User* > *Secure Question.*

GUI item	Description
Edit (button)	Select a question and click *Edit* to modify it. You cannot edit a predefined question except to disable or enable it.
Language	From the drop-down list, select the language that applies to all questions on this page. For more information, see "Language" on page 344.
Enabled	Select to enable a question. Clear the check box to remove a question from use.
Question	Displays the content of the question in the selected language.
Language	Displays the language selected in the *Language* drop-down list..

To add a new security question

1. Double-click an empty row beneath the predefined questions.

   A dialog appears.
2. Select *Enable* to activate the question.
3. Enter the question in the *Question* box.

   The language is determined by the language choice on the tab.
4. Click *OK*.

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 345.

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 450.

To configure IBE authentication rules

1. Go to *Domain & User* > *IBE User* > *IBE Authentication*.
2. Configure the following and click *Create*.

GUI item	Description
ID	Displays the sequential number of the entry.
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 450.
LDAP profile	Select the LDAP profile you want to use to authenticate the domain users.
Status	Select to enable this rule.

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 342.
Expired User Count	Displays the expired mail users in a domain. For more information about active users, see "Configuring expired users" on page 343.

Managing the address book (server mode only)

The *Domain & User* > *Address Book* tab lets you create and maintain a global or domain-based address book and contact groups, or to configure LDAP attribute mapping templates to retrieve existing address books in your LDAP server.

This menu option appears only when the FortiMail unit is operating in server mode.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

This section contains the following topics:

- Adding contacts (server mode only)
- Adding contact groups (server mode only)
- Configuring LDAP attribute mapping template (server mode only)

Adding contacts (server mode only)

Go to *Domain & User* > *Address Book* > *Contact* to add contacts to a global or domain-based address book in server mod. You can also create contact groups using the contacts. For more information, see "To add or remove users from contact groups" on page 348.

The address book contains the contacts you add, the contact groups created, and the contact list retrieved from your LDAP server based on the LDAP mapping configuration. For information on LDAP mapping configuration, see "Configuring LDAP attribute mapping template (server mode only)" on page 350.

Individual FortiMail webmail users can access the global or domain-based address books for a common set of contact information when composing email messages. For more information, log in to FortiMail webmail and click *Help*.

To view and edit the address book

1. Go to *Domain & User* > *Address Book* > *Contact*.

GUI item	Description
More > Export (dropdow list)	Click to download a copy of the address book in comma-separated value (.csv) or vCard (.vcf) file format. Exporting the address book can be useful for backup purposes, or when using a spreadsheet application such as Microsoft Excel to make large numbers of changes to the address book before importing it again.
More > Import (dropdow list)	Click to select a comma-separated value (.csv) or vCard (.vcf) file format. Then click *Browse* to import address book entries. Click *OK* to upload the file. Click and select LDAP allows you to import contacts from your LDAP server. For details, see "To import contacts from the LDAP server" on page 348. **Note:** An LDAP attribute mapping template must be set up before you can import contacts from the LDAP server. For details, see "Configuring LDAP attribute mapping template (server mode only)" on page 350. Importing the address book can be useful when restoring a backup of the address book, or when importing large numbers of address book entries. **Note:** To replace existing entries, first delete those entries, then import the address book file. The FortiMail unit compares the `Webmail_ID` value of each entry in the address book file, and will not overwrite existing address book entries.
More > Manage Group (dropdow list)	Select a contact and click this button to add a contact to or remove a contact from a contact group. To do so, you must first add contact groups. For more information on managing groups, see "To add or remove users from contact groups" on page 348. For more information on adding group names, see "Adding contact groups (server mode only)" on page 349.
Domain (drop-down list)	Select *System* to display a contact in the global address book, or a domain to display a contact in the domain address book. For information on creating domains, see "Configuring protected domains" on page 307.
Search	Enter a search value for a contact, such as the first name, last name, or email address, and click this button to find the contact from the list.
Display Name	Displays the contacts display name.
First Name	Displays the first name of the contact.
Last Name	Displays the last name of the contact.
Email	Displays the email address of the contact.

2. Either click *New* to create a contact or double-click a contact to modify it.

   A dialog appears.

3. Enter information for the contact.

   Note: Before 5.4 release, an email address in valid format is required and other fields are optional. After 5.4 release, the email address field is also optional and can be in any format.

4. Click *Create* or *OK*.
5. To add additional contact information, click the *Address, Custom,* and *Advanced* tabs.

To import contacts from the LDAP server

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Click *Import* and select *LDAP*.

   A dialog appears.

GUI item	Description
Select LDAP profile	Select an LDAP profile that contains the configuration for the LDAP server from which you want to import the contacts. For information on creating LDAP profiles, see "Configuring LDAP profiles" on page 450.
Select LDAP mapping	Select an LDAP attribute mapping template. The FortiMail unit will import the contacts from the LDAP server based on this template. For information on creating the template, see "Configuring LDAP attribute mapping template (server mode only)" on page 350.
New (button)	Click to create a new LDAP attribute mapping template. For details, see "To view and configure an LDAP mapping list" on page 350.
Edit (button)	Click to modify the LDAP attribute mapping template you selected in the *Select LDAP mapping* field.
Overwrite existing contacts	Select if you want to overwrite the same contacts in your current address book with the imported contact list. This is especially useful when you want to update the imported list.
Delete nonexistent contacts	Select if you want to remove the contacts that were in a previous imported list but are not available in the updated list. This is especially useful when you want to update the imported list.

3. Select *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.

To add or remove users from contact groups

1. Go to *Domain & User* > *Address Book* > *Contact*.
2. Select one or more contacts to add or delete from an existing group.
3. Click *Manage Group* and do one of the following:
   - Select *Add to Group* from the pop-up menu to add users.
   - Select *Delete from Group* from the pop-up menu to remove users.

   In either case, a dialog appears. Only the title varies.

4. In *Domain*, select *System* to display all system-wide contact groups, or a domain name to display all contact groups under that domain. For information on creating domains, see "Configuring protected domains" on page 307.
5. Whether adding or removing users, both dialogs work the same.
   - To add the users to a group or groups, select one or more groups under *Available group(s)* on the *Add to Group* dialog and click -> to move them to the *Selected group(s)* field.
   - To remove the users from a group or groups, select one or more groups under *Available group(s)* on the *Delete from Group* dialog and click -> to move them to the *Selected group(s)* field.

     Users are not removed from the contacts list, just removed from a group.
6. Click *OK*.

Adding contact groups (server mode only)

Before you can add contacts to a contact group, you must first create a contact group. Individual FortiMail webmail users can access the global or domain-based contact groups for a common set of contact information when composing email messages. For more information, log in to FortiMail webmail and click *Help*.

To view and add a contact groups

1. Go to *Domain & User* > *Address Book* > *Contact Group*.
2. From the *Domain* drop-down list, select *System* to display a global contact group or a domain to display a domain-based contact group. For information on creating domains, see "Configuring protected domains" on page 307.
3. Click *New* to create a new group.

   A dialog appears.
4. In *Domain*, select *System* to add a global contact group or a domain to add a domain-based contact group.
5. Enter the name for the group.
6. Click *Create*.

To add a contact to a group

1. Go to *Domain & User* > *Address Book* > *Contact Group*.
2. From the *Domain* drop-down list, select *System* to display a global contact group or a domain to display a domain-based contact group.
3. Select a group and click *Edit*.

   A new page appears.
4. Create a new contact or import contacts.

GUI item	Description
Export (button)	Click to download a copy of the contacts in this contact group in comma-separated value (.csv) or vCard (.vcf) file format. Exporting the contact group can be useful for backup purposes, or when using a spreadsheet application such as Microsoft Excel to make large numbers of changes to the contact group before importing it again.
Import (button)	Click to import contacts. Select a comma-separated value (.csv) or vCard (.vcf) file format. Then click *Browse* to import address book entries. Click *OK* to upload the file. Click and select LDAP allows you to import contacts from your LDAP server. For details, see "To import contacts from the LDAP server" on page 348. **Note:** An LDAP attribute mapping template must be set up before you can import contacts from the LDAP server. For details, see "Configuring LDAP attribute mapping template (server mode only)" on page 350. Click and select *Existing Contacts* displays the system or domain-based address book, depending on your selection. Select one or more contacts and click *Add to Group*. Importing the address book can be useful when restoring a backup of the address book, or when importing large numbers of address book entries. **Note:** To replace existing entries, first delete those entries, then import the address book file. The FortiMail unit compares the `Webmail_ID` value of each entry in the address book file, and will not overwrite existing address book entries.
Back	Click to return to the *Contact Groups* tab.
Search	Enter a search value for a group member, such as the first name, last name, or email address, and click this button to find the group member from the list.

Configuring LDAP attribute mapping template (server mode only)

If you have an existing email address book in your LDAP server, you can configure the LDAP attribute mapping template to retrieve the address book and add it to the contact list. Before doing so, you must configure your LDAP server. For details, see "Configuring LDAP profiles" on page 450.

For information on retrieving the address book, see "More > Import" on page 347 and "To import contacts from the LDAP server" on page 348.

To view and configure an LDAP mapping list

1. Go to *Domain & User* > *Address Book* > *LDAP Mapping*.
2. Either click *New* to create a template or double-click an entry to modify it.

   A mapping template appears.
3. Configure the following:

GUI item	Description
Mapping Name	Enter the name of the LDAP attribute mapping template.
Contact Field	Select the FortiMail attributes used for the contacts, such as *First name, Last name*, or *Mobile*. **Note**: The *Email* attribute must be entered.
LDAP Attribute	Enter the matching contact attributes used in the LDAP server. For example, Name may be used to represent first name and Surname may be used for last name.
LDAP query filter	Specify the query filter.
Add (button)	Click to add an attribute row in the *Mapping content* table.
Delete (button)	Select an attribute row in the *Mapping content* table and click this button to remove it.

4. Click *Create*.

Sharing calendars and address books (server mode only)

FortiMail v5.0 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

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

This section contains the following topics:

- Calendar sharing
- Address book sharing

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* > *Settings*.
2. Select *Enable WebDAV* and *Enable CalDAV*.
3. Click *Apply*.

FortiMail calendar service supports resource management, such as meeting room and equipment.

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 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 352).
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 352).

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 web UI.
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 352).
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 352).
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 web UI.
4. Not e 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:

```
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. The default is 389.
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=outlook, ou=people, dc=example, dc=com, assuming your user name is user1, your domain name is example.com. “ou=outlook, ou=people” should be constant. Password: 123
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.

```
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 357.
   c. Create a domain for the to-be-migrated users. In v5.0 release, the domain name must be the same as the users' domain on the remote mail server. Beginning from v5.0.1 release, the domain name can be different. For details, see "Creating domains for mail migration" on page 357.
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. First create an authentication profile that uses the remote mail server as the authentication server. For details, see "Configuring authentication profiles" on page 446.

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 381.

iii. Use one of the following two methods to collect user passwords:

a. 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.

b. 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 *Mail Settings* > *Mail Migration* > *Migration Users*.

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:

   i. Go to *Domain & User* > *Mail Migration* > *Migration User.*

   ii. From the *Action* dropdown list, select *Migrate* > *Selected Users* or *All Users*.

   iii. If needed, you can click the *Stop* and *Start* button to control the migration process.

   iv. 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 356.

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 if different from the default one (port 993).
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 356.

1. Go to *Domain & User* > *Domain* > *Domain.*
2. Click *New*.
3. Configure the settings as described in "Configuring protected domains" on page 307.

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 357.
7. Click *Create*.

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?
- How to use policies
- Controlling SMTP access and delivery
- Controlling email based on sender and recipient addresses
- Controlling email based on IP addresses

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 389), 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 362)
- Recipient-based policies (see "Controlling email based on sender and recipient addresses" on page 381)
- IP-based policies (see "Controlling email based on IP addresses" on page 375)

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.

For more information on protected domains, see "Configuring protected domains" on page 307.

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.

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.

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 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.

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 5.
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, if any, only if you have enabled *Take precedence over recipient based policy match* in the IP-based policy, or if there is no recipient-based policy match.

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.

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.

Controlling SMTP access and delivery

The *Policy* > *Access Control* submenu lets you configure access control rules 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 163.

Access control rules are categorized separately based on whether they affect either the receipt or delivery of email messages by the FortiMail unit; that is, whether the FortiMail unit initiated the SMTP session or was the destination.

- Configuring access control rules
- Configuring delivery rules
- Troubleshoot MTA issues

Configuring access control rules

The *Receiving* tab displays a list of access control rules that apply to SMTP sessions being ***received*** by the FortiMail unit.

Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages for SMTP sessions that are initiated by SMTP clients.

When an SMTP client attempts to deliver email through the FortiMail unit, the FortiMail unit compares each access control rule to the commands used by the SMTP client during the SMTP session, such as the envelope's sender email address (`MAIL FROM:`), recipient email address (`RCPT TO:`), authentication (`AUTH`), and TLS (`STARTTLS`). Rules are evaluated for a match in the order of their list sequence, from top to bottom. If all attributes of a rule match, the FortiMail unit applies the action selected in the matching rule to the SMTP session, and no subsequent access control rules are applied.

Only one access control rule is ever applied to any given SMTP session.

If no access control rules are configured, or no matching access control rules exist, ***and*** if the SMTP client is not configured to authenticate, the FortiMail unit will perform the default action, which varies by whether or not the recipient email address in the envelope (`RCPT TO:`) is a member of a protected domain.

- For protected domains, the default action is delivery (with greylisting).
- For ***un***protected domains, the default action is *REJECT*.

For information on protected domains, see "Configuring protected domains" on page 307.

In the absence of access control rules, the FortiMail unit prevents SMTP clients from using your protected server or FortiMail unit as an open relay: senders can deliver email incoming to protected domains, but cannot deliver email outgoing to unprotected domains.

For information on the sequence in which access control rules are used relative to other antispam methods, see "Order of execution" on page 16.

If you want to allow SMTP clients, such as your email users or email servers, to send email to unprotected domains, you must configure at least one access control rule. You may need to configure additional access control rules if, for example, you want to:

- discard or reject email from or to some email addresses, such as email addresses that no longer exist in your protected domain
- discard or reject email from some SMTP clients, such as a spammer that is not yet known to blocklists

Like IP-based policies, access control rules can reject connections based on IP address. Unlike IP-based policies, 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 cannot be overruled by recipient-based policies, and cannot match connections based on the SMTP server's IP address. (By the nature of how ACL controls access to or through the FortiMail unit, the SMTP server 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 375.

If possible, verify configuration of access control rules in a testing environment before applying them to a FortiMail unit in active use. Failure to verify correctly configured reject, discard, and accept actions can result in inability to correctly handle SMTP sessions.

Do ***not*** create an access control rule whose "Sender pattern" on page 365 is *, "Recipient pattern" on page 366 is *, "Authentication status" on page 367 is *Any*, "TLS profile" on page 367 is *None*, and *Action* is *RELAY*. This access control rule matches and relays all connections, allowing open relay, which could result in other MTAs and DNSBL servers blocklisting your protected domain.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

To view and configure access control rules

1. Go to *Policy* > *Access Control* > *Receiving*.

GUI item	Description
Move (button)	Select a policy, 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.
Enabled	Select to enable or disable an existing rule.
ID	Displays the number identifying the rule. 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.
Sender Pattern	Displays the pattern that defines email senders for the rule.
Recipient Pattern	Displays the pattern that defines email recipients for the rule.
Sender/IP Netmask	Displays the IP address and netmask of the SMTP client attempting to deliver the email message.
Reverse DNS Pattern	Displays the used in a reverse DNS look-up.
Authentication Status	Displays which authentication status is used with the rule.
TLS Profile	Displays the TLS profile, if any, used to allow or reject a connection.
Actions	Displays the action to take when SMTP sessions match the rule.

2. Either click *New* to add an access control rule or double-click an access control rule to modify it.

   A dialog appears.

3. Configure the following:

GUI item	Description
Enabled	Select whether or not the access control rule is currently in effect.
Sender pattern	Select either *User Defined* and enter a complete or partial sender (`MAIL FROM:`) email address to match, or select: • *Internal*: Match any email address from a protected domain. • *External*: Match any email address from an ***un***protected domain. • *Email Group*: Match any email address in the group. If you select this option, select an email group from the *Email Group Selection* field. Click *New* to add a new email group or *Edit* to modify an existing one. For more information, see "Configuring email groups" on page 490. • *LDAP Group*: Match any email address in the group. If you select this option, select an LDAP profile from the *LDAP Profile* field. • *LDAP Verification*: Match any individual email address queried by the LDAP profile. If you select this option, select an LDAP profile from the dropdown list or click *New* to create a new one. **Note**: Use "$s" to match sender addresses. For example, to reject senders that are not in the recipient's allowed sender list: **a.** Create an ACL rule and choose LDAP verification in the sender pattern. **b.** Choose a LDAP profile where below user query string is used: (&(mail=$m)(!(allowedSenders=$s))) **c.** Set the ACL rule action to *Reject*. This will match a sender that is not in the allowedSenders list of the recipient and reject email from such senders. • *Regular Expression*: Use regular expression syntax instead of wildcards to specify the pattern. See "Using wildcards and regular expressions" on page 368. • *User Defined*: Specify the email addresses. The pattern can use wildcards or regular expressions. See "Appendix D: Regular expressions" on page 623. For example, the sender pattern `*@example.???` will match messages sent to any email user at example.com, example.net, or any "example" domain ending with a three-letter top-level domain name.

GUI item	Description
Recipient pattern	Either select *User Defined* and enter a complete or partial recipient (`RCPT TO:`) email address to match, or select: • *Internal*: Match any email address from a protected domain. • *External*: Match any email address from an ***un***protected domain. • *Email Group*: Match any email address in the group. If you select this option, select an email group from the *Email Group Selection* field. Click *New* to add a new email group or *Edit* to modify an existing one. For more information, see "Configuring email groups" on page 490. • *LDAP Group*: Match any email address in the group. If you select this option, select an LDAP profile from the *LDAP Profile* field. • *LDAP Verification*: Match any individual email address queried by the LDAP profile. If you select this option, select an LDAP profile from the dropdown list or click *New* to create a new one. **Note**: Use "$m" to match recipient addresses. • *Regular Expression*: Use regular expression syntax instead of wildcards to specify the pattern. See "Using wildcards and regular expressions" on page 368. • *User Defined*: Specify the email addresses. The pattern can use wildcards or regular expressions. See "Appendix D: Regular expressions" on page 623. For example, the recipient pattern `*@example.???` will match messages sent to any email user at example.com, example.net, or any "example" domain ending with a three-letter top-level domain name.
Sender IP/netmask	Select *User Defined* and enter the IP address and netmask of the SMTP client attempting to deliver the email message. 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. To match any address, enter `0.0.0.0/0`. Select *IP Group* to choose an IP group. Click *New* to add a new IP group or *Edit* to modify an existing one. For more information, see "Configuring IP groups" on page 491.

GUI item	Description
Reverse DNS pattern	Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message. Because domain names in the SMTP session are self-reported by the connecting SMTP server and easy to fake, the FortiMail unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail does a DNS lookup using the SMTP server's IP address. The resulting domain name is compared to the reverse DNS pattern for a match. If the reverse DNS query fails, the access control rule match will also fail. If no other access control rule matches, the connection will be rejected with SMTP reply code 550 (`Relaying denied`). The pattern can use wildcards or regular expressions. See "Using wildcards and regular expressions" on page 368. For example, the recipient pattern `mail*.com` matches messages delivered by an SMTP server whose domain name starts with "mail" and ends with ".com". **Note:** Reverse DNS queries for access control rules require that the domain name be a valid top level domain (TLD). For example, ".lab" is not a valid top level domain name, and thus the FortiMail unit cannot successfully perform a reverse DNS query for it.
Authentication status	Select whether or not to match this access control rule based on client authentication. • *Any*: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit. • *Authenticated*: Match this access control rule only for clients that have authenticated with the FortiMail unit. • *Not Authenticated*: Match this access control rule only for clients that have ***not*** authenticated with the FortiMail unit.
TLS profile	Select a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile. • If the attributes match, the access control action is executed. • If the attributes do ***not*** match, the FortiMail unit performs the *Failure* action configured in the TLS profile. Click *New* to add a new TLS profile or *Edit* to modify an existing one. For more information on TLS profiles, see "Configuring TLS security profiles" on page 483.

GUI item	Description
Action	Select which action the FortiMail unit will perform for SMTP sessions matching this access control rule. • *DISCARD*: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client. • *REJECT*: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (`Relaying denied`). • *RELAY*: Relay or proxy, process, and deliver the email normally if it passes all configured scans. ***Do not apply greylisting.*** • *SAFE*: Relay or proxy and deliver the email, ***only if*** the recipient belongs to a protected domain or the sender is authenticated. All antispam profile processing will be skipped; but antivirus, content and other scans will still occur. • *SAFE & RELAY*: Relay or proxy and deliver the email. All antispam profile processing will be skipped; but antivirus, content, and other scans will still occur.
Comments	Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.

4. Click *Create or OK*.

   The access control rule appears at the bottom of the list of access control rules. As a result, the FortiMail unit will evaluate it as a match for the SMTP session only if no previous access control rule matches. If you want your new rule to be evaluated before another rule, move your new access control rule to its intended position in the list.

Using wildcards and regular expressions

You can enter wildcards or regular expressions in any pattern field, such as *Reverse DNS pattern*, on the *Access Control Rule* dialog.

To use a regular expression as a pattern, first enable *Regular expression*, which is beside the pattern field.

If a pattern is listed on the *Receiving* tab with the `R/` prefix, it is set to use regular expression syntax. If the pattern is listed with a `-/` prefix, it does not use regular expression syntax.

Wildcard characters (* and ?) allow you to enter partial patterns that can match multiple reverse DNS lookup results. An asterisk (*) represents one or more characters. A question mark (?) represents any single character.

When configuring access control rules, ***do not leave*** any pattern fields blank. Instead, to have the FortiMail unit ignore a pattern:

- If *Regular expression* is ***disabled*** for the field, enter an asterisk (*) in the pattern field.
- If *Regular expression* is ***enabled*** for the field, enter a dot-star (`.*`) character sequence 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, and therefore will not exclude any SMTP sessions from matching the access control rule.

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 as long as they authenticate their identities and use TLS, you might configure the following access control rule:

Table 44: Example access control rule

Sender Pattern	`user*@example.com`
Recipient Pattern	`*`
Sender IP/Netmask	`0.0.0.0/0`
Reverse DNS Pattern	`*`
Authentication Status	`authenticated`
TLS Profile	`tlsprofile1`
Action	`RELAY`

Example: Access control rules with regular expressions

Example Corporation uses a FortiMail unit operating in gateway mode, and that has been configured with only one protected domain: example.com. The FortiMail unit was configured with the access control rules illustrated in Table 45.

Table 45: A list of example access control rules

Enabled	ID	Sender Pattern	Recipient Pattern	Sender IP/Netmask	Reverse DNS Pattern	Authentication	TLS Profile	Action
Yes	1	-/*	-/user932@example.com	0.0.0.0/0	-/*	Any		REJECT
Yes	2	R/^\s*$	-/*	0.0.0.0/0	-/*	Any		REJECT
Yes	3	-/*	-/*@example.com	172.20.120.0/24	-/mail.example.org	Any		RELAY
Yes	4	-/*@example.org	-/*	0.0.0.0/0	-/*	Any		REJECT
Yes	5	-/*	R/^user\d*@example\.com$	0.0.0.0/0	-/*	Any		RELAY

Rule 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 the user's external contacts were informed of their new Example Corporation employee contacts, messages addressed to the former employee's address must be spam.

Rule 1 uses only the recipient pattern. All other access control rule attributes are configured to match any value. This rule 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.

This rule is placed first because it is the most specific access control rule 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 rule that matched all messages were placed at the top of the list, no rule after the first would ever be checked for a match, because the first would always match.

SMTP sessions not matching this rule are checked against the next rule.

Rule 2

Much of the spam received by the Example Corporation has no sender specified in the message envelope. Most valid email messages will have a sender email address.

Rule 2 uses only the sender pattern. The regular expression `^\s*$` will match a sender string that contains one or more spaces, or is empty. If any non-space character appears in the sender string, this rule does not match. This rule will reject all messages with a no sender, or a sender containing only spaces.

Not all email messages 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. The FortiMail administrators at the Example Corporation decided that the advantages of this rule outweigh the disadvantages.

Messages not matching this rule are checked against the next rule.

Rules 3 and 4

Recently, the Example Corporation has been receiving spam that appears to be sent by example.org. The FortiMail log files revealed that the sender address is being spoofed and the messages 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 with the proper 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.

Rule 3 uses the recipient pattern, the sender IP, and the reverse DNS pattern. This rule will relay messages to email users of example.com sent from a client whose domain name is mail.example.org and IP address is between 172.20.120.1 and 172.20.120.255.

Messages not matching this rule are checked against the next rule.

Rule 4 works in conjunction with rule 3. It uses only the sender pattern. Rule 4 rejects all messages from example.org. But because it is positioned after rule 3 in the list, rule 4 affects only messages that were not already proven to be legitimate by rule 3, thereby rejecting only email messages with a fake sender.

Rules 3 and 4 ***must*** appear in the order shown. If they were reversed, all mail from example.org would be rejected. The more specific rule 3 (accept valid mail from example.org) is placed first, and the more general rule 4 (reject all mail from example.org) follows.

Messages not matching these rules are checked against the next rule.

Rules 5

The 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 verification. Verification is performed with the aid of an LDAP 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”.

Rule 5 uses only the recipient pattern. The recipient pattern is a regular expression that will match all email addresses that start with “user”, end with “@example.com”, and have one or more numbers in between. Email messages matching this rule are relayed.

Default implicit rules

For messages not matching any of the above rules, the FortiMail unit will perform the default action, which varies by whether or not the recipient email address in the envelope (RCPT TO:) is a member of a protected domain.

- For protected domains, the default action is delivery (with greylisting).
- For unprotected domains, the default action is REJECT.

Configuring delivery rules

The *Delivery* tab displays a list of delivery rules that apply to SMTP sessions being ***initiated*** by the FortiMail unit in order to deliver email.

Delivery rules let you to require TLS for the SMTP sessions the FortiMail unit initiates when sending email to other email servers. They also let you to apply secure MIME (S/MIME) or IBE.

For more information about IBE, see “Configuring IBE encryption” on page 543.

When initiating an SMTP session, the FortiMail unit compares each delivery rule to the domain name portion of the envelope recipient address (`RCPT TO:`). Rules are evaluated for a match in the order of their list sequence, from top to bottom. If a matching delivery rule does not exist, the email message is delivered. If a match is found, the FortiMail unit compares the TLS profile settings to the connection attributes and the email message is sent or the connection is not allowed, depending on the result; if an encryption profile is selected, its settings are applied. No subsequent delivery rules are applied. Only one delivery rule is ever applied to any given SMTP session.

If you are using a delivery rule to apply S/MIME encryption, the destination of the connection can be another FortiMail unit, but it could alternatively be any email gateway or server, as long as either:

- the destination’s MTA or mail server
- the recipient’s MUA

supports S/MIME and possesses the sender’s certificate and public key, which is necessary to decrypt the email. Otherwise, the recipient cannot read the email.

To access this part of the web UI, your administrator account’s:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see “About administrator account permissions and domains” on page 179.

To configure a delivery rule list

1. Go to *Policy* > *Access Control* > *Delivery*.

GUI item	Description
Move (button)	Click a delivery rule to select it, click *Move*, then select either: • the direction in which to move the selected rule (*Up* or *Down*), or • *After* or *Before*, then in *Move right after* or *Move right before* indicate the rule's new location by entering the ID of another delivery rule FortiMail units match the rules in sequence, from the top of the list downwards.
Enabled	Indicates whether or not the delivery rule is currently in effect. To disable a delivery rule, select the button, then click *Yes* to confirm.
ID	Displays the number identifying the rule. 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 delivery rules in sequence. Only the topmost matching delivery rule will be applied.
Sender Pattern	Displays the complete or partial envelope sender email address to match.
Recipient Pattern	Displays the complete or partial envelope recipient email address to match.
TLS Destination IP	Displays the IP address and netmask of the system to which the FortiMail is sending the email message. `0.0.0.0/0.0.0.0` matches any IP address.
TLS Profile	Displays the TLS profile, if any, used to allow or reject a connection. • If the attributes match, the access control action is executed. • If the attributes do ***not*** match, the FortiMail unit performs the *Failure* action configured in the TLS profile. To edit the TLS profile, click its name. For details, see "Configuring security profiles" on page 483.
Encryption Profile	Indicates the encryption profile used to apply S/MIME or IBE encryption to the email. To edit the encryption profile, click its name. For details, see "Configuring encryption profiles" on page 485.

2. Either click *New* to add a delivery control rule or double-click a delivery control rule to modify it.

   A dialog appears.

3. Configure the following:

GUI item	Description
Enabled	Select whether or not the access control rule is currently in effect.
Sender pattern	Enter a complete or partial envelope sender (`MAIL FROM:`) email address to match. Wild card characters allow you to enter partial patterns that can match multiple sender email addresses. The asterisk (*) represents one or more characters. The question mark (?) represents any single character. For example, the sender pattern `??@*.com` will match messages sent by any email user with a two letter email user name from any ".com" domain name.
Recipient pattern	Enter a complete or partial envelope recipient (`RCPT TO:`) email address to match. Wild card characters allow you to enter partial patterns that can match multiple recipient email addresses. The asterisk (*) represents one or more characters. The question mark (?) represents any single character. For example, the recipient pattern `*@example.???` will match messages sent to any email user at example.com, example.net, example.org, or any other "example" domain ending with a three-letter top-level domain name.
TLS Destination IP/netmask	Enter the IP address and netmask of the system to which the FortiMail unit is sending the email message using TLS connection. 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. To match any address, enter `0.0.0.0/0`. **Note:** This field is not used when considering whether or not to apply an encryption profile.
TLS profile	Select a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile. • If the attributes match, the access control action is executed. • If the attributes do ***not*** match, the FortiMail unit performs the *Failure* action configured in the TLS profile. Click *New* to add a new TLS profile or *Edit* to modify an existing one. For more information on TLS profiles, see "Configuring TLS security profiles" on page 483.

GUI item	Description
Encryption profile	Select an encryption profile used to apply S/MIME or IBE encryption to the email. Note that if you create a delivery rule that uses both IBE encryption profile and TLS profile, the TLS profile will override the IBE encryption profile and the IBE encryption will not be used. If you select an S/MIME profile here and an IBE profile in the *Encryption with profile* field (*Profile* > *Content* > *Action*), the S/MIME profile will override the IBE encryption profile. Click *New* to add a new encryption profile or *Edit* to modify an existing one. For more information, see "Configuring encryption profiles" on page 485 and "Configuring certificate bindings" on page 547. For information about content action profiles, see "Configuring content action profiles" on page 439.
Comments	Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.

Configuring delivery control policies

MTA IP addresses might be blacklisted if sending outgoing email at a high rate; marketing mail campaigns can cause the corporate IP addresses to be registered in DNSBL.

To solve this problem, you can rate limit email delivery when configuring domain settings (see "Sender address rate control" on page 321). You can also rate limit email delivery at system level.

To configure an email delivery control policy

1. Go to *Policy* > *Access Control* > *Delivery Control*.
2. Click New to add a new delivery control policy.
3. Configure the following:

GUI item	Description
Enabled	Toggle to enable or disable the policy.
Recipient domain	Specify the recipient domain to apply the policy on. Use wildcard * to represent all recipient domains.
Restrict the number of concurrent connections	Specify to limit the number of concurrent connections to the above domain. 0 means no limit.

GUI item	Description
Restrict the number of messages per connection	Specify to limit the number of email messages to be sent for one connection session. 0 means no limit.
Restrict the number of recipients per period (30 minutes)	Specify to limit the number of email recipients in an interval of 30 minutes. 0 means no limit.

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 488.

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 rules" on page 363.

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 360.

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.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

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 179.

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 361 and "Which policy/profile is applied when an email has multiple recipients?" on page 362.
Source	Displays the IP address of the SMTP source to which the policy applies.
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 389.
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 "Managing antispam profiles" on page 407.

GUI item	Description
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 and antivirus action profiles” on page 425.
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 430.
DLP	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 553.
IP Pool	Displays the name of the IP pool profile applied by this policy. 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 380 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 ***NOT*** 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 above rule is applied (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 446
Exclusive	Indicates whether or not “Take precedence over recipient based policy match” on page 380 is enabled in this policy. See “Order of execution of policies” on page 361 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 491. To match all clients, enter `0.0.0.0/0`.
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 491. 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 pool) 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.
Comments	Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.

Profiles

Session Select the name of a session profile to have this policy apply.

This option is applicable only if "Action" on page 378 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 378 is *Scan*.

AntiVirus Select the name of an antivirus profile to have this policy apply.

This option is applicable only if "Action" on page 378 is *Scan*.

Content Select the name of a content profile to have this policy apply.

This option is applicable only if "Action" on page 378 is *Scan*.

DLP Select the name of a DLP profile to have this policy apply.

This option is applicable only if "Action" on page 378 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 ***NOT*** 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 above rule is applied (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 378 is *Scan*.

For details about IP pools, see "Configuring IP pools" on page 488.

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 445.

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 386 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 139.

Authentication profile

Select an existing authentication profile to use with this policy.

Click *New* to create on or *Edit* to modify the selected profile.

Use for 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 386 to authenticate the connection.

Disable to make SMTP authentication unavailable.

This option is available only if you have selected an "Authentication profile" on page 386.

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 rules" on page 363.

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 360.

This option is applicable only if *Action* is *Scan*.

Note: Enabling this option also causes the FortiMail unit to ignore the option "Hide the transparent box" on page 313 in the protected domain.

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.

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 380. 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 360.

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 375.
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 307)
- 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 325 or "Configuring LDAP profiles" on page 450)
- 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 332)

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

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

1. Go to the *Policy* > *Recipient Policy.*
2. Select *Inbound* or *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 the domain is “All”, the *Move* button is disabled **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 (drop-down list)	• All: Select to display all system-level and domain-level policies. • System: Select to display all 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 361 and “Which policy/profile is applied when an email has multiple recipients?” on page 362.

GUI item	Description
Domain Name (column)	Indicates the domain part of the recipient's email address in the envelope (`RCPT TO:`) that an email must match in order to be subject to the policy. • For incoming recipient-based policies, this is the name of a protected domain. • For outgoing recipient-based policies, this is *System*, indicating that the recipient does ***not*** belong to a protected domain.
Sender Pattern	A sender email address (`MAIL FROM:`) as it appears in the envelope or a wildcard pattern to match sender email addresses.
Recipient Pattern	A recipient email address (`RCPT TO:`) as it appears in the envelope or a wildcard pattern to match recipient email addresses.
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 "Managing antispam profiles" on page 407.
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 and antivirus action profiles" on page 425.
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 430.
DLP	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 551.
Resource (server mode only)	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 443.
Authentication (not in server mode)	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 446 or "Configuring LDAP profiles" on page 450.

To configure recipient-based policies

1. Go to *Policy* > *Recipient Policy* > *Inbound* or *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 inbound recipient policies" on page 384
- "Configuring the outbound recipient policies" on page 384
- "Configuring the profiles section of a recipient policy" on page 385
- "Configuring authentication for inbound email" on page 386
- "Configuring the advanced settings of inbound policies" on page 387

Configuring the inbound recipient policies

If you are configuring a policy for incoming email, configure the *Sender Pattern* and *Recipient Pattern* sections.

GUI item	Description
Sender Pattern	Select one of the following ways to define recipient (`RCPT TO:`) email addresses that match this policy: • *User*: Enter a recipient email address or a pattern with wild cards, such as `*@protected.example.com`. • *Local group:* Select the name of a protected domain in the second drop-down list, then select the name of a user group in the first drop-down 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" on page 455, 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 490. 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.
Recipient Pattern	See above descriptions.

Configuring the outbound recipient policies

If you are configuring a policy for outgoing email, configure the *Sender Pattern* and *Recipient Pattern* sections.

GUI item	Description
Sender Pattern	Select one of the following ways to define sender (`MAIL FROM:`) email addresses that match this policy: • *User*: Enter a sender email address or a pattern with wild cards, such as `*@` • `.example.com`. • *Local group*: Select the name of a protected domain in the second drop-down list, then select the name of a user group in the first drop-down 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 490. 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.
Recipient Pattern	See above descriptions.

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 drop-down 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 "Managing antispam profiles" on page 407. **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 and antivirus action profiles" on page 425.

GUI item	Description
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 430.
DLP	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 553.
Resource (server mode only)	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 443.

Configuring authentication for inbound email

The *Authentication and Access* section appears only for inbound policies.

For more information on configuring an authentication profile, see "Workflow to enable and configure authentication of email users" on page 445.

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 386 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 139.
Authentication profile	Select an existing authentication profile to use with this policy.
Use for 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 386 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an "Authentication profile" on page 386. **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 rules" on page 363.

GUI item	Description
Allow quarantined email access through POP3 (gateway and transparent mode only)	Enable to allow email users matching this policy to use POP3 to retrieve the contents of their personal quarantine. For more information, see "How to enable, configure, and use personal quarantines" on page 139. This option is available only if you have selected a profile in *Authentication profile*. **Note:** This option is for POP3 access only. Email users cannot access their personal quarantine through IMAP.
Allow quarantined email access through webmail (gateway and transparent mode only)	Enable to allow email users matching this policy to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their personal quarantine. For more information, see "How to enable, configure, and use personal quarantines" on page 139. This option is available only if you have selected a profile in "Authentication profile" on page 386.

Configuring the advanced settings of inbound policies

The *Advanced Settings* 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.

GUI item	Description
Enable PKI authentication for web mail access (Inbound policy only)	Enable if you want to allow web mail users to log in by presenting a certificate rather than a user name and password. Also configure "Certificate validation is mandatory". For more information on configuring PKI users and what defines a valid certificate, see "Configuring PKI authentication" on page 332.
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.

This section includes:

- Configuring session profiles
- Configuring antispam profiles and antispam action profiles
- Configuring antivirus profiles and antivirus action profiles
- Configuring content profiles and content action profiles
- Configuring resource profiles
- Configuring authentication profiles
- Configuring LDAP profiles
- Configuring dictionary profiles
- Configuring security profiles
- Configuring IP pools
- Configuring email and IP groups
- Configuring notification profiles

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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 as needed:
   - “Configuring connection settings” on page 390
   - “Configuring sender reputation options” on page 391
   - “Configuring endpoint reputation options” on page 393
   - “Configuring sender validation options” on page 394
   - “Configuring session settings” on page 396
   - “Configuring unauthenticated session settings” on page 398
   - “Configuring SMTP limit options” on page 401
   - “Configuring error handling options” on page 402
   - “Configuring header manipulation options” on page 403
   - “Configuring list options” on page 403
   - “Configuring advanced MTA control settings” on page 404

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 389.

1. Go to *Profile* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Expand the *Connection Settings* 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. Disable to replace the 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 313.
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.

GUI item	Description
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. For server mode, gateway mode, and transparent MTA mode, 0 means the default value 30 seconds. For transparent proxy mode, 0 means no limit.
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.

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 389.

You can also view the sender reputation statuses by going to *Monitor* > *Sender Reputation*. See "Viewing sender reputation statuses" on page 151.

To configure sender reputation options

1. Go to *Profile* > *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 Reputation*.

   Configure the sender reputation settings to restrict the number of email messages sent from SMTP clients based upon whether they have a reputation of sending an excessive number of email messages, email with invalid recipients, or email infected with viruses.

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 checking	Enable to accept or reject email based upon sender reputation scores. The following options have no effect unless this option is enabled.
Throttle client at *n*	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.
Restrict number of emails per hour to *n*	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 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 *n*	Enter a sender reputation score over which the FortiMail unit will return a temporary failure error when the SMTP client attempts to initiate a connection. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increase or decrease the sender reputation scores accordingly.
Reject client at *n*	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.
Check FortiGuard Block IP at connection phase	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. In an antispam profile, you can also enable FortiGuard block IP checking. But that action happens after the entire message has been received by FortiMail. Therefore, if this feature is enabled in a session profile and the action is reject, the performance will be improved.

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 389.

1. Go to *Profile* > *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 527.

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 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 391.
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 531.
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 389.

1. Go to *Profile* > *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 authenticity.

   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 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:** Before FortiMail 4.0 MR3 Patch 1 release, you must enable SPF checking in the session profile before SPF checking in the antispam profile takes effect. Starting from 4.0 MR3 Patch 2 release, SPF checking can be enabled in either a session profile or an antispam profile, or both profiles. However, 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 messages	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 Setting" on page 319.

GUI item	Description
Enable DKIM signing for authenticated senders only	Enable to sign outgoing email with a DKIM signature only if the sender is authenticated. This option is effective only if *Enable DKIM signing for outgoing messages* is enabled.
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 523.
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 450.

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 389.

1. Go to *Profile* > *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 Settings*.
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 439.
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.

GUI item	Description

Reject EHLO/HELO commands with invalid characters 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 ^^&^&^#$`
	`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 (transparent mode only)	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.

GUI item	Description
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`
	`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 completed 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 389.

1. Go to *Profile* > *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 Settings.*
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.
	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`
	`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.`

GUI item	Description

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 domains	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`

GUI item	Description
Prevent open relaying (transparent mode only)	Enable to prevent clients from using open relays to send email by blocking sessions that are unauthenticated. (Unauthenticated sessions are assumed to be occurring to an open relay.) If you permit SMTP clients to use open relays to send email, email from your domain could be blocklisted by other SMTP servers. This option is effective only if you have enabled "Use client-specified SMTP server to send email" on page 217 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 201), 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.

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 389.

1. Go to *Profile* > *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 Limits*.
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 emails 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.

GUI item	Description
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 360), only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. FortiMail will use the smaller size.
Cap header size (KB) at	Enter the limit of the message header size. Messages with headers over the threshold size are rejected.
Maximum number of NOOPs allowed for each connection	Enter the limit of `NOOP` commands permitted per SMTP session. Some spammers use `NOOP` commands to keep a long session alive. Legitimate sessions usually require few `NOOP`s.
Maximum number of RSETs allowed for each connection	Enter the limit of `RSET` commands permitted per SMTP session. Some spammers use `RSET` commands to try again after receiving error messages such as unknown recipient. Legitimate sessions 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 389.

1. Go to *Profile* > *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 number of errors permitted before the FortiMail unit imposes a delay. By default, five errors are permitted before the FortiMail unit imposes the first delay.
Delay for the first non-free error (seconds)	Enter the delay time for the first error after the number of ***free*** errors is reached.
Delay increment for subsequent errors (seconds)	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.
Maximum number of errors allowed for each connection	Enter the total number of errors the FortiMail unit accepts before dropping the connection.

Configuring header manipulation 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 389.

1. Go to *Profile* > *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 *Header Manipulation*.

   Email processing software and hardware can add extra 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 header manipulation settings to reduce the number of message headers.
4. Configure the following:

GUI item	Description
Remove received header	Enable to remove all `Received:` message headers from email messages. You can alternatively remove this header on a per-domain basis. For details, see "Remove received header of outgoing email" on page 324.
Remove headers	Enable to remove other configured headers from email messages, then click *Edit* to configure which headers should be removed.

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 389.

1. Go to *Profile* > *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 504.

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 "Managing the address book (server mode only)" on page 346.

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:`) and email header (`From:`) 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:`) and email header (`From:`) 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 389.

In addition to global MTA settings, you can configure the following MTA settings in a session profile. These session-specific MTA settings will overwrite the global settings configured elsewhere.

By default, this feature is hidden. To use this feature, you must enable it by using the following CLI command:

```
config system global
   set mta-adv-ctrl-status enable
end
```

After this feature is enabled, the following options will appear in the session profile settings. In addition, four new tabs (Address Rewrite, Mail Routing, Access Control, and DSN) will also appear under *Profile* > *Session*.

1. Go to *Profile* > *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 *Advanced Control*.
4. Configure the following:

GUI item	Description
Email queue	Select which email queue to use for the matching sessions. For other general queue settings, see "Configuring mail queue setting" on page 198.
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 Envelope From value to rewrite the Header From and/or Header 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 406.
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 envelope recipient/RCPT TO 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 406.
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 406.
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 407.

DSN	Select a DNS profile or click *New* to create one. For details, see "Configuring DSN profiles in a session profile" on page 407.
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 "Configuring logging to a Syslog server or FortiAnalyzer unit" on page 570.

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 404), 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 email "Envelope From", "Header From", or "Reply-to" 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 463.
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 404), 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 recipient pattern and the relay type:
   - *Host*: Relay the matched sessions to the specified 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 specify the alternate domain name.
6. Specify the SMTP port number. The default port is 25.
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 404), 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 rules" on page 363.
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 404), the *DSN* tab will appear. Configure this setting to overwrite the global setting configured in "Configuring DSN options" on page 198.

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 when to send DSN email (after how many time of unsuccessful email sending retries).
5. Click *Create*.

Configuring antispam profiles and antispam action profiles

The *AntiSpam* submenu lets you configure antispam profiles and related action profiles.

This section contains the following topics:

- Managing antispam profiles
- Configuring a FortiGuard URI filter profile
- Configuring email impersonation analysis/Business Email Compromise settings
- Configuring antispam action profiles

Managing antispam profiles

The *AntiSpam* tab lets you manage and configure antispam profiles. Antispam profiles are sets of antispam scans that you can apply by selecting one in a policy.

FortiMail units can use various methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, Bayesian scanning, and heuristic scanning. Antispam profiles contain settings for these features that you may want to vary by policy. Depending on the feature, before you configure antispam policies, you may need to enable the feature or configure its system-wide settings.

For information on the order in which FortiMail units perform each type of antispam scan, see "Order of execution" on page 16.

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 450 and "Configuring scan override options" on page 463.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

To view and manage incoming antispam profiles

1. Go to *Profile* > *AntiSpam* > *AntiSpam*.

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*.
Batch Edit (button)	Edit several profiles simultaneously. See "Performing a batch edit" on page 420.
Domain (drop-down 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. The profile name is editable.
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 multisection dialog appears.

3. Configure the following:

GUI item	Description
Domain	Select the entire FortiMail unit (*System*) or name of a protected domain.You can see only the domains that are permitted by your administrator profile. For more information, see "About administrator account permissions and domains" on page 179.
Profile name	For a new profile, enter the name of the profile.
Default action	Select the default action to take when the policy matches. See "Configuring antispam action profiles" on page 422.

GUI item	Description
FortiGuard	See "Configuring FortiGuard options" on page 411.
Greylist	Enable to apply greylisting. For more information, see "Configuring greylisting" on page 512. **Note:** Enabling greylisting can improve performance by blocking most spam before it undergoes other resource-intensive antispam scans.
SPF check	If the sender domain DNS record lists SPF authorized IP addresses, use this option to compare the client IP address to the IP addresses of authorized senders in the DNS record (RFC 4408). 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. If the client IP address fails the SPF check, FortiMail will take the antispam action configured in this antispam profile. But unlike SPF checking in a session profile, failed SPF checking in an antispam profile will not increase the client's reputation score. Starting from 6.0.3 release, you can specify different actions towards different SPF check results: • **Fail**: the host is not authorized to send messages. • **Softfail**: the host is not authorized to send messages but not a strong statement. • **Sender Alignment**: Header From and autorization domain mismatch. • **Permanent Error**: the SPF records are invalid. • **Temporary Error**: Proccessing error. • **Pass**: the host is authorized to send messages. • **Neutral**: SPF record is found but no definitive assertion. • **None**: No SPF record. **Note:** No SPF check is performed for direct connections from RFC 1918 private IP addresses. **Note:** Before FortiMail 4.0 MR3 Patch 1 release, you must enable SPF checking in the session profile before SPF checking in the antispam profile takes effect. Starting from 4.0 MR3 Patch 2 release, SPF checking can be enabled in either a session profile or an antispam profile, or both profiles. However, if you select to *Bypass* SPF checking in the session profile (see "Configuring sender validation options" on page 394), 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.

GUI item	Description
DMARC	Domain-based Message Authentication, Reporting & Conformance (DMARC) performs email authentication with SPF and DKIM checking. If either SPF check or DKIM check passes, DMARC check will pass. If both of them fails, DMARC check fails. More DMARC features will be added in future releases.

Behavior analysis	Behavior analysis (BA) analyzes the similarities between the uncertain email and the known spam email in the BA database and determines if the uncertain 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	Enable this option to examine the entire message header for spam characteristics.
Impersonation analysis	See “Configuring email impersonation analysis/Business Email Compromise settings” on page 420.
Heuristic	See “Configuring heuristic options” on page 413.
SURBL	See “Configuring SURBL options” on page 414.
DNSBL	See “Configuring DNSBL options” on page 414.
Banned word	See “Configuring banned word options” on page 415.
Safelist word	See “Configuring safelist word options” on page 416.
Dictionary	See “Configuring dictionary options” on page 417.
Image spam	See “Configuring image spam options” on page 417.
Bayesian	See “Configuring Bayesian options” on page 418.

GUI item	Description
Suspicious newsletter	Suspicious newsletters are part of the newsletter category. But FortiMail may find them to be suspicious because they may actually be spam under the disguise of newsletters. Note that if you enable detection of both newsletters and suspicious newsletters and specify actions for both types, if a newsletter is found to be suspicious, the action towards suspicious newsletters will take effect, not the action towards newsletters.
Newsletter	Although newsletters and other marketing campaigns are not spam, some users may find them annoying. Enable detection of newsletters and select an action profile to deal with them. For example, you can tag newsletter email so that users can filter them in their email clients.
Scan Conditions	See "Configuring scan conditions" on page 419.

Configuring FortiGuard options

The *FortiGuard* section of antispam profiles lets you configure the FortiMail unit to query the FortiGuard Antispam service to check the following:

- **IP Reputation**: if the SMTP client IP address is a public one, the FortiMail unit will query the FortiGuard Antispam service to determine if the current SMTP client is blocklisted; 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. If the *Extract IP from Received Header* option is enabled, the FortiGuard scan will also examine the public IP addresses of all other SMTP servers that appear in the `Received:` lines of the message header.

  FortiGuard Antispam scans do not examine private network addresses, as defined in RFC 1918.

- **URI filter**: this option determines if any uniform resource identifiers (URI) in the message body are associated with spam. FortiGuard URI filter groups URI into various categories, such as hacking, drug abuse and so on. You can configure the FortiGuard URI filter to check for certain categories only. For details, see "Configuring a FortiGuard URI filter profile" on page 412. If a URI is blocklisted, the FortiMail unit treats the email as spam and performs the associated action. You can also exempt URLs from spam filtering. For details, see "Configuring the URL exempt list" on page 523.

  To take different actions towards different URI filters/categories, you can specify a primary and a secondary filter, and specify different actions for each filter. If both URI filters match an email message, the primary filter action will take precedence.

  To reduce false positives, unrated IP addresses will be ignored and no actions will be taken.

- **Spam outbreak protection**: enable this option to temporarily hold suspicious email for a certain period of time (configuragle with CLI command `config system fortiguard antispam set outbreak-protection-period`) if the enabled FortiGuard antispam check (block IP and/or URI 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*.

Note: If email messages are temporarily held by FortiGuard spam outbreak protection, and the "reject" action is configured in the action profile, the actual action will fallback to "system quarantine" if spam is detected afterwards.

Note: Email from some sources, such as whitelisted IP addresses and ACL relay rules, will be exempted from FortiGuard spam outbreak protection scan.

Before enabling *FortiGuard,* you must enable and configure FortiGuard Antispam rating queries.

FortiGuard URI filter and URI scanning have two levels of control: strict or aggressive. For details see "URI types" on page 413.

Starting from 6.0.4 release, the aggressive setting also scans the domain part of envelope `MAIL FROM,` header `From`, and `Reply-To` addresses. If the domains are identified as spam, the configured antispam actions will be applied.

If the *FortiGuard o*ption is enabled, you may improve performance and the spam catch rate by also enabling *Block IP* and caching. For details on enabling caching, see ""Configuring FortiGuard services" on page 287.

To configure FortiGuard scan options

1. When configuring an antispam profile, select the *FortiGuard* check box in the *AntiSpam Profile* dialog.
2. From *Action*, select the action profile that you want the FortiMail unit to use if the FortiGuard Antispam scan finds spam email. This action is the default action for all the FortiGuard filters, including IP reputation, URI filter, and spam outbreak protection.

   For more information, see "Configuring antispam action profiles" on page 422.
3. 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 *IP Reputation*. 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. Then select an action profile. The default action means to use the FortiGuard action, not the antispam profile action.

   If you want to check all SMTP servers in the `Received:` lines of the message header, enable the *Extract IP from Received Header* option.
4. If you want to use the FortiGuard URI filter service, select a filter profile from the *Primary* or *Secondary URI filter* list. For details, see "Configuring a FortiGuard URI filter profile" on page 412. Then select an action profile. The default action means to use the FortiGuard action, not the antispam profile action.

   Note: If the secondary URI filter is matched, the email will be deferred in the spam outbreak queue if the spam outbreak protection is enabled.
5. If you want use the spam outbreak protection feature, enable it. Then select an action profile. The default action means to use the FortiGuard action, not the antispam profile action.
6. Continue to the next section, or click *Create* to save the antispam profile.

Configuring a FortiGuard URI filter profile

FortiGuard URI filter service allows you choose which categories of URI in the email body you want to check, rewrite, or block. Then you can use the filters in the antispam profiles (see

"Configuring FortiGuard options" on page 411) and the FortiGuard URI Click Protection settings (see "Configuring FortiGuard URI click protection service" on page 293).

To configure a URI filter profile

1. Go to *Profile* > *AntiSpam* > *URI Filter*.
2. Click *Create New*.
3. Enter a profile name.
4. Select the URI categories you want to check in the email body.
5. Click *Create*.

URI types

There are two types of URIs:

- Absolute URIs strictly follow the URI syntax and include the URI scheme names, such as "http", "https", and "ftp". For instance, http://www.example.com.
- Reference URIs do not contain the scheme names. For instance, example.com.

By default, FortiMail scans for absolute URIs.

You can use the following CLI command to change the default setting:

```
config antispam settings
  set uri-checking {aggressive | strict}
end
```

- `aggressive`: Choose this option to scan for both the absolute and reference URIs.
- `strict`: Choose this option to scan for absolute URIs only. Note that web sites without "http" or "https" but starting with "www" are also treated as absolute URIs. For instance, www.example.com.

For more information about this command, see *FortiMail CLI Reference*.

Configuring heuristic options

The FortiMail unit includes rules used by the heuristic filter. Each rule has an individual score used to calculate the total score for an email. A threshold for the heuristic filter is set for each antispam profile. To determine if an email is spam, the heuristic filter examines an email message and adds the score for each rule that applies to get a total score for that email. For example, if the subject line of an email contains "As seen on national TV!", it might match a heuristic rule that increases the heuristic scan score towards the threshold.

- Email is spam if the total score equals or exceeds the threshold.
- Email is not spam if the total score is less than the threshold.

The FortiMail unit comes with a default heuristic rule set. To ensure that the most up-to-date spam methods are included in the percentage of rules used to calculate the score, update your FortiGuard Antispam packages regularly. See "Configuring FortiGuard services" on page 287.

To configure heuristic scan options

1. When configuring an antispam profile, enable *Heuristic* in the *AntiSpam Profile* dialog.
2. Click the arrow to expand *Heuristic*.
3. From *Action*, select the action profile that you want the FortiMail unit to use if the heuristic scan finds spam email.

   For more information, see "Configuring antispam action profiles" on page 422.
4. In *Threshold*, enter the score at which the FortiMail unit considers an email to be spam. The default value is recommended.

5. In the *The percentage of rules used* field, enter the percentage of the total number of heuristic rules to use to calculate the heuristic score for an email message.
6. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

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 this scan to PDF attachments. For more information, see "Configuring scan conditions" on page 419.

Configuring SURBL options

In addition to supporting Fortinet's FortiGuard Antispam SURBL service, the FortiMail unit supports third-party Spam URI 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 (URI) in the message body are associated with spam. If a URI is blocklisted, the FortiMail unit treats the email as spam and performs the associated action. There are two types of URIs. For details, see "URI types" on page 413.

To configure SURBL scan options

1. When configuring an antispam profile, enable *SURBL* in the *AntiSpam Profile* dialog.
2. From *Action*, select the action profile that you want the FortiMail unit to use if the SURBL scan finds spam email.

   For more information, see "Configuring antispam action profiles" on page 422.
3. Next to *SURBL* click *Configuration*.

   A pop-up window appears that displays the domain name of the SURBL servers.
4. To add a new SURBL server address, click *New* and type the address in the field that appears.

   Since the servers will be queried from top to bottom, you may want to put the reliable servers with less traffic to the top of the list. Click the drop-down menu in the title bar to sort the entries.
5. Select a server and click *OK*.

   The pop-up window closes.
6. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring DNSBL options

In addition to supporting Fortinet's FortiGuard Antispam DNSBL service, the FortiMail unit supports third-party DNS blocklist servers. You can enable DNSBL filtering as part of the antispam profile, and define multiple DNSBL servers for each antispam profile. Consult the third-party DNSBL service providers for any conditions and restrictions.

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 located 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. For more information, see ““Configuring FortiGuard options” on page 411.

DNSBL scans do not examine private network addresses, which are defined in RFC 1918.

The *DNSBL* section of antispam profiles lets you configure the FortiMail unit to query one or more DNS block list (DNSBL) servers to determine if the IP address of the SMTP client has been blocklisted. If the IP address is blocklisted, the FortiMail unit treats the email as spam and performs the associated action.

To configure DNSBL scan options

1. When configuring an antispam profile, enable *DNSBL* in the *AntiSpam Profile* dialog.
2. From *Action*, select the action profile that you want the FortiMail unit to use if the DNSBL scan finds spam email.

   For more information, see “Configuring antispam action profiles” on page 422.
3. Next to *DNSBL* click *Configuration*.

   A pop-up window appears where you can enter the domain names of DNSBL servers to use with this profile.
4. To add a new DNSBL server address, click *New* and type the address in the field that appears.

   Since the servers are queried from top to bottom, you may want to put the reliable servers with less traffic to the top of the list. Click the drop-down menu in the title bar to sort the entries.
5. Select a server from the list and click *OK*.

   The pop-up window closes.

Closing the pop-up window does ***not*** save the antispam profile and its associated DNSBL server list. To save changes to the DNSBL server list, in the antispam profile, click *OK* before navigating away to another part of the web UI.

6. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring banned word options

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 a banned word is found, the FortiMail unit treats the email as spam and performs the associated action.

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 about wildcards and regular expressions, see "Appendix D: Regular expressions" on page 623.

You can also apply this scan to PDF attachments. For more information, see "Configuring scan conditions" on page 419.

To configure banned word scan options

1. When configuring an antispam profile, enable *Banned word* in the *AntiSpam Profile* dialog.
2. From *Action*, select the action profile that you want the FortiMail unit to use if the banned word scan finds spam email.

   For more information, see "Configuring antispam action profiles" on page 422.
3. Next to *Banned word*, click *Configuration*.

   A pop-up window appears, showing the words or phrases that will be prohibited by this profile. You can add or delete words on this window.
4. Click *New*, then enter the banned word in the field that appears.
5. Select *Subject* to have the subject line inspected for the banned word. If the check box is clear, the subject line is not inspected.
6. Select *Body* to have the message body inspected for the banned word. If the check box is clear, the message body is not inspected.
7. Click *OK*.

   The pop-up window closes.

Closing the pop-up window does ***not*** save the antispam profile and its associated banned word list. To save changes to the banned word list, first click *OK* before navigating away to another part of the web UI.

8. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring safelist word options

The *Safelist word* section of antispam profiles lets you configure the FortiMail unit to consider email messages whose subject line and/or message body contain a safelisted word to be indisputably not spam. If the email message contains a safelisted word, the FortiMail unit does not consider the email to be spam.

You can use wildcards in safelisted words. But unlike dictionary scans, safelist word scans do ***not*** support regular expressions. For details about wildcards and regular expressions, see "Appendix D: Regular expressions" on page 623.

To configure safe list scan options

1. When configuring an antispam profile, enable *Safelist word* in the *AntiSpam Profile* dialog.
2. Next to *Safelist word*, click *Configuration*.

   A pop-up window appears, showing the words or phrases that are allowed by this profile. You can add or delete words on this window.
3. Click *New*, then enter the allowed word in the field that appears.

4. Select *Subject* to have the subject line inspected for the allowed word. If the check box is clear, the subject line is not inspected.
5. Select *Body* to have the message body inspected for the allowed word. If the check box is clear, the message body is not inspected.
6. Click *OK*.

   The pop-up window closes.

Closing the pop-up window does ***not*** save the antispam profile and its associated banned word list. To save changes to the banned word list, first click *Save* before navigating away to another part of the web UI.

7. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring dictionary options

The *Dictionary* section of antispam profiles lets you configure the FortiMail unit to use dictionary profiles to determine if the email is likely to be spam. If the FortiMail unit considers email to be spam, it performs the associated action.

Before you can use this feature, you must have existing dictionary profiles. For information on creating dictionary profiles, see "Configuring dictionary profiles" on page 479.

When dictionary scanning is enabled and an email is found to contain 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.

Unlike 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.

To configure dictionary scan options

1. When configuring an antispam profile, enable *Dictionary* in the *AntiSpam Profile* dialog.
2. Click the arrow to expand *Dictionary.*
3. From *Action*, select the action profile that you want the FortiMail unit to use if the dictionary scan finds spam email.

   For more information, see ""Configuring antispam action profiles" on page 422.
4. From the *With dictionary group* drop-down list, select the name of a group of dictionary profiles to use with the dictionary scan. Or, from the *With dictionary profile* drop-down list, select the name of a dictionary profile to use with the dictionary scan.
5. In the *Minimum dictionary score* field, enter the number of dictionary term matches above which the email will be considered to be spam. Note that the score value is based on individual dictionary profile matches, not the dictionary group matches.
6. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring image spam options

The *Image spam* section of antispam profiles lets you configure the FortiMail unit to analyze the contents of GIF, JPG, and PNG graphics to determine if the email is spam. If the email message contains a spam image, the FortiMail unit treats the email as spam and performs the associated action.

Image spam scanning may be useful when, for example, the message body of an email contains graphics but no text, and text-based antispam scans are therefore unable to determine whether or not an email is spam.

To configure image scan options

1. When configuring an antispam profile, enable *Image spam* in the *AntiSpam Profile* dialog.
2. From *Action*, select the action profile that you want the FortiMail unit to use if the image scan finds spam email.

   For more information, see "Configuring antispam action profiles" on page 422.
3. Enable *Aggressive scan* to inspect image file attachments in addition to embedded graphics.

   Enabling this option increases workload when scanning email messages that contain image file attachments. If you do not require this feature, disable this option to improve performance.

   This *Aggressive scan* option applies only if you enable PDF scanning. For more information, see "Configuring scan conditions" on page 419.
4. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring Bayesian options

The *Bayesian* section of antispam profiles lets you configure the FortiMail unit to use Bayesian databases to determine if the email is likely to be spam. If the Bayesian scan indicates that the email is likely to be spam, the FortiMail unit treats the email as spam and performs the associated action.

FortiMail units can maintain two Bayesian databases: global and per-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 533.

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.

To configure Bayesian scan options

1. When configuring an antispam profile, enable *Bayesian* in the *AntiSpam Profile* dialog.
2. Click the arrow to expand *Bayesian.*
3. From *Action*, select the action profile that you want the FortiMail unit to use if the Bayesian scan finds spam email.

   For more information, see "Configuring antispam action profiles" on page 422.
4. Configure the following:

GUI item	Description
Accept training messages from users	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 503. 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 safe lists 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.)

5. Continue to the next section, or click *Create* or *OK* to save the antispam profile.

Configuring scan conditions

The *Scan Conditions* section of antispam profiles lets you configure conditions that cause the FortiMail unit to omit antispam scans, or to apply some antispam scans to PDF attachments.

To configure scan condition options

1. When configuring an antispam profile, click the arrow to expand *Scan Conditions* in the *AntiSpam Profile* dialog.
2. Configure the following:

GUI item	Description
Max message size to scan	Enter the maximum size of email messages, in bytes, that the FortiMail unit will scan for spam. Messages larger than the set size are not scanned for spam. To disable the size limit, causing all messages to be scanned, regardless of size, enter `0`. **Note:** Resource requirements for scanning messages increase with the size of the email message. If the spam you receive tends not to be smaller than a certain size, consider limiting antispam scanning to messages under this size to improve performance.
Bypass scan on SMTP authentication	Enable to bypass spam scanning for authenticated SMTP connections. **Note:** If you can trust that authenticating SMTP clients are not a source of spam, consider enabling this option to improve performance.

GUI item	Description
Scan PDF attachment	Spammers may attach a PDF file to an otherwise empty message to get their email messages past spam safeguards. The PDF file contains the spam information. Since the message body contains no text, antispam scanners cannot determine if the message is spam. Enable this option to use the heuristic, banned word, and image spam scans to inspect the first page of PDF attachments. This option applies only if you have enabled and configured heuristic, banned word, and/or image spam scans. For information on configuring those scans, see “Configuring heuristic options” on page 413, “Configuring banned word options” on page 415, and “Configuring image spam options” on page 417.
Apply default action without scan upon policy match	Select this option to take the default antispam action right away without applying other antispam filters if the email matches the relevant IP or recipient policy.

Performing a batch edit

You can apply changes to multiple profiles at once.

1. Go to *Profile* > *AntiSpam* > *AntiSpam*.
2. In the row corresponding to existing profiles whose settings you want to modify, mark their check boxes.

   The ability to batch edit antispam profiles does not apply to predefined profiles.
3. Click *Batch Edit*.

   The *AntiSpam Profile* dialog appears.
4. Modify the profile, as explained in “Managing antispam profiles” on page 407, 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 email impersonation analysis/Business Email Compromise settings

Email impersonation, or Business Email Compromise (BEC), 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 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 "CEO ABC <ceo@external.com>" in the Email header From, 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.

There are two ways to do the mapping:

- **Manual**: you manually enter mapping entries and create impersonation analysis profiles as described below. Then you enable the impersonation profile in an antispam profile ("Managing antispam profiles" on page 407). Eventually, you will apply the antispam profie in the IP-based or recipient-based policies ("Controlling email based on IP addresses" on page 375 and "Controlling email based on sender and recipient addresses" on page 381).
- **Dynamic**: FortiMail Mail Statistics Service can automatically learn the mapping. See details below.

Impersonation analysis checks both the Header From and Reply-To fields.

To avoid false positives, impersonation analysis follows some exempt rules.

To create an impersonation analysis profile

1. Go to *Profile* > *AntiSpam* > *Impersonation*.
2. Click *New* to create a new profile.
3. Enter a profile name.
4. Select a domain or System from the dropdown list. The profile will be applied to your selection.
5. Under *Impersonation Entry*, click *New* to add an entry.

GUI item	Description
Display name pattern	Enter the display name to be mapped to the email address. You can use wildcard or regular expression.
Pattern type	Either wildcard or regular expression.
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.

Enabling impersonation analysis dynamic scanning

In addition to manually entering mapping entries and creating impersonation analysis profiles, FortiMail Mail Statistics Service can automatically/dynamicaly learn and track the mapping.

To use the FortiMail manual, dynamic, or both manual and dynamic impersonation analysis scanning, use the following command:

```
config antispam settings
  set impersonation-analysis dynamic manual
end
```

By default, FortiMail uses manual analysis only.

Also enable the FortiMail Mail Statistics Service with the following command. This service is disabled by default:

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

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

To view and configure antispam action profiles

1. Go to *Profile* > *AntiSpam* > *Action*.

GUI item	Description
Domain (drop-down 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	Select if the action profile will be system-wide or domain-wide. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter a name.
Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[spam]`, in the *With value* field. 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 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	Starting from 6.0.1 release, you can insert disclaimer as an action. You can modify the default discaimer or add new disclaimers by going to *System* > *Customization* > *Custom Message* > *Email Content Resources* > *Disclaimer insertion message*.

GUI item	Description
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.
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. You can choose to deliver the original email or the modified email.
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 555.
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 491 and "Customizing email templates" on page 226.
Final action	For details about final and non-final actions, see "Order of execution" on page 16.
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 sent to FortiSandbox, the actual action will fallback to "system quarantine" if spam or viruses are detected afterwards.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
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 138. For outgoing email, this action will fallback to the system quarantine. You can choose to quarantine the original email or the modified email.

GUI item	Description
System quarantine to folder	Enable to redirect spam to the system quarantine folder. For more information, see "Managing the system quarantine" on page 141. You can choose to quarantine the original email or the modified email. The system quarantine and personal quarantine options are mutually exclusive.
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*.

   To apply an antispam action profile, select it in one or more antispam profiles. For details, see "Managing antispam profiles" on page 407.

Configuring antivirus profiles and antivirus action profiles

The *AntiVirus* submenu lets you configure antivirus profiles and related action profiles. See the following topics for details:

- Managing antivirus profiles
- Configuring antivirus action profiles

Managing antivirus profiles

Go to *Profile* > *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 427.

FortiMail keeps its antivirus scan engine and virus signature database up-to-date by connecting to Fortinet FortiGuard Distribution Network (FDN) antivirus services. For details, see "Configuring FortiGuard services" on page 287.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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.

   A dialog appears.
3. Click the arrows to expand each section as needed and 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 specific protected domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, type its name. The profile name is editable later.
Default action	Select an action profile or create a new action profile. See "Configuring antivirus action profiles" on page 427.
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 realtime malware analysis, or heuristic antivirus scan, when performing antivirus scanning.
File signature check	Enable to scan for file signatures. For details, see "Adding file signatures" on page 540.
Grayware	Enable to scan for grayware, such as mail bomb detection.
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 285.
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.

GUI item		Description
	Malicious/Virus **High risk** **Medium risk** **Low risk** **No Result**	Specify the action to take if the FortiSandbox analysis determines that the email messages have virus or other threat qualities. You can specify different actions according to the threat levels.
URI analysis		Enable to send the URIs 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.

Configuring antivirus action profiles

Go to *Profile* > *Antivirus* > *Action* to define one or more actions that the FortiMail unit should do if the antivirus profile determines that an email is infected by viruses.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

To view and configure antivirus action profiles

1. Go to *Profile* > *AntiVirus* > *Action*.

GUI item	Description
Domain (drop-down 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	Select if the action profile will be system-wide or domain-wide. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter a name.
Tag email's subject line	Enable and enter the text that appears in the subject line of the email, such as `[virus]`, in the *With value* field. The FortiMail unit will prepend this text to the subject line of spam before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.
Insert header	Enable and enter the message header key in the field, and the values in the *With value* field. The FortiMail unit adds this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as virus by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. Starting from 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	Starting from 6.0.1 release, you can insert disclaimer as an action. You can modify the default discaimer or add new disclaimers by going to *System* > *Customization* > *Custom Message* > *Email Content Resources* > *Disclaimer insertion message*.

GUI item	Description
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*.
BCC	Enable to send a blind carbon copy (BCC) of the email. You can choose to deliver the original email or the modified email. Configure BCC recipient email addresses by entering each one and clicking *Create* in the *BCC* area.
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 491 and "Customizing email templates" on page 226.
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 sent to FortiSandbox, the actual action will fallback to "system quarantine" if spam or viruses are detected afterwards.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
System Quarantine	Enable to redirect email to the system quarantine. For more information, see "Managing the system quarantine" on page 141. You can choose to quarantine the original email or the modified email.
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 scan, virus replacement messages will be used. • For FortiSanbox scan, virus replacement messages will be used. • For heuristic scan, suspicious replacement messages will be used. You can customize replacement messages. For more information, see "Customizing GUI, replacement messages and email templates" on page 218.

GUI item	Description
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 226.
Repackage email with original 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* submenu lets you configure content profiles for incoming and outgoing content-based scanning. The available options vary depending on the chosen directionality.

This topic includes:

- Configuring content profiles
- Configuring file filters
- Configuring file password
- Configuring content action profiles

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 access this part of the web UI, your administrator account’s access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see ““About administrator account permissions and domains” on page 179.

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 (drop-down 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 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.

   A multisection dialog appears.
3. For a new profile, select *System* in the *Domain* list to see profiles that apply to t he entire FortiMail unit or 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 439.
6. Configure the following sections as needed:
   - "Configuring attachment scan rules" on page 431
   - "Configuring scan options" on page 432
   - "Configuring content disarm and reconstruction" on page 433
   - "Configuring archive handling" on page 434
   - "Configuring password decryption options" on page 436
   - "Configuring content monitor and filtering" on page 436
7. Click *Create* or OK to save the entire 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 438.

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 430.

1. Go to *Profile* > *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 Rules* section.

4. Click *New* to add a rule:

GUI item	Description
Enabled	Select to enable the rule.
File filter	Select the file filter. See "Configuring file filters" on page 438.
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 whitelist 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 430.

1. Go to *Profile* > *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 Options* 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 Outlook, can fragment big emails into multiple sub-messages. This is used to bypass oversize limits/scanning.
Detect password protected Office/PDF document	Enable to apply the block action configured in the content action profile if an attached MS 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 the MS Office, OpenOffice, or PDF attachments using the predefined or user-defined passwords. For details, see "Configuring file password" on page 439.
Detect embedded component	Documents, similar to an archive, can sometimes contain video, graphics, sounds, and other files that are used by the document. By embedding the required file within itself instead of linking to such files externally, a document becomes more portable. However, it also means that documents can be used to hide infected files that are the real attack vector. Enable to, for MIME types such as Microsoft Office, Microsoft Visio, OpenOffice.org , and PDF documents, scan files that are encapsulated within the document itself.

GUI item	Description
Defer delivery of message on policy match	Enable to defer mail delivery from specific senders configured in policy to conserve peak time bandwidth at the expense of sending low priority, bandwidth consuming traffic at scheduled times. For example, you can apply this function to senders of marketing campaign emails or mass mailing. For information on policy, see "How to use policies" on page 360. For information on scheduling deferred delivery, see "Configuring mail server settings" on page 195.
Defer delivery of messages larger than	Enter the file size limit over which the FortiMail unit will defer processing large email messages. If not enabled, large messages are not deferred. For information on scheduling deferred delivery, see "Configuring mail server settings" on page 195.
Maximum number of attachment	Specify how many attachments are allowed in one email message. The valid range is between 1 and 100. The default value is 10.
Maximum size	You can specify the actions to take against the email (either the message itself or the attachments) that exceeds the specified maximum size.
Adult image analysis	If you have purchase the adult image scan license, you can enable it to scan for adult images. You can also configure the scan sensitivity and image sizes under *Security* > *Other* > *Adult Image Analysis*. For details, see "Configuring adult image analysis" on page 541.

Configuring content disarm and reconstruction

HTML contents in email body and attachments may contain potentially hazardous tags and attributes (such as hyperlinks and scripts). MS Office and PDF attachments may contain potentially hazardous macros, active scripts, and other active contents.

FortiMail provides the capability to remove or neutralize the potentially hazardous contents and reconstruct the email messages and attachment 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 430.

1. Go to *Profile* > *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	Either use the default action or specify an action.

HTML content	Enable to detect hypertext markup language (HTML) tags in the content type text/html parts of the email messages. • *Convert HTML to text*: convert the HTML content to text only content. • *Sanitize HTML content*: produce new HTML content by removing the potentially hazardous tags and attributes (such as hyperlinks and scripts) and only preserving the safe and essential tags (such as formatting tags). • *Remove URIs*: remove the URIs in email message. To define which URI category to remove URIs from, click *View settings* (see "Configuring FortiGuard URI click protection service" on page 293). • *Click Protection*: Rewrite the URIs and in case the user clicks on the URIs, scan the URIs and then take the configured actions (see "Configuring FortiGuard URI click protection service" on page 293).
Text content	Enable to detect URIs in the content type text/plain parts of the email messages. • *Remove URIs*: Removes URIs in the text parts of email messages. To define which URI category to remove URIs from, click *View settings* (see "Configuring FortiGuard URI click protection service" on page 293). • *Click Protection*: Rewrite the URIs and in case the user clicks on the URIs, scan the URIs and then take the configured actions (see "Configuring FortiGuard URI click protection service" on page 293).
MS Office	Enable to disarm and reconstruct the MS Office attachments. This also includes the .zip files that are compressed once.
PDF	Enable to disarm and reconstruct the PDF attachments. This also includes the .zip files that are compressed once.

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 430.

1. Go to *Profile* > *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:

Check Archive Content	Enable to determine which action to perform with the archive attachments. • blocking password protected archives if you have selected *Detect Password Protected Archive* • blocking archives that could not be successfully decompressed if you have selected *Detect on Failure to Decompress* • passing/blocking by comparing the depth of nested archives with the nesting depth threshold configured in *Max Level of Compression* By default, archives with less than 10 levels of compression will be blocked if they cannot be successfully decompressed or are password-protected. Depending on the nesting depth threshold and the attachment's depth of nested archives, the FortiMail unit may ***also*** consider the file types of files within the archive when determining which action to perform. For details, see the section below. If disabled, the FortiMail unit will perform the *Block/Pass* action solely based upon whether an email contains an archive. It will disregard the depth of nesting, password protection, successful decompression, and the file types of contents within the archive.
Detect on Failure to Decompress	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 436. If 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 MIME 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 MIME 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 430.

1. Go to *Profile* > *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*: use the words before and after the keywords as the passwords. *Number of words to try*: specify how many words before and after the keywords to use. For example, in the email content, there is such a sentence: "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, "please", "use" (two words before the keyword "password"), "123456", and "If" (two words after the keyword "password") will be used as one by one as the password to decrypt the attachments.
   - *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 password" on page 439.

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 MS 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 430.

To configure a content monitor profile

1. Go to *Profile* > *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.
Enable	Select or clear the check box to enable or disable a content monitor.

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 drop-down 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 479.
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.

GUI item	Description
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 439*.

Scan Condition	Specify the content type 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 <size_in_MB>`
	`end`

6. Click *Create* or OK on the *Content Monitor Profile* dialog to save and close it.

Configuring file filters

File filters are used in the attachment scan rules (see "Configuring attachment scan rules" on page 431. File filters defines the email attachment file types and file extensions to be scanned.

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 430.

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 "Configuring scan options").

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 box (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 439.
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 password

When you configure the content profile, you can choose to decrypt PDF documents (see "Configuring scan options" on page 432) and archived files (see "Configuring archive handling" on page 434. To decrypt the documents, you need passwords. For details, see "Configuring password decryption options" on page 436.

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

To view and manage the list of content action profiles

1. Go to *Profile* >*Content* > *Action*.

GUI item	Description
Domain (drop-down 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 email's subject line	Enable and enter the text that will appear in the subject line of the email, such as "`[PROHIBITED-CONTENT]`", in the *With value* field. The FortiMail unit 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.
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 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. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. Starting from 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	Starting from 6.0.1 release, you can insert disclaimer as an action. You can modify the default discaimer or add new disclaimers by going to *System* > *Customization* > *Custom Message* > *Email Content Resources* > *Disclaimer insertion message*.
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.

GUI item	Description
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, replacement messages and email templates" on page 218. ***Note***: When the action profile is used in a DLP profile, the replace action will fallback to system quarantine action.
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 555.
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 491 and "Customizing email templates" on page 226.
Final action	
Treat as spam	Enable to perform the *Actions* selected in the antispam profile of the policy that matches the email. For more information, see "Configuring antispam action profiles" on page 422.
Reject	Enable to reject the email and reply to the SMTP client with SMTP reply code 550.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
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 138. For outgoing email, this action will fallback to the system quarantine. You can choose to quarantine the original email or the modified email.
System quarantine to folder	Enable to redirect the email to the system quarantine and specify the quarantine folder. For more information, see "Managing the system quarantine" on page 141. The two quarantine options are mutually exclusive. You can choose to quarantine the original email or the modified email.

GUI item	Description
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 485. 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 371.

To apply a content action profile, select it in the *Action* drop-down list of one or more antispam profiles. For details, see "Managing antispam profiles" on page 407.

Configuring resource profiles

Go to Profile > *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 325 and "Configuring user preferences" on page 329.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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 (drop-down 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 maximum amount of FortiMail webmail disk space that you will allow to be consumed, or enter 0 to allow unlimited use.
User account status	Select to enable email user accounts using this resource profile.
Webmail access	Enable to allow email users to access FortiMail webmail and other webmail features, such as auto reply and address books.
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 381 and "Controlling email based on IP addresses" on page 375.

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 rules" on page 363.

2. For secure (SSL or TLS) authentication:
   - Upload a local certificate. For details, see "Managing local certificates" on page 276.
   - Enable *SMTP over SSL/TLS*. For details, see "Configuring mail server settings" on page 195.
   - 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 483 and "Configuring access control rules" on page 363.
   - 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 332, "Managing certificate authority certificates" on page 283, and "Managing OCSP server certificates" on page 284.

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 446)
   - LDAP (see "Configuring LDAP profiles" on page 450)
   - RADIUS (see "Configuring authentication profiles" on page 446)

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 325 and "Configuring resource profiles" on page 443.

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 381 and "Controlling email based on IP addresses" on page 375.

   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 381.

Configuring authentication profiles

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS
- LDAP

When the FortiMail unit is operating in server mode, only local and RADIUS authentication are available.

LDAP profiles can configure many features other than authentication, and are not located in the *Authentication* menu. For information on LDAP profiles, see "Configuring LDAP profiles" on page 450.

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.

Depending on the mode in which your FortiMail unit is operating, you may be able to apply authentication profiles through incoming recipient-based policies, IP-based policies, and email user accounts. For more information, see "Controlling email based on sender and recipient addresses" on page 381, "Controlling email based on IP addresses" on page 375, and "Configuring local user accounts (server mode only)" on page 325.

For the general procedure of how to enable and configure authentication, see "Workflow to enable and configure authentication of email users" on page 445.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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:

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 editabel 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. The default value varies by the protocol. You must change this value if the server is configured to listen on a different port number, including if the server requires use of SSL. For example, the standard port number for SMTP is 25. However, for SMTP with SSL, the default port number is 465. Similarly, IMAP is 143, while IMAP with SSL is 993; POP3 is 110, while POP3 with SSL is 995; and RADIUS is 1812.
Use generic LDAP mail host if available (SMTP authentication only)	*Use generic LDAP mail host if available*: 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 465. 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).

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.

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.
Authentication type	Select the protocol used to connect to the authentication server, either SMTP, POP3, IMAP, or RADIUS.
(not in server mode)	This drop-down list does not appear if the FortiMail unit is operating in server mode, which can only use RADIUS authentication profiles.
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. The default value varies by the protocol. You must change this value if the server is configured to listen on a different port number, including if the server requires use of SSL. For example, the standard port number for SMTP is 25. However, for SMTP with SSL, the default port number is 465. Similarly, IMAP is 143, while IMAP with SSL is 993; POP3 is 110, while POP3 with SSL is 995; and RADIUS is 1812.
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.

GUI item	Description
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 Settings	When you add a FortiMail administrator (see "Configuring administrator accounts" on page 182), 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.

To apply the authentication profile, you must select it in a policy. You may also need to configure access control rules, user accounts, and certificates. For details, see "Workflow to enable and configure authentication of email users" on page 445.

Configuring LDAP profiles

Like all profiles, none of the VIP profile settings are global. They are applied only to traffic which is controlled by a policy which includes the appropriate VIP Map profile.

For the sender and recipient patterns, the @ symbol must appear even if you're using wildcards. For example, if you want to match all addresses, you must use *@* rather than just * to work properly.

The *LDAP* submenu lets you configure LDAP profiles which can query LDAP servers 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 468.

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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*.
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.
(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.

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 multisection dialog appears.
3. Configure the following general settings:

GUI item	Description
Profile name	For a new profile, enter its name.
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*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
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*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.

GUI item	Description
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-secured (LDAPS) connection. Click *Test LDAP Query* to test the connection. A pop-up window appears. For details, see "To verify user query options" on page 477. **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 ActiveDirectory-style schema, you must select *SSL*. ActiveDirectory servers require a secure connection for queries that change user passwords.
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, such as `cn=FortiMailA,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*, *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 453
- "Configuring group query options" on page 454
- "Configuring user authentication options" on page 456
- "Configuring user alias options" on page 457
- "Configuring mail routing" on page 462
- "Configuring address mapping options" on page 463
- "Configuring scan override options" on page 463
- "Configuring domain lookup options" on page 465
- "Configuring remote access override options" on page 466
- "Configuring advanced options" on page 467

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 450.

1. Go to *Profile* > *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 (dropdown list)	You can select a schema style by clicking *Schema*. Then you can edit the schema as desired. 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 "LDAP user query example" on page 453. You can select a schema style by clicking *Schema*. Then you can edit the schema as desired. Or select *User Defined* and write your own schema. 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.

LDAP user query example

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 ActiveDirectory-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 457.

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 450.

1. Go to *Profile* > *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 381 or ""Controlling email based on IP addresses" on page 375.

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 distinguished name (DN) in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query. For example, you might find it more convenient in each recipient-based policy to type only the group name, `admins`, rather than typing the full DN, `cn=admins,ou=Groups,dc=example,dc=com`. In this case, you could enable this option, then configure *Group base DN* (`ou=Groups,dc=example,dc=com`) and *Group name attribute* (`cn`). When performing the query, the FortiMail unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the *Group name attribute* and the *Group base DN* configured in the LDAP profile. **Note:** Enabling this option is appropriate ***only if*** your LDAP server's schema specifies that the group membership attribute's value must use DN syntax. It is ***not*** appropriate if this value uses another type of syntax, such as a number or common name. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`. Because a group ID number does not use DN syntax, you would not enable this option.

GUI item	Description
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	Sepcify how many levels of nested groups will be expanded for lookup. Valid range is 1-6. Defult 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 316 and "Managing the personal quarantines" on page 138.
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 450.

1. Go to *Profile* > *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 381.

4. Configure the following:

GUI item	Description
Try UPN or mail address as bind DN	Select to form the user's bind DN by prepending the user name portion of the email address ($u) to the User Principle Name (UPN, such as `example.com`). By default, the FortiMail unit will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, enter that UPN in the field named *Alternative UPN suffix*. This can be useful if users authenticate with a domain other than the mail server's principal domain name.
Try common name with base DN as bind DN	Select to form the user's bind DN by prepending a common name to the base DN. Also enter the name of the user objects' common name attribute, such as `cn` or `uid` into the field. This option is preconfigured and read-only if, in *User Query 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 450.

1. Go to *Profile* > *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)	You can select a schema style by clicking *Schema*. Then you can edit the schema as desired. 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 461. 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*. 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 non-user/alias objects. For details, see "Alias member query example" on page 461. For more information on required object types and their attributes, see "Preparing your LDAP schema for FortiMail LDAP profiles" on page 468. For details on query syntax, refer to any standard LDAP query filter reference manual.

GUI item	Description
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 461. 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.

GUI item	Description
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 an email address. This option is preconfigured and read-only if you have selected from *Schema* any schema style other than *User Defined*. If you have selected *User Defined*, this option is available only if *User group expansion In advance* is enabled. For details on query syntax, refer to any standard LDAP query filter reference manual.
Max alias expansion level	Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand.
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.
Max alias expansion level	Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand.
Use separate bind (configure the following if "Default Bind Options" on page 452 is not desired)	

GUI item	Description
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**, a**lias 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, such as `cn=FortiMailA,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*.

Alias member query example

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 461.

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 450.

1. Go to *Profile* > *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. 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 450.

1. Go to *Profile* > *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 Header From before the external email address. For example, 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 450.

1. Go to *Profile* > *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, 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 value syntaxes are permissible. For details, see "LDAP directory requirements for each FortiMail LDAP profile query" on page 470. 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 465). 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 470. 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 465). 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 470. 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 465). 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 450.

1. Go to *Profile* > *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.

   Organizations with multiple domains may maintain a list of domains on the LDAP server. The FortiMail unit can query the LDAP server to verify the domain portion of a recipient's email address.

   For this option to work, your LDAP directory should contain a single generic user for each domain such as `generic@dom1.com` because the FortiMail unit will only look at the domain portion of the generic user's mail address, such as `dom1.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.

   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.
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 check settings and quarantine report settings. The name of this attribute may vary by the schema of your LDAP directory.
Mail host attribute	Enter the name of the attribute, such as `mailHost`, whose value is the IP address of the backend mail server hosting the mailboxes of the domain. The name of this attribute may vary by the schema of your LDAP directory.

AntiSpam attribute	Enter the name of the attribute, such as `genericAntispam`, whose value is the name of the antispam profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute at all (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 at all (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 at all (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 450.

When you add a FortiMail administrator (see "Configuring administrator accounts" on page 182), 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 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*.
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 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 450.

1. Go to *Profile* > *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.
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.

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.
Password schema	Select your LDAP server's user schema style, either *Openldap* or *Active Directory*.
Bypass user verification if server is unavailable	If you have selected using LDAP server to verify recipient or sender address and your LDAP server is not accessible, enabling this option will 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 312.

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.

Table 46: 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			

Table 46: LDAP directory requirements for each FortiMail LDAP profile query

(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 461.	`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 461.

Table 46: LDAP directory requirements for each FortiMail LDAP profile query

User group object classes such as `group` or `groupOfNames`. User groups are not inherently associated with email aliases, but for some schemas, such as Microsoft ActiveDirectory, group objects play the role of email alias objects, and are used to indirectly resolve email aliases. For details, see "Base DN" on page 461.	`member`	A user object's DN, or the DN of another alias object.	Query retrieves the DN of a user object that is a member of the group. This attribute is required only if aliases resolve to user email addresses indirectly. For details, see "Base DN" on page 461.
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			

Table 46: LDAP directory requirements for each FortiMail LDAP profile query

(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)	Query retrieves whether or not to perform ***antivirus*** processing 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`, `DISABLE`, or `DISABLED`, or any other value not associated with "on" (off)	Query retrieves whether or not to perform ***antispam*** processing for any user defined by *User Query Options*.
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 full 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.

Figure 37: 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.

Table 47: Possible failure messages from LDAP query tests

Failure Message	Meaning and Solution
Empty input	The query cannot be performed until you provide the information required by the query.

Table 47: Possible failure messages from LDAP query tests

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.
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 DN*. If the value does not match, verify that you have supplied the *Group DN* according to the syntax expected by both your LDAP server and your configuration of *Group Query Options*.
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 *Change Password*, 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 U*ser Alias Options*, or the value of the alias' email address attribute does not match the value that you supplied in *Mail address*.

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.

To clear the LDAP query 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 antispam action profiles" on page 407 and "Configuring content profiles and content action profiles" on page 430.

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 543.

Table 48: 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.

Table 48: Predefined patterns

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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.
	
	Regular expressions do not require slash (`/`) boundaries. For example, enter:
	
	`v[i1]agr?a`
	
	Matches are case ***in***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==?=`
	
	the pattern must match:
	
	`Se trata del spam.`
	
	Entering the pattern `*iso-8859-1*` would ***not*** match.
	
	This option is not editable for predefined patterns.

Pattern type	For a new dictionary entry, select either: • *Wildcard*: *Pattern* is verbatim or uses only simple wild cards (? or *). • *Regex*: *Pattern* is a Perl-style regular expression. 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. For more information about antispam profiles, see "Configuring dictionary options" on page 417. For more information about content monitor profiles, see "Configuring content monitor and filtering" on page 436.
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*.

GUI item	Description
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 482, "Managing antispam profiles" on page 407, and "Configuring content profiles" on page 430.

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 479.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

To view and configure a dictionary group

1. Go to *Profile* > *Dictionary* > *Group*.

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*.
Group Name	Displays the name of the dictionary group or dictionary group item.

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 "Managing antispam profiles" on page 407, and "Configuring content profiles" on page 430.

Configuring security profiles

Go to *Profile* > *Security* to create transport layer security (TLS) profiles and encryption profiles.

This section includes:

- Configuring TLS security profiles
- Configuring encryption profiles

Configuring TLS security profiles

The *TLS* tab lets you create TLS profiles, which contain settings for TLS-secured connections.

TLS profiles, unlike other types of profiles, are applied through access control rules and message delivery rules, not policies. For more information, see "Controlling SMTP access and delivery" on page 362.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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*: Allow a simple TLS connection, but do not require it. Data is not encrypted, nor is the identity of the server validated with a certificate. • *Encrypt*: Requires a basic TLS connection. Failure to negotiate a TLS connection results in the connection being rejected according to the *Action* on failure setting. • *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 283.

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. This option does not apply and will be empty for profiles whose *TLS Level* is *Preferred*.
(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 name of the profile in *Profile name*. The profile name is editable later.
4. From *TLS level*, select the security level of the TLS profile:
   - *None*: Disables TLS. Requests for a TLS connection will be ignored.
   - *Preferred*: Allows a simple TLS connection, but does not require it. Data is not encrypted, nor is the identity of the server validated with a certificate.
   - *Encrypt*: Requires a basic TLS connection. Failure to negotiate a TLS connection results in the connection being rejected according to the *Action on failure* setting.
   - *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.

   The availability of the following options varies by your selection in *TLS level.*
5. Configure the following, as applicable:

GUI item	Description
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. This option does not appear if *TLS level* is *Preferred*.
Check CA issuer	Enable and enter a string on the *CA issuer* field. The FortiMail unit will compare the string in the *CA issuer* field with the field with that same name in the installed CA certificates. This option appears only if *TLS level* is *Secure*.

GUI item		Description
	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 283. *Check CA issuer* must be enabled for *CA issuer* to have any effect. 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. 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*.
Check encryption strength		Enable to require a minimum level of encryption strength. Also configure *Minimum encryption strength*. This option appears only if *TLS level* is *Encrypt* or *Secure*.
	Minimum encryption strength	Enter the bit size of the encryption key. Greater key size results in stronger encryption, but requires more processing resources.

Configuring encryption profiles

The *Encryption* tab lets you create encryption profiles, which contain encryption settings for secure MIME (S/MIME) and identity-based encryption (IBE).

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 371 and *"Configuring content action profiles" on page 439*.

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 547.

For more information about using S/MIME encryption, see "Using S/MIME encryption" on page 487.

For more information about using IBE, see "Configuring IBE encryption" on page 543.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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 or IBE.
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	Either Encrypt or Sign.
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 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. For more information, see "Configuring delivery rules" on page 371 and "Configuring TLS security profiles" on page 483.
IBE Action	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.
Max Push Size (KB)	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 487 and "Configuring certificate bindings" on page 547.
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 failur*e, 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 275.
   - 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 547.
   - create an S/MIME encryption profile. For details, see "Configuring encryption profiles" on page 485.
   - 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 371), 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 381, "Controlling email based on IP addresses" on page 375, *"Configuring content action profiles" on page 439*, and "Configuring content profiles" on page 430).

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 275.
   - 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* 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 destination IP addresses of multiple protected SMTP servers if you want to load balance ***incoming*** email between them (see "Relay type" on page 310)
- 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 323)
- 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 323)

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, *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 ***NOT*** 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 above rule is applied (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.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

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.
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 323, and/or "IP Pool" on page 377.

Configuring email and IP groups

The *Profile* > *Group* tab displays the list of email and IP group profiles.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category.

For details, see "About administrator account permissions and domains" on page 179.

Configuring email groups

Email groups include groups of email addresses that can be used when configuring access control rules. For information about access control rules, see "Configuring access control rules" on page 363.

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.

   A dialog appears.

3. For a new group, enter a name for this email group.

   The name must contain only alphanumeric characters. Spaces are not allowed.

4. In *New member*, enter the email address of a group member and click -> to move the address to the *Current members* field.

   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.

To remove a member's email address, select the address in the *Current members* field and click <-.

5. Click *Create* or *OK*.

Configuring IP groups

IP groups include groups of IP addresses that can be used when configuring access control rules. For information about access control rules, see "Configuring access control rules" on page 363.

To configure an IP group

1. Go to *Profile* > *Group* > *IP Group*.
2. Either click *New* to add a profile or double-click profile to modify it.

   A dialog appears.

3. For a new group, enter a name in *Group name*.

   The name must contain only alphanumeric characters. Spaces are not allowed.

4. Under *IP Groups*, click *New*.

   A field appears under *IP/Netmask or IP Range*.

5. 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.

   To match any address, enter `0.0.0.0/0`.

6. Click Create.

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 422, "Configuring antivirus action profiles" on page 427, and "Configuring content action profiles" on page 439.

To create a notification profile

1. Go to *Profile* > *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 322), 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.
5. Choose whom you want to send notification to: sender, recipient, or other users. If you choose *Others*, you click 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 226.
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 antispam action profiles" on page 407.

This section contains the following topics:

- Configuring authentication reputation
- Configuring email quarantines and quarantine reports
- Configuring the block lists and safe lists
- Configuring greylisting
- Configuring the URL exempt list
- Configuring bounce verification and tagging
- Configuring endpoint reputation
- Training and maintaining the Bayesian databases
- Adding file signatures
- Configuring action profile preferences
- Configuring adult image analysis

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 and Telnet
- **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 2 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 peoriod 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 154.

To configure authentication reputation settings

1. Go to Security > Authentication Reputation > Settings.

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 422) and content action profiles (see "Configuring content action profiles" on page 439).
- Configure the system quarantine administrator account who can manage the system quarantine. See "Configuring the system quarantine setting" on page 502.
- 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 503.
- 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 495.

- Configure domain-wide quarantine report settings for specific domains. See "Quarantine Report Setting" on page 316.
- View and manage personal quarantines and system quarantines. See "Managing the quarantines" on page 137.
- 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 613.
- Configuring global quarantine report settings
- Configuring the system quarantine setting
- Configuring the quarantine control options

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 422 and "Configuring content action profiles" on page 439. For general steps about how to use email quarantine, see "Configuring email quarantines and quarantine reports" on page 494.

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 316.

Starting from v4.1, domain-wide quarantine report settings are independent from the system-wide quarantine report settings.
However, in older releases, domain-wide quarantine report settings are a subset of the system-wide quarantine report settings. For example, if the system settings for schedule include only Monday and Thursday, when you are setting the schedule for the quarantine reports of the protected domain, you can only select Monday or Thursday.

For information on the contents of the plain text and HTML format quarantine report, see "About the plain text formatted quarantine report" on page 497 and "About the HTML formatted quarantine report" on page 499.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Quarantine* category.

For details, see "About administrator account permissions and domains" on page 179.

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 226.
Webmail Access Setting		
	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 161. 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*.

Table 49: 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 307.
	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 454. 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 501.

The contents of quarantine reports are customizable. For more information, see "Customizing GUI, replacement messages and email templates" on page 218.

Figure 38: Sample plain text quarantine report

```
Subject: Quarantine Summary: [ 3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00 ]
   From: release-ctrl@example.com
   Date: 12:00 PM
     To: user1@example.com

Date:       Thu, 04 Sep 2008 11:52:51
Subject:    [SPAM]  information leak
From:       User 1 <user1@example.com>
Message-Id: MTIyMDU0MzU3MS43NDJfNTk5ODcuRm9ydGlNYWlsLTQwMCwjRiNTIzYzMyNFLFU4OjIsUw==

Date:       Thu, 04 Sep 2008 11:51:10
Subject:    [SPAM]  curious?
From:       User 1 <user1@example.com>
Message-Id: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsI0YjUyM2MjUjRSxVNzoyLA==

Date:       Thu, 04 Sep 2008 11:48:50
Subject:    [SPAM]  Buy now!!!! lowest prices
From:       User 1 <user1@example.com>
Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsI0YjUyM2NDIjRSxVNToyLA==


Actions:

o) Release a message:     Send an email to <release-ctrl@example.com> with subject line set to
"user1@example.com:Message-Id".
o) Delete a message:     Send an email to <delete-ctrl@example.com> with subject line set to
"user1@example.com:Message-Id".
o) Delete all messages: Send an email to <delete-ctrl@example.com> with subject line set to
"delete all:user1@example.com:e4d46814:ac146004:05737c7c111d68d0111d68d0111d68d0".
```

Table 50: 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==

Table 50: Sample plain text quarantine report

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 Figure 39 on page 500)
- contain links to release individual email messages (see Figure 39 on page 500)

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 501.

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 496.

The contents of quarantine reports are customizable. For more information, see "Customizing GUI, replacement messages and email templates" on page 218.

Figure 39: Sample HTML quarantine report

Table 51: 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

Table 51: Sample HTML quarantine report

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:MTIyMDU0MDk1Ni43NDRfMTk2ODU0LkZvcnRpTWFpbC00MDAs I0YjUyM2NjUjRQ==`

Figure 40: 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 503.

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 495.

For more information on the differences between plain text and HTML format quarantine reports, see "About the plain text formatted quarantine report" on page 497 and "About the HTML formatted quarantine report" on page 499.

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 the following two methods:

- IMAP -- use an IMAP email client to access the FortiMail unit with the system quarantine account name (without any domain name) and password.
- Administrator Web UI -- create an administrator account with the quarantine access privilege in the access profile and access the web UI using this administrator account.

The system quarantine cannot be accessed through POP3 or webmail.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Quarantine* category.

For details, see "About administrator account permissions and domains" on page 179.

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 Settings	
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.

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 messages 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.

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 *Release account* is `release-ctrl` and the local domain name of the FortiMail unit is `example.com`, an email user could release an email message from their per-recipient quarantine by sending an email to `release-ctrl@example.com`. For more information on releasing and deleting quarantined items through email, see "Releasing and deleting email via quarantine reports" on page 501.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Quarantine* category.

For details, see "About administrator account permissions and domains" on page 179.

To configure the quarantine control settings

1. Go to *Security* > *Quarantine* > *Quarantine Control*.

2. Under *Quarantine Release Re-scan Settings*, 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*.

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 web UI 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 "Configuring the global block and safe list" on page 506, "Configuring the per-domain block lists and safe lists" on page 508, and "Configuring the personal block lists and safe lists" on page 510.
- For per-user block lists and safe lists, you can alternatively go to *Domain & User* > *User* > *User Preferences*. For details, see "Configuring user preferences" on page 329.
- 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 389.

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 504.

All block and safe list entries are automatically sorted into alphabetical order, where wildcard characters (* and ?) and numbers sort before letters.

- Order of execution of block lists and safe lists
- About block list and safe list address formats
- Configuring the global block and safe list
- Configuring the per-domain block lists and safe lists
- Configuring the personal block lists and safe lists
- Configuring the block list action

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 generally take precedence over per-domain lists, while per-domain lists take precedence over per-user lists.

Table 52 displays 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).

Table 52: 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	Domain safe list	Sender address, Client IP	Accept message
4	Domain block list	Sender address, Client IP	Invoke block list action
5	Session recipient safe list	Recipient address	Accept message for matching recipients
6	Session recipient block list	Recipient address	Invoke block list action
7	Session sender safe list	Sender address, Client IP	Accept message for all recipients
8	Session sender 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 message envelope (`MAIL FROM:`) and message header (`From:`)
- 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 389), 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 16.

About block list and safe list address formats

Acceptable input for block and safe list entries may vary by the type of the block or safe list, but may be:

- all or part of an IP address
- all or part of a domain name
- all or part of an email address

Domain name portions (for example, example.com) and user name portions (for example, user1) may use wild cards (? and *).

Table 53: Examples of valid block/safe list entries

Example	Description of match
172.168.1	Email from the IP addresses 172.168.1.0/24
example.com	Email from any sender at example.com, such as user1@example.com.
spammer@example.com	Email from the sender spammer@example.com
?ser1@example.com	Email from any sender name ending in "ser1" at example.com
***@example.com**	Email from any sender at 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

The following formats are ***not*** valid:

- 172.16.1.0
- 172.16.1.0/24
- @spam. example.com

Configuring 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.

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 295.

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.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Block/Safe List* category. For details, see "About administrator account permissions and domains" on page 179.

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, click *Block List*.
   - To allow email by sender, click *Safe List*.

   The dialogs that appear are identical except for the single line of description.
3. In the field to the left of the *Add* button, type the 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 506.
4. Click *Add*.

   The entry appears in the text area.
5. Click the window close button (X) to close the dialog.

To delete an entry from the system-wide block or safe list

1. Go to *Security* > *Block/Safe List* > *System*.
2. Click either *Block List* or *Safe List*.
3. In the text area below the *Add* button, select the entry that you want to remove.
4. Click *Remove Selected*.

To back up the system-wide block or safe list

1. Go to *Security* > *Block/Safe List* > *System*.
2. Click either *Block List* or *Safe List*.
3. Click *Backup*.
4. If your web browser prompts you for a location, select the folder where you want to save the file. The list will be saved as a cvs file.

To restore the system-wide block or safe list

Back up the block list and safe list before beginning this procedure. Restoring the block list and safe list overwrites any existing block or safe list.

1. Go to *Security* > *Block/Safe List* > *System*.
2. Click either *Block List* or *Safe List*.
3. Click *Browse*, locate and select the file that you want to restore, then click *OK*. The list must be a cvs file.
4. Click *Restore*.

Configuring 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 295.

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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Block/Safe List* category. For details, see "About administrator account permissions and domains" on page 179.

To view and edit per-domain block or safe lists

1. Go to *Security* > *Block/Safe List* > *Domain*.

GUI item	Description
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 307.
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. Do one of the following:
   - To block email by sender, in the row corresponding to the protected domain whose block list you want to modify, click either the *New* or *Edit* icon.
   - To allow email by sender, in the row corresponding to the protected domain whose safe list you want to modify, click either the *New* or *Edit* icon.

   The dialogs that appear are identical except for the single line of description.
3. In the field to the left of the *Add* button, type the email address, domain name, or IP address of the sender. For information on valid formats, see "About block list and safe list address formats" on page 506.
4. Click *Add*.

   The entry appears in the text area below the *Add* button.
5. Click the window close button (X) to close the dialog.

To delete an entry from a per-domain block list or safe list

1. Go to *Security* > *Block/Safe List* > *Domain*.
2. In the row corresponding to the protected domain whose block list or safe list you want to modify, click the *List* icon.
3. In the text area below the *Add* button, select the entry that you want to remove.
4. Click *Remove Selected*.

To back up a per-domain block list or safe list

1. Go to *Security* > *Block/Safe List* > *Domain*.
2. In the row corresponding to the protected domain whose block list or safe list you want to back up, click the *List* icon.
3. Click *Backup*.
4. If your web browser prompts you for a location, select the folder where you want to save the file. The list will saved as a cvs file.

To restore a per-domain block list or safe list

Back up the block list and safe list before beginning this procedure. Restoring the block list and safe list overwrites any existing block list or safe list.

1. Go to *Security* > *Block/Safe List* > *Domain*.
2. In the row corresponding to the protected domain whose block list or safe list you want to restore, click the *List* icon.
3. Click *Choose file*, locate and select the file that you want to restore, then click *Open*. The list must be a cvs file.
4. Click *Restore*.

Configuring 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 access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Block/Safe List* category. For details, see "About administrator account permissions and domains" on page 179.

To view and add to personal block lists or safe lists

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. Select the name of the protected domain for the user in Domain. For more information on protected domains, see "Configuring protected domains" on page 307
3. Enter a user name and click the *Search User* icon.

   Two additional options appear: .

GUI item	Description
Add outgoing email addresses to Safe list	Click *On* to automatically add the recipient email addresses of outgoing email messages to this email user's per-user safe list.
Block/Safe lists	Click *Block* to display, modify, back up, or restore the block list for this email user. Click *Safe* to display, modify, back up, or restore the safe list for this email user.

4. To edit a list, do one of the following:
   - To block email by sender, click *Block*.
   - To allow email by sender, click *Safe*.

   The dialogs that appear are identical except for the single line of description.
5. In the field to the left of the *Add* button, type the email address, domain name, or IP address of the sender. For information on valid formats, see "About block list and safe list address formats" on page 506.
6. Click *Add*.

   The entry appears in the text area below the *Add* button.

7. Click the window close button (X) to close the dialog.

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.

To delete an entry from a per-user block list or safe list

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. From *Domain*, select the name of the protected domain to which the email user belongs.
3. In *User name*, type the user name of the email user whose per-user block list or safe list you want to modify.
4. Click the *Search User* icon.

   If the email user exists, options appear allowing you to configure the user's per-user block list and safe list.

   If the email user does not exist, a dialog appears, asking you if you want to create one and proceed. Click *OK*.
5. Click either *Block* or *Safe*.
6. In the text area below the *Add* button, select the entry that you want to remove.
7. Click *Remove Selected*.

To back up a per-user block list or safe list

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. From *Domain*, select the name of the protected domain to which the email user belongs.
3. In *User name*, type the user name of the email user whose per-user block list or safe list you want to back up.
4. Click the *Search User* icon.

   If the email user exists, options appear allowing you to back up the user's per-user block list and safe list.
5. Click either *Block* or *Safe*.
6. Click *Backup*.
7. If your web browser prompts you for a location, select the folder where you want to save the file.

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 295.

To restore a per-user block list or safe list

Back up the block list and safe list before beginning this procedure. Restoring the block list and safe list overwrites any existing block list or safe list.

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. From *Domain*, select the name of the protected domain to which the email user belongs.

3. In *User name*, type the user name of the email user whose per-user block list or safe list you want to restore.
4. Click the *Search User* icon.

   If the email user exists, options appear allowing you to restore the user's per-user block list and safe list.
5. Click either *Block* or *Safe*.
6. Click *Browse*, locate and select the file that you want to restore, then click *OK*.
7. Click *Restore*.

Configuring the block list action

The *Blocklist Action* tab lets you configure the action to take if an email message arrives from a blocklisted domain name, email address, or IP address.

The FortiMail unit will apply this action to email matching system-wide, per-domain, and per-session profile block lists.

For the personal level block lists, the only option is to discard. For more information, see "Configuring the personal block lists and safe lists" on page 510.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Block/Safe List* category. For details, see "About administrator account permissions and domains" on page 179.

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 actions

1. Go to *Security* > *Block/Safe List* > *Blocklist Action*.
2. Select one of the following:
   - 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 actions configured in the antispam profile that you selected in the policy that matches the email message. For more information on actions, see "Configuring antispam action profiles" on page 422.
3. Click *Apply*.

Configuring greylisting

Go to *Security* > *Greylist* to configure greylisting and to view greylist-exempt senders.

This section contains the following topics:

- About greylisting
- Manually exempting senders from greylisting
- Configuring the grey list TTL and initial delay

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.

Figure 41: 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 16.

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 517)
2. consolidated automatic greylist entries, also known as autoexempt entries (see "Automatic greylist entries" on page 516)

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 516 and “Automatic greylist entries” on page 516.

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 148) 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 greylist entries” on page 515. For information on configuring the greylisting delay, window, and entry expiry/TTL, see “Configuring the grey list TTL and initial delay” on page 517.

Matching 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 517.

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 148)
- individual (see "Viewing the pending and individual automatic greylist entries" on page 148)
- consolidated (see "Viewing the consolidated automatic greylist exemptions" on page 150)

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 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 greylist or autoexempt list.

After a greylist entry is consolidated, both the consolidated 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 519.

Configuring the grey list TTL and initial delay

The *Settings* 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 513.

To access this part of the web UI, your administrator account’s:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see “About administrator account permissions and domains” on page 179.

To configure greylisting intervals

1. Go to *Security* > *Greylist* > *Settings*.

2. Configure the following:

GUI item	Description
TTL	Enter the time to live (TTL) that determines the maximum amount of time that unused automatic greylist entries will be retained. Expiration dates of automatic greylist entries are determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings`. The default initial expiry time is 4 hours. If the initial expiry time elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. • TTL: Between the entry's PASSTHROUGH time and initial expiry time, if the entry is hit again (the sender retries to send the message again), the entry's expiry time will be reset by adding the TTL value (time to live) to the message's "Received" time. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. For more information on automatic greylist entries, see "Viewing the greylist statuses" on page 147.
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 148.

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 16.

For more information on the automatic greylisting process, see "About greylisting" on page 513. For more information on manual greylist entries, see "Manual greylist entries" on page 517.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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. • **-/**: 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. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (* or ?).

GUI item	Description
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. • **-/**: 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. For example, entering the pattern `??@*.com` will match messages sent by any sender with a two-letter user name from any ".com" domain.
Regular expression	For any of the pattern options, select the accompanying *Regular expression* check box if you entered a pattern using regular expression syntax.
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, `.*`. 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. For example, entering the pattern `*@example.???` will match email sent to any recipient at example.com, example.net, example.org, or any other "example" top level domain.

GUI item	Description
Sender IP/Netmask	Enter the IP address and netmask that defines SMTP clients that match this entry. To match any SMTP client IP address, enter `0.0.0.0/0`. You can create a pattern that matches multiple addresses by entering any bit mask other than `/32`. For example, entering `10.10.10.10/24` would match the 24-bit subnet of IP addresses starting with 10.10.10, and would appear in the list of manual greylist entries as `10.10.10.0/24`.
Reverse DNS pattern	Enter the pattern that defines valid host names for the IP address of the SMTP client (the last hop address). Since the SMTP client can use a fake self-reported host name in its SMTP greeting (`EHLO/HELO`), you can use a reverse DNS lookup of the SMTP client's IP address to get the real host name of the SMTP client. Then the FortiMail greylist scanner can compare the host name resulting from the reverse DNS query with the pattern that you specify. If the query result matches the specified pattern, the greylist exempt rule will apply, Otherwise, the rule will not apply. You can create a pattern that matches multiple addresses either by: • including wild card characters (* or ?). An asterisk (*) matches one or more characters; a question mark (?) matches any single character. • using regular expressions. You must also enable the *Regular expression* option. For example, entering the pattern `mail*.com` will match messages delivered by an SMTP client whose host name starts with "mail" and ending with ".com".

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.

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.

The manual greylist entries used by Example Corporation are shown in Figure .

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 the URL exempt list

If you want to exempt URLs from FortiGuard URL query (see “Configuring FortiGuard options” on page 411), or FortiSandbox scanning (see “Configuring FortiGuard services” on page 287), you can add the URLs to the exempt list.

To configure the URL exempt list

1. Go to *Security* > *URL Exempt List* > *Exempt.*
2. Click *New*.
3. Enter an exempt pattern. The pattern can use wildcards (default) or regular expressions. For more information about URI types and how they are processed, see “URI types” on page 413.
4. Click *Create*.

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 307)
- 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 307)
- in the session profile, the *Bypass Bounce Verification check* option is disabled (see “Configuring session profiles” on page 389)
- 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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

To configure bounce verification settings

1. Go to *Security* > *Bounce Verification* > *Settings*.
2. Configure the following as required:

GUI item	Description
New, Edit, Delete (buttons)	Click to 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	Displays the string of text that is the private key. This can be any arbitrary string of text, and will be used together with randomizing data to generate each bounce address tag.
Status	Indicates which key is activated for use. • *Active*: The key is activated. • *Inactive*: The key is deactivated. Only one of the keys may be activated at any given time. The activated key is the one that will be used to generate the bounce address tags for outgoing email. Both activated and deactivated keys will be used for bounce address tag verification of incoming email. To activate or deactivate a key, double-click it and modify its *Status*.
Last Used	Displays the date and time when the key was generated or last used to verify the bounce address tag of an incoming email, whichever is later.
Enable bounce verification	Mark this check box to 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 307 and "Configuring session profiles" on page 389.
Bounce verification tag expires in (days)	Enter the number of days after creation when bounce message keys will expire and their resulting tags will fail verification.

GUI item	Description
Keys will be automatically removed	Displays the period of time after which unused, deactivated keys will be automatically removed. The activated key will not be automatically removed.
Bounce verification 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 actions configured in the antispam profile that you selected in the policy that matches the email message. For more information on actions, see "Configuring antispam action profiles" on page 422.

To configure a bounce address tagging and verification key

1. Go to *Security* > *Bounce Verification* > *Settings*.
2. Click *New* to add a key or double-click to a key to modify it.

   A dialog appears:
3. Configure the following:

GUI item	Description
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 tagging 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 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.

This section contains the following topics:

- About endpoint reputation
- Manually blocklisting endpoints
- Exempting endpoints from endpoint reputation
- Configuring the endpoint reputation score window
- Viewing endpoint reputation statuses

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.

Figure 42: 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 389. For information on configuring the automatic blocklisting window, see "Configuring the endpoint reputation score window" on page 531.

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 web UI, go to *Security* > *Endpoint Reputation* and configure the settings described in "Manually blocklisting endpoints" on page 529, "Exempting endpoints from endpoint reputation" on page 530, and "Configuring the endpoint reputation score window" on page 531.
3. Go to *Profile* > *Session* > *Session*. Mark the check box of the "Enable Endpoint Reputation" on page 393 option, then select either *Reject* or *Monitor* from "Action" on page 393. For details, see "Configuring session profiles" on page 389.
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 375.
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 569 and "Viewing log messages" on page 131.

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 154.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

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 *AntiSpam* > *Endpoint Reputation* > *Exempt.*
2. Click the *Search* button.

   A dialog appears.
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 (*) 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 *Settings* 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 389.

For more information on the role of the automatic blocklisting window in the endpoint reputation scan, see "Configuring endpoint reputation" on page 527.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

To configure the automatic endpoint blocklisting window

1. Go to *Security* > *Endpoint Reputation* > *Settings*.
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*.

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* > *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 "Managing antispam profiles" on page 407.

This section contains the following topics:

- Types of Bayesian databases
- Training the Bayesian databases
- Example: Bayesian training
- Backing up, batch training, and monitoring the Bayesian databases
- Configuring the Bayesian training control accounts

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 533.

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 324.

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 324.

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 324.

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 536.

   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 156.

   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 536.

   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 539, "Accept training messages from users" on page 419, and "Training Bayesian databases" on page 612.

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 AS/AV Settings*.
4. Disable the option *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* > *Bayesian* > *Domain*.
2. 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.

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 533.

You can alternatively back up, restore, and reset all Bayesian databases at once. For more information, see "Backup and restore" on page 295.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category.

Domain administrators cannot access the global Bayesian settings.

For details, see "About administrator account permissions and domains" on page 179.

To individually train, view and manage Bayesian databases

1. Go to *Security* > *Bayesian* > *Domain*.
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 324.
   - 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 537
   - "To back up a Bayesian database" on page 537
   - "To restore a Bayesian database" on page 538
   - "To reset a Bayesian database" on page 538

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 156.

1. Go to *Security* > *Bayesian* > *Domain*.
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* > *Bayesian* > *Domain*.
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 537 or "Backup and restore" on page 295.

1. Go to *Security* > *Bayesian* > *Domain*.
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 295.

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 537 or "Backup and restore" on page 295.

1. Go to *Security* > *Bayesian* > *Domain*.
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.

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 the "Accept training messages from users" option is enabled. For more information, see "Accept training messages from users" on page 419.

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. The following factor determines which Bayesian database or databases will be trained:

- whether the sender's protected domain is configured to use the global or per-domain Bayesian database (see "Use global Bayesian database" on page 324)

Depending on those factors, the FortiMail unit uses the training message to train either the global or per-domain Bayesian database.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Policy* category

For details, see "About administrator account permissions and domains" on page 179.

To configure the Bayesian control email addresses, go to *Security* > *Bayesian* > *Control Account*.

GUI item	Description
"is really spam" user name	Enter the user name portion of the email address, such as `is-spam`, to which email users will forward spam false negatives.Forwarding false negatives corrects the Bayesian database when it inaccurately classifies spam as being legitimate email.
"is not really spam" user name	Enter the user name portion of the email address, such as `is-not-spam`, to which email users will forward spam false positives.Forwarding false positives corrects the Bayesian database when it inaccurately classifies legitimate email as being spam.
"learn is spam" user name	Enter the user name portion of the email address, such as `learn-is-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
"learn is not spam" user name	Enter the user name portion of the email address, such as `learn-is-not-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
training group	Enter the user name portion of the email address, such as `default-grp`, that FortiMail administrators can use as their sender email address when forwarding email to the “learn is spam” email address or “learn is not spam” email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain).

Adding file signatures

If you already have the SHA-1/SHA-256(Secure Hash Algorithm) hash values of some known virus-infected files, you can add these values as file signatures and then, in the antivirus profile, enable the actions against these files. See “Configuring antivirus profiles and antivirus action profiles” on page 425.

You can manually add the SHA-1/256 checksums one by one. You can also import such a checksum list in csv or txt format. The signatures can be exported as a csv file.

Because not all attachment files are virus carriers, FortiMail file signature check only supports the following file types: .7z, .bat, .cab, .dll, .doc, .docm, .dotm, exe, .gz, .hta, .inf, .jar, .js, .jse, .msi, .msp, pdf, .pif, .potm, .ppam, .ppsm, .ppt, .pptm, .pptx, .reg, .scr, .sldm, .swf, .tar, .vbe, .ws, .wsc, .wsf, .wsh, .xlam, .xls, .xlsm, .xlsx, .xltm, .Z, and .zip files.

To add a new file signature

1. Go to *Security* > *Other* > *File Signature* and click *New*.
2. Enter a name fo the signature group.
3. Select either SHA-1 or SHA-256.
4. Under *File Signature List*, click *New* and then enter the checksum value.
5. Click *OK* and then *Create*.

To import a signature list in cvs format

1. Go to *Security* > *Other* > *File Signature* and click *Import*.

2. Browse to the cvs file and click *OK*. The cvs file must contain the hash values, and the type must be SHA1 or SHA256.

To export the file signatures

1. Go to *Security* > *Other* > *File Signature* and click *Export*.
2. Click *Save File* to save the file in cvs format to your local machine.

Configuring action profile preferences

When you configure action profiles (see "Configuring antispam action profiles" on page 422, "Configuring antivirus action profiles" on page 427, and "Configuring content action profiles" on page 439), you may use the following actions:

- Deliver to alternate host
- Deliver to original host
- System quarantine
- Personal quarantine

For the above actions, you can choose to deliver or quarantine the original email or the modified email.

- Modified copy means that the email message to be delivered or quarantined is not the original one. It has been modified by the matching FortiMail actions.
- Unmodified copy means that the email message to be delivered or quarantined still contains the original header and body. However, the envelope recipient or RCPT TO might have been rewritten by the relevant action profile.

For example, when the HTML content is converted to text, if you choose to deliver the unmodified copy, the HTML version will be delivered; if you choose to deliver the modified copy, the plain text version will be delivered.

To configure the action profile preferences

1. Go to *Security* > *Other* > *Preference*.
2. Select either *Modified copy* or *Unmodified copy* for each action.
3. If the action in one 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 the option to "enforce delivery action if delivery to original/alternate host is enabled.
4. For spam email that is sent to personal quarantine, you have the option to continue or stop further scanning the email attachments.

Configuring adult image analysis

When you configure a content profile (see "Configuring scan options" on page 432), you can choose to scan for adult images in the email body and attachments.

To configure adult image analysis settings

1. Go to *Security* > *Other* > *Adult Image Analysis*.
2. Enable the analysis.
3. Adjust the rating sensitivity according to your requirements. The higher the number, the higher the sensitivity. The default setting is 75 and the valid range is 0-100.

4. Specify the minimum and maximum image size to scan.

Adjust the rating sensitivity properly to avoid false positives and false negatives.

Enabling this feature affects the FortiMail performance. And by default, this feature is enabled.

Configuring encryption settings

Use the *Encryption* menu to configure IBE encryption settings and certificate binding for S/MIME encryption.

This section includes:

- Configuring IBE encryption
- Configuring certificate bindings

Configuring IBE encryption

The *Encryption* > *IBE* 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 IBE
- About FortiMail IBE
- FortiMail IBE configuration workflow
- Configuring IBE services

About IBE

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 or 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.

What happens is that 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. Figure 44 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. Figure 43 shows how FortiMail IBE works:

Figure 43: How FortiMail works with IBE

Figure 44: Sample secure message notification

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 545.
- Manage IBE users. See "Configuring IBE users" on page 341.
- Configure an IBE encryption profile. See "Configuring encryption profiles" on page 485.

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 439.
- 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 430.
- 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 381, and "Controlling email based on IP addresses" on page 375.

  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 479)
  - 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 MS 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 569.
- View logs of IBE encryption. See "Viewing log messages" on page 131.

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 371.
- Configure IBE email storage.
- Configure log settings for IBE encryption. See "Configuring logging" on page 569.
- View logs of IBE encryption. See "Viewing log messages" on page 131.

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 544.

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.
User 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.
User 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.
Encrypted email storage expiry time (days)	Enter the number of days that the secured mail will be saved on the FortiMail unit.
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.
Allow secure replying	Select to allow the secure mail recipient to reply the email with encryption.
Allow secure forwarding	Select to allow the secure mail recipient to forward the email with encryption.
Allow secure composing	Select to allow the secure mail recipient to compose an email. The FortiMail unit will use policies and mail delivery rules to determine if this mail needs to be encrypted. For encrypted email, the domain of the composed mail's recipient must be a protected one, otherwise an error message will appear and the mail will not be delivered.
IBE base URL	Enter the FortiMail unit URL, for example, https://192.168.100.20, on which a mail recipient can register or authenticate to access the secure mail.
"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.

GUI item	Description
"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.
Notification Settings	You can choose to send 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 226. Depending on the IBE email access method (either PUSH or PULL) you defined in “Configuring encryption profiles” on page 485, 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) as per 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 it has a matching **private key**, it will decrypt the email before delivering it. If it does ***not***, it forwards the still-encrypted email to the recipient.

If you have selected an encryption profile with encryption action in the message delivery rule that applies to the session, the FortiMail unit compares the recipient’s identity with the list of certificate bindings to determine if it has a certificate and **public key**. If it has a matching public key, it will encrypt the email using the algorithm specified in the encryption profile (see “Configuring encryption profiles” on page 485). If it does ***not***, it 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. The 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, the FortiMail unit compares the sender's identity with the list of certificate bindings to determine if it has a certificate and **private key**. If it has a matching private key, it will add a digital signature using the algorithm specified in the encryption profile (see "Configuring encryption profiles" on page 485). If it does ***not***, it performs the failure action indicated in the encryption profile.

The FortiMail unit does ***not*** check if an outgoing email is already encrypted. Email clients can apply their own additional layer of S/MIME encryption if they want to (such as if they require non-repudiation) before they submit email for delivery through the FortiMail unit.

The destination of an S/MIME email can be another FortiMail unit, 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:

- the destination's MTA or mail server
- the recipient's MUA

This is necessary to decrypt the email; otherwise, the recipient cannot read the email.

To access this part of the web UI, your administrator account's access profile must have *Read* or *Read-Write* permission to the *Policy* category. For details, see "About administrator account permissions and domains" on page 179.

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 283.

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.

GUI item	Description
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. From *Type*, select whether the keys and certificate will be used for validating the signature of and decrypting incoming email (*External*), or to sign and encrypt outgoing email (*Internal*).

   Certificate import formats vary by this selection.
4. 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.
5. 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).
6. 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 server certificate that you have previously uploaded to the FortiMail unit. For details, see "Managing local certificates" on page 276.

   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 487, "Configuring encryption profiles" on page 485 and "Configuring delivery rules" on

page 371. It will also be used in the content profile and then in the policies which use the content profile.

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

To use the DLP feature

1. Enable the DLP feature. Be default, this feature is disabled.
```
config system global
  set data-loss-prevention enable
end
```
2. Define the sensitive data first. See “Defining the sensitive data” on page 551.
3. Define the DLP scan rules which specify the information to be checked in the email traffic. See “Configuring DLP rules” on page 553.
4. Define DLP profiles, which use one or more rules. See “Configuring DLP profiles” on page 553. 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 439.
5. Apply the DLP profiles to the IP or recipient based policies. See “Controlling email based on sender and recipient addresses” on page 381 and “Controlling email based on IP addresses” on page 375.

Defining the sensitive data

Sensitive data can be any of the following types:

- User-defined: specify what information should be checked, such as a word, a phrase, or a regular expression.
- 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 552.
- File filters: these are the same file filters you use in the content profiles. See “Configuring file filters” on page 438.

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.

Any type of file 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.

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.

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.
Description	Optionally enter a description.
Server type	This refers to the type of server share that is being accessed. The default is Windows Share 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.

GUI item	Description
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	
Scan 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 chunks	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.
Retain old chunks	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.

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 and Profile* > *Rule*.
2. 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 439). 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 and 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 439.
Comment	Optionally enter a comment.
Content Scan Settings	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.

This section contains the following topics:

- Email archiving workflow
- Configuring email archiving accounts
- Configuring email archiving policies
- Configuring email archiving exemptions

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 555.

   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 621.
2. Create email archive policies or exemption policies to specify the archiving criteria. See "Configuring email archiving policies" on page 559 and "Configuring email archiving exemptions" on page 560. Or, when creating antispam action profiles and content action profiles, choose to archive email as one of the actions. See "Configuring antispam profiles and antispam action profiles" on page 407 and "Configuring content profiles and content action profiles" on page 430.
3. Assign the administrator account access privilege to the email archive. See "Configuring administrator accounts and access profiles" on page 179.
4. You can search or view the archived email as the FortiMail administrator. See "Managing archived email" on page 156. You can also access email archives remotely through IMAP. See "Configuring email archiving accounts" on page 555.
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 558,

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 621.

When email is archived, you can view and manage the archived email messages. For more information, see "Managing archived email" on page 156. You can also access the email archive remotely through IMAP.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

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"
   - "Configuring rotation settings"
   - "Configuring destination settings"

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 555. For information about how to use the email archiving feature, see "Email archiving workflow" on page 555.

1. Go to *Email Archiving* > *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. Also enable *IMAP access* .
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 555. For information about how to use the email archiving feature, see "Email archiving workflow" on page 555.

1. Go to *Email Archiving* > *Archive Account*.
2. Click *New* to create a new account or double click on an existing account to edit it.
3. Under *Rotation Settings*, 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 options 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 576.

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 555. For information about how to use the email archiving feature, see "Email archiving workflow" on page 555.

1. Go to *Email Archiving* > *Archive Account*.
2. Click *New* to create a new account or double click on an existing account to edit it.
3. Under *Destination Settings,* 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. 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, the local data cache cannot exceed 80% of the total mail partition either. The 95% disk usage rule applies.

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 the journaled email 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 configurations.

To archive the journaled email from an Exchange Server

1. Add a journaling source (that is, the Exchange Server). See the below procedures.
2. Create an archive account for the journaled email. See "Configuring email archiving accounts" on page 555.
3. Create a archive policy to specify what email should be archived. See "Configuring email archiving policies" on page 559.

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
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.

GUI item	Description
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 that this is not the recipient address in the email messages being archived.
Comments	Optionally enter a comment.

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 560).

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and configure archiving policy

1. Go to *Email Archiving* > *Policy* > *Archive Policy*.

GUI item	Description
Clone (button)	Click the row corresponding to the policy 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 policy. Click *OK*.
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.
Account (drop-down list)	Select *All* to see policy for every account on the FortiMail unit, or select an account name to see policy for that account. See "Configuring email archiving accounts" on page 555.
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 4.
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* drop-down 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 555.

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.

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*.

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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and configure archiving exemptions

1. Go to *Email Archiving* > *Policy* > *Exempt Policy*.

GUI item	Description
Clone (button)	Click the row corresponding to the policy 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 policy. Click *OK*.
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.
Account (drop-down list)	Select *All* to see policy for every account on the FortiMail unit, or select an account name to see policy for that account. See "Configuring email archiving accounts" on page 555.
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 4 of "Click New to add an entry or double-click an entry to modify it." on page 561.
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* drop-down 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 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 (*) wildcard when specifying a partial address.
   - *Spam emails*: 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
- Configuring logging
- Configuring report profiles and generating reports
- Configuring alert email
- Viewing generated reports

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 565.

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 569. It can also use log messages as the basis for reports. For more information, see "Configuring report profiles and generating reports" on page 572.

Accessing FortiMail log messages

There are several ways you can access FortiMail log messages:

- On the FortiMail web UI, you can view log messages by going to *Monitor* > *Log*.
- On the FortiMail web UI, under *Monitor* > *Log*, you can download log messages to your local PC and view them later.
- You can send log messages to a FortiAnalyzer unit by going to *Log and Report* > *Log Settings* > *Remote* and view them on FortiAnalyzer.
- You can send log messages to any Syslog server by going to *Log and Report* > *Log Settings* > *Remote*.

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.***

Figure 45: 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=event 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 web UI or download them to your local PC, 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

Starting from v5.0 release, two new fields -- policy ID and domain -- have been added 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

Starting from 4.0 MR3, a field called `endpoint` was added 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

For FortiMail 3.0 MR3 and up, 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 web UI 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 web UI to your PC 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 565.

FortiMail log types

FortiMail units can record the following types of log messages. The Event log also contains several subtypes. You can view and download these logs from the *Log* submenu of the *Monitor* tab.

Table 54: Log types

Log type	Subtype	Description
system	config admin system update ha	Includes system and administration events, such as downloading a backup copy of the configuration.
mail	pop3 imap smtp webmail	Includes all the mail activities.
virus	fortisandbox malware-outbreak file-signature infected	Includes detections of viruses, as well as antivirus subsystem-related events.
spam	spam	Includes detections of spam, as well as antispam subsystem-related events, such as when the FortiMail unit loads new FortiGuard Antispam heuristic rules.
statistics (history)	(no subtype)	Includes all email handled by the FortiMail unit's build-in MTA or proxies, no matter the email that was successfully or unsuccessfully delivered.
encrypt	(no subtype)	Includes detection of IBE-related events. For more information about IBE, see "Configuring IBE encryption" on page 543.

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.

Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `pri=warning`.

Table 55: Log severity levels

Levels	Description
0 - Emergency	Indicates the system has become unusable.
1 - Alert	Indicates immediate action is required.
2 - Critical	Indicates functionality is affected.
3 - Error	Indicates an error condition exists and functionality could be affected.
4 - Warning	Indicates functionality could be affected.
5 - Notification	Provides information about normal events.
6 - Information	Provides general information about system operations.

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 web UI 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 web UI to your PC and open them, the dispositions and classifiers are displayed in hex numbers.

The following tables map the hex numbers with English terms.

Table 56: Classifiers

Hex number	Classifier	Hex Number	Classifier
0x00	Undefined	0x21	Domain Safe
0x01	User Safe	0x22	Domain Block
0x02	User Block	0x23	SPF
0x03	System Safe	0x24	Domain Key
0x04	System Block	0x25	DKIM
0x05	DNSBL	0x26	Recipient Verification
0x06	SURBL	0x27	Bounce Verification
0x07	FortiGuard AntiSpam	0x28	Endpoint Reputation
0x08	FortiGuard AntiSpam-Safe	0x29	TLS Enforcement
0x09	Bayesian	0x2A	Message Cryptography
0x0A	Heuristic	0x2B	Delivery Control
0x0B	Dictionary Filter	0x2C	Encrypted Content
0x0C	Banned Word	0x2D	SPF Failure as Spam
0x0D	Deep Header	0x2E	Fragmented email
0x0E	Forged IP	0x2F	Email contains image
0x0F	Quarantine Control	0x30	Content Requires Encryption
0x10	Virus as Spam (before v4.3 release)	0x31	FortiGuard AntiSpam-IP
0x11	Attachment Filter (see note above)	0x32	Session Remote
0x12	Grey List	0x33	FortiGuard Phishing
0x13	Bypass Scan On Auth	0x34	AntiVirus
0x14	Disclaimer	0x35	Sender Address Rate Control
0x15	Defer Delivery	0x36	SMTP Auth Failure
0x16	Session Domain	0x37	Access Control List Reject
0x17	Session Limits	0x38	Access Control List Discard
0x18	Session Safe	0x39	Access Control List Bypass
0x19	Session Block	0x3a	FortiGuard Antispam Webfilter
0x1A	Content Monitor and Filter	0x3b	Newsletter Suspicious
0x1B	Content Monitor as Spam	0x3c	TLS Streaming
0x1C	Attachment as Spam	0x3d	Policy Match

0x1D	Image Spam	0x3e	Dynamic Safe List
0x1E	Sender Reputation	0x3f	Sender Verification
0x1F	Access Control List Relay Denied	0x40	Behavior Analysis
0x20	Safelist Word	0x41	File Signature

When the classifier is “Attachment Filter”, a new field “atype” (attachment type) is also displayed. This field is for debug purpose only.

Table 57: Dispositions

Hex number	**Disposition**	**Hex Number**	**Disposition**
0x00	Accept	0x1000	Disclaimer Header
0x01	Accept	0x2000	Defer
0x04	Reject	0x4000	Quarantine to Review
0x08	Add Header	0x8000	Content Filter as Spam
0x10	Modify Subject	0x10000	Encrypt
0x20	Quarantine	0x20000	Decrypt
0x40	Accept	0x40000	Alternate Host
0x80	Discard	0x80000	BCC
0x100	Replace	0x100000	Archive
0x200	Delay	0x200000	Customized repackage
0x400	Rewrite	0x400000	Repackage
0x800	Disclaimer Body	0x800000	Notification

The disposition field in a log message may contain one or more dispositions/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.

Configuring logging

The *Log Settings* submenu includes two tabs, *Local* and *Remote*, that let you:

- 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 at both locations.

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 565.

For information on viewing locally stored log messages, see "Viewing log messages" on page 131.

Configuring 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 131.

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 185.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure logging to the local hard disk

1. Go to *Log and Report* > *Log Settings* > *Local*.
2. Select the *Enable* option to allow logging to the local hard disk.
3. In *Log file size*, enter the file size limit of the current log file in megabytes (MB).
4. In *Log time*, enter the time (in days) of file age limit. Valid range is between 1 and 365 days.
5. In *At hour*, enter the hour of the day (24-hour format) when the file rotation should start.

   When a log file reaches either the age or size limit, the FortiMail unit rotates the current log file: that is, 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 23 o'clock of the 10th day.

Large log files may decrease display and search performance.

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.

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.

For information about severity levels, see "Log message severity levels" on page 565.

7. For *Log retention period*, specify how long (in days) the logs will be kept. Valid range is 0 to 1461 days. 0 means no limit.
8. From *Log options when disk is full*, select what the FortiMail unit will do when the local disk is full and a new log message is caused, either:
   - *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 message.
9. In *Logging Policy Configuration*, enable the types of logs that you want to record to this storage location. Click the arrow to review the options.
10. Click *Apply*.

Configuring 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 621.

Logs stored remotely cannot be viewed from the web UI of the FortiMail unit. If you require the ability to view logs from the web UI, also enable local storage. For details, see "Configuring logging to the hard disk" on page 569.

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 185.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log and Report* > *Log Settings* > *Remote*.

2. Click *New* to create a new entry or double-click an existing entry to modify it.

   A dialog appears.

3. Select *Enable* to allow logging to a remote host.
4. In *Profile name*, enter a profile name.
5. In *IP*, enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiMail unit will store the logs.
6. In *Port*, if the remote host is a FortiAnalyzer unit, enter 514; if the remote host is a Syslog server, enter the UDP port number on which the Syslog server listens for connections (by default, UDP 514).
7. From *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 565.

8. From *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.

9. Enable *CSV format* if you want to send log messages in comma-separated value (CSV) format.

Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.

10. From *Log protocol*, select *Syslog* if you want send logs to a Syslog server (including FortiAnalyzer). Select *OFTPS* if you want to use this secure protocol to send logs to FortiAnalyzer. Also specify the Hash algorithm for OFTPS. Note that FortiAnalyzer supports both Syslog and OFTPS.
11. If you enabled advanced MTA control (see "Configuring advanced MTA control settings" on page 404), the *Matched session only* option appears. Select this option if you want to send only the matched session logs to the remote server. Otherwise, all logs will be sent.
12. In *Logging Policy Configuration*, enable the types of logs you want to record to this storage location. Click the arrow to review the options.
13. Click *Create*.
14. 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*.
15. 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 web UI 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 163 and "About the management IP" on page 161) and static routes (see "Configuring static routes" on page 173), 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*.

Configuring report profiles and generating reports

The *Log and Report* > *Report Settings* > *Configuration* tab displays a list of report profiles.

A report profile is a group of settings that contains the report name, its subject matter, its schedule, and other aspects that the FortiMail unit considers when generating reports from log data. The FortiMail unit presents the information in tabular and graphical format.

You can create one report profile for each type of report that you will generate on demand or on a schedule.

Generating reports can be resource intensive. To avoid email processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see "Configuring the report schedule" on page 574.

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To view and configure report profiles

1. Go to *Log and Report* > *Report Settings* > *Configuration*.

GUI item	*Description*
Generate (button)	Select a report and click this button to generate a report immediately. See "Generating a report manually" on page 575.
Report Name	Displays the name of the report profiles.
Domain	Displays the name of the protected domain that is the source of the report.
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.

2. Click *New* to add a profile or double-click a profile to modify it.

   A multisection dialog appears.

3. In *Report Name*, enter a name for the report profile.

   Report names cannot include spaces.

4. Expand your desired option and configure the following as needed:
   - "Configuring the report time period" on page 573.
   - "Configuring the report query selection" on page 573.
   - "Configuring the report schedule" on page 574.
   - "Selecting the protected domains to report" on page 575.
   - "Configuring report conditions" on page 575.
   - "Configuring report email notification" on page 575.
5. Click *Create* or *OK*.

Configuring the report time period

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

When configuring a report profile, you can select the time span of log messages from which to generate the report.

1. Select the arrow next to *Time Period* to expand the section, if closed.
2. Select the time span option you want. This sets the range of log data to include in the report.
   - If you select "User Defined" or "The Last N hours", another field appears that requires more inform ai ton.

Configuring the report query selection

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

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, you might 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, you might expand the query group *Virus by Sender* and select only the individual query *Top Virus Sender By Date*.

GUI item	*Description*
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*.

GUI item	Description
Spam by Recipient	Select to include information on spam by each recipient, such as *Top Spam Recipient By Date*.
Spam by Sender	Select to include information on spam by each sender, such as *Top Spam Sender By Date*.
Statistics	Select to include information on generalized email message statistics (less granular than *Mail Statistics*).
Total Summary	Select to include summary information, such as *Total Sent And Received*.
Virus by Sender	Select to include information on infected email messages by each sender, such as *Top Virus Sender By Date*.
Virus by Recipient	Select to include information on infected email messages by each recipient, such as *Top Virus Recipient By Date*.

Configuring the report schedule

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

When configuring a report profile, you can select when the report will generate. Or, you can leave it unscheduled and generate it on demand. See "Generating a report manually" on page 575.

Generating reports can be resource-intensive. To improve performance, generate reports during times when traffic volume is low, such as at night or during weekends.

Selecting the Schedule dropdown menu reveals the following options:

GUI item	Description
Not Scheduled	Select if you do ***not*** want the FortiMail unit to generate the report automatically according to a schedule. If you select this option, the report can only be generated on demand. See "Generating a report manually" on page 575.
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 first and 30th day of every month, enter `1,30`. Also configure *At hour*.

Selecting the protected domains to report

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

When configuring a report profile, you must specify at least one protected domains whose log messages are used when generating the report. You can select more than one domain.

1. Select *All domains* to disable it and reveal the available and selected domains sections.
2. In the *Available domains* area, select one or more domains that you want to include in the report and select the right arrows to move the domain to the *Selected domains* area.
3. To remove a domain from a report, select it in the *Selected domains* area and select the left arrows.

Configuring report conditions

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

When configuring a report profile, you can choose to report only on logged email messages matching the directionality that you select: incoming, outgoing, or both. You can also choose to report on logged email messages destined to certain IP addresses or IP group.

Configuring report email notification

This is part of the procedures for report generation. For information about the entire procedures, see "Configuring report profiles and generating reports" on page 572.

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. In *Report format*, select the format of the generated attachment, either *html* or *pdf*.
2. In the *Email address* field, enter the email address of a recipient. Click -> to add the email address to the list of recipients.
3. The *All notification Email address* text box displays the list of recipients to whom the FortiMail unit will send a copy of reports generated using this report profile. To remove a recipient address, select it and click <-.

Generating a report manually

You can always generate a report on demand whether the report profile includes a schedule or not.

To manually generate a report

1. Go to *Log and Report* > *Report Settings* > *Configuration*.
2. Click to select the report profile whose settings you want to use when generating the report.
3. Click *Generate*.

The FortiMail unit immediately begins to generate a report. To view the resulting report, see "Viewing generated reports" on page 158.

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 576) and which event categories will trigger an alert email message (see "Configuring alert categories" on page 576).

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 174.

- 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 access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To configure recipients of alert email messages

1. Go to *Log and 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.

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 576).

To access this part of the web UI, your administrator account's:

- *Domain* must be *System*
- access profile must have *Read* or *Read-Write* permission to the *Others* category

For details, see "About administrator account permissions and domains" on page 179.

To select events that will trigger an alert email message

1. Go to *Log and 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 555.
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 in HA" on page 243.
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 557.
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.

Installing firmware

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 packages.

New firmware can also introduce new features which you must configure for the first time.

For information specific to the firmware release version, see the Release Notes available with that release.

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
- Installing firmware
- Clean installing firmware
- Upgrading firmware on HA units

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.
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 3 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 580.
    - 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.

Installing firmware

You can use either the web UI or the CLI to upgrade or downgrade the firmware of the FortiMail unit.

Administrators whose *Domain* is *System* and whose access profile contains *Read-Write* access in the *Others* category, such as the `admin` administrator, can change the FortiMail firmware.

Firmware changes are either:

- an upgrade to a newer version
- a reversion 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.

When upgrading, there may also be additional considerations. For details, see "Upgrading the firmware" on page 585.

Therefore, no matter you are upgrading or downgrading, it is always a good practice to back up the configuration and mail data.

To install firmware using the web UI

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 web UI as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. In the advanced mode of the web UI, 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 web UI and correctly displays all changes.
6. To verify that the firmware was successfully installed, log in to the web UI 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 web UI, clear the cache of your web browser and restart it to ensure that it reloads the web UI 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 582 and "Restoring the configuration" on page 583.

    If you have upgraded the firmware version, to verify the conversion of the configuration file, see "Verifying the configuration" on page 584. 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.

14. After upgrading to FortiMail v3.0 from any older version, create new LDAP profiles. LDAP profiles cannot be automatically converted from the FortiMail v3.0 configuration format. For details, see "Configuring LDAP profiles" on page 450.

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 web UI 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 web UI.

If your FortiMail unit has not been reset to its default configuration, but you cannot connect to the web UI 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 585.

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 4 to 6 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 web UI or CLI through that network interface using. For information on restoring the configuration, see "Restoring the configuration" on page 583.

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 web UI or CLI through that network interface. For information on restoring the configuration, see "Restoring the configuration" on page 583.

Restoring the configuration

You can restore a backup copy of the configuration file from your local PC using either the web UI 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.

To restore the configuration file using the web UI

1. Clear your browser's cache. If your browser is currently displaying the web UI, also refresh the page.

2. Log in to the web UI.
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 584.

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 web UI.

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 584.

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 web UI 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.

Upgrading the firmware

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.

Clean installing firmware

Clean installing the firmware can be useful if:

- you are unable to connect to the FortiMail unit using the web-based manager or the CLI
- you want to install firmware ***without*** preserving any existing configuration
- 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 582.

If you are reverting to a previous FortiMail version (for example, reverting from v3.0 to v2.80), 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 3 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 web UI 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 583.

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.

Upgrading firmware on HA units

If you are installing or upgrading firmware to a high availability (HA) group, install firmware on the slave unit/units before installing firmware on the master unit.

Similar to upgrading the firmware of a standalone FortiMail unit, normal email processing is temporarily interrupted while firmware is being installed on the master unit, but, if the HA group is active-passive, it is ***not*** interrupted while firmware is being installed on slave units.

Installing firmware on an active-passive HA group does not necessarily trigger a failover. Before a firmware installation, the master unit signals the slave unit that a firmware upgrade is taking place. This causes the HA daemon operating on the slave unit to pause its monitoring of the master unit for a short time. When the firmware installation is complete, the master unit signals the slave unit to resume HA heartbeat monitoring. If the slave unit has not received this signal after a few minutes, the slave unit resumes HA heartbeat monitoring anyway, and, if the master unit has failed during the firmware installation, the HA group fails over to the slave unit, which becomes the new master unit.

To upgrade firmware on an active-passive HA pair

1. Back up configuration on both the master and slave units by going to *System* > *Maintenance* > *Configuration*.

2. Upgrade the firmware on the slave unit according to the upgrade path specified in the release notes.

   The reboot event of the slave unit will be logged in the master unit's HA logs. For details, see "Failover scenario 3: System reboot or reload of the secondary unit" on page 263.

3. Upgrade the firmware on the master unit.

   The master unit will send a holdoff command to the slave unit so that the slave unit will not take over the master role during the master unit's reboot. For details, see "Failover scenario 2: System reboot or reload of the primary unit" on page 262.

   Optionally, you can manually force a failover to the slave unit before upgrading the master unit. But this will cause some unnecessary data synchronization. Therefore, it is recommended to upgrade the master unit directly during your maintenance window.

4. Verify the traffic flow on the master unit.

To upgrade firmware on a config-only HA cluster

1. Back up configuration on each unit.
2. Upgrade the firmware on the config-slave unit one by one according to the upgrade path specified in the release notes.
3. Lastly, upgrade the firmware on the config-master 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:

- System security tuning
- Network topology tuning
- High availability (HA) tuning
- SMTP connectivity tuning
- Antispam tuning
- Policy tuning
- System maintenance tips
- Performance tuning

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.
- Avoid generic administrator account names such as “admin”. If an attacker can guess your admin name they will only need to determine your password.
- 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 web-based manager 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.

Figure 46: Administrator security

- 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 config-only HA group consisting of only two FortiMail units, directly connect the HA interfaces using a crossover cable. For a config-only 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 config-only HA if you want to create a mail server farm for a large organization. You can also install a FortiMail config-only HA group behind a load balancer. The load balancer can balance the mail processing load to all FortiMail units in the config-only 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 236.
- 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 v1/v2c*. Syslog output can be configured in *Log and Report* > *Log Settings* > *Remote*. Email alerts can be configured in *Log and 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 Settings* > *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 Settings* > *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 Settings* > *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.

Antispam tuning

- ***If the spam catch rate is low, see "Troubleshoot antispam issues" on page 605 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 one 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 checking* 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* > *Settings*) 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* > *Settings*). 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 both scheduled and push 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* > *License*.
- 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 and Report* > *Log Settings* > *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*).
- If possible, format the mail and log disks regularly to improve disk performance.

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 web UI. Each troubleshooting item describes both the problem and the solution.

Some CLI commands provide troubleshooting information not available through the web UI. The web UI 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 589.

This section contains the following topics:

- Establish a system baseline
- Define the problem
- Search for a known solution
- Create a troubleshooting plan
- Gather system information
- Troubleshoot hardware issues
- Troubleshoot GUI and CLI connection issues
- Troubleshoot FortiGuard connection issues
- Troubleshoot MTA issues
- Troubleshoot antispam issues
- Troubleshoot HA issues
- Troubleshoot resource issues
- Troubleshoot bootup issues
- Troubleshoot installation issues
- Contact Fortinet customer support for assistance

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 forgot 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 web UI'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 web UI, go to *Monitor* to view the system information and all other mail delivery information. For details, see “Monitoring the system” on page 131.

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 65 535 ports available for each of the 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 appliances on your network. See the Fortinet Knowledge Base article, "Traffic Types and TCP/UDP Ports used by Fortinet Products" at:

http://kb.fortinet.com

Many UDP and TCP port numbers have internationally recognized ANA port assignments and are commonly associated with specific applications or protocols.

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 230).

Troubleshoot GUI and CLI connection issues

Problem

An administrator account can connect to the advanced mode of the web UI, 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 24.

If you require the ability to restrict the account to specific areas of the GUI, consider using access profiles instead. For details, see “Configuring admin profiles” on page 184.

Problem

Administrators cannot log in to the web UI or the CLI.

Solution

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. Logon 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 web UI 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.

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 satisfy the following requirements:

- Register your FortiMail unit with the Fortinet Technical Support web site, https://support.fortinet.com/.
- Obtain 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, including those operating in high availability (HA), you must obtain separate contracts for each FortiMail unit. 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 174.
- 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 173.

You can verify that you have satisfied DNS and routing requirements by using the following CLI commands.

To check DNS resolution of the FortiGuard antispam service, use:

```
execute nslookup name service.fortiguard.net
```

To check DNS resolution of the FortiGuard antivirus service, use:

```
execute nslookup name fds1.fortinet.com
```

To check network connectivity, use:

```
execute traceroute <address_ipv4>
```

where `<address_ipv4>` is one of the FortiGuard servers.

If you have satisfied these requirements, verify that you have also satisfied the requirements specific to the type of connection that is failing, listed in Table 58.

Table 58: FortiGuard connectivity requirements

scheduled updates (FortiGuard Antivirus/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 185. • 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.
push updates (FortiGuard Antivirus)	• Satisfy all requirements for scheduled updates (above). • If there is a NAT device installed between the FortiMail unit and the FDN, you must configure it to forward push traffic (UDP port 9443) to the FortiMail unit. You must also configure "Use override push IP".
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 rules" on page 363).
- For outgoing connections, relay will be allowed only if explicitly granted by authentication (see "Controlling email based on IP addresses" on page 375) or by the access control list (see "Configuring access control rules" on page 363). 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 4 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 URI that redirects to another URI, the FortiMail unit is able to send a request to the shortened URI to get the redirected URI 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 URI.

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 523).
2. Next, disable both the *Bypass bounce verification* option (see "Configuring protected domains" on page 307) and the *Bypass bounce verification chec*k option (see "Configuring session profiles" on page 389).
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 523.

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 555) 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 system option 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 backup 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 (master) without affecting the HA heartbeat.

To cause failover when an individual service fails, configure service monitoring (see "Configuring service-based failover" on page 258) on both the primary unit and backup unit.

Problem

Mail queues do not appear on the HA backup unit.

Solution

In order to display queue content in the backup 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 backup unit or the 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 web UI, 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.

- A. Do you see the boot options menu
- B. Do you have problems with the console text
- C. Do you have visible power problems
- D. You have a suspected defective FortiMail unit

A. 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 C. Do you have visible power problems.

B. Do you have problems with the console text

1. Do you see any console messages?
   - If no, go to C. 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 D. 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 D. 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 D. You have a suspected defective FortiMail unit.

C. 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 D. You have a suspected defective FortiMail unit.
   - If yes, try replacing the power adapter.
3. Is the power supply defective?
   - If no, go to D. You have a suspected defective FortiMail unit.
   - If yes, replace the power supply and begin the tests again at A. Do you see the boot options menu.

D. 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 114.

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.

This section includes:

- Training Bayesian databases
- Managing tagged spam
- Accessing the personal quarantine and webmail
- Sending email from an email client (gateway and transparent mode)

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.

Administrators can provide initial training. For details, see "Training the Bayesian databases" on page 533. If you have enabled it (see "Configuring the Bayesian training control accounts" on page 539 and "Accept training messages from users" on page 419), 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 antispam 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 action profiles" on page 422.

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 495, "Configuring protected domains" on page 307, and "Using quarantine reports" on page 615). 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 381 and "Configuring authentication profiles" on page 446.

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 informs email users of the IP address and POP3/IMAPv4 port number of the FortiMail unit, 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 action profiles" on page 422) 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 495)
- the quarantine control email addresses (see "Configuring the quarantine control options" on page 503)

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.

Figure 47: 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.

Table 59: Sample quarantine report in plain text format

```
To:      user1@example.com
From:    release-ctrl@fm3.example.com
Subject: Quarantine Summary: [3 message(s) quarantined from Wed, 11
Jul 2007 11:00:01 to Wed, 11 Jul 2007 12:00:01]
Date:    Wed, 11 Jul 2007 12:00:01 -0400


Date:       Wed, 11 Jul 2007 11:11:25
Subject:    Sign up for FREE offers!!!
From:       "Spam Sender" <spamsender@example.org>
Message-Id: 1184166681.l6BFAj510009380000@fm3.example.com


Date:       Wed, 11 Jul 2007 11:14:16
Subject:    Buy cheap stuff!
From:       "Spam Sender" <spamsender@example.org>
Message-Id: 1184166854.l6BFDchG0009440000@fm3.example.com


Date:       Wed, 11 Jul 2007 11:15:46
Subject:    Why pay more?
From:       "Spam Sender" <spamsender@example.org>
Message-Id: 1184166944.l6BFF7HI0009460000@fm3.example.com


Actions:


o) Release a message:
Send an email to <release-ctrl@fm3.example.com> with subject line set
to "user1@example.com:Message-Id".


o) Delete a message:
Send an email to <delete-ctrl@fm3.example.com> with subject line set
to "user1@example.com:Message-Id".


o) Delete all messages:
Send an email to <delete-ctrl@fm3.example.com> with subject line set
to
"delete_all:user1@example.com:ea809095:ac146004:05737c7c111d68d0111d6
8d0111d68d0".
```

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 rules” on page 363.
- Create an authentication profile to authenticate the users. For details, see “Configuring authentication profiles” on page 446.
- Enable SMTP authentication in the incoming recipient-based policy. For details, see “Controlling email based on sender and recipient addresses” on page 381.

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 Extentsion (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) **Note**: 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 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, inlcuding the VM versions, has hard-coded maximum values for various features and functionalities. As such, they may not be practical limits for every situation and are not a promise of performance.

Starting from 5.2.0, a new mechanism (warning limit/soft limit and hard limit) was introduced to the following three settings: number of protected domains, number of domain associations, and number of mailboxes/mail users in server mode. When the warning limit is reached, FortiMail will display a warning message; when the hard limit is reached, FortiMail will not allow you to add more.

Starting from 6.0.0, the warning/soft limit is removed.

To view the maximum values of all FortiMail models, see the FortiMail Maximum Values document on docs.fortinet.com.

Appendix C: Port Numbers

By default, FortiMail opens many outbound ports and listening ports to communicate with other devices.

For a detailed list of open ports, see the Fortinet Communication Ports and Protocols on http://docs.fortinet.com.

Appendix D: Regular expressions

Some FortiMail features support the use of wild card 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 wild cards

A wild card character is a special character that represents one or more other characters. The most commonly used wild card characters are the asterisk (*), which typically represents zero or more characters, and the question mark (?), which typically represents any one character.

In Perl-style regular expressions, the period (`.`) character refers to any single character. It is similar to the question mark (?) character in wild card match pattern. As a result, example.com not only matches example.com but also exampleacom, examplebcom, exampleccom, and so forth.

To match a special character such as "`.`" and "`*`" use the backslash (`\`)escape character. For example, to match example.com, the regular expression should be: `example\.com`

In Perl regular expressions, an asterisk (*) matches the character before it 0 or more times, not 0 or more times of any character. For example, `example*.com` matches `exampleeeeee.com` but does ***not*** match `example.com`.

To match any character 0 or more times, use "`.*`" where "`.`" means any character and the "`*`" means 0 or more times. For example, the wild card match pattern `exampl*.com` should therefore be `exampl.*\.com`.

Case sensitivity

Regular expression pattern matching in FortiMail is case ***in***sensitive. For example, `bad language` blocks `bad language`, `Bad LAnguaGe`, etc.Therefore, the regular expression `/i`, which may be used to make a word or phrase case insensitive in other products, should not be used in the FortiMail configuration.

Modifiers

FortiMail supports the following match operator modifiers:

`/m`	Treat the string as multiple lines. For example, `m/^b.*.d.w.o.r.d$/m` will match the string spread into multiple lines.
`/s`	Treat the string as a single line.
`/x`	Ignore the white spaces in the expression. For example, `m/a b c/x` will also match `abc`.

Word boundary

In Perl-style regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression `test` not only matches the word “test” but also any word that contains “test”, such as attest”, “mytest”, “testimony”, “atestb”. The notation `\b` specifies the word boundary. To match exactly the word “test”, the expression should be `\btest\b`.

Syntax

Table 60 lists some example regular expressions, and describes matches for each expression. Regular expressions on FortiMail units use Perl-style syntax.

Table 60: Regular expression syntax

Expression	Matches
`abc`	`abc` (the exact character sequence, but 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
`ab{2,4}c`	`a` followed by two, three or four `b` characters, followed by `c`
`ab{2,}c`	`a` followed by at least two “b”s followed by a “c”
`ab*c`	`a` followed by any number (zero or more) of “b”s followed by a “c”
`ab+c`	`a` followed by one or more b's followed by a c
`ab?c`	`a` followed by an optional “b” followed by a” c”; that is, either “abc” or “ac”
`a.c`	`a` followed by any single character (not newline) followed by a “c”
`a\.c`	`a.c`
`[abc]`	Any one of `a`, `b` or `c`
`[Aa]bc`	Either `Abc` or `abc`
`[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}`
`\w+`	A word (a non-empty sequence of alphanumeric characters and underscores), such as `foo`, `12bar8`, or `foo_1`
`100\s*mk`	`100` and `mk` separated by zero or more white space characters (spaces, tabs, newlines)
`abc\b`	`abc` when followed by a word boundary (for example, `abc!` but ***not*** `abcd`)

Table 60: Regular expression syntax (continued)

`start\B`	`start` when ***not*** followed by a word boundary (for example, `starting` but ***not*** `start time`)
`\x`	Ignores white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into (slightly) more readable parts.
`/x`	Used to add regular expressions within other text. If the first character in a pattern is forward slash (`/`), the `/` is treated as the delimiter. The pattern must contain a second `/`. The pattern between `/` will be taken as a regular expression, and anything after the second `/` will be parsed as a list of regular expression options (`i`, `x`, etc). An error occurs If the second `/` is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Examples

To block any word in a phrase

```
/block|any|word/
```

To block purposefully misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
^.*v.*i.*a.*g.*r.*o.*$
cr[eéèêë][\+\-\*=<>\.\,;!\?%&§@\^°\$£€\{\}()\[\]\|\\_01]dit
```

To block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

```
try it for free
student loans
you’re already a

pproved
special[\+\-\*=<>\.\,;!\?%&~#§@\^°\$£€\{\}()\[\]\|\\_1]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
- How TLS/SSL works
- FortiMail support of TLS/SSL
- Troubleshooting FortiMail TLS issues

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:

Figure 48: 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 two mail flow directions

This section explains FortiMail TLS behavior in mail receiving and delivering.

- 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 Settings* > *Mail Server Settings*.

- If you uncheck 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 first 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 four choices that you need to understand to configure this feature.

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.
Encrypt	Enforces TLS encryption. Failure of server certificate validation will not fail the delivery of the email in encryption. In other words, this option only cares about the encryption of the message.
Secure	Enforces both TLS encryption and certificate validation. Failure of server certificate validation will fail mail delivery.

The *Action on failure* option has two choices: *Temporarily Fail* and *Fail*.

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` have to 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 fail the validation of the certificate.

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*.

From now on, all emails 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 emails 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
- Useful tools

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.

smtp	to=<bjia@feqa.com>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=36367, relay=feqa.com. [172.20.140.190], dsn=2.0.0, stat=Sent (<201004140545.o3E5j0O1023543@localhost
smtp	STARTTLS=client, cert-subject=/CN=Exchange 2003-new, cert-issuer=/DC=com/DC=feqa/CN=FEQAROOT, verifymsg=unable to get local issuer certificate
smtp	STARTTLS=client, relay=feqa.com., version=TLSv1, verify=CAFAIL, cipher=RC4-SHA, bits=128/128

To fix this issue

1. Do one of the following:
   - 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 631.

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 Openssl tool output:

Figure 49: Sample Openssl tool output

```
yongsun@yongsun-linux:~$ openssl s_client -connect 172.20.140.138:25 -starttls smtp -showcerts
CONNECTED(00000003)
depth=1 /DC=ca/DC=sy/CN=myca
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=CA/ST=ON/L=Ottawa/O=Foobar Inc/OU=IT/CN=172.20.140.138/emailAddress=support@foobar.com
   i:/DC=ca/DC=sy/CN=myca
-----BEGIN CERTIFICATE-----
MIIFfDCCBGSgAwIBAgIKQkWjtgAAAAAAMzANBgkqhkiG9w0BAQUFADA3MRIwEAYK
CZImiZPyLGQBGRYCY2ExEjAQBgoJkiaJk/IsZAEZFgJzeTENMAsGA1UEAxMEbXlj
YTAeFw0xMDA5MTMxNTM2MTZaFw0xMjA5MTMxNTQ2MTZaMIGJMQswCQYDVQQGEwJD
QTELMAkGA1UECBMCT04xDzANBgNVBAcTBk90dGF3YTETMBEGA1UEChMKRm9vYmFy
IEluYzELMAkGA1UECxMCSVQxFzAVBgNVBAMTDjE3Mi4yMC4xNDAuMTM4MSEwHwYJ
KoZIhvcNAQkBFhJzdXBwb3J0QGZvb2Jhci5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAM3P9p3hs+fYngESPRoQvRDiIVx+70iPkB/9x0PvcBVKznAY9hID
3VqEZpEg6Qs0CCq9rRDtv/n91qfu8oOaBArJcEwgE9rewsRUAXyya6QBGZnIN541
blHjQgrfQ5dQ2JdJ4Z4frjppFY2SQsn+mDSoQAjS3v+Tfxdi8Llr7kSZAgMBAAGj
ggK5MIICtTAdBgNVHQ4EFgQUFjVLCro6MyZbwrh/TBsBgF526FowHwYDVR0jBBgw
FoAUU6ifUOLD+AAPQ9SjGZHnvNz0/7IwgeAGA1UdHwSB2DCB1TCB0qCBz6CBzIaB
omxkYXA6Ly8vQ049bXljYSxDTj13MmszLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXN5LERD
PWNhP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1j
UkxEaXN0cmlidXRpb25Qb2ludIYlaHR0cDovL3cyazMuc3kuY2EvQ2VydEVucm9s
bC9teWNhLmNybDCB7gYIKwYBBQUHAQEEgeEwgd4wgZ0GCCsGAQUFBzAChoGQbGRh
cDovLy9DTj1teWNhLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXN5LERDPWNhP2NBQ2VydGlm
aWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MDwG
CCsGAQUFBzAChjBodHRwOi8vdzJrMy5zeS5jYS9DZXJ0RW5yb2xsL3cyazMuc3ku
Y2FfbXljYS5jcnQwDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCBaAwPAYJKwYBBAGC
NxUHBC8wLQYlKwYBBAGCNxUIhOy/UoPF0HDdlyWHpNJehaCkJj+B7bAhhtyIPgIB
ZAIBAjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwJwYJKwYBBAGCNxUK
BBowGDAKBggrBgEFBQcDATAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQUFAAOCAQEA
h1kj4IuXUIZ2XPfQNzLvYyhLIcnhZMw1WF+ORrZLGvpFccKBvRrB1y2TMIOWI83A
rMC5KFtmK3lc3dnTYgQTLY/j2glFEV5f/6WZ10pBgVWTx7Ci6kJF628liKTlIm1S
iIA95r/QV6RHHzrlzlvyRDjHjqk+P812NR8MyTjKKrUxZKWQi62710GPckCAPb7R
okT/MQE5xYM59QmJ9a7yoAPLsZeJ3ls+NrpCYWPKVpwNGozOB/ChQYVGOo1BZcMY
lphH4NUl5uGsqIgH2zMMT06MxclzEqc5qVrgrq8Htq4lkLwdNR9PJC8/sSfjtrIm
l56vXZP6tmLy0IE5olsw6w==
-----END CERTIFICATE-----
 1 s:/DC=ca/DC=sy/CN=myca
   i:/DC=ca/DC=sy/CN=myca
-----BEGIN CERTIFICATE-----
MIIERTCCAy2gAwIBAgIQGkXtgKUv07pHe+iGSmm0jzANBgkqhkiG9w0BAQUFADA3
MRIwEAYKCZImiZPyLGQBGRYCY2ExEjAQBgoJkiaJk/IsZAEZFgJzeTENMAsGA1UE
AxMEbXljYTAeFw0xMDA1MTQxMzUzMjJaFw0xNTA1MTQxNDAyMzhaMDcxEjAQBgoJ
```

Note that 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:

Figure 50: Sample Openssl command output

```
yongsun@yongsun-linux:~$ openssl x509 -in server-cert.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            42:45:a3:b6:00:00:00:00:00:33
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=ca, DC=sy, CN=myca
        Validity
            Not Before: Sep 13 15:36:16 2010 GMT
            Not After : Sep 13 15:46:16 2012 GMT
        Subject: C=CA, ST=ON, L=Ottawa, O=Foobar Inc, OU=IT, CN=172.20.140.138/emailAddress=support@foobar.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:cd:cf:f6:9d:e1:b3:e7:d8:9e:01:12:3d:1a:10:
                    bd:10:e2:21:5c:7e:ef:48:8f:90:1f:fd:c7:43:ef:
                    70:15:4a:ce:70:18:f6:12:03:dd:5a:84:66:91:20:
                    e9:0b:34:08:2a:bd:ad:10:ed:bf:f9:fd:d6:a7:ee:
                    f2:83:9a:04:0a:c9:70:4c:20:13:da:de:c2:c4:54:
                    01:7c:b2:6b:a4:01:19:99:c8:37:9e:35:6e:51:e3:
                    42:0a:df:43:97:50:d8:97:49:e1:9e:1f:ae:3a:69:
                    15:8d:92:42:c9:fe:98:34:a8:40:08:d2:de:ff:93:
                    7f:17:62:f0:b9:6b:ee:44:99
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                16:35:4B:0A:BA:3A:33:26:5B:C2:B8:7F:4C:1B:01:80:5E:76:E8:5A
            X509v3 Authority Key Identifier:
                keyid:53:A8:9F:50:E2:C3:F8:00:0F:43:D4:A3:19:91:E7:BC:DC:F4:FF:B2

            X509v3 CRL Distribution Points:
                URI:ldap:///CN=myca,CN=w2k3,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sy,DC=ca
                URI:http://w2k3.sy.ca/CertEnroll/myca.crl

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=myca,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sy,
                CA Issuers - URI:http://w2k3.sy.ca/CertEnroll/w2k3.sy.ca_myca.crt
```

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.

Figure 51: Importing the CA certificate

```
yongsun@yongsun-linux:~$ wget http://w2k3.sy.ca/CertEnroll/w2k3.sy.ca_myca.crt
--2010-12-01 15:03:47--  http://w2k3.sy.ca/CertEnroll/w2k3.sy.ca_myca.crt
Resolving w2k3.sy.ca... 172.20.140.139
Connecting to w2k3.sy.ca|172.20.140.139|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1097 (1.1K) [application/x-x509-ca-cert]
Saving to: `w2k3.sy.ca_myca.crt'

100%[=============================================================================

2010-12-01 15:03:47 (135 MB/s) - `w2k3.sy.ca_myca.crt' saved [1097/1097]
```

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 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 332.

This section contains the following topics:

- Introduction to PKI authentication
- FortiMail PKI architecture
- Configuring PKI authentication on FortiMail

Introduction to PKI authentication

Public key infrastructure (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. Table 61 on page 635 describes the impact of operation mode on each FortiMail user type.

s

Table 61: 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

Figure 52 on page 636 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.

Figure 52: 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 web UI 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

Figure 53 on page 638 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 636.
- 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.

Figure 53: 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 637.

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 drop-down 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 5 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 641 to create client certificates, or "Downloading a CA certificate for FortiMail" on page 648 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* drop-down list, select the new template created in "Creating a custom certificate request template using MMC" on page 639.

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 649.
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 7.
12. Return to the *Microsoft Certificate Services* (MSCS) home page for your local CA and repeat steps 3 through 11 for each end-user that will communicate with FortiMail using PKI authentication.
13. Proceed to "Exporting a client certificate" on page 644 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 641 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 641.

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 9.

    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 646 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 644.

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.
1. 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.

2. Open the *Personal* tab and select *Import*.

   The *Certificate Import Wizard* welcome page appears.
3. Click *Next* to continue from the *Certificate Import* welcome page.

   The *File to Import* window appears.
4. 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 644.
5. Browse to the location on the end-user computer where the .pfx file is stored, select the certificate file and select *Open*.
6. The path to the certificate location appears in the *File to Import* window. Select *Next*.

   The *Password* window appears.
7. Type the password supplied by the administrator that is used to retrieve the private key and select *Next*.

   The *Certificate Store* window appears.
8. Select the *Place all certificates in the following store* button, browse to the *Personal Certificate Store* and select *Next.*
9. When *Completing Certificate Import Wizard* appears, click *Finish* to import the certificate and private key to the location specified in step 8.

   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.
10. Proceed to "Creating email accounts on FortiMail for PKI users" on page 649.

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 649 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 648.

Use the FortiMail web UI 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 325 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 137.

Once the email accounts are created on FortiMail, proceed to "Configuring PKI authentication" on page 332.

A PKI user can be either an individual email user, all email users associated with a specific domain, or a FortiMail administrator.

Caution:

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 651.

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 649.

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 650.

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 649.
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 332.
3. From *Policy* > *Recipient Policy,* select *New* to create a new Recipient Based Policy, or *Modify* to change an existing policy. For more information on recipient base policies, see "Controlling email based on sender and recipient addresses" on page 381.
4. In the *Recipient Base Policy*, expand *Advanced Settings* and configure the following:
   - Ensure the *Enable PKI authentication for webmail access* is enabled.
   - If desired, select a PKI user name from the drop-down 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 332.

   - Ensure *Certificate validation is mandatory* is enabled. This will enforce PKI authentication for the specified PKI user.
5. Repeat steps 3 and 4 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 650. Otherwise, proceed to "Configuring PKI access for administrators" on page 651.

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 137.

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 649.
2. Create a PKI user for each email user that requires access to quarantine email. For more information, see "Configuring PKI authentication" on page 332.
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 381.

4. Expand *Advanced Settings* and configure the following:
   - Ensure the *Enable PKI authentication for webmail access* is enabled.
   - If desired, select a PKI user name from the drop-down 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 3 and 4 for each PKI user that requires access to quarantine email.
6. Proceed to "Configuring PKI access for administrators" on page 651

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 649.
2. Create a PKI user for each administrator that requires to access FortiMail administrative functions. For more information, see "Configuring PKI authentication" on page 332.
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 179.
4. In the *Administer* window, configure the following:
   - Select *PKI* from the *Auth type* drop-down list.
   - Select the appropriate PKI user name from the *PKI user* drop-down list.
5. Repeat steps 3 and 4 for each administrative PKI user.
6. Return to the "Enabling PKI authentication globally with CLI" on page 651.

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 652 to validate that PKI authentication is working properly.

Testing PKI authentication

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 5.

   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.

   ```
   exec reload
   ```

4. Return to step 1 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.

Index

Symbols

"Configuring an antispam profile" on page 327 420
"Relay Server section" on page 212 314

Numerics

421 399
451 378, 398, 603
5.7.1 602
501 397, 399
503 398
550
19, 367, 368, 378, 392, 400, 424, 429, 442, 484, 512, 526, 602
553 400

A

A
record 8, 9, 10, 11
A record 399
A records 399, 400
access control
default action 363
example rules 369
rules 363
TLS 372
access controls 179
ACL 363
action
default 363
discard 424, 429, 442
quarantine 442
quarantine for review 425, 429, 442
reject 424, 429, 442
replace 442
rewrite recipient email address 425, 430, 443
tag email in header 423, 428, 441
tag email in subject 423, 428, 441
active-passive 24
active-passive HA 236, 241, 244, 245, 250
address book 346
address map 339, 358
LDAP 345, 450
address verification 12
admin 29
administrative access 25, 164
administrator
"admin" account 27, 580, 581, 584, 585, 586
advanced mode 39
alert email 243, 245, 562, 575, 576
recipients 576
alert messages 128
alias 337, 339, 358, 457, 458
object 469
antispam 24
Bayesian scan 531
determining which profile applies 362
DNSBL 14, 414
FortiGuard Antispam 14
heuristic scan 413
log 121
profile 407
SHASH 14
spam quarantine 138
SURBL 14, 414
system quarantine 141
antivirus 24
determining which profile applies 362
preferences 470
profile 425
scan 426
appearance, web-based manager 218
archive
search 157
archived email
exporting 157
policies 559
using for Bayesian training 157
ASCII 229, 417, 479
associated domains 318
asynchronous digital subscriber line (ADSL) 86, 528
ATM 86, 528
attachment 430
filtering 431
AUTH 363
authentication 27, 203, 213, 367, 446
administrator 183
and open relays 401
certificate vs. password 388
how-to 445
LDAP 345, 445, 450
SMTP 363, 380, 386, 445
to bypass the greylist 148
authorization 395
autoexempt list
filter 153, 155, 530

B

back up
Bayesian database
global or group 537
block/safe lists
domain 509
system 507, 511
mail queues 296
using the CLI 297

backscatter 593, 605
backup unit 238
banned word scan 415, 417, 420
Base64 281
baseline 126
basic mode 39
batch edit 408
Bayesian control account
  configuring 539
Bayesian database
  back up
    global or group 537
  global 324
  per protected domain 324
  reset
    global or group 538
  restore
    global or group 538
  scan 407, 531
  training 197, 537
    example 534
    from archived email 157
  types 532
Bayesian database training 40
bind DN 452, 457
bits per second (bps) 29
blind carbon copy (BCC) 424, 429, 442
block 171
block/safe list 504
  action 512
  backing up
    domain 509
    system 507, 511
  order 504
  restoring
    domain 509
    system 508, 511
blocklisted by DNSBL 364
Boolean 470
boot interrupt 28, 585
bounce address 524
  tag key 524
  tagging 523
  verification 523, 524
  verification failure 524, 526
bounce message 523
  verification
    bypass 396
    disable 324
bridge 161, 164, 165, 169, 172, 213, 258
browser 26
  warnings 27
Buffalo TeraStation 205
bypass
  antispam scan 368, 419, 603
  antispam scans 507
  antivirus scan 603
  bounce message verification 396
  content profile 432
  greylist 148
  physical 602
  using safe lists 404

C

carriage return and line feed (CRLF) 398
carrier 527
  end point 151, 154, 155, 156, 527, 529, 530
cellular phone 527
centralized quarantine 205
certificate
  backup 282
  binding profile 547
  default 27
  local 445
  mismatch 27
  options 278
  personal 388, 445
  server 276
certificate authority (CA)
    27, 277, 278, 280, 281, 283, 284, 333, 445, 548
certificate request
  downloading and submitting 280
certificate revocation list (CRL) 283, 284, 333
certificate, security 27
class C 515
clean install firmware 585
clear
  Bayesian database
    global or group 538
CLI 167, 169
  not available 25
cluster 24, 238
column view
  logs 133
command line interface (CLI) 26
  backup via the 297
comma-separated value (CSV) 326, 347, 350, 571
common name (CN) field 27
compact 142
confidential 13
config master 251
config slave 251
config-only HA 236, 244, 245, 250
configuration example
  HA 267
configuration, verifying the 584
configured operating mode 246
connecting
  CLI 28
connecting to the FortiMail CLI using SSH 32
connecting to the FortiMail CLI using Telnet 33
console port 28

content
profile 430
content monitor
profile 436
quarantine 141
control buttons 33
controller card 233
CPU 189
CSV import 328
custom messages 218
custom variables 219

D

daemon
HA 241
MSISDN reputation 529
dashboard 128
DATA 20, 363, 375
date 185
daylight savings time (DST) 185
DB-9 28
debug log 306
deep header scan 394, 395, 396
default
action 363
administrator account
27, 29, 580, 581, 584, 585, 586
attribute name 473
bridge configuration 161
certificate 27
gateway 166, 173
network interface configuration 164
operation mode 38
password 27, 29
route 40, 172, 173
settings 26, 33
URL 26
default variables 220
delay period, greylist 518
delivery status notification (DSN)
13, 144, 146, 197, 199, 370, 486, 487, 523, 605
demilitarized zone (DMZ) 56, 63, 107
destination IP address 210
DHCP 166
dictionary profile 479
dictionary group 482
dictionary scan 417
differentiated services 361
digital certificate requests 543
digital subscriber line (DSL) 86, 527, 528
directionality 575
of SMTP connections 211
directory harvest attacks (DHA) 593
discard 368, 424, 429, 442, 512, 526
disclaimer 203, 204
domain 320
log in 186
system 203
disk space
email archive 557
quarantine 138, 139, 141, 144
quota 443
reclaim 142
user account 443
user accounts 329
display name 143, 327
mail user 326
Distinguished Name (DN) 277, 283, 284, 285, 470
distribution list 337, 469
DKIM 395, 396
DNS 8, 9, 10, 11, 40, 42, 116
DNS block list (DNSBL) 14, 407, 414, 415
DNS server 166, 174, 576
failure 146
record for DKIM 395
record for SPF 395, 409
DNS-resolvable 40
documentation
Release Notes 585
domain
email 12
protected 12, 307
query 465
domain associations 318
domain name
certificate 27
local 41, 197
DomainKeys 395, 396
domain-part 139
dominoPerson 470
DOS 26
downgrade 580
download
report 158
drop 171
DSN notifications 40
dynamic DNS (DDNS) 174, 279
dynamic IP address 86, 166
dynamic public IP address 174, 528

E

edit
batch 408
effective operating mode 248
HA 246
EHLO 12, 17, 213, 313, 323, 390, 397, 398, 401
email
gateway 24, 35
email access
configuring 363
email archiving
configuring settings 555
policies 559
email domain 12
email settings 307
encoding 417

encryption
profile 485
end of message (EOM) 398
endpoint reputation score 393
end-user guide 612
envelope 143
EOM 21, 398
Error Correcting Code (ECC) 234
Ethernet 26
event log 292
execution order 16
expired user 343
export archived email 157
Extended Simple Mail Transfer Protocol (ESMTP) 199
extended SMTP (ESMTP) 7
extended unique identifier (EUI) 207, 304
externalAddress 463

F

factory default settings 26
failed to mount archive filesystem 301
failover 187, 245, 250, 254, 256
HA 239, 260
false positive or false negative 138, 510, 540
FDN
HTTPS 601
port 443 601
port 53 601
port 9443 601
firmware 580
clean install 585
downgrade 580
restoring 28
upgrade 580
version 128
flow control 29
folder size 142
formatted view
logs 133
formatting the boot device 585
FortiAnalyzer 205, 569, 570
FortiGuard
Antispam 14, 238, 244, 287, 391, 407, 412
Antivirus 238, 239, 244, 287
scheduling updates 45
FortiGuard Antispam 44
FortiGuard Antivirus 44
FortiGuard Distribution Network (FDN)
161, 287, 288, 601
FortiGuard Distribution Server (FDS) 289
FortiMail IBE encryption
about 543
using 544
FortiMail-2000 138, 230, 233
FortiMail-2000A 235
FortiMail-2000B 235
FortiMail-400 230, 267, 269
FortiMail-4000A 235, 236
Fortinet
MIB 192, 193
Technical Support 288, 306
Fortinet Distribution Network (FDN) 43, 44, 116
Fortinet Distribution Server (FDS) 44
Fortinet Technical Support 44
forwarding 156
frame size 168, 170
FreeNAS 205
front panel 33
fully qualified domain name (FQDN)
10, 41, 42, 196, 197, 279, 308, 318
fully-qualified domain name (FQDN) 279

G

gateway 173, 401
email 35
route 40
gateway mode
8, 10, 24, 34, 35, 38, 47, 140, 166, 308, 329, 35
9, 379, 445
deployment 46
gidNumber 455, 471
global
Bayesian database 324, 532
graphical user interface (GUI) 26
green
check mark 377
checkmark 332
greylist 147, 512, 513
configuring 512
delay period 518
filter 149
search 150
TTL 515, 516, 518
window 518
group
LDAP 384, 385
name 384, 385
profile 490
group object 469
groupOfNames 471, 472
groupOwner 456, 471
GSM 527

H

HA
- active-passive 236, 241, 244, 245, 250
- alert email 243, 245
- and NAS 251, 253, 255
- backup unit 238, 273
- config-only 236, 244, 245, 250
- configuration not synchronized 240
- configuration options 241, 250
- configured operating mode 246
- daemon options 241
- effective operating mode 246, 248
- example 267
- failover 187, 239, 245, 250, 254, 256, 260
- forcing configuration synchronization 247
- forcing data synchronization 247
- heartbeat 239, 244
- host name 196
- HTTP service 259
- interface configuration synchronization 240
- local domain name 242
- log messages 243, 245
- mail queue sync after a failover 242
- management IP 241
- master 238
- monitoring 239, 258
  - HTTP 259
  - POP3 259
  - SMTP 259
- MTA spool directory sync after a failover 242
- network interface 240
- overview 236
- primary unit 238, 272
- restarting HA processes on a stopped primary unit 249
- service monitoring 241, 245
- slave 238
- SNMP 241, 243
- static routes 242
- synchronization 238, 244
- virtual IP 258, 267, 268
- virtual IP DNS settings 271
- virtual IP firewall settings 271
- wait for recovery then assume slave role 252, 262
- wait for recovery then restore original role 252, 262

hard disk
- logging to 569
- usage 329

header 143

header rewrite
- antispam action 425, 430
- content action 443

heartbeat 244
- HA 239

HELO 12, 17, 213, 313, 323, 390, 397, 398, 401

heuristic scan 407, 413, 420
- antivirus 426

hide 313

high availability (HA) 10, 24, 41, 43, 47, 95, 236
- active-passive 24
- config-only 24

history log 131, 211, 393

host name 27, 41, 128, 139, 175, 196, 323
- in HA 240

hot spare 231

how-to
- authentication 445
- HA 244
- quarantine 139

HTTP 7
- monitoring for HA 259
- quarantine access 140
- web-based manager 167, 169
- webmail access 167, 169, 387, 446

HTTP service
- monitoring for HA 259

HTTPS 7, 27, 140, 167, 169, 276, 279, 387, 446
- webmail 167, 169

hypertext markup language (HTML) 434

I

IBE active user
- configuring 342

IBE domain
- configuring 345

IBE encryption
- about 543
- configuring 543

IBE expired user
- configuring 343

IBE secure question
- configuring 344

IBE services
- configuring 545

IBE user
- configuring 341

IBM Lotus Domino 469

ICMP ECHO 167, 169

idle timeout 186

image spam scan 417, 420

IMAP 6, 7, 8, 24, 325
- secure 276
- system quarantine access 503

implicit relay 170, 210, 211

import
- user in CSV 328

inbox 138, 142

incoming proxy 209, 210, 211, 314

inetLocalMailRecipient 470

inetOrgPerson 455, 470

internalAddress 463

Internet service provider (ISP) 10, 36, 174, 201, 217, 361, 381, 527

IP 130

IP address 27, 33, 174

IP pool 323
- profile 488

IP-based policy 359, 375, 446

iSCSI 300, 303
- qualified name (IQN) 207, 304

iso-8859-1 481

K

key 32
key size, certificate 280
key type, certificate 280

L

language
  quarantine 322
  web-based manager 194, 228
  webmail 322, 329
last hop address 505
Layer 2 bridge 164, 165, 258
Layer 2 loop 258
Layer 2 switch 591
LCD 26, 33
LCD panel 186
LDAP 311, 313, 316, 370
  address map 345, 450
  attribute 469
  authentication 445
  bind 452
  bind DN 457
  cache 467, 468
  email alias objects 469
  group objects 469
  password 452
  profile 315, 450
  query 315, 453, 465
  query string 458, 460, 470
  schema 468, 469
  secure connection 452
  syntax 470
  timeout 467
  TTL 468
  user objects 469
LDAPS 451, 452
Linux 205
load balancer 238
local certificate
  options 278
local domain name 41, 175, 197, 503, 539
  in HA 242
local-part 139, 143, 504, 539
log
  antispam 121
  column view 133
  formatted view 133
  FortiAnalyzer 570
  HA log messages 243
  messages 563
  rotate 569
  search 135
  severity level 565
  storage 569
  storing 569
  Syslog 570
  to the hard disk 569
logging in 27
login
  dialog 27
  ID 86
login ID 155, 528
login prompt 29

M

mail delivery rules 371
mail exchanger (MX) 308, 310, 406
  failover 311
  primary 42, 311
  record 8, 9, 10, 11, 42, 46, 47, 94, 95
MAIL FROM
  17, 18, 19, 20, 21, 145, 148, 150, 151, 323, 339, 340, 363, 365, 373, 380, 383, 385, 387, 398, 401, 505, 514, 521, 523, 524
  18, 20
mail queue 210, 211
mail queues
  back up and restore 296
mail routing 210, 213, 316
mail settings 307
mail statistics 129
mail transfer agent (MTA) 6, 8, 24, 35
mail user
  adding 102, 106, 114
mail user agent (MUA) 6, 8, 212
mailbox
  backup 302
  disk usage 329
  email archive 557
  file 157
  inbox 138
  personal quarantine 139, 457
  restoration 305
  spam 423, 428
mailHost 472
mailRoutingAddress 472
maintenance
  Bayesian database back up
    global or group 537
  Bayesian database restore
    global or group 538
  block/safe list back up
    domain 509
    system 507, 511
  block/safe list restore
    domain 509
    system 508, 511
  mail queue back up and restore 296
  user option 326, 330
management IP 161, 165, 169, 213, 496
  in HA 241
manual
  virus definition updates 291
mass mailing 401
master 238
master, HA mode 251
maximum message header size 402
maximum message size 200, 322, 402, 419

maximum transmission unit (MTU) 168, 170
MD5 397
media access control (MAC) 37, 165, 168, 591
memberOf 455, 471
message header 143
Message-Id 501
MIB 193
    Fortinet 192
    RFC 1213 192
    RFC 2665 192
Microsoft Active Directory 335, 452, 454, 469, 472
Microsoft Excel 347, 350
Microsoft Office 432
Microsoft Visio 432
Microsoft Windows Service for NFS 205
MM3 393
mobile phone 527
mobile subscriber IDSN (MSISDN) 86, 154, 528
    blocklisting 87, 154, 529
    reputation score 528
    reputation score window 531
mobile subscriber IDSNs (MSISDN) 155
mode
    advanced 39
    basic 39
    default operation mode 38
    gateway 8, 10, 24, 34, 35, 38, 47
    HA 236
    operation 24, 34, 38, 43, 240
    server 7, 8, 10, 24, 34, 95
    transparent 10, 24, 34
    web UI 39
monitor
    HA 239
monitoring services
    for HA 241
multimedia messaging service (MMS) 87, 393, 529
MX
    record 400
MX record 202, 258, 271, 308, 399
    configuration 174
    priority number 602

N

NAS server 255
network access server (NAS) 86, 528
network address authority (NAA) 207, 304
network area storage (NAS)
    server 251, 253
network attached storage (NAS) 205
    server 206, 244
    storing mail data in HA mode 255
network file system (NFS) 205, 207, 244, 301, 303
network interface 26, 166, 169
    as the source IP address 213
    connected to protected server 313
    in HA 240
    of proxies 77, 81
    port1 40
network time protocol (NTP) 185
network topology 8, 43, 46, 94
next-hop router 173, 174
nisMailAlias 471
non-delivery report (NDR) 146
non-repudiation 548
NOOP 398, 402
notification
    log level 121
null modem 28, 31

O

objectClass 453, 460, 461
on HA failure
    wait for recovery then assume slave role 252, 262
    wait for recovery then restore original role 252, 262
Online Certificate Status Protocol (OCSP)
        284, 333, 334, 336
open relay 363, 364, 401
Openfiler 205
OpenLDAP 469
OpenOffice.org 432
operation mode 24, 34, 38, 43, 240
    default 38
order of execution 16
outbound relay server 40
outgoing proxy 209, 210, 211, 217
out-of-bridge 213
out-of-office 329
override server 161

P

parity 29
pass through 149, 171
password 27, 29, 388
    administrator 183
    certificate 282
    encrypt 447
    LDAP bind 452
    user 327, 445
    user option 326
password-based encryption (PBE) 549
PDF report 575
PDF scan 420
peer connection 30
permissions 179
per-recipient quarantine 137
personal digital assistant (PDA) 527
personal quarantine 613
phone 527
pick-up, connection 209, 213
ping 167, 169
pipelining 397
PKCS #10 281
PKCS #12 281, 282, 549
point-to-point protocol
    over ATM (PPPoA) 86
    over Ethernet (PPPoE) 86

point-to-point protocol over ATM (PPPoA) 528
point-to-point protocol over Ethernet (PPPoE) 528
policy
  archive 559
  defined 359
  IP-based 359, 375, 446
  order 361, 375
  recipient-based 359, 381
    incoming 381
    outgoing 381
  usage guidance 360
POP3 6, 7, 8, 24, 198, 325
  monitoring for HA 259
  quarantine access 359, 387
  secure 276
  system quarantine access 503
port
  numbers 599
port number 6, 7, 197, 198, 311
port1 26, 40, 169, 172
posixAccount 455
postmaster 147
power on 608
preferences 140, 330, 510
primary unit 238
privacy-enhanced email (PEM) 281, 549
private key 524
processing flow 16
profile
  administrator access 184
  antispam 407
  antivirus 425
  certificate binding 547
  content 430
  content monitor 436
  dictionary 479
  encryption 485
  group 490
  IP pool 488
  LDAP 450
  resource 443
  TLS 483
protected domain 12, 41, 307, 575
  and directionality 212
  masquerade 323
  recipient address verification 13
  recipient email address 324
  relay for 213
  sender email address 324
  subdomain 309
protocol 467
  administrative access 181, 183
proxy 209
  incoming 209, 210
  outgoing 209, 210
  web 601
proxyAddresses 460
public key 281, 395, 396
public key infrastructure (PKI) 140, 332, 388, 445

Q

quarantine 24
  access 140
  centralized 205
  control email address 501
  disk space 138, 139, 141, 144
  display 7
  language 322, 330
  per-recipient
    137, 139, 167, 169, 359, 387, 424, 442
  POP3 access 359
  release manually 138
  release via email 503
  report 495
  search 140
  spam 138
  system 138, 141
  to review 141
quarantine report 137, 138, 139, 197, 242, 456
  for aliases 457
  HTML format 499
  recipient 497
query
  authentication 445
  cache 467
  DDNS 176
  DNS
    failure 146
  filter 453, 458, 460, 465, 470, 474
  for user group 384, 385
  FortiGuard Antispam 412
  LDAP 315, 316, 453, 465
  MX record 401
  password change 473
  report 573
  reverse DNS 367
  SMTP 313
  SNMP 190, 192
questions 344
Quick Start Wizard 34, 38, 39, 46
quota 443, 557, 558

R

RAID 241
  controller card 233
  level 230
  support 230
RAID 0 231
RAID 10 231
rate limit 390, 391
RCPT TO
  17, 18, 19, 20, 143, 146, 149, 150, 202, 210, 21
  1, 212, 312, 314, 339, 340, 361, 363, 366, 371,
  373, 383, 384, 398, 401, 514, 519, 521
reachable 173
read & write
  administrator 181, 183, 289
Received 324, 390, 403, 411, 412, 415
recipient address rewrite 425, 430, 443
recipient address verification 12, 147, 313

recipient-based policy 359, 381
incoming 381, 446
outgoing 381
reconnecting to the FortiMail unit 582
red
X icon 332
Redundant Array of Independent Disks (RAID) 230
regular expression
150, 365, 366, 417, 481, 519, 520, 521, 623
syntax 624
reject 19, 368, 378, 392, 424, 429, 442, 484, 512, 526
relay 8, 368
access denied 368, 512, 526, 602
Relaying denied 367, 368, 400, 512, 526
Release Notes 585
remote authentication dial-in user service (RADIUS)
86, 446, 528
and endpoint reputation 393
replacement messages 13, 218
custom 218
report
configure 572
directionality
incoming and outgoing 575
download 158
HTML format 499, 575
on demand 572
PDF format 575
periodically generated 572
protected domain 575
query 573
subject matter 573
text format 497
time span 573
view 158
reset
Bayesian database
global or group 538
effective operating mode for HA 248
resource profile 140, 379, 443, 445
restart
HA 250
primary unit 249
restore
Bayesian database
global or group 538
block/safe lists
domain 509
system 508, 511
mail queues 296
previous configuration 583
restoring the firmware 28
retry 145
reverse DNS 367
RDNS 73
RFC
1213 188, 192
1869 199
1918 176, 411, 415
2476 197
2634 547
2665 188, 192
2821 313, 398, 513
2822 423, 428, 441
2920 398
4408 395, 409
4871 395
822 458, 461, 471
compliance 398
rfc822MailMember 458, 461, 471
RJ-45 28, 31
RJ-45-to-DB-9 28, 31
route
default 40, 173
static 173
in HA 242
RSET 398, 402

S

S/MIME encryption,using 487
scan
sequence 16
schedule 496
scheduling updates 45
schema, LDAP 468
score
endpoint reputation 528
sender reputation 151
search 140, 150, 156, 157, 557
secure (S/MIME) 283
secure MIME (S/MIME) 371, 372, 374, 485, 547
Secure Shell (SSH) 26
key 32
secure shell (SSH) 167, 169, 303
secure SMTP 197
security certificate 27
security questions 344
self-signed 27
sender address
tagging 523
verification 523, 524
verification failure 524, 526
sender policy framework (SPF) 395
sender reputation 151, 392
session profile settings 391
sender validation
DKIM 395, 396
domain keys 395, 396
SPF 395
sequence of scans 16
serial communications (COM) port 28, 31
serial port parameters 609
server mode
7, 8, 10, 24, 34, 95, 140, 166, 308, 346, 359, 37

9, 445, 446, 457, 614
email user 102, 106, 114, 325
services
monitoring for HA 241
session
IP 130
SMTP 363
Session-Id 145
setting administrative access for SSH or Telnet 30
severity level 565
share 303
SHASH 14
short message service (SMS) 87, 529
slave 238
slave, HA mode 251
SMB 207, 303
SMTP 6, 8
AUTH 203, 213, 363, 380, 386, 398, 445
block 171
client, definition of 8
DATA 20, 363, 375, 398
discard 368, 424, 429, 442, 512, 526
drop 171
envelope 143, 380, 387
greeting 12, 307, 323, 390, 397, 401
MAIL FROM 363
monitoring for HA 259
NOOP 398, 402
pass through 171
pipelining 397
proxy 368
proxy or use implicit relay 171
RCPT TO 363
reject 368, 512, 526
relay 368
reply code 421 399
reply code 451 378, 398, 603
reply code 501 397, 399
reply code 503 398
reply code 550
19, 367, 368, 378, 392, 400, 424, 429, 442, 484, 512, 526, 602
reply code 553 400
RSET 398, 402
session 389
STARTTLS 363, 397, 398
VRFY 313
SMTPS 197, 203, 276, 311, 312, 313
SNMP 167, 169, 241, 243
community 189, 190, 191
event 190, 192
manager 190, 191, 193
MIB 193
MIBs 192
query 190, 192
RFC 12123 192
RFC 2665 192
traps 192, 259
spam 24
reports 40
also see antispam
spam report 137, 138, 139, 197, 242, 456, 495
for aliases 457
host name in HA 242
HTML format 499
query to determine recipient 456
recipient 497
text format 497
spam URI realtime block list (SURBL) 14, 414
splice 398
spool 253, 266
SSH 28, 30, 31, 32
key 32
SSL 197, 203, 445, 447, 448, 451, 452
standalone 269
STARTTLS 363
static route 173
static routing 172, 173
in HA 242
status bar 41
storing logs 569
subdomain 309
subject information, certificate 278
subject line 143, 423, 428, 430, 441
subject matter 573
subscriber ID 86, 155, 393, 528
blocklisting 87, 154, 529
subscriber identity module (SIM) card 86, 528
synchronization 238
Syslog 569, 570
system options
changing 186
data and time 185
system quarantine 138, 141
system resource usage 128
system time 128

T

T11 network address authority (NAA) 207, 304
tag 441
Telnet 26, 28, 30, 33, 119
telnet 167, 169
temporary failure 147, 149, 152, 392, 484, 604
terminal 26
test
configuration 114
text messages 87, 529
throughput 128
time 185
zone 44
time to live (TTL)
cache 467, 468
greylist 515, 516, 518
LDAP 467, 468
time zone 288
timeout 398, 467

TLS 197, 203, 373
about 626
access control 372
case study of 630
profile 483
troubleshooting 630
TLS/SSL
FortiMail support 628
workflow of 626
top level domain (TLD) 367
trace file 306
train Bayesian databases 537
training messages 419, 539
transparency 213
transparent mode
10, 24, 34, 140, 163, 164, 169, 172, 258, 329, 359, 360, 361, 379, 445
transparent proxy 24
transparent proxy, true 213
transport layer security (TLS) 283, 397, 445, 447, 483
traps, SNMP 192
troubleshooting 287, 292, 415, 417, 474, 596
Syslog 571
trust 27
trusted host 181, 183, 600
Try again later 398

U

unauthenticated sessions 367, 399
undeliverable 147
uniform resource identifier (URI) 411, 414
UNIX 26
update 580
antivirus definitions, manually 291
logging 289
verify 584
upgrade
FortiGuard Antivirus and FortiGuard Antispam 44
uptime 128
URL 27
default 26
US-ASCII 123, 229, 417
USB 300, 303, 305
Use secure connection 451
user 325
account 446
display name 326
expired 343
group 450
home directory 239, 242
mail client 212
mailbox backup 302
mailbox disk usage 329
name 388, 503
password 445
preferences 140, 330
query 453
quota 443
unknown 13
user guide 612
user name 326, 330, 480
user object 469
User Principle Name (UPN) 457
UTF-8 229, 417, 479, 481

V

variable 454
Predefined 226
variables 219, 474
predefined list 220
verify
configuration 114, 116
virtual IP
DNS settings 271
firewall settings 271
HA 258, 267, 268
virus 24
virus definition
manual update 291
viruses
and sender reputation 391
hidden in encryption connections 397
scan for 426
spliced scanning 398
VLAN 37, 591
VRFY 313

W

wait for recovery then assume slave role
on HA failure 252, 262
wait for recovery then restore original role
on HA failure 252, 262
warnings, security 27
web browser 26
warnings 27
web proxy 601
web release host name 242, 496
web UI
default IP 27
initial setup 26
web-based manager
customizing appearance 218
HTTP 167, 169
HTTPS 167, 169
language 194, 228
webmail 7, 8, 24
access 164, 167, 169, 387, 446
address book 347, 349
authentication 359
disk space 444
event 562
failure 259
IP address for access 161
language 322, 329
online help 614
password 452, 473
preferences 510
widget 128
System Information 38

wild cards 506, 519, 520, 521, 560
window
    endpoint reputation 529
    greylist 515, 516, 518
    MSISDN reputation 154, 531
    sender reputation 152
Windows share 207, 303

X

X-Content-Filter 441
X-Custom-Header 423, 428
X-FEAS-BANNEDWORD 415
X-FEAS-DICTIONARY 417