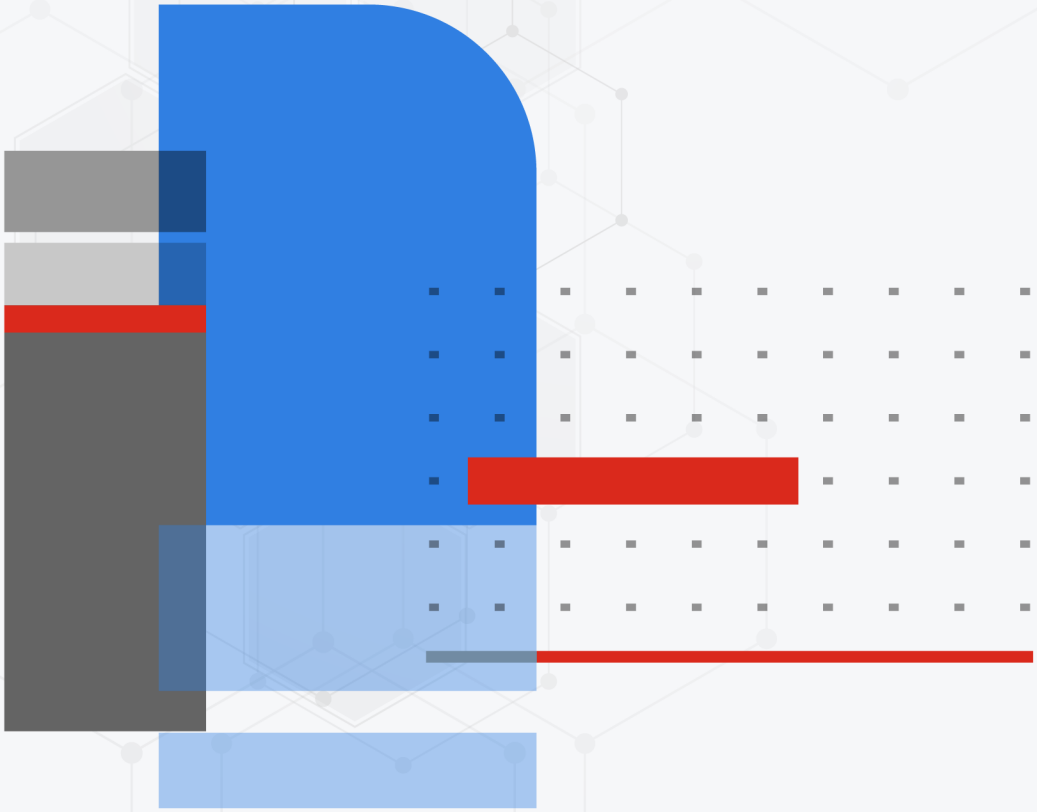
Administration Guide

FortiMail Cloud 24.2.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 12, 2024
FortiMail Cloud 24.2.0 Administration Guide
06-242-000000-20240412

TABLE OF CONTENTS

Change log

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

Date	Change Description
2024-04-10	Initial release of FortiMail Cloud 24.2.0 Administration Guide.

Using the dashboard

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

This section includes:

Viewing the dashboard

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

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

Hiding, showing and moving widgets

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

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

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

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

FortiMail Cloud User-add feature (license based)

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

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

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

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

Using the CLI Console

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

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 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.

Mail statistics may also be viewed by scan speed and by transfer speed.

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.

The FortiMail unit can also generate reports on the total number of active mailboxes during a particular time period, as specified in the report profile creation under *Log & Report* > *Report Setting* > *Mailbox Statistics*. For more information, see Configuring mailbox statistics.

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 144 and Configuring policies on page 117.

Microsoft 365 and Google Workspace notification statistics

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

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

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

For more information on Microsoft 365 and Google Workspace specific mail statistics and other protection features, see Microsoft 365 and Google Workspace threat remediation on page 316.

View threat statistics

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

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

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

Logs stored remotely cannot be viewed from the GUI of the FortiMail Cloud unit. If you require the ability to view logs from the GUI, also enable local storage. For details, see Configuring logging on page 306.

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 configuration change 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 287.
- *Log Search Task*: Where you can configure and view the log results of advanced searches. For more information, see To conduct advanced log search tasks on page 20.

For more information on log types, see FortiMail log types on page 301.

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 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 during a specified time range, match conditions, and keywords. Alternatively, click *Advanced Search* from the dropdown menu for the ability to apply And/Or search filter criterion. Unlike the search when viewing the contents of an individual log file, this search displays results regardless of which log file contains them. For more information, see Searching log messages on page 18.
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 18.
   - 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 20.

Log messages can appear in either raw or formatted views.

- Raw view displays log messages exactly as they appear in the plain text log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying

log messages in formatted view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

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

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

Displaying and arranging log columns

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

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see Searching log messages on page 18.

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.

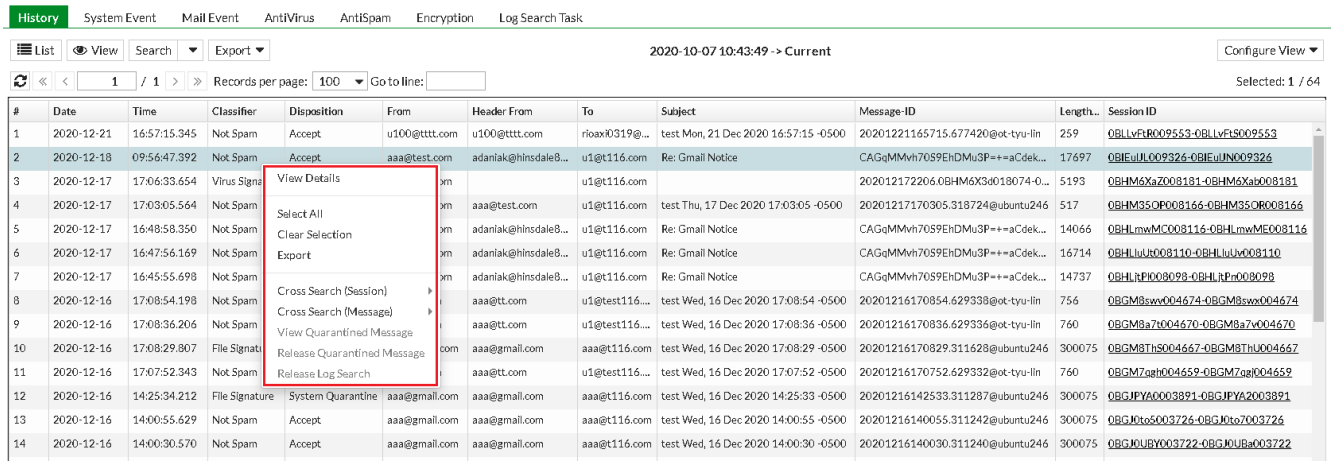
To change the order of the columns

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.

Using the right-click menus on log reports



Log report right-click menu options

GUI item	Description
View Details	Select to view the log message in a pop-up window.
Select All	Select to select all log messages in the current page, so that you can export all messages to a table.
Clear Selection	Select to deselect one or multiple log messages.
Export	Select to export the selected log messages to .CSV format, allowing you to review the information elsewhere.
Cross Search (Session)	Select to search for the log messages triggered by the same SMTP session. This may result in multiple email messages if multiple messages were sent in the same SMTP session.search log messages by session ID and message ID. For details, see Cross-searching log messages on page 20.
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 20.
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 21.
Release Quarantined Message	When viewing quarantine logs on the *History* tab, select one or multiple log entries of the “System Quarantine” messages, then from the right-click 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 21.
Release Log Search	When viewing quarantine logs on the *History* tab, select one or multiple log entries of the “System Quarantine” messages, then from the right-click popup menu, select the Release Log Search option to release the selected message/messages.

GUI item	Description
	A message will show that the qurantined message was released, along with all logs related to the email being quarantined.

Searching log messages

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

Search appearance varies by the log type.

Some email processing such as mail routing and subject-line tagging modifies the recipient email address, the sender email address, and/or the subject line of an email message. If you search for log messages by these attributes, enter your search criteria using text exactly as it appears in the log messages, not in the email message. For example, you might send an email message from sender@example.com; however, if you have configured mail routing on the FortiMail Cloud unit or other network devices, this address, at the time it was logged by the FortiMail Cloud 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
Time Range	Select a time range of log messages to include in the search results. Either search the last hour, 4 hours, 8 hours, 12 hours, or a custom date or time span. For example, you might want to search only log messages that were recorded during the last 10 days and 8 hours previous to the current date. In that case, you would select *Custom*, select *Date*, and specify the required dates and time of day to conduct the search.
Match condition	Select from one of the following options: • *Contains*: searches for the exact match. • *Does not contain*: searches exclude keyword instances. • *Matches (wildcard)*: supports wildcards in the entered search criteria. • *Does not match (wildcard)*: searches exclude wildcard instances.
Keyword	Enter any word or words to search for within the log messages. For example, you might enter `starting daemon` to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the message log field. This option does not appear for history log searches.
Subject	Enter all or part of the subject line of the email message as it appears in the log message. This option appears only for history log searches.
Message-ID	Enter all or part of the message ID in the log message.
From	Enter all or part of the sender's email address as it appears in the log message. This option does not appear for event log searches.
Header From	Enter all or part of the email header from address. This option does not appear for event log searches.
To	Enter all or part of the recipient's email address as it appears in the log message. This option does not appear for event log searches.
Session ID	Enter all or part of the session ID in the log message.
Client location (History log search only)	Select a geographical location by country from the dropdown menu.
Client name/IP (History log search only)	Enter all or part of the domain name or IP address of the SMTP client. For email users connecting to send email, this is usually an IP address rather than a domain name. For SMTP servers connecting to deliver mail, this may often be a domain name.
Classifier	Enter the classifier in the log message. The classifier field displays which FortiMail scanner applies to the email message. For example, *Banned Word* means the email messages was detected by the FortiMail banned word scanning. For information about classifiers, see Classifiers and dispositions in history logs on page 303.
Disposition	Enter the disposition in the log message.

GUI item	Description
	The disposition field specifies the action taken by the FortiMail unit. For information about dispositions, see Classifiers and dispositions in history logs on page 303.

Click *Search*.

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

To conduct advanced log search tasks

1. Go to *Monitor* > *Log* > *Log Search Task*.
2. Click *New*.
   A log search task dialog appears.
3. Enter your search criteria by configuring one or more of the following:

GUI item	Description
Log type	Select one of the log type tabs: *History*, *Mail Event*, *AntiVirus*, *AntiSpam*, *Encryption*, or *System Event*.
Description	Enter an optional description for the log search task.
Time Range	Select a time range of log messages to include in the search results. Either search between two dates and times, or a custom time span. For example, you might want to search only log messages that were recorded during the last 10 days and 8 hours previous to the current date. In that case, you would select *Time span* and specify the number of days and hours before a specific end date and time.
Search Filter	Click *Add* to apply fields and operations (or match conditions) and define their values. For multiple search filter criterion, apply And/Or search logic under *Relationship*.

4. Click *Search*.

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

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

Cross-searching log messages

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

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

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

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.

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

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

If this occurs, it is recommended to conduct a search in antispam logs.

Managing the quarantines

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

Personal quarantine

Quarantines email messages into separate folders for each recipient address in each protected domain. The FortiMail unit periodically sends quarantine reports to notify recipients, their designated group owner, and/or another email address of the email messages that were added to the quarantine folder for that recipient. See Managing the personal quarantines on page 22.

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 25.

Domain quarantine

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

Quarantines email messages into separate folders for each protected domain, in the case of a multi-tenant environment. Unlike the per-recipient quarantine, the FortiMail unit does **not** send a quarantine report. The FortiMail administrator, assigned to their respective domain, should review the quarantined email messages to decide if they should be released or deleted. See Managing the domain quarantines on page 27.

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

- Configuring antispam profiles and antispam action profiles on page 160
- Configuring antivirus profiles, file signatures, and antivirus action profiles
- Configuring content profiles and content action profiles on page 186
- Configuring content profiles and content action profiles

Sample Submission

You may also submit samples of spam email to a specified email account so it may either be reviewed by an administrator or sent directly to FortiGuard. See Managing the spam sample submissions on page 29.

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

Managing the personal quarantines

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

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

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

The quarantine report, by default sent once a day at 9 AM, lists all email messages that were withheld since the previous quarantine report. Using the quarantine report, email users can review email message details and release any email messages that are false positives by clicking the link associated with them. The email message will then be released from quarantine and delivered to the email user's inbox. Using the GUI, FortiMail administrators can also manually release or delete quarantined email. For more information on deleting email that has been quarantined to the per-recipient quarantine, see Managing the personal quarantines on page 22. For information on configuring the schedule and recipients of the quarantine report, see Configuring global quarantine report settings on page 248.

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 178 and Configuring content profiles on page 186.

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 23.

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

1. Go to *Monitor* > *Quarantine* > *Personal Quarantine*.
2. Select the name of a protected domain from *Domain*.

You can view, delete, and release email that has been quarantined to each personal quarantine mailbox.

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

Email users can also manage their own per-recipient quarantines through quarantine reports. For more information, see Releasing and deleting email via quarantine reports on page 253.

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 249. 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 71 for quarantine report settings that are domain-specific, or Configuring global quarantine report settings on page 248 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 255.
4. For gateway mode or transparent mode, configure authentication profiles that will allow email users to authenticate when accessing their per-recipient quarantine.

   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 201.
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 88, or the online help for FortiMail webmail and per-recipient quarantines.

6. If the FortiMail unit is operating in server mode and you want to enable web release/delete, configure resource profiles in which Webmail access on page 200 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 178 and/or Configuring content action profiles on page 195.
8. Select the antispam and/or content profiles in incoming recipient-based policies. If you configured a resource profile in step If the FortiMail unit is operating in server mode and you want to enable web release/delete, configure resource profiles in which Webmail access on page 199 is enabled. on page 246, 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 138.
9. Either email users or FortiMail administrators can manage email in the per-recipient quarantines.

   For details, see Managing the personal quarantines on page 22 and Releasing and deleting email via quarantine reports on page 253.

Searching email in the personal quarantine

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

The search action involves the following steps:

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

See below for detailed instructions.

To search the personal quarantine

1. Go to *Monitor* > *Quarantine* > *Personal Quarantine*.
2. Click *Search*. The *Personal Quarantine Search* tab appears, displaying all search tasks, if there are any.
3. Click *New* to add a search task.
   A dialog appears.
4. Configure the search criteria, including *Time Range* to define the date/s and time of the search, various *Search Filter* criterion, and determine whether the search should be conducted across all or multiple domains.
   Email messages must match all criteria that you configure to be included in the search results. For example, if you configure *From* and *Subject*, only email messages matching **both** *From* and *Subject* will be included in the search results. Select from the list of available header options under *Field*:
   - *From*
   - *To*
   - *Cc*
   - *To or Cc*
   - *From, To or Cc*
   - *Subject*
   - *Text*
   - *Attachment*

- *Message-ID*
- *Client IP*
- *Endpoint ID*
- *Policy ID*
- *Release Status*
- *Custom Header*

Wildcard header search support is also available.

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

Managing the system quarantine

The *System Quarantine* tab displays the system quarantine.

Unlike the per-recipient quarantine, the system quarantine cannot be accessed remotely by email users. Also, they do not receive quarantine reports for email held in the system quarantine and cannot manage the system quarantine themselves. A FortiMail administrator should periodically review the contents of the system quarantine. Alternatively, you can configure a special-purpose system quarantine administrator for this task. For more information, see Configuring the system quarantine setting on page 255.

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

By default, the system quarantine is not used until you configure the FortiMail unit to send per-recipient quarantine to system quarantine by selecting *System quarantine* in antivirus action profiles, content action profiles, and antispam action profiles. For more information, see Configuring antivirus action profiles on page 184, Configuring antispam action profiles on page 178, and Configuring content action profiles on page 195.

To view and manage system quarantine folders

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

GUI item	Description
View (button)	Select a item in the table and click View to open item.
Delete (button)	Click to delete the selected item.
Compact (button)	Select the check boxes of each email user whose quarantine folder you want to compact and click *Compact*.

GUI item	Description
	For performance reasons, when you delete an email, it is marked for deletion but not actually removed from the hard disk at that time, and so still consumes some disk space. Compaction reclaims this hard disk space. **Note:** FortiMail updates folder sizes once an hour. The reduction in folder size is not immediately reflected after compacting.
Search (button)	Click to search the mail data.
Release (button)	Starting from 6.2.0 release, you can select a folder and batch release the email in the folder according to the criteria you specify: • Start date • End date • Message type: Either *Unreleased Only* or *All Messages*. • Release to: Original recipient(s) or other recipient(s) you specify.
Folder (dropdown list)	From the dropdown list, select a folder to view.
Folder	Lists the current folder. Older system quarantine mailboxes, also called rotated folders, are named according to their creation date and the rename date. For information on configuring rotation of the system quarantine mailbox, see Configuring the system quarantine setting on page 255. To view email messages quarantined in that mailbox, double-click its row. For more information, see Managing the system quarantine on page 25.
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 255.

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	Click to return to viewing the list of system quarantine folders.

GUI item	Description
(button)	
Filter	Use the filter to display the released or unreleased email only. By default, FortiMail only displays the unreleased email.
Search (button)	Click to search the system quarantine folder that you are currently viewing. For details, see Searching email in the system quarantine on page 27.
Subject	Lists the subject line of the email. Click to display the email message.
From	Lists the display name of the sender as it appears in the message header, such as `"User 1"`.
To	Lists the display name of the recipient as it appears in the message header, such as `"User 2"`.
Rcpt To	Lists the user name portion (also known as the local-part) of the recipient email address (`RCPT TO:`) as it appears in the message envelope, such as `user2` where the full recipient email address is user2@example.com.
Session ID	Lists the session ID of each email.
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 24.

Managing the domain quarantines

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

In multi-tenant environments with multiple domains, administrators are given per-domain permissions to view and perform actions on quarantined messages within their domain. Domain administrators are provided their privileges from the *Domain Quarantine* access control permission within their assigned admin profile. See Configuring administrator profiles on page 48 for more information. Note that domain/domain-group administrators cannot access system quarantined messages.

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

Options for viewing and managing the domain quarantine folders is similar to the options available for system quarantine. See To view and manage system quarantine folders on page 25 for more information.

Searching email in the domain quarantine

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

The search action involves the following steps:

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

See below for detailed instructions.

To search the domain quarantine

1. Go to *Monitor* > *Quarantine* > *Domain Quarantine*.
2. Click *Search*. The *Domain Quarantine Search* tab appears, displaying all search tasks, if there are any.
3. Click *New* to add a search task.
   A dialog appears.
4. Configure the search criteria, including *Time Range* to define the date/s and time of the search, various *Search Filter* criterion, the particular domain to search, and determine whether the search should be conducted across all or multiple folders, or mailboxes.
   Email messages must match all criteria that you configure to be included in the search results. For example, if you configure *From* and *Subject*, only email messages matching **both** *From* and *Subject* will be included in the search results. Select from the list of available header options under *Field*:
   - *From*
   - *To*
   - *Cc*
   - *To or Cc*
   - *From, To or Cc*
   - *Subject*
   - *Text*
   - *Attachment*
   - *Message-ID*
   - *Client IP*
   - *Endpoint ID*
   - *Policy ID*
   - *Custom Header*

   Wildcard header search support is also available.
5. Click *Search* to execute and save the task. The task name is the time when the task is created. The *Domain Quarantine Search* tab displays the search tasks and their search status as follows:

- *Done*: The FortiMail unit has finished the search. You can click the *View Search Result* button to view the search results.
- *Pending*: The search task is in the waiting list.
- *Running*: The search task is still running. You can choose to stop the task by clicking the *Stop* button.
- *Stopped*: The search task is stopped. You can choose to resume the task by clicking the *Resume* button.

Managing the spam sample submissions

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

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

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

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

To submit and view sample submissions, the service must first be enabled. See Configuring spam sample submission service on page 67 for more information.

To view and manage sample submission folders

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

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

GUI item	Description
Folder (dropdown list)	From the dropdown list, select a folder to view.
Folder	Lists the current folder. Older system quarantine mailboxes, also called rotated folders, are named according to their creation date and the rename date. For information on configuring rotation of the system quarantine mailbox, see Configuring the system quarantine setting on page 255.
Size	Lists the size of the quarantine folder in kilobytes (KB). **Note:**Mailbox sizes are updated once an hour.
Message Count	Lists the total number of quarantined messages in the mailbox.

3. Double-click a spam sample submission folder.
You can view, delete, submit, and filter sample submissions.

GUI item	Description
Filter	Use the filter to display the submitted or unsubmitted email only. By default, FortiMail only displays the unsubmitted email.
Subject	Lists the subject line of the email. Click to display the email message.
From	Lists the display name of the sender as it appears in the message header, such as `"User 1"`.
To	Lists the display name of the recipient as it appears in the message header, such as `"User 2"`.
Rcpt To	Lists the user name portion (also known as the local-part) of the recipient email address (`RCPT TO:`) as it appears in the message envelope, such as `user2` where the full recipient email address is user2@example.com.
Session ID	Lists the session ID of each sample submission.
Received	Lists the time that the email was received.
Size	Lists the size of the email message in kilobytes (KB).

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

Managing the mail queue

FortiMail Cloud units prioritize mail delivery according to queues:

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

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

Delivery failure can be caused by temporary reasons such as interruptions to network connectivity. FortiMail units will periodically retry delivery (administrators can also manually initiate a retry). If the email is subsequently sent successfully, the FortiMail unit simply removes the email from the queue. It does not notify the sender. But if delivery continues to be deferred, the FortiMail unit eventually sends an initial delivery status notification (DSN) email message to notify the sender that delivery has not yet succeeded. Finally, if the FortiMail unit cannot send the email message by the end of the time limit for delivery retries, the FortiMail unit sends a final DSN to notify the sender about the delivery failure and deletes the email message from the deferred queue. If the sender cannot receive this notification, such as if the sender's SMTP server is unreachable or if the sender address is invalid or empty, the FortiMail unit will save a copy of the email in the dead mail folder. For more information, see Managing undeliverable mail on page 33.

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

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

GUI item	Description
View (button)	Select a message and click *View* to see its contents.
Delete (button)	Click to deleted the selected item.
Resend (button)	Mark the check boxes of the rows corresponding to the email messages that you want to immediately retry to send, then click *Resend*. To determine if these retries succeeded, click *Refresh*. If a retry succeeds, the email will no longer appear in either the deferred mail queue or the dead mail folder. Otherwise, the retry has failed.
Type	Select the directionality and priority level of email to filter the mail queue display. • *Default*: 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 287. After three failed delivery retries, the mail will be moved to

GUI item	Description
	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. • *Delivery control*: Displays the email throttled by delivery control policies (see Configuring delivery control policies on page 132). After three attempts, the mail will be moved to the outgoing-slow queue.
Search (button)	Select to filter the mail queue display by entering criteria that email must match in order to be visible.
Client IP	Lists the client IP addresses.
Location	Lists the GeoIP locations/country names.
Envelope From	Lists the sender (`MAIL FROM:`) of the email.
Envelope To	Lists the recipient (`RCPT TO:`) of the email.
Subject	Lists the email subjects.
First Processed	Lists the date and time that the FortiMail unit first tried to send the email.
Last Processed	Lists the date and time that the FortiMail unit last tried to send the email.
Tries	Lists the number of times that the FortiMail unit has tried to send the email.

Viewing the FortiGuard spam outbreak protection mail queue

If you enabled spam outbreak protection in an antispam profile, FortiMail will temporarily hold suspicious email for a certain period of time (configurable with CLI command `config system fortiguard antispam set outbreak-protection-period`) if the enabled FortiGuard antispam check (block IP and/or URL filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs.

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

Viewing the FortiGuard virus outbreak protection mail queue

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

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

Viewing the FortiSandbox mail queue

The FortiSandbox unit is used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus profiles (see Managing antivirus profiles on page 181). 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 https://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, 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 72.

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

Configuring mail queue search tasks

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

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

To configure a mail queue search task:

1. Go to *Monitor* > *Mail Queue* > *Mail Queue Search Task* and select *New*.
2. Select a *Queue type*. Additionally, set a *Subtype* for general mail queue searches.

3. Define the *Time Range* start and end times for the search to take place.
4. For more granularity, use the *And*/*Or* logic filters under *Search Filter* and click *Add* to add relationship settings.
5. Under *Search Result*, define the action to take place for search results.
6. When finished configuring, click *Search*.

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

Viewing the mail queue size

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

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

```
diagnose system mailqueue status
```

Viewing email continuity queue

When FortiMail is running in either gateway or transparent mode, with this email continuity feature enabled, end users are allowed to access inbound emails in instances where the email server behind the FortiMail unit goes offline. This feature is only available with a valid license from FortiGuard.

You can view the email continuity queue that is hold by FortiMail under *Monitor* > *Continuity* > *Queue*.

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 264.

To use greylisting, you must enable the greylist scan in the antispam profile. For more information, see Managing antispam profiles on page 160.

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 138, and Controlling email based on IP addresses on page 132), **or** if the matching access control rule's *Action* is *RELAY* (see Order of execution).

You can configure the initial delay associated with greylisting, and manually exempt senders. For details, see Configuring the greylist TTL and initial delay on page 268 and Manually exempting senders from greylisting on page 269.

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 37.

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

Viewing the list of pending and individual greylist entries

GUI item	Description
Search (button)	Click to filter the displayed entries. For details, see Filtering pending and individual automatic greylist entries on page 36.
IP	Lists the IP address of the SMTP client that delivered or attempted to deliver the email message. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Location	Lists the GeoIP locations/country names.
Sender	Lists the sender email address in the message envelope (`MAIL FROM:`), such as user1@example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Recipient	Lists the recipient email address in the message envelope (`RCPT TO:`), such as user1@example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Status	Lists the current action of the greylist scanner when the FortiMail unit receives a delivery attempt for an email message matching the entry. • *TEMPFAIL*: The greylisting delay period has not yet elapsed, and the FortiMail unit currently replies to delivery attempts with a temporary failure code. For information on configuring the greylist delay period, see Configuring the greylist TTL and initial delay on page 268.

GUI item	Description
	• *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 37. *N/A* appears if the greylisting period has already elapsed.
Expire	Lists the time and date when the entry will expire. The greylist entry's expiry time is determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings` (for details, see the FortiMail CLI Reference). The default initial expiry time is 4 hours. If the initial expiry time elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. • TTL: Between the entry's PASSTHROUGH time and initial expiry time, if the entry is hit again (the sender retries to send the message again), the entry's expiry time will be reset by adding the TTL value (time to live) to the message's "Received" time. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires. But the entry will not be removed. For information on configuring the TTL, see Configuring the greylist TTL and initial delay on page 268.

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`.

GUI item	Description
	• *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 35. For more information on consolidation requirements, see Automatic greylist entries on page 267.

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

Auto Exempt tab options

GUI item	Description
Search (button)	Click to filter the displayed entries.
IP	Lists the /24 subnet of the IP address of the SMTP client that delivered or attempted to deliver the email message. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Location	Lists the GeoIP locations/country names.
Sender	Lists the domain name portion of the sender email address in the message envelope (`MAIL FROM:`), such as example.com. If the displayed entries are currently restricted by a search filter, a filter icon appears in the column heading. To remove the search filter, click the tab to refresh the display.
Expire	Lists the time and date when the entry will expire, determined by adding the TTL value to the time the last matching message was received. For information on configuring the TTL, see Configuring the greylist TTL and initial delay on page 268.

Viewing sender, authentication and endpoint reputation

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

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

For more information on enabling sender reputation and configuring the score thresholds, see Configuring sender reputation options on page 145.

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

Viewing the sender reputation statuses

GUI item	Description
Search (button)	Click to filter the displayed entries. For more information, see Filtering sender reputation score entries on page 39.
Clear (button)	Click to remove any search filter conditions.
IP	The IP address of the SMTP client.
Location	Lists the GeoIP locations/country names.
Score	The SMTP client's current sender reputation score.
State	Lists the action that the sender reputation feature is currently performing for delivery attempts from the SMTP client. • *Score controlled*: The action is determined by comparing the current *Score* value to the thresholds in the session profile.
Last Modified	Lists the time and date the sender reputation score was most recently modified.

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

In this case, bad email is defined as:

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

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

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

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

1. **Throttle client at:** For scores less than this threshold, senders are allowed to deliver email without restrictions. For scores greater than this threshold but less than the temporary fail threshold, senders are rate-limited in the number of email messages that they can deliver per hour, expressed as either an absolute number or as a percentage of the number sent during the previous hour. If a sender exceeds the limit and keeps sending email, the FortiMail unit will send temporary failure codes to the sender. See descriptions for *Temporary fail* in Configuring sender reputation options on page 145.
2. **Temporarily fail:** For scores greater than this threshold but less than the reject threshold, the FortiMail unit replies to senders with a temporary failure code, delaying delivery and requiring senders to retry later when their score is reduced.
3. **Reject:** For scores greater than this threshold, the FortiMail unit replies to senders with a rejection code.

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

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

Filtering sender reputation score entries

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

To filter the sender reputation score entries

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

GUI item	Description
Field	Select one of the following in the entries that you want to use to filter the display. • IP • Score • State • Last Modified

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

Blank fields match any value. Regular expressions and wild cards are not supported.

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

Viewing authentication reputation statuses

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

To view the authentication reputation statuses

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

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

Viewing endpoint reputation statuses

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

configure endpoint reputation, see Configuring endpoint reputation.

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

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

If a carrier end point has attempted to deliver during the automatic blocklisting window a number of spam text messages that is greater than the automatic endpoint blocklisting threshold, FortiMail unit adds the carrier end point to the automatic endpoint block list for the duration configured in the session profile. While the carrier end point is on the automatic block list and it does not expire, all text messages or email messages from it will be rejected. For information on configuring the automatic block list window, see Configuring the endpoint reputation score window. For information on enabling the endpoint reputation scan and configuring the automatic block list threshold in a session profile, see Configuring session profiles on page 144.

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

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

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

GUI item	Description
Move (button)	To move entries to the manual endpoint block list or safe list, in the check box column, mark the check boxes of entries that you want to move, then click *Move*.
Search (button)	Click to filter the displayed entries. For more information, see Filtering automatic endpoint block list entries on page 41.
Clear (button)	Click to remove any search filter conditions.
Endpoint ID	Lists the mobile subscriber IDSN (MSISDN), subscriber ID, login ID, or other unique identifier for the carrier end point.
Score	Lists the number of text messages or email messages that the FortiMail has detected as spam or infected from the MSISDN/subscriber ID during the automatic endpoint block list window.
Expire	Lists the time at which the automatic endpoint blocklisting entry expires and is removed from the list. *N/A* appears if the endpoint ID has not reached the threshold yet.

Filtering automatic endpoint block list entries

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

To filter the endpoint block list entries

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

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

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

Viewing 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 mail statistic reports on page 309.

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

Mailbox statistic reports must be configured under *Log & Report* > *Report Setting* > *Mailbox Statistics*. See Configuring mailbox statistics.

The configuration of mailbox statistic reports is license based. If you do not purchase the advanced management license, this feature is not available.

Note that the *Mailbox Statistics* tab is only available when `mailbox-service` is enabled under `config system global`. For more information, see the FortiMail CLI Reference.

To view and generate reports

1. Go to *Monitor* > *Report* > *Mail Statistics* and/or *Monitor* > *Report* > *Mailbox Statistics*.

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.

Configuring administrator accounts and access profiles

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

About administrator account permissions and domains

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

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

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

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

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

Areas of the GUI that domain administrators cannot access

Monitor **except**:

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

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

Permission	*Access level*: System	*Access level*: Domain
Administrator (also known as *all*)	• View, create, and change all other administrator accounts except the `admin` administrator account	• View, delete, and change other administrator accounts with *Read/Write* and *Read* permissions in

Permission	*Access level*: System	*Access level*: Domain
	• Change another administrator's password using the current password. The `admin` account can also reset unknown passwords. See Configuring administrator accounts and access profiles on page 44. • View and change all parts of the FortiMail Cloud unit's configuration, including uploading configuration backup files and restoring firmware default settings • Release and delete quarantined email messages for **all** protected domains • Back up and restore databases • Manually update firmware and antivirus definitions • Restart and shut down the FortiMail Cloud unit	the same protected domain, but cannot create new accounts • View and change settings, including profiles and policies, only in its own protected domain and elsewhere if permitted • View profiles and policies created by an administrator whose *Access level* is *System*
Read/Write	• View and change its own administrator account settings • View and change parts of the FortiMail Cloud unit's configuration for **all** protected domains, and the FortiMail Cloud unit itself • Release and delete quarantined email messages for **all** protected domains • Back up and restore databases	• View and change its own administrator account settings • View and change parts of the FortiMail Cloud unit's configuration only in the same protected domain • View profiles and policies created by an administrator whose *Access level* is *System* • Release and delete quarantined email messages in the same protected domain.
Read/Update		
Read	• View and change only that administrator account's own settings • View the FortiMail Cloud unit configuration for **all** protected domains, and the FortiMail Cloud unit itself • Back up databases • For *Monitor* > *Quarantine*, *Mail Queue*, and *Archive* categories, administrators with either *Read* privileges or better can view email contents if *Content detail* is enabled	• View and change only that administrator account's own settings • View settings only in the same protected domain. • View profiles and policies created by an administrator whose *Access level* is *System*
Custom	Permissions vary by which is selected (*Read* etc.) in each area. • For *Monitor* > *Quarantine*, *Mail Queue*, and *Archive*, you can select action-specific permissions. If *Content detail* is enabled, administrators with *Read* privileges or better can view email contents. • For Monitor > Quarantine > System Quarantine, you can assign either *All folders* or some folders to the administrator. By default, all folders are assigned. To change the setting, click on *All folders*. In the popup box, disable *All folders*, and then move the folders from the *Available* list to the *Members* list.	

Configuring administrator accounts

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

By default, FortiMail Cloud units have the admin account that customer request in provision wizard. For more granular control over administrative access, you can create more administrator accounts that are restricted to a specific protected domain and permissions. For details, see About administrator account permissions and domains on page 44.

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

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

If you configured a system quarantine administrator account, this account does **not** appear in the list of standard FortiMail Cloud administrator accounts. For details, see Configuring the system quarantine setting on page 255.

To configure administrator accounts

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

GUI item	Description
Status	Enable or disable the account. If disabled, the account cannot access FortiMail Cloud.
Administrator	Enter the name for this administrator account. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
Access level	Select the scope of the administrator account: • *System* • *Domain* • *Domain Group* For details, see About administrator account permissions and domains on page 44.  If *Access level* is *Domain*, the administrator cannot use the CLI nor the basic mode of the GUI.
Domain	Select the name of a protected domain. This setting is available only if *Access level* is *Domain*.
Domain Group	Select the name of a group of protected domains. This setting is available only if *Access level* is *Domain group*.
Admin profile	Select the name of an administrator profile that determines which functional areas the administrator account may view or affect.

GUI item	Description
	Click New to create a new profile or Edit to modify the selected profile. For details, see Configuring administrator profiles on page 48.
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`.  For additional security, restrict all trusted host entries to administrator computers on your trusted private network. For information on restricting administrative access protocols that can be used by administrator computers, see Editing network interfaces on page 1.

Configuring administrator profiles

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

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

To configure an administrator account

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

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

2. Either click *New* to add an account or double-click an access profile to modify it.
3. In *Profile name*, enter the name for this access profile.
4. For each row in the *Access Control* column, select the permissions such as *Read/Write* to grant to administrator accounts associated with this access profile. For more granular control of permissions, select *Custom*. For details, see About administrator account permissions and domains on page 44.
5. Optionally, select the *Privilege level*:
   - *Low:* No access to `diagnose` and `config system xxx` commands in the CLI.
   - *Medium:* Normal access except for super admin privileges. This is the default setting.
   - *High:* Same as medium.

Configuring system time

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

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

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

NTP is recommended to achieve better time accuracy.See also Appendix C: Port Numbers on page 1.

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

Configuring mail settings

Go to *System* > *Mail Setting* to configure disclaimer settings.

Configuring global disclaimers

The *System* > *Mail Setting* > *Disclaimer* tab lets you configure system-wide disclaimer messages. A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential.

Disclaimers can be appended to both incoming and outgoing email. For an explanation of directionality, see Inbound versus outbound email on page 117.

If Allow per-domain settings on page 49 is enabled, you can configure disclaimer messages that are specific to each protected domain. For more information, see Disclaimer for a domain on page 78.

To configure disclaimer messages

1. Go to *System* > *Mail Setting* > *Disclaimer*.
2. Configure the following:

GUI item	Description
Allow per-domain settings	Enable to allow protected domains to select from either the system-wide disclaimer messages, configured below, or their own separate disclaimer messages. Disable to require that all protected domains use the system-wide disclaimer messages.

GUI item	Description
	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 78.
Outgoing (or Incoming)	Enable to insert customized disclaimers for incoming and/or outgoing mail.
Custom message	Select a predefined message from the dropdown menu provided (*default*, *incoming-system-disclaimer*, or *outgoing-system-disclaimer*), or click *Edit* to configure a custom message.
External only	Enable if you want to insert a header warning disclaimer cautioning against any email originating from outside your organization.
Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[External Email]`. FortiMail will prepend this text to the subject line of email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, such as an external email mailbox, based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.
Insert header	Enable to insert a new header to the email and append a disclaimer message to the new header, then enter the disclaimer message. The maximum length is 256 characters. Enable and enter the message header key in the field, and the values in the *With value* field. FortiMail adds this text to the message header of the email before forwarding it to the recipient. The maximum length is 256 characters. Many email clients can sort incoming email messages into separate mailboxes, such as an external email mailbox, based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: ALERT-External email from outside of our organization.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.
Enable disclaimer exclusion list	Enable if you do not want to insert disclaimers to the email messages from certain senders or to certain recipients. For details about disclaimer exclusion list, see Configuring disclaimer exclusion list on page 50.

Configuring disclaimer exclusion list

In some cases, you may not want to insert disclaimers to some email messages. For example, you may not want to insert disclaimers to paging text or SMS text messages. To do this, you add the specific source IP netmasks, senders, sender domains, recipients, or recipients domains to the exclusion list, and when you configure the global disclaimer settings (see Configuring global disclaimers on page 49), you can enable the exclusion list.

To create a disclaimer exclusion list

1. Go to *System* > *Mail Setting* > *Disclaimer Exclusion List*.
2. Click *New* to create or new list or double click on an existing one to edit it.
3. Enter a sender pattern, recipient pattern, and/or source IP/mask.
   For example, for sender pattern, if you add *@example.com, all messages from example.com users will be exempted from disclaimer insertion.
   For source IP/mask, if you add 1.1.1.0/24, and both sender and recipient pattern are set to * (wildcard), then emails within the specified IP range are exempted from disclaimer insertion.
4. Click *Create*.

See also

Configuring global disclaimers

Configuring custom messages and email templates

Configuring custom messages and email templates

Configuring custom messages

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

These custom message are used for login pages, IBE messages, and other system-relate message. The content, DLP, and antivirus replacement messages used in the action profiles are configured under Profile > Replacement Massage. For details, see Configuring replacement message profiles and variables on page 198.

All the disclaimers, custom messages, and IBE login page are customizable. When you create email template on the *System* > *Customization* > *Custom Email Template* tab, you can use many of the replacement messages.

Viewing the custom messages list

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

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

You can reword existing messages or create new ones.

Modifying custom messages

You can modify the text and HTML code within a custom message to suit your requirements.

You can change the content of the custom message by editing the text and HTML codes and by working with custom message variables. For descriptions of the default custom message variables, see Default custom message variables on page 52.

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

1. Go to *System* > *Customization* > *Custom Message*.
2. To edit a message, double-click it or select it and click Edit.
3. In the Content area, enter the custom message.
   Some messages include a Subject and From area. You can edit their content too and add variables.
4. There is a limit of 8191 characters for each custom message.
5. If custom variables exist, you can add them to the text. To do so:
   - Click *Insert 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 new variables on page 52.
6. Click *OK*, or click *Reset To Default* to revert the custom message to its default text.

Creating new variables

In addition to the predefined variables, you can create new ones to customize custom messages and email templates. Typically, these variables represent messages that you will use frequently. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

1. To create new variables to be used in custom messages, go to *System* > *Customization* > *Custom Message*. To create new variables to be used in email templates, go to *System* > *Customization* > *Custom Email Template*.
2. Select a custom message or email template where you want to add a new variable, and click *Edit Variable*.
   The *Edit Variable* page appears.
3. Click *New*.
   A dialog appears.
4. Configure the following:
   - In Name, enter the variable name to use in the custom message. Its format is: `%%<variable_name>%%`. For example, if you enter the word `virus`, this variable will appear as `%%virus%%` in the custom message if you select to insert it. This is usually a simple and short form for a variable.
   - In Display Name, enter words to describe the variable. For example, use `virus name` for the variable `virus`. The display name appears in the variable list when you select Insert Variables while customizing a message or creating a variable.
   - In Content, enter the variable's content. Click Insert Variables to include any other existing variables, if needed. For example, you may enter
     `The file %%FILE%% has been detected containing virus %%VIRUS%%, and has been removed. File type is %%FILE_TYPE%%.`
     where `%%FILE%%` is the file name, `%%VIRUS%%` provides the virus name, and `%%FILE_TYPE%%` is the file type of the infected file.

   To add a color code, use HTML tags, such as `<tr bgcolor="#3366ff">`. You can select a color code, such as `"#3366ff"` in the HTML tag, from the color palette after selecting *Insert Color Code*.
5. Click *Create*.

Default custom message variables

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

Variable	Description	Location
%%QUARANTINE_TO%%	The end time of the quarantine summary.	System > Customization > Custom Email Template > Report > Quarantine summary
%%SPAM_DELETE_ALL_EMAIL%%	Under email actions in the quarantine summary, the Click Here link that, if being clicked, sends an email to delete all quarantined messages.	
%%SPAM_DELETE_ALL_URL%%	Under spam web actions in the quarantine summary, the Click Here link that, if being clicked, sends a HTTP or HTTPS request to delete all quarantined messages.	
%%SPAM_DELETE_SUBJECT%%	The subject of the email that is sent to delete a quarantined message when you click Delete under email actions in the quarantine summary.	
%%SPAM_RELEASE_EMAIL%%	The email address, such as release-ctrl@example.com, used to release an email from the recipient's personal quarantine. For details, see Configuring the quarantine control options on page 255.	
%%QMSG_DATE%%	The date and time when a message was quarantined.	
%%QMSG_EMAIL_RELEASE%%	Under email actions in the quarantine summary, the Release link that, if being clicked, sends an email to have a quarantined message sent to you.	
%%QMSG_SUBJECT%%	The subject of a quarantined message.	
%%QMSG_WEB_RELEASE%%	Under web actions in the quarantine summary, the Release link that, if being clicked, releases the message to your inbox.	
%%QUARANTINE_MESSAGES_COUNT%%	The number of quarantined messages in this summary.	

Variable	Description	Location
%%SPAMREPORT_SENDER%%	The email address, such as release-ctrl-svr@example.com, used to send quarantine summaries.	System > Customization > Custom Email Template > Report > Quarantine summary
%%SPAM_DELETE_ALL_SUBJECT%%	The subject of the email that is sent to delete all quarantined messages when you select Click Here under email actions in the quarantine summary.	
%%SPAM_DELETE_EMAIL%%	The email address, such as delete-ctrl@example.com, used to delete an email from the recipient's personal quarantine. For details, see Configuring the quarantine control options on page 255.	
%%SPAM_PREFERENCE%%	The Click Here link under Other in the quarantine summary that, if being clicked, opens your entire quarantine inbox for you to manage your preferences.	
%%SPAM_RELEASE_SUBJECT%%	The subject of the email that is sent to release a quarantined message when you click Release under email actions in the quarantine summary.	
%%SERVICE_NAME%%	Copyright information of the secure message.	System > Customization > Custom Message > Secure message > Secure message footer
%%SERVICE_NAME%%	The From, To, and Subject lines of the secure message.	System > Customization > Custom Message > Secure message > Secure message header
%%DISCLAIMER_REPLY_TO%%	The disclaimer reply to address.	System > Customization > Custom Message > Email Content Resources > Disclaimer insertion message
%%FILE%%	The name of the file that was removed from the email.	
%%FILE_TYPE%%	The file type of the suspicious file. This variable is only applicable to files with extensions.	
%%MESSAGE_ID%%	The standard message ID in the header of the email.	
%%ORIG_ENVELOPE_FROM%%	The original envelope sender address (MAIL FROM) of the email.	
%%ORIG_FROM%%	The header From of the email.	
%%ORIG_FROM_DOMAIN%%	The original header From domain of the email.	
%%VIRUS%%	The name of the virus that has infected the file.	

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

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

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

Customizing email templates

The FortiMail Cloud unit may send notification email for:

- quarantine reports (see Configuring email quarantines and quarantine reports on page 248)
- IBE (see FortiMail IBE configuration workflow on page 289)
- repackaging virus-infected email with new email body (see Configuring antivirus action profiles on page 184)
- notifying the recipeint for any FortiMail actions (see Configuring notification profiles on page 242)

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

1. Go to *System* > *Customization* > *Custom Email Template*.
2. To edit a template, double-click it or select it and click Edit.
3. Enter the replacement message and click OK, or click Reset To Default to revert the replacement message to its default text.
4. To format replacement messages in HTML, use HTML tags, such as `<b>some bold text</b>`.
   There is a limit of 250 characters for the Subject field, 60 characters for the From field, and 4000 characters for HTML and Text messages each in the Content field.
5. To add a variable:
   - Select Insert Variables next to the area to insert a variable. A pop-up window appears.
   - Place your mouse cursor in the text message at the insertion point for the variable.
   - Click the name of the variable to add. It appears at the insertion point.
   - To add another variable, click the message area first, then click the variable name.
   - Click the Close (X) icon to close the window.
6. To insert a color:
   - Click Insert Color Code. A pop-up window of color swatchs appears.
   - Place your mouse cursor in the text at the insertion point for the color code, or highlight an existing color code to change.
   - Click a color in the color swatch. For example, to replace the color code in the HTML tag `<tr bgcolor="#3366ff">`, you can highlight `"#3366ff"`, then select the color you want from the color palette.

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

Configuring single sign-on (SSO)

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

FortiMail Cloud supports SSO for webmail users.

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

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

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

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

To configure SAML SSO

1. On the IdP server:
   a. Download its IdP metadata XML.

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

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

   e. Click *Create* or *OK*.

      Now FortiMail Cloud automatically generates its SP metadata, entity ID, and ACS URL. (You might need to navigate away from the tab and return in order for it to display.)
   f. Go to *System* > *Single Sign On* > *Setting*.

g. Copy the following:

GUI Item	Description
Enabled	Enable or disable SSO.
Entity ID	A globally unique identifier for FortiMail Cloud when it connects to the IdP, such as: `https://FortiMail Cloud.example.com/sp`
Signature	The hash algorithm(for example, `SHA256`) that will be used by the signature.
ACS URL	The URL where FortiMail Cloud will receive authentication responses from the IdP (the assertion consumer service (ACS)), such as: `https://FortiMail Cloud.example.com/sso/SAML2/POST`

h. Click *Download* to retrieve the FortiMail Cloud SP metadata XML file.

i. Click *Apply*.

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

Using FortiNDR malware inspection

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

FortiNDR is the next generation of Fortinet's malware detection technology, using Artificial Neural Networks (ANN) which can deliver sub-second malware detection and verdict. You can send suspicious email attachments to FortiNDR for inspection when you configure antivirus profiles (see Managing antivirus profiles on page 181). If the file exhibits risky behavior, or is found to contain a malware, the result will be sent back to FortiMail and you can take actions according to the verdict.

For more information about FortiNDR, see the FortiNDR Administration Guide.

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

To add a FortiNDR service

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

GUI item	Description
Status	Enable FortiNDR protection.
Base URL	Enter the FortiNDR base URL.
API key	Enter the API key that you generated on FortiNDR. For details, see the FortiNDR Administration Guide.
Test Connection	Click to test the network connection to the URL.
Upload timeout	Specify the timeout (in seconds) for uploading email attachments. Default setting is 10 seconds.
Rating timeout	Specify the timeout (in seconds) for FortiNDR to scan the uploaded files. Default setting is 10 seconds.

Using FortiSandbox antivirus inspection

The FortiSandbox appliance and FortiSandbox cloud service are used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus profiles (see Managing antivirus profiles on page 181). If the file exhibits risky behavior, or is found to contain a virus, the result will be sent back to FortiMail and a new virus signature is created and added to the FortiGuard antivirus signature database as well.

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

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

To add a FortiSandbox unit

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

GUI item	Description
FortiSandbox type	If you use an appliance, specify the appliance's host name or IP address; If you use the regular or enhanced cloud service, see FortiCloud service on page 63.

GUI item	Description
Server name/IP	Enter the FortiSandbox host name or IP address. The port to use is 514. If you have a firewall in between FortiMail and FortiSandbox, make this port is allowed.
Notification email	This is the email address that FortiSandbox will use to send out notifications and reports. If you want to receive such email, enter your email address. For details, see the FortiSandbox documentation.
Statistics interval	Specify how long FortiMail should wait to retrieve some high level statistics from FortiSandbox. The default interval is 5 minutes. The statistics include how many malware are detected and how many files are clean among all the files submitted.
Scan timeout	Specify how long FortiMail will wait to get the scan results. If you receive timeouts and want to wait longer for the results, you can increase the timeout.
Scan result expires in	Specify how long FortiMail will cache the results. 0 means no local cache.
File Scan Setting	
File types	Select what types of attachment files will be uploaded to FortiSandbox for scanning.
File patterns	Create your own file pattern that will be uploaded to FortiSandbox, for example, *.txt.
File size	Specify the maximum file size to upload to FortiSandbox. You may want to limit the file size to improve performance.
URL Scan Setting	
URL selection	Specify a URL category profile or click *New* to create one. You can also click *Edit* to modify the selected profile.
Upload URL on rating error	Sometimes, FortiMail may not be able to get results from the FortiGuard queries (for example, ratings errors due to network connection failures). In this case, you can choose whether to upload those URLs to FortiSandbox for scanning. Choosing not to upload those URLs may help improving the FortiSandbox performance.
Bypass one-time URL	When enabled, any URLs that are in the personal or business category and are a pre-defined filter pattern, or if the URL is locally defined, bypass URL submission to FortiSandbox.
Number of URLs per email	Specify how many URLs will be scanned in one email message. **Note**: If the FortiSandbox type is set to *Appliance*, the valid range is 1 to 100; if it is set to *Cloud* or *Enhanced Cloud*, the valid range is 1 to 12.

FortiCloud service

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

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

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

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

To use the FortiCloud service

1. Go to *Dashboard* > *Status*.
2. Under *License Information*, click *Activate* besides *FortiCloud*.
3. In the popup dialog box, enter the email address and password for the FortiCloud account.
4. Click *OK* to log on to FortiCloud.
   Now the *License Information* should display as *Paid Contract* (if you use a demo unit, it displays as *Trial License)*.
5. Go to *System* > *FortiSandbox* > *FortiSandbox* and select *Cloud* or *Enhanced Cloud* for *FortiSanbox type* depending on your FortiCare contract. Also configure other scan settings (see Using FortiSandbox antivirus inspection on page 62).
6. After you activate FortiCloud and configure the FortiSandbox scan settings, you can access the FortiCloud web portal by going to *Dashboard* > *Status* and clicking *Launch Portal* besides *FortiCloud* under *License Information*.
   The portal allows you view the FortiMail file submission status and FortiSandbox cloud scan results.
7. If you upgrade from older releases, a reminder will appear on the dashboard, telling you to activate FortiCloud (that is, to create an FortiCloud account) before you can access the FortiCloud portal.

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

See also

Viewing the mailbox backup/restoration status

Backing up and restoring the mailboxes

Configuring mailbox backups

Configuring FortiGuard services

FortiMail uses Fortinet FortiGuard antivirus, antispam, and URL protection services.

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

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

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

Configuring FortiGuard antivirus service

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

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

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

To configure FortiGuard Antivirus options

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

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

See also

Configuring FortiGuard services

Configuring FortiGuard antivirus service

Manually requesting updates

Troubleshoot FortiGuard connection issues

Manually requesting updates

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

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

To manually request updates

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

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

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

3. After a few minutes, click the *System* > *FortiGuard* > *License* tab to check the update status. If an update was available, new version numbers appear for the packages that were updated. If you have enabled logging, messages are recorded to the event log indicating whether the update was successful or not. For details, see Log and report on page 299.

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 antispam service.

To configure the FortiGuard Antispam options

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. Under *FortiGuard AntiSpam*, verify that *Status* is enabled.
3. Specify a spam outbreak protection level. Higher level means more strict filtering.
4. Optionally enable cache and specify the cache TTL time. Enabling cache can improve performance.
5. Use FortiGuard servers either in the United States only, or in any location in the world.
6. Click *Apply*.

About spam outbreak protection from FortiGuard

This feature temporarily hold email for a certain period of time (spam outbreak protection period) if the enabled FortiGuard antispam check (block IP and/or URL filter) returns no result (see Configuring FortiGuard options on page 164). After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs.

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

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

Configuring spam sample submission service

You can designate an email address to receive and review sample submissions of spam for an administrator to review, or send directly to FortiGuard. Spam submissions can be made using the *Report Spam* plugin within Microsoft Outlook available for download at https://support.fortinet.com/.

Emails that have been submitted can be reviewed under *Monitor* > *Quarantine* > *Sample Submission*. For more information, see Sample Submission on page 22.

To configure a spam sample submissions service

1. Go to *System* > *FortiGuard* > *AntiSpam*.
2. Under *Sample Submission*, verify that *Enable submission service* is enabled.
3. Select whether you want an administrator to manually review spam sample submissions or whether you want the submissions to be sent directly to FortiGuard.
4. Define a *Retention period* of between 0-60 days, after which the sample submission will be deleted.

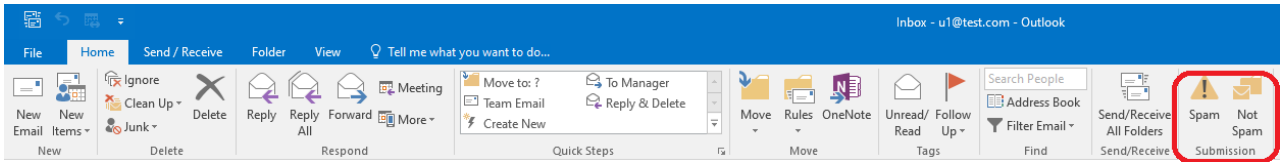
5. Enter the email addresses to receive spam and non-spam (or ham) sample submissions.

   For the email addresses:
   - The two email accounts cannot be the same.
   - The two accounts are reserved for spam and non-spam submissions; they cannot receive other email.
     Therefore, you cannot use any email accounts in use for spam and non-spam submissions.

6. Click *Apply*.

To use the report spam plugin for Microsoft Outlook

1. Go to https://support.fortinet.com/ and login to your account.
2. Go to *Support* > *Firmware Download*.
3. Go to *FortiMail* > *Plugins*.
4. Double-click the appropriate install file to start the installation process, and follow the on-screen instructions.
5. After the plugin is successfully installed, restart Outlook.
   Upon reopening Outlook, you can *Report Spam* to report any uncaught suspicious email, and use *Not Spam* to report any caught spam email that you wish to mark as not spam.



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, URL, or a Hash value of an email message.

To query FortiGuard antispam service

1. Go to *System* > *FortiGuard* > *License*.
2. Enter an IP, URL or hash value of an email message.
3. Click *Query*.
   If the query is successful, the *Query result* field will display if the IP/URL is spam or unknown (not spam).
   If the query is unsuccessful, the *Query result* field will display *No response*. In this case, you should contact Fortinet Technical Support.

System utility

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

FortiGuard query

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

For more detailed information, see Manually querying FortiGuard Antispam service on page 68.

Traffic capture

When troubleshooting networks, it helps to look inside the contents of the packets. This helps to determine if the packets, route, and destination are all what you expect. Traffic capture can also be called packet sniffing, a network tap, or logic analyzing.

Packet sniffing tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- finding missing traffic
- seeing if sessions are setting up properly
- locating ARP problems such as broadcast storm sources and causes
- confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks
- confirming routing is working as you expect
- intermittent missing PING packets.

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, how the port enters and exits the FortiRecorder unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start sniffing packets, you need to have a good idea of what you are looking for. Sniffing is used to confirm or deny your ideas about what is happening on the network. If you try sniffing without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to sniff enough packets to really understand all of the patterns and behavior that you are looking for.

To capture the traffic

1. Go to *System* > *Utility* > *Traffic Capture*.
2. Click *New*.
3. Enter a description for the file generated from the captured traffic.
4. Enter the time period for performing the packet capture.
5. Specify which interface you want to capture.
6. If you want to limit the scope of traffic capture, in the *IP/HOST* field, enter a maximum of 3 IP addresses or host names for which you want to capture.
7. Select the filter for the traffic capture:
   - *Use protocol*: Only UDP or TCP traffic on the specified port number will be captured.
   - *Capture all*: All network traffic will be captured.
8. For *Exclusion*, enter the IP addresses/host names and port numbers for which do not want to capture.
9. Click *Create*.

Regular expression validator

Go to *System* > *Utility* > *Regex Validator* to validate and test regular expressions and string text. See also Syntax on page 1.

Message file converter

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

To evade email attachment inspection, a sender may use the Outlook file format .msg to hide malicious links, since FortiMail couldn't scan the content of an email attachment with .msg files attached.

Trace log

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

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

To download a trace file

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

Configuring domains and users

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

Configuring protected domains

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

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

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

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

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

For FortiMail Cloud 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 Cloud unit itself.

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

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

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

Many FortiMail Cloud 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 Cloud unit compares the domain name of the protected domain to the domain name portion of the recipient email addresses.

Usually, you have already configured at least one protected domain during installation of your FortiMail Cloud 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 76.

If the FortiMail Cloud 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 Cloud 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 Cloud unit if it is operating in server mode.

To configure protected domains

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
   A dialog appears. Its options vary with the operation mode. Then you can configure the following sections:

- Configuring recipient address verification
- Configuring removal of invalid quarantine accounts
- Configuring LDAP Options
- Configuring advanced settings

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 Cloud 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. Select the protected domain and click *Edit* 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.

GUI item	Description

SMTP Server	Query the SMTP server using either the SMTP `VRFY` command or `RCPT` command to verify that the recipient address is an email user account that actually exists. `RCPT` is the default command.
	If you want to query an SMTP server other than the one you have defined as the protected SMTP server, also enable Use alternative server, then enter the IP address or FQDN of the server in the field next to it. Also configure *Port* with the port number on which the SMTP server listens, and enable *Use SMTPS* if you want to use SMTPS for recipient address verification connections with the server. See also Appendix C: Port Numbers on page 1.
	In case you want to use different sender email addresses in the SMTP envelope (`MAIL FROM:`) for different domains, set *Mail from address* to *Use domain setting* and specify the address to use. If you select *Use system setting* (the default setting), FortiMail will use an emtpy sender email address unless you specify a global one with the following CLI commands:
	`config mailsetting smtp-rcpt-verification`
	`  set mail-from-addr <sender_email>`
	`end`
	Note: Microsoft 365 does not accept an empty MAIL FROM for SMTP recipient verification. You must specify an envelope from address if FortiMail is protecting Microsoft 365 domains.
	Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).

LDAP Server	Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. For more information on configuring LDAP profiles, see Configuring LDAP profiles on page 205. Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).
Imported User	Query an LDAP or Microsoft 365 server to verify that the imported users actually exist. For more information, see Managing imported users on page 90 Additionally, set *Action on invalid recipient* to either reject any unknown users, or discard unknown users (initially accept and silently discard).

Configuring removal of invalid quarantine accounts

This section does not apply to server mode.

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

If you select either SMTP or LDAP server, the FortiMail Cloud 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 Cloud unit removes all spam quarantined for that email user account.

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

If you have also enabled Recipient Address Verification (see Configuring recipient address verification on page 72), the FortiMail Cloud 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 Cloud unit by disabling this option.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
   A multisection dialog appears. Its options vary with the operation mode.
3. Expand the *Automatic Removal of Invalid Quarantine Accounts* section.
4. Configure the following:

GUI item	Description
Disable	Do not verify that the recipient address is an email user account that actually exists.
SMTP Server	Query the SMTP server to verify that the recipient address is an email user account that actually exists.
LDAP Server	Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. For more information on configuring LDAP profiles, see Configuring LDAP profiles on page 205.
Purge Inactive	Checks how many days an email user account has been inactive. If the account has been inactive for more than the designated *Retention period*, the account is purged.

Configuring LDAP Options

Use this section to configure the LDAP service usages.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
   A multisection dialog appears. Its options vary with the operation mode.
3. Expand the *LDAP Options* section.
4. Configure the following:

GUI item	Description
User alias / address mapping profile (transparent and gateway mode only)	Select the name of an LDAP profile in which you have enabled and configured, enabling you to expand alias email addresses or replace one email address with another by using an LDAP query to retrieve alias members and/or address mappings. To use this option make sure that the email alias and/or address mappings do exist on the LDAP server. If the alias cannot be retrieved or LDAP server is not accessible, the email will be temp failed (451 error). For more information, see Configuring LDAP profiles on page 205.

GUI item	Description
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 205.
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 205.

Configuring advanced settings

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

- Quarantine Report Setting
- Domain Association
- DKIM and ARC Setting
- 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.

For information on system-wide quarantine report settings and quarantine reports in general, see Configuring global quarantine report settings on page 248 and Configuring custom messages and email templates on page 51.

To configure per-domain quarantine report settings

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
3. Click to expand Advanced Setting.
4. Click to expand Quarantine Report Setting.
5. Configure the following:

GUI item	Description
Report destination	
Original recipient	Enable to send the quarantine report to all recipients. For more information, see Managing the personal quarantines on page 22.

GUI item	Description
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 209. Also configure the following two options for more granular control: • Only when original recipient is group • When group owner is found, do not send to original recipient
Report schedule	Click the arrow to expand the options.
Schedule	Select the schedule to use when sending quarantine reports. • *System settings*: Use the system-wide quarantine report schedule. For more information, see Configuring global quarantine report settings on page 248. • *Domain settings*: Use a quarantine report schedule that is specific to this protected domain. Also configure These Hours and These Days.
These Hours	Select which hours to send the quarantine report for this protected domain. This option is available only when Schedule is *Use domain settings*.
These Days	Select which days to send the quarantine report for this protected domain. This option is available only when Schedule is *Use domain settings*.
Report template	Select an email template to use. If you choose to use the system settings, you can view the template but cannot edit from this page. But you can edit the system-wide template by going to *System* > *Customization* > *Custom Email Template*. If you choose to use the domain settings, you can click *Edit* to modify the template.

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

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

6. Click *Create* or *OK*.

Domain Association

The Domain Association section that appears when configuring a protected domain lets you configure associated domains. An associated domain uses the settings of the protected domain or subdomain with which it is associated.

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.

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. Select the protected domain and click *Edit* to modify it.
3. Under *Advanced Setting*, click Domain Association.
4. If the relay type of this protected domain uses MX record (this domain) or MX record (alternative domain), for the MX record lookup option of the domain associations, you can choose to use the domain association's (self) MX record, or this protected domain's (parent) MX record.
5. To create a domain association, click *New* and enter the fully qualified domain name (FQDN) of a mail domain that will use the same settings as the same protected domain. You can use wildcard, such as *.example.com.
6. Click Create.
   The name of the associated domain appears in the Members area.
7. Repeat the previous steps for all domains that you want to associate with this protected domain.
8. When done, click Create or OK.

DKIM and ARC Setting

The FortiMail Cloud 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 144.

FortiMail also supports Authenticated Received Chain (ARC) validation and sealing.

DKIM signing requires a public-private key pair. The private key is kept on and used by the FortiMail Cloud unit to generate the DKIM signatures for the email messages; the public key is stored on the DNS server in the DNS record for the domain name, and used by receiving parties to verify the signature.

You can generate the key pair by creating a domain key selector; you can also manually import an existing key pair in PEM format.

After you generate or import the key pair, you can export the DNS record that contains the public key. The following is a sample of the exported DNS record:

```
example_com._domainkey IN TXT "t=y; k=rsa;
```

```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5xvUazqp2sBovpfumPuR5xC+yDvGbfndyHZuVQdSHhwdKAds
fiyOa03iPniCfQEbuM0d+4/AoPyTXHHPFBBnChMMHkWgHYlRDm5UMjrH5J1zDT5OyFxUEur+NtfS6LF29Te+6vSS+
D3asfZ85V6WJDHSI9JV0504uwDeOOh/aewIDAQAB"
```

This DNS record can be generated either in multiple string or single string format.

Then you can publish the public key by adding it to the DNS zone file as a text record for the domain name on the DNS server. The recipient SMTP server, if enabled to use DKIM verification, will use the public key to decrypt the signature and compare the hash values of the email message in order to verify that the hash values match.

FortiMail performs DKIM signing for an associated domain with its parent domain DKIM key. You must publish the DKIM public key for the associated domain in order for the receiving MTA to validate the DKIM signature.

To configure DKIM and ARC settings

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Double-click to modify an existing protected domain. Note that you can only configure DKIM and ARC setting for existing domains.
3. Click to expand Advanced Setting.
4. Click DKIM and ARC Setting.
5. Enable *DKIM signing for outgoing email*, if desired.
6. Specify the *ARC sealing option*: Disable, Incoming, Outgoing, or All.
7. Under *Key Selectors*, click *New* to configure the key pair required for DKIM signing.
8. If you want to generate a key pair, enter a new selector to use for the DKIM key, such as `example_com2`, then select *Auto Generation* and click *OK*.
9. If you want to import an existing key pair, enter a selector name, then select *Manual Import*, and upload the public key and private key. Optionally enter a password for the private key. Note that the key files must be in PEM format.
10. Click Create.
    The selector name for the key pair appears in the list of domain key selectors. The key pair is generated and public key can be exported for publication on a DNS server.

    When a new key is created or imported, it is not active by default. This allows you to publish the public key on the DNS server before you activate the key. Also note that only one key pair can be active at a time.

11. Click to select the domain key, then click Download.
    Optionally, specify whether you want to download the domain key in either multi-string or single-string format.
    Your web browser downloads the plain text file which contains the exported DNS record (.dkim) file.
12. 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.
13. Now you can activate the key by selecting the key and then clicking *Activate*.

Disclaimer for a domain

The Disclaimer section that appears when configuring a protected domain lets you configure disclaimer messages specific to this protected domain. This option is only available when Allow per-domain settings is enabled under *System* > *Mail Setting* > *Disclaimer*.

A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential. For disclaimers added to outgoing messages, you need to configure an IP-based policy or an outgoing recipient-based policy.

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

If the FortiMail Cloud 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 Configuring mail settings on page 49.

To configure a per-domain disclaimer messages

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
3. Click to expand *Advanced Setting*.
4. Click to expand Disclaimer.

You cannot configure the domain disclaimer unless the *Allow per-domain settings* option is enabled under*System* > *Mail Setting* > *Disclaimer*.

5. Configure the following:

GUI item		Description
Setting		Select which type of disclaimer message to append. • *Disable*: Do not append disclaimer messages. • *Use system setting*: Append the system-wide disclaimer messages. For more information, see Configuring global disclaimers on page 49. • *Use custom message*: For outgoing and incoming mail, select a predefined message from the dropdown menu provided (*default*, *incoming-system-disclaimer*, or *outgoing-system-disclaimer*), or click *Edit* to configure a custom message. • *Use domain setting*: 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 only available only when you have enabled per-domain disclaimer messages. For more information, see Configuring global disclaimers on page 49.
Outgoing		
	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. This option is only available when *Setting* is set to *Use domain setting*.
	Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[External Email]`. FortiMail will prepend this text to the subject line of email before forwarding it to the recipient. This option is only available when *Setting* is set to *Use domain setting*.
	Insert disclaimer at	Enable to append a disclaimer message to the start or end of 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 only available when *Setting* is set to *Use domain setting*.

GUI item		Description
Incoming		
	External email only	Enable if you want to insert a header warning disclaimer cautioning against any email originating from outside your organization. This option is only available when *Setting* is set to *Use domain setting*.
	Tag subject	Enable and enter the text that appears in the subject line of the email, such as `[External Email]`. FortiMail will prepend this text to the subject line of email before forwarding it to the recipient. This option is only available when *Setting* is set to *Use domain setting*.
	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. This option is only available when *Setting* is set to *Use domain setting*.
	Insert disclaimer at	Enable to append a disclaimer message to the start or end of 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 only available when *Setting* is set to *Use domain setting*.

Sender address rate control

For users under this domain, you can rate control how much each user can send email.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
3. Click to expand Advanced Setting.
4. Click to expand Sender Address Rate Control.
5. For email users under this domain, you can configure the following rate control settings per user:
   - Maximum number of messages per half hour. The default value is 30.
   - Maximum number of recipients per half hour. The default value is 60.
   - Maximum data size per half hour (MB). The default value is 100 MB.
   - Maximum number of spam messages per half hour. The default value is 5.
   - Send email notification upon rate control violations and select a notification profile (see Configuring notification profiles on page 242).

See also

Configuring mail settings

Configuring global disclaimers

Incoming versus outgoing email messages

Configuring protected domains

Other advanced domain settings

The following procedure is part of the domain configuration process. For information about domain configuration, see Configuring protected domains on page 71.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
   A multisection dialog appears. Its options vary with the operation mode.
3. Click to expand the *Advanced Setting* section.
4. Click to expand the *Other* section.
5. Configure the following:

GUI item	Description
Webmail theme	Either use the system setting or choose a color to overwrite the system setting.
Webmail language	Select either to use the default system language or a different language that the FortiMail Cloud unit will use to display webmail and quarantine folder pages. By default, the FortiMail Cloud unit uses the same language as the GUI.
Disk quota (GB)	Enter the disk quota in gigabytes (GB). If the maximum disk quota of this domain is exceeded, users of this domain will no longer receive any new email. If the disk quota reaches 90% threshold, a warning email is sent to the domain customer email. For instances where a resource profile disk quota is set to 0, the domain quota is enforced. Setting any value on resource profile higher than the domain quota value results in the domain quota value being imposed. Resource profile quota values are imposed instead when they are lower than the domain quota. **Note:** This option is only available in server mode.
Webmail single sign on	For webmail SSO, enable the service and select an SSO profile from the dropdown menu. For more information, see Configuring single sign-on (SSO) on page 59.
Maximum message size (KB)	Enter the limit in kilobytes (KB) of the message size. Email messages over the threshold size are rejected. **Note**: If the same email message is sent to recipients in multiple protected domains and the maximum message size limits in the domain settings are different, the smallest size setting will take effect and thus the email won't be delivered to any recipients. In this case, you can use the maximum message size setting in the content profile instead (under *Profile* > *Content* > *Content*). However, you can use the reject action only for separate SMTP sessions, not for one same session. **Note:** When you configure session profile settings under *Profile* > *Session* > *Session*, you can also set the message size limit. Here is how the two settings work together: • For outgoing email, only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. The smaller size will be used.

GUI item	Description
SMTP greeting (EHLO/HELO) Name (As Client)	Select how the FortiMail Cloud 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 Cloud unit will identify itself using the domain name for this protected domain. If the FortiMail Cloud 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 Cloud unit and the protected SMTP server will be using the same domain name when greeting each other. • *Use system host name*: The FortiMail Cloud unit will identify itself using its own host name. This is the default setting. • *Use other name*: Specify a greeting name if you want to use a customized host name. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.
Remove received header of outgoing email	Enable to remove the `Received:` message headers from email whose: • sender email address belongs to this protected domain • recipient email address is outgoing (that is, does not belong to this protected domain); if there are multiple recipients, only the first recipient's email address is used to determine whether an email is outgoing Alternatively, you can remove this header from any matching email using session profiles. See Received: on page 156.
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 279 and Training the Bayesian databases on page 279.
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 272.
Email continuity	Enable email continuity for this domain. When FortiMail is running in either gateway or transparent mode, with this feature enabled, end users are allowed to access inbound emails in instances where the email server behind the FortiMail unit goes offline. This feature is only available with a valid license from FortiGuard.

Domain level service settings (server mode only)

If you are a managed security service provider (MSSP) which host multiple domains for multiple customers, for billing purpose, the super admin may want to set limits on the usage of FortiMail resources. The domain administrators are not

allowed to modify these settings.

The following procedure is part of the domain configuration process. For information about domain configuration, see Configuring protected domains on page 71.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
3. Click *Other* under *Advanced Setting*.
4. Configure the following under *Service Setting*:

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

Configuring customer information

Use this section to configure the customer account information.

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the protected domain and click *Edit* to modify it.
   A multisection dialog appears. Its options vary with the operation mode.
3. Expand the *Customer Information* section.
4. Configure the following:

GUI item	Description
Name	Enter the customer name.
Email	Enter the customer email address.
Account limit	Enter the user account limit.
Description	Optionally, enter a description.

Managing users

The User menu enables you to configure email user-related settings, such as user preferences. 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)

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

When the FortiMail unit operates in server mode and the GUI operates in advanced mode, the User tab is available. It lets you configure email user accounts whose mailboxes are hosted on the FortiMail Cloud unit. Email users can then access their email hosted on the FortiMail Cloud 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 323.

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

GUI item	Description
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of each mailbox, and empty or delete mailboxes as required. The SecureMail mailbox contains the secured email for the user. The Bulk mailbox contains spam quarantined by the FortiMail unit. Click Back to return to the Users tab.
Export .CSV (button)	Click to download a backup of the email users list in comma-separated value (CSV) file format. The user passwords are encoded for security. **Caution:** Most of the email user accounts data, such as mailboxes and preferences, is not included in the .csv file. For information on performing a complete backup, see Backup and restore.
Import .CSV (button)	In the field to the right of Import .CSV, enter the location of a CSV-formatted email user backup file, then click Import .CSV to upload the file to your FortiMail Cloud 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 86. 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 71. You may also want to back up the existing email user accounts. For details, see Backup and restore.
Password (button)	Select a user and click this button to change a user's password. A dialog appears. Choose whether to change the user password or to switch to LDAP authentication. You can create a new LDAP profile or edit an existing one. For details, see Configuring LDAP profiles on page 205.
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.

GUI item	Description
Search user	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users displays again with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
User Name	Displays the user name of an email user, such as `user1`. This is also the local portion of the email user's primary email address.
Type	Displays the type of user: local, LDAP, or RADIUS.
Display Name	Displays the display name of an email user, such as `"J Smith".` This name appears in the `From:` field in the message headers of email messages sent from this email user.
Disk Usage (KB)	Displays the disk space used by mailboxes for the email user in kilobytes (KB).

Configuring users in server mode

You can create users one at a time or import a list of users. Before importing a user list or adding an email user, you must first configure one or more protected domains to which the email users will belong. For more information, see Configuring protected domains on page 71.

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 Cloud 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 Cloud unit at the selected domain; such as, `jsmith` if the email address is `jsmith@example.com`.
5. You can change the user's domain if it necessary. In the dropdown menu to the right of the `@` symbol, select the name of the protected domain to which the email user belongs.
6. For *Authentication type*, select one of the following:
   - select *Local* and then enter the password for this email account
   - select *LDAP* and select the name of an existing LDAP profile in the dropdown list
   - select *RADIUS* and select the name of an existing RADIUS profile in the dropdown list.

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

   The LDAP option requires that you first create an LDAP profile in which you have enabled and configured user authentication options. See Configuring user authentication options on page 210.
7. In *Display Name*, enter the name of the user as it should appear in the `From:` field in the message header.

For example, an email user whose email address is `user1@example.com` may prefer that their *Display Name* be `"J Zang"`.

8. Click *OK*.
   For a new user, the FortiMail unit creates the account. Authentication is not yet enabled and a policy may not exist that allows the account to send and receive email.
   Complete the next two steps as applicable.
9. To enable the user account, create a recipient-based policy that both matches its email address and uses a resource profile in which User account status on page 200 is enabled. For details, see Workflow to enable and configure authentication of email users on page 201 and Configuring resource profiles on page 199.
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 117.

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

Importing a list of users

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

To create and import user records

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

Sample CSV format:

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

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

The import feature does not overwrite existing records.

To change the password of multiple email user accounts

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

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

   You can create LDAP profiles using the advanced mode of the GUI. For more information, see Configuring LDAP profiles on page 205.
6. Click OK.

See also

Managing the disk usage of email users mailboxes

Configuring user preferences

Configuring user aliases

Configuring address mappings

Configuring LDAP profiles

Managing the disk usage of email users mailboxes

If your email users often send or receive large attachments, email users' mailboxes may rapidly consume the hard disk space of the FortiMail Cloud 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 199.

To empty a mailbox folder

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

See also

Configuring local user accounts (server mode only)

Configuring resource profiles

Configuring user preferences

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

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

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

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

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

To view and manage existing user preferences

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

GUI item	Description
Delete User Data (button)	Select the user and then click this button to delete the user preference settings and mail data.
Maintenance (button)	Click to reveal a dropdown menu with preference management options. • *Clear Safe List* • *Clear Block List* • *Enable Safelisting Outgoing Recipient* • *Disable Safelisting Outgoing Recipient* • *Enable Adding Recipient of Sent Email to Personal Address Book*

GUI item	Description
	• *Disable Adding Recipient of Sent Email to Personal Address Book* • *Reset* (resets preferences to their defaults)
Domain	Select the protected domain to display its email users, or to select the protected domain to which you want to add an email user account before clicking New. You can see only the domains that are permitted by your administrator profile.
Search user	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users redisplays with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
User Name	Displays the user name of an email user, such as `user1`.
Display name (server mode only)	Displays the display name of the email user.
Language	Displays the language in which this email user prefers to display their quarantine and, if the FortiMail Cloud 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 Configuring custom messages and email templates on page 51.
Safe List	The icon in this column indicates whether or not a personal safe list currently exists for this email user. Hover the mouse pointer over the list icon to determine its status: • New: A personal safe list does not exist for this email user. • Edit: A personal safe list exists for this email user. Click the icon to open a dialog where you can configure, back up, or restore the personal safe list. Safe lists include sender IP addresses, domain names, and email addresses that the email user wants to permit. **Note:** System-level lists take precedence over domain-level lists while domain-level lists take precedence over personal-level lists. For more information on safe lists and block lists, see Managing the personal block lists and safe lists on page 262.
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 Managing the personal block lists and safe lists on page 262.
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.

GUI item	Description
	A list of email accounts in sub-domains that are linked to a user on the parent domain. For example, if user1@example.com can have that email address linked to the following secondary accounts: user1@one.example.com, and user1@two.example.com. Select the New or Edit icon to add accounts to the secondary accounts for this user. Note that any accounts must first be created before they can be added to this list. Click the icon to open a dialog where you can add or remove secondary accounts. The addresses must exist in one of the existing FortiMail domains to be added.
Outgoing Recipient Safelisting (icon)	The icon indicates whether or not the FortiMail Cloud 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 Cloud webmail, then click Help. This setting can be initialized manually or automatically. FortiMail Cloud 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 Cloud webmail • an email user sends outgoing email through the FortiMail Cloud unit • a FortiMail Cloud administrator configures the email user's personal block or safe list (see Managing the personal block lists and safe lists on page 262) then the FortiMail Cloud unit will automatically initialize this setting as disabled.
Preference	The green check mark indicates that the user preference has been configured and the settings will be used. The red check mark indicates that the user preference has not be configured and the default settings will be used.
Disk Usage	Displays how much disk space each user mailbox is using.

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

See also

Configuring local user accounts (server mode only)

Configuring user preferences

Configuring user aliases

Configuring address mappings

Managing imported users

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

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

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

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

Note that this advanced management feature is only available when *User management* is enabled under *System* > *FortiGuard* > *Licensed Feature*. For more information, see Configuring FortiGuard services on page 64.

To view and manage imported users

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

GUI item	Description
Import (button)	Select to import users/groups by uploading a .CSV file.
Export (button)	Select to export the selected imported users/groups to .CSV format, allowing you to review the information elsewhere.
Type	Select whether the view individual imported users or groups.
Domain	Select the protected domain to display its imported email users/groups, or to select the protected domain to which you want to add an email user/group before clicking New. You can see only the domains that are permitted by your administrator profile.
Status	A green check mark icon indicates that the imported user/group is enabled.
Display Name	Display name of the imported email user/group. This name appears in the `From:` field in the message headers of email messages sent from this email.
Email	Displays the email address of the imported email user/group.
Type	Displays the entity type: *User* or *Group*.
Profile	Displays the user import profile the recipient belongs to. See Configuring user import profiles on page 91 for more information.

Configuring user import profiles

Go to *Domain & User* > *User* > *User Import Profile* to map remote users/groups and to maintain a synchronization schedule from LDAP or Microsoft 365 servers.

Note that this advanced management feature is only available when *User Management* is enabled under *System* > *FortiGuard* > *Licensed Feature*. For more information, see Configuring FortiGuard services on page 64.

To view and manage user import profiles

Go to *Domain & User* > *User* > *User Import Profile*.

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

To configure user import profiles

1. Go to *Domain & User* > *User* > *User Import Profile*.
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.
Domain	Select the name of a protected domain to apply to the user import profile. You can see only the domains that are permitted by your administrator profile.
Search timeout	Define the synchronization query timeout period in seconds. Set the value between 60-600.
Type	Define the remote server type, either *LDAP* or *Microsoft 365*.
Tenant ID	Enter the Microsoft 365 tenant ID.
Application ID	Enter the Microsoft 365 application ID.
Application secret	Enter the Microsoft 365 application secret.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.
Port	Enter the port number where the LDAP server listens. The default port number varies by Secure LDAP connection. See also Appendix C: Port Numbers on page 1.

GUI item	Description
Secure LDAP connection	Enable to connect to the LDAP servers using an encrypted connection.
Protocol version	Select the LDAP server protocol version.
Scope	Define the search scope of the LDAP server, either *Base*, *One Level*, or *Subtree*.
Description	Optionally enter a description for the profile.
Default Bind Option	Click to expand and configure the following: • *Base DN*: Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for user objects, such as `ou=People,dc=example,dc=com`. User objects should be child nodes of this location. • *Bind DN*: Enter the bind DN, such as `cn=fortimail,dc=example,dc=com`, of an LDAP user account with permissions to query the Base DN. • *Bind password*: Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in Base DN, or, if you have not yet entered a *Base DN*, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your *Base DN*, or need to look up attribute names. For example, if the *Base DN* is unknown, browsing can help you to locate it. Before using, first configure *Server name/IP*, *Secure LDAP connection*, *Bind DN*, *Bind password*, and *Protocol version*, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.
User Query Option	Click to expand and configure the following: • *User query*: Enter the LDAP query string to get all users.For example, *(mail=*)* if using OpenLDAP. • *Display name attribute*: Enter the LDAP display name attribute, such *CN*. • *Primary address attribute*: Enter the LDAP user's primary email address attribute, such as *mail*. • *Secondary address attribute*: Enter the LDAP user's secondary email address attribute.
Group Query Option	Click to expand and configure the following: • *Group query*: Enter the LDAP query string to get all groups. • *Display name attribute*: Enter the LDAP group/mailinglist display name attribute. • *Primary address attribute*: Enter the LDAP group's primary email address attribute. • *Secondary address attribute*: Enter the LDAP group's secondary email address attribute.
Schedule	Click to expand and configure the following: • *Schedule*: Define a synchronization schedule of either Daily, Weekly, or Monthly (or none). If setting a weekly or monthly schedule, set the days of the week or days of the month that you wish to schedule synchronizations to occur. • *At hour*: Define the hour of the day at which synchronization will occur.

Configuring user aliases

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

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

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

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

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

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

Alternatively to configuring aliases locally, you can configure the FortiMail unit to query an LDAP directory. For details, see Configuring LDAP profiles on page 205.

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

To view and configure alias addresses

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

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

2. Either click *New* to add an alias or double-click an alias to modify it.
3. A dialog appears. Its features vary with the operation mode.

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

See also

Configuring address mappings

Configuring user alias options

Configuring mail routing

Configuring address mappings

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

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

Like aliases, address mappings translate email addresses.

Unlike aliases:

- Mappings cannot translate one email address into many.
- Mappings cannot translate an email address into one that belongs to an unprotected domain (this restriction applies to locally defined address mappings only; it is not enforced for mappings defined on an LDAP server).
- Mappings are applied bidirectionally, when an email is outgoing as well as when it is incoming to the protected domain.

- Mappings may affect both sender and recipient email addresses, and may affect those email addresses in both the message envelope and the message header, depending on the match condition.

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

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

Match evaluation and rewrite behavior for email address mappings

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

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

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

You can alternatively create address mappings by configuring the FortiMail unit to query an LDAP server that contains address mappings. For more information, see Configuring LDAP profiles on page 205.

To view and configure an address map list

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

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

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

GUI item	Description
Internal email address	Enter either an email address, such as `user1@example.com`, or an email address pattern, such as `*@example.com`, that exists in a protected domain. This email address is hidden when passing to the external network by being rewritten into the external email address according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 96.
External email address	Enter either an email address, such as `sales@example.com`, or an email address pattern, such as `*@example.net`, that exists in a protected domain. This email address is visible to the internal network, but will be rewritten into the internal email address according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 96. The external email address must **not** be within the same protected domain as the internal address. Otherwise, it may cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable.

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

See also

Configuring user aliases

Configuring address mapping options

Configuring mail routing

Configuring IBE users

You can send secured email with Identity Based Encryption (IBE) through the FortiMail Cloud unit. The IBE User option lets you manage the IBE mail users and IBE domains. For details about how to use IBE service, see FortiMail IBE configuration workflow on page 289.

This section contains the following topics:

Configuring active users

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

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

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

GUI item	Description
Delete (button)	Select to remove a selected user in the list. A deleted user cannot access the FortiMail unit.
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of a mailbox and empty a mailbox as required. The SecureMail mailbox contains the secured email for the user. The encrypted email are put into this mailbox if Pull is selected to retrieve IBE mail. The Bulk mailbox contains spam that are quarantined by the FortiMail unit.
Reset User (button)	Click to reset a mail user and require new login information to access the FortiMail unit. Resetting a user sends the user a new notification and the user needs to re-register on the FortiMail unit.
IBE domain	Select the name of an IBE domain to view its active users. For more information about IBE domain, see Configuring IBE authentication on page 100.
Search	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users redisplays with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
Enabled	Select the check box to activate a mail user. A disabled user cannot access the FortiMail unit.
Email	Displays the email address of mail users.
First Name, Last Name	Displays the first and last name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Recovery Email	Displays the recovery email address of the mail users.
Status	The mail user has four status possibilities:

GUI item	Description
	• Pre-registered: The FortiMail unit encrypts an email and sends a notification to the recipient. • Activated: The mail recipient registers on the FortiMail unit. • Password reset: When a mail recipient who is provided with new password to access the FortiMail unit has actually changed the password, this status appears. • LDAP: When a mail recipient. who belongs to an IBE domain bound with an LDAP profile authenticates on the FortiMail unit, this status appears. For more information about IBE domain, see Configuring IBE authentication on page 100.
Creation Time	Displays when IBE user was registered and created.
Last Access	Displays the time stamp when: • the FortiMail unit sends a notification (Pre-registered status) • the mail recipient registers on the FortiMail unit (Activated status) • a mail user changes the password (Password reset status) • a mail recipient, who belongs to an IBE domain, authenticates on the FortiMail unit (LDAP status)

See also

Configuring expired users

Configuring IBE authentication

Configuring expired users

Depending on the configuration of User registration expiry time and User inactivity expiry time in the IBE service, if email recipients fail to register or authenticate on the FortiMail unit, or fail to access the FortiMail unit after registration for a certain period of time, they become expired users. For more information about IBE service configuration, see Configuring IBE encryption on page 287.

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

GUI item	Description
Delete (button)	Select to remove a selected user in the list. A deleted user cannot access the FortiMail unit.
Maintenance (button)	Select a user and click this button to manage that user's mailboxes, such as Inbox, Drafts and Sent. You can check the size of a mailbox and empty a mailbox as required. The SecureMail mailbox contains the secured email for the user. The encrypted email are put into this mailbox if Pull is selected to retrieve IBE mail. The Bulk mailbox contains spam that are quarantined by the FortiMail unit.
Re-activate	Select the expired IBE user record(s) you wish to re-activate and select **Re-activate**. Any re-activated IBE users will move to the **Active User** tab.
Export	Select from the dropdown menu if you wish to **Export All** or **Export Selected** expired IBE users in comma-separated value (CSV) file format.

GUI item	Description
	Note that **Export All** will export all records on the current page. If you wish to export a larger number of records, set **Records per page** to a higher value (maximum of **500**).
Records per page	Define the maximum number of expired IBE user records appear on the current page.
IBE domain	Select the name of an IBE domain to view its active users. For more information about IBE domain, see Configuring IBE authentication on page 100.
Search	Enter the name of a user, or a partial user name with wildcards, and press Enter. The list of users redisplays with just those users that meet the search criteria. To return to the complete user list, clear the search field and press Enter.
Email	Displays the email address of mail users.
First Name, Last Name	Displays the first name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Last Name	Displays the last name of a mail user. This information appears when a mail user registers on the FortiMail unit.
Status	The mail user has four status possibilities: • **Pre-registered**: The FortiMail unit encrypts an email and sends a notification to the recipient. • **Activated**: The mail recipient registers on the FortiMail unit. • **Password reset**: When a mail recipient who is provided with new password to access the FortiMail unit has actually changed the password, this status appears. • **LDAP**: When a mail recipient. who belongs to an IBE domain bound with an LDAP profile authenticates on the FortiMail unit, this status appears. For more information about IBE domain, see Configuring IBE authentication on page 100.
Expiry Time	Displays when the user's registration expired.
Last Access	Displays the time stamp when the user was last active.

See also

Configuring active users

Configuring IBE authentication

Configuring IBE authentication

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

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

In both cases, the FortiMail unit will record the domain names of the recipients who register or authenticate on it under the IBE Domain tab. For details, see Viewing and managing IBE domains on page 102.

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 205.

To configure IBE authentication rules

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

GUI item	Description
Status	Select to enable this rule.
Domain pattern	Enter a domain name that you want to bind to an LDAP authentication profile. If you want all IBE users to authenticate through an LDAP profile and do not want other non-LDAP-authenticated users to get registered on FortiMail, you can use wildcard * for the domain name and then bind it to an LDAP profile. For more information about LDAP profiles, see Configuring LDAP profiles on page 205.
LDAP profile	Select the LDAP profile you want to use to authenticate the domain users.

User registration process with two-factor authentication

As of FortiMail 6.4.0, the enforcement of security questions has been removed and replaced with two-factor authentication, via email and/or SMS text message.

See Configuring IBE services on page 290 for more information on configuring two-factor authentication settings.

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

IBE user registration and check email process via email:

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

IBE user registration and check email process via SMS:

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

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

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

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

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

See also

Configuring active users

Viewing and managing IBE domains

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

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

GUI item	Description
Delete (button)	Select to remove a selected domain. Deleting a domain also disables all its users. These users cannot access the FortiMail unit until they receive new secure mail notifications from the FortiMail unit.
Remove All Users (button)	Select to delete all mail users in a selected domain. These users cannot access the FortiMail unit until they receive new secure mail notifications from the FortiMail unit.
Search (button)	Select to search IBE domains. A search dialog appears.
Active User Count	Displays the active mail users in a domain. For more information about active users, see Configuring active users on page 98.
Expired User Count	Displays the expired mail users in a domain. For more information about active users, see Configuring expired users on page 99.

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, or in gateway and/or transparent mode but only when *Email Continuity* is enabled under *System* > *FortiGuard* > *Licensed Feature*.

This section contains the following topics:

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 105.

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 107.

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 (dropdown 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 (dropdown 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 105. **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 107. 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 (dropdown 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 105. For more information on adding group names, see Adding contact groups (server mode only) on page 106.
Domain (dropdown 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 71.
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.
3. A dialog appears.
4. Enter information for the contact.

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.

5. Click Create or OK.
6. 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 205.
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 107.
New (button)	Click to create a new LDAP attribute mapping template. For details, see To view and configure an LDAP mapping list on page 107.
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 71.
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 contact groups

1. Go to *Domain & User* > *Address Book* > *Contact Group*.
2. From the Domain dropdown 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 71.
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 dropdown 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 105. **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 107. 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.

GUI item	Description
	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 205.

For information on retrieving the address book, see More > Import on page 104 and To import contacts from the LDAP server on page 105.

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.

Configuring LDAP synchronization tasks (server mode only)

Once you have configured your LDAP attribute mapping template and an LDAP profile, you can configure LDAP synchronization tasks that allow email continuity in the event of a mail service outage. Before doing so, you must configure your LDAP server. For details, see Configuring LDAP profiles on page 205.

For information on retrieving the address book, see More > Import on page 104 and To import contacts from the LDAP server on page 105.

To view and configure an LDAP synchronization task

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

GUI item	Description
LDAP profile	Select an LDAP profile from the dropdown menu. For details, see Configuring LDAP profiles on page 205.
LDAP mapping	Select an LDAP mapping list from the dropdown menu. For details, see Configuring LDAP attribute mapping template (server mode only) on page 107.
Synchronize to	Select a contact domain from the dropdown menu. Once the LDAP synchronization task is created, this selection cannot be changed.
Description	Optional description of the LDAP synchronization task.
Overwrite existing contacts	Enable to make modifications to the contact (if any) since the last LDAP address book synchronization. This option (enabled by default) is recommended in order to avoid duplicate entries.
Delete nonexistent contacts	Enable to remove any entries that no longer exist in the records since the last LDAP address book synchronization.
Schedule	Determine the timeframe for the LDAP synchronization tasks to be performed: either *Daily*, *Weekly*, or *Monthly*, configuring the appropriate time interval as required.

4. Click *Create*.

Sharing calendars and address books (server mode only)

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

To be specific, the following features are supported:

- FortiMail internal calendar sharing from/to FortiMail webmail users
- Internet calendar sharing from/to FortiMail webmail users
- Calendar sharing from/to Microsoft Outlook users using WebDAV (Outlook does not support CalDAV)
- Calendar sharing from/to Mozilla Thunderbird users using WebDAV or CalDAV
- Address book query from Outlook using LDAP

- Address book query from Thunderbird using LDAP
- Option to manually send reminders (organizer only)
- Organizer display name support

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

Calendar sharing

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

FortiMail calendar settings

To enable the WebDAV and CalDAV services

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

To create a calendar resource for sharing

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

FortiMail webmail settings

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

To access the WebDAV and CalDAV service URL

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

Thunderbird settings

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

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

To publish a calendar to FortiMail WebDAV service

1. In Thunderbird, go to *Events and Tasks* > *Calendar*.
2. Right-click on a calendar and select *Publish Calendar*.
3. For *Publishing URL*, enter the URL you get from the FortiMail webmail (see FortiMail webmail settings on page 109).
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 109).
5. Enter the display name and other settings, then click *Next*.
6. Enter the user name and password required for FortiMail authentication.
7. The new calendar will appear in the left calendar pane. And it can be synchronized with the FortiMail CalDAV service automatically or manually.

To configure the free/busy settings in Thunderbird

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

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

To schedule a meeting in Thunderbird

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

Outlook settings

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

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

To publish a calendar to FortiMail WebDAV service

1. In Outlook, go to *Go* > *Calendar*.
2. Right-click on a calendar and select *Publish to Internet*.
3. Select *Publish to WebDAV Server*.
4. In the popup window, enter the URL you get from the FortiMail webmail (see FortiMail webmail settings on page 109).
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 109).
5. Specify the folder name and description.
6. Click *OK*.

To configure the free/busy settings in Outlook 2007

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

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

To schedule a meeting in Outlook 2007

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

Address book sharing

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

FortiMail settings

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

To enable the LDAP service

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

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

By default, the LDAP service is enabled.

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

To create a policy

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

Thunderbird settings

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

To configure the address book LDAP settings in Thunderbird

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

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

To search contacts FortiMail address books

1. Go to *Edit* > *Advanced address book search*.
2. Specify the address book to be searched.
3. Enter the user name.
4. Click *Search*.

To download contacts from FortiMail address books

1. Open the address book in Thunderbird.
2. Click *Properties* of an address book.
3. Click *Offline*.
4. Click *Download Now*.
5. Enter the password of the binding user required for FortiMail authentication.

Outlook settings

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

To configure the address book LDAP settings in Outlook 2007

1. Go to *Tools* > *Account Setting*.
2. Select *Address Books*.
3. Click *New*.
4. Enter the server name or IP address of FortiMail.
5. Enter the user name and password.
   For example, User name: cn=user1,ou=people, dc=example, dc=com, assuming your user name is `user1`, your domain name is `example.com`.
   In this example, `user1` is a user under the protected domain `example.com` in FortiMail. The password is the same password used for `user1`'s domain.
6. Select *More Settings*.
7. Select the *Connection tab*.
8. Specify the display name and connection port.
9. Switch to the *Search* tab, and specify the *Search Base* to *Custom*: dc=example, dc=com.
10. Click *OK*.

To access FortiMail address books

1. Open the address book in Outlook.
2. Select the target address book.
3. Enter the user name you want to find.
4. Click *Go*.

Migrating email from other mail servers (server mode only)

If you already have other mail servers, such as Exchange or FortiMail server, and you want to consolidate the mail user and data into one FortiMail server, you can do so by migrating the users and data to your FortiMail unit.

The email migration process involves the following procedures:

1. **Preparation**
   a. Enable the mail migration feature using the following CLI commands (available in server mode only):
   ```
   config system global
      set email-migration-status enable
   end
   ```

   By default, the email migration feature does not appear on the GUI until you enable it with the above CLI commands.

   b. Define the remote mail server settings. For details, see Defining a remote mail server for mail migration on page 115.
   c. Create a domain for the to-be-migrated users. For details, see Creating domains for mail migration on page 115.
2. **User migration**

   Because FortiMail will act as an IMAP client on behalf of the users to get their email from the remote mail server, you must import the user/password information first. To do this, you can use one of the following methods:

   - If you only need to migrate email for a few users and you know the users' login credentials, you can manually enter their user name/password information by going to *Domain & User* > *Mail Migration* > *Migration User* and click *New*.
   - If you can export the user name/non-encrypted password list into a CSV file, you can import the CSV file by going to *Domain & User* > *Mail Migration* > *Migration User* and click *Action* > *Import* > *From .CSV File.*
   - If the to-be-migrated users already have accounts on the FortiMail server, you can import/copy the local user list to the migration user list by going to *Domain & User* > *Mail Migration* > *Migration User* and click *Action* > *Import* > *From Local Domain.*
   - If the user passwords are encrypted, you have to collect their passwords through FortiMail webmail login or SMTP client login. To do this:
     i. Create an authentication profile that uses the remote mail server as the authentication server. For details, see Configuring authentication profiles on page 202.
     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 138.
     iii. Use one of the following two methods to collect user passwords:
       i. Through FortiMail webmail login: Inform the users to log in to the FortiMail webmail portal, using their email addresses of the remote domain (the domain part needs to match proper authentication policy) and their passwords. Upon successful login, the users will be shown an empty webmail mailbox. This is because the email data has not been migrated yet and this step is only meant to collect user passwords.
       ii. Through SMTP client login: Inform the users to use the FortiMail host name as their outgoing mail server.

     After you have done the above, when the users try to send email, they will have to authenticate through FortiMail. Then FortiMail will record the user names and passwords into the migration user list under *Domain*

& User > *Mail Migration* > *Migration User*.

3. **Mail data migration**

   After you have migrated the users, you can start to migrate the their mail boxes from the remote server. To do this:

   a. Go to *Domain & User* > *Mail Migration* > *Migration User.*

   b. From the *Action* dropdown list, select *Migrate* > *Selected Users* or *All Users*.

   c. If needed, you can click the *Stop* and *Start* button to control the migration process.

   d. After the user's mail data is successfully migrated, you can export the user to the local user list by clicking *Action* > *Export* > *Selected Users* or *All Users*. The exported users will appear as local users under *User* > *User*.

Defining a remote mail server for mail migration

This is one of the email migration procedures. For the entire procedures, see Migrating email from other mail servers (server mode only) on page 114.

1. Go to *Domain & User* > *Mail Migration* > *Remote Mail Server.*
2. Click *New*.
3. Enter a name for the remote server.
4. Enter the host name or IP address of the remote server.
5. For Protocol, select either IMAP or IMAPS, FortiMail will act as an IMAP client on the users' behalf to get email from the remote server.
6. Enter the IMAP port number. See also Appendix C: Port Numbers on page 1.
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 114.

1. Go to *Domain & User* > *Domain* > *Domain.*
2. Click *New*.
3. Configure the settings as described in Configuring protected domains on page 71.

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 115.
7. Click *Create*.

See also:

Configuring protected domains

Configuring policies

The Policy menu lets you create policies that use profiles to filter email.

It also lets you control who can send email through the FortiMail unit, and stipulate rules for how it will deliver email that it proxies or relays.

Modify or delete policies and policy settings with care. Any changes made to a policy take effect immediately.

This section includes:

What is a policy?

A policy defines which way traffic will be filtered. It may also define user account settings, such as authentication type, disk quota, and access to webmail.

After creating the antispam, antivirus, content, authentication, TLS, or resource profiles (see Configuring profiles on page 144), 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 121)
- Recipient-based policies (see Controlling email based on sender and recipient addresses on page 138)
- IP-based policies (see Controlling email based on IP addresses on page 132)

Recipient-based policies versus IP-based policies

- Recipient-based policies

  The FortiMail unit applies these based on the recipient's email address or the recipient's user group. May also define authenticated webmail or POP3 access by that email user to their per-recipient quarantine. Since version 4.0, the recipient-based policies also check sender patterns.

- IP-based policies

  The FortiMail unit applies these based on the SMTP client's IP address (server mode or gateway mode), or the IP addresses of both the SMTP client and SMTP server (transparent mode).

Inbound versus outbound email

There are two types of recipient-based policies: inbound and outbound. The FortiMail unit applies inbound policies to the incoming mail messages and outbound policies to the outgoing mail messages.

Whether the email is inbound or outbound is decided by the domain name in the recipient's email address. If the domain is a protected domain, the FortiMail unit considers the message to be inbound and applies the first matching inbound recipient-based policy. If the recipient domain is not a protected domain, the message is considered to be outbound, and applies outbound recipient-based policy.

To be more specific, the FortiMail unit actually matches the recipient domain's IP address with the IP list of the protected SMTP servers where the protected domains reside. If there is an IP match, the domain is deemed protected and the email destined to this domain is considered to be inbound. If there is no IP match, the domain is deemed unprotected and the email destined to this domain is considered to be outbound.

IP-based policies are not divided into inbound and outbound types. The client IP address and, for transparent mode, the server IP address are only used to determine whether or not the IP-based policy matches.

See also

How to use policies

Controlling SMTP access and delivery

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

How to use policies

Use access control rules and delivery rules to control which SMTP clients can send email through an SMTP relay and how SMTP will deliver email that it proxies or relays.

Recipient-based policies are applied to individual email messages based on the recipient's email address.

IP-based policies are applied based on the IP address of the connecting SMTP client and, if the FortiMail Cloud unit is operating in transparent mode, the SMTP server.

See also

What is a policy?

Whether to use IP-based or recipient-based policies

Order of execution of policies

Which policy/profile is applied when an email has multiple recipients?

Whether to use IP-based or recipient-based policies

Since there are two types of policies, which type should you use?

You can use either or both.

Exceptions include the following scenarios, which require IP-based policies:

- mail hosting service providers
  There is a great number of domains, and it is not feasible to configure them all as protected domains on the FortiMail Cloud 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 Cloud unit, an IP-based policy must be created in order to apply a session profile. Session profiles are only available in IP-based policies.
- differentiated services based on the network of origin
  To apply antispam and antivirus protection based on the IP address of the SMTP client or based on a notion of the internal or external network, rather than the domain in a recipient's email address, you must use an IP-based policy.

As a general rule, it is simpler to use IP-based policies. Use recipient-based policies only where they are required, such as when the policy must be tailored for a specific email address.

For webmail login, select an appropriate **Authentication type** and **Authentication profile** under **Authentication and Access** when configuring an inbound recipient-based policy. This option is only available when the FortiMail unit is operating in either Gateway or Transparent mode.

IP-based policy authentication does not support webmail login.

For example, if your company is an ISP, you can use recipient-based policies to apply antispam and antivirus profiles for only the customers who have paid for those services.

If both a recipient-based policy and an IP-based policy match the email, unless you have enabled *Take precedence over recipient based policy match* in the IP-based policy, the settings in the recipient-based policy will have precedence.

See also

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

Order of execution of policies

Arrange policies in the policy list by placing the most specific policy at the top and more general policies at the bottom.

For example, a recipient-based policy created with an asterisk (*) entered for the user name is the most general policy possible because it will match all users in the domain. When you create more specific policies, you should move them above this policy. Otherwise, the general policy would always match all email for the domain, and no other recipient-based policy would ever be applied.

FortiMail Cloud 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 Cloud unit looks for a matching IP-based policy.
   The FortiMail Cloud 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 Cloud 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 Cloud unit applies the profiles in the IP-based policy. In this case, it ignores recipient-based policies in the following two steps and jumps to step The FortiMail Cloudunit applies the profiles in the matching IP-based policy, if any, only if you have enabledTake precedence over recipient based policy matchin the IP-based policy, or if there is no recipient-based policy match3. on page 120.

3. The FortiMail Cloud unit looks for a matching recipient-based policy.
   The FortiMail Cloud 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 Cloud unit does not evaluate subsequent recipient-based policies.
4. The FortiMail Cloud unit applies the profiles in the matching recipient-based policy, if any.
5. The FortiMail Cloudunit 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 match3.

If SMTP traffic does not match any IP-based or recipient-based policy, it is allowed. However, no antivirus or antispam protection may be applied.
If you are certain that you have configured policies to match and allow all required traffic, you can tighten security by adding an IP policy at the bottom of the policy list to reject all other, unwanted connections.

See also

Controlling email based on sender and recipient addresses

Controlling email based on IP addresses

Which policy/profile is applied when an email has multiple recipients?

When applying recipient-based policies, an email message with multiple recipients is treated as if it were multiple email messages, each with a single recipient. This allows a fine degree of control for each recipient, but also means that separate recipient-based policies may block the email for some recipients but allow it for others.

Exceptions include use of an antivirus profile. In this case, the FortiMail Cloud unit will treat an email with multiple recipients as a single email. Starting with the first recipient email address, the FortiMail Cloud unit will look for a matching recipient-based policy. If none is found, the FortiMail Cloud unit will evaluate each subsequent recipient email address for a matching policy. The FortiMail Cloud 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 Cloud unit will apply the antivirus profile from the IP-based policy, if any.

If no recipient-based or IP-based policy matches, no profiles is applied.

See also

Controlling email based on sender and recipient addresses

Controlling SMTP access and delivery

The *Policy* > *Access Control* submenu lets you configure access control 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 Cloud unit. For details, see Configuring the network interfaces.

Access control rules are categorized separately based on whether they affect either the receipt or delivery of email messages by the FortiMail Cloud unit; that is, whether the FortiMail Cloud unit initiated the SMTP session or was the destination. Incoming/outgoing does not apply in the same sense for ACLs. Matching the domain name portion of the `HELO/EHLO` or sender address to a protected domain is not the core issue; rather, it is whether or not the FortiMail unit is the connection initiator.

See also

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 Cloud unit (initiated by SMTP clients).

Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail Cloud unit will process and relay/proxy, reject, or discard email messages in SMTP sessions.

When an SMTP client tries to send email through the FortiMail Cloud unit, the FortiMail Cloud unit compares each access control rule to the commands used by the SMTP client during the SMTP session, such as:

- sender email address in the SMTP envelope (`MAIL FROM:`)
- recipient email address in the SMTP envelope (`RCPT TO:`)
- authentication (`AUTH`)
- session encryption (`STARTTLS`).

Rules are evaluated for a match in sequential order, from top to bottom of the list. If all attributes of a rule match, then the FortiMail Cloud unit applies the action in the rule or TLS profile, and stops match evaluation. Remaining access control rules, if any, are not applied.

Only one access control rule is applied to an SMTP session.

If no access control rules exist, or none match, then the action varies by whether the SMTP client authenticated:

- **Authenticated**: Email is relayed/proxied.
- **Not authenticated**: Default action is performed.

The default action varies by whether or not the recipient email address in the SMTP envelope (`RCPT TO:`) is a member of a protected domain:

- **Protected domain**: Relay/proxy with greylisting.
- **Not protected domain**:Reject.

See also Configuring protected domains on page 71.

Rejecting unauthenticated SMTP clients that send email to unprotected domains prevents your email service from becoming an open relay. Open relays are abused by spammers, and therefore DNSBLs block them, so this FortiMail behavior helps to protect the reputation of your email server. Senders can deliver email incoming to your protected domains, but cannot deliver email outgoing to unprotected domains

If you want to allow your email users or email servers to send email to unprotected domains, then you must configure at least one access control rule. You may need to configure more access control rules if, for example, you want to discard or reject email from:

- specified email addresses, such as ones that no longer exist in your protected domain
- specified SMTP clients, such as a spammer that is not yet known to public blocklists

Like IP-based policies, access control rules can reject connections based on IP address.

Unlike IP-based policies, however, access control rules **cannot** affect email in ways that occur after the session's `DATA` command, such as by applying antispam profiles. Access control rules also cannot be overruled by recipient-based policies, and cannot match connections based on the SMTP server (which is always the FortiMail unit itself, **unless** the FortiMail Cloud unit is operating in transparent mode). For more information on IP-based policies, see Controlling email based on IP addresses on page 132.

For information about the sequence in which access control rules are used relative to other antispam methods, see Order of execution.

If possible, verify configuration of access control rules in a testing environment before applying them to a FortiMail Cloud unit in production environments. Failure to verify actions can result in incorrectly handled email delivery.

Do **not** create an access control rule where:

- Sender is `*`
- Recipient is `*`
- Authentication status is *Any*
- TLS profile is *None*
- Action is *Relay*

This creates an open relay, which could result in other MTAs and DNSBL servers blocklisting your protected domain.

To configure an access control rule

1. Go to *Policy* > *Access Control* > *Receiving*.

GUI item	Description
Move (button)	Select a policy, click *Move*, then select either: • *Up* or *Down* • *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 Cloud 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	Displays the pattern that defines matching email senders).
Recipient	Displays the pattern that defines matching email recipients.
Source	Displays the IP address and netmask of the SMTP client attempting to deliver the email message.
Reverse DNS Pattern	Displays whether a reverse DNS look-up is used for matching.
Authentication Status	Displays whether authentication status is used for matching.
TLS Profile	Displays the TLS profile, if any, used to allow or reject an SMTP session.
Actions	Displays the action to take when SMTP sessions match the rule (unless a TLS profile is used).

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	Select either *User Defined* and enter a complete or partial sender email address to match, or select: • *Internal*: Match any email address from a protected domain. • *External*: Match any email address from an unprotected 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 240. • *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

GUI item	Description
	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=$s)))` **c.** Set the ACL rule action to *Reject*. This will match a sender that is not in the allowedSenders list of the recipient and reject email from such senders. • *Regular Expression*: Use regular expression syntax instead of wildcards to specify the pattern. Optionally, click *Validate* to test regular expressions and string text.See Using wildcards and regular expressions on page 126. • *User Defined*: Specify the email addresses. The pattern can use wildcards or regular expressions. See Appendix D: Regular expressions. For example, the sender pattern `*@example.???` will match messages sent to any email user at example.com, example.net, or any “example” domain ending with a three-letter top-level domain name.
Recipient	Either select *User Defined* and enter a complete or partial recipient email address to match, or select: • *Internal*: Match any email address from a protected domain. • *External*: Match any email address from a domain that is **not** protected. • *Email Group*: Match any email address in the group. If you select this option, select an email group from the Email Group Selection field. Click New to add a new group, or Edit to modify an existing one.See also Configuring email groups on page 240. • *LDAP Group*: Match any email address in the group. If you select this option, select an LDAP profile from the LDAP Profile field. • *LDAP Verification*: Match any individual email address queried by the LDAP profile. If you select this option, select an LDAP profile from the dropdown list or click New to create a new one. **Note**: Use `$m` to match recipient addresses. • *Regular Expression*: Use regular expression syntax instead of wildcards to specify the pattern. Optionally, click *Validate* to test the regular expression. See Using wildcards and regular expressions on page 126. • *User Defined*: Specify the email addresses. The pattern can use wildcards or regular expressions.
Source	Specify the source IP address of the SMTP client attempting to send the email message, using one of these types: • *IP/Netmask*: Enter the IP address and netmask of the SMTP client. For example, you can enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. In the access control rule table, this appears as `10.10.10.0/24`, with the `0` indicating that any value is matched in that position of the address. Similarly, if you enter `10.10.10.10/32`, it appears as `10.10.10.10/32` because a 32-bit netmask only matches one address, 10.10.10.10 specifically. To match any address, enter `0.0.0.0/0`.

GUI item	Description
	• *IP Group*: Select an IP group, click *New* to add a new group, or click *Edit* to modify an existing one. See also Configuring IP groups on page 240. • *GeoIP Group*. Select a GeoIP group, or lick *New* to add a new group, or click *Edit* to modify an existing one. See also Configuring GeoIP groups on page 241. • *ISDB*: Select an ISDB. The Internet Service Database (ISDB) is an automatically updated collection of IP addresses and subnets used by popular services such as Microsoft 365 or 8x8.
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 `HELO/EHLO` are self-reported by the connecting SMTP server and easy to fake, the FortiMail Cloud unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail Cloud 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. If you enable *Regular Expression*, you may optionally click *Validate* to test regular expressions and string text. See Using wildcards and regular expressions on page 126. 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 because it is reserved for testing on private networks, not the Internet, and thus the FortiMail Cloud unit cannot successfully perform a reverse DNS query for it.
Authentication status	Select whether or not to match this access control rule based on whether the sender authenticates with the FortiMail Cloud unit. • *Any*: Do not consider client authentication. • *Authenticated*: Match this rule only if the client authenticates. • *Not Authenticated*: Match this rule only if the client did **not** authenticate.
TLS profile	Optional. Select a TLS profile to allow or reject the connection based on whether the session attributes match the TLS profile. • If matching, perform, the access control rule action. • If **not** matching, then perform the TLS profile *Failure* action instead. Click *New* to add a new TLS profile, or *Edit* to modify an existing one. See Configuring TLS security profiles on page 235.
Action	Select which delivery action the FortiMail Cloud unit will perform for SMTP sessions that match this access control rule. • *Reject*: Reject delivery of the email (SMTP reply code `550 Relaying denied`). • *Discard*: Accept the email (SMTP reply code `250 OK`), but then silently delete it and do not deliver it. • *Relay*:Accept the email (SMTP reply code `250 OK`), regardless of authentication or protected domain. **Do not greylist**, but continue with remaining antispam and other scans. If all scans pass, the email is delivered. • *Safe*: Accept the email (SMTP reply code `250 OK`) if the sender authenticates or

GUI item	Description
	skip remaining antispam scans and but continue with others such as antivirus. Otherwise, if the sender does not authenticate, or the recipient does not belong to a protected domain, then reject delivery of the email (SMTP reply code `554 5.7.1 Relaying denied`). In older FortiMail Cloud versions, this setting was named *Bypass*. • *Safe & Relay*: Like *Safe*, except **do not greylist**. • *Receive*: Like *Relay*, except **greylist**, and require authentication or protected domain. Otherwise, if the sender does not authenticate or the recipient does not belong to a protected domain, then FortiMail Cloud rejects (SMTP reply code `554 5.7.1 Relaying denied`). **Tip:** Usually, the *Receive* action is used when you need to apply a TLS profile, but do not want to safelist nor allow outbound, which *Relay* does. If you do **not** need to apply a TLS profile, then a rule with this action is often not required because by default, email inbound to protected domains is relayed/proxied.
Comments	Optional. Enter a descriptive comment. The comment will appears as a mouse-over tooltip in the ID column of the rule list.

4. Click *Create or OK*.
5. 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.

Initially, the access control rule appears at the bottom of the list of access control rules. As a result, the rule will match an SMTP session only if no previous access control rule matches.

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.

Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. General regular expression validation can be carried out under *System* > *Utility* > *Regex Validator*. See also Syntax on page 1.

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.

When configuring access control rules, **do not leave** any pattern fields blank. Instead, if you want the FortiMail Cloud unit to 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*, then the asterisk matches all recipient addresses, and therefore will not exclude any SMTP sessions from matching the access control rule.

See also

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, then you might configure the following access control rule:

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`

See also

Configuring access control rules

Example: Access control rules with regular expressions

Controlling SMTP access and delivery

Example: Access control rules with regular expressions

Example Corporation uses a FortiMail Cloud unit operating in gateway mode, and that has been configured with only one protected domain: example.com. The FortiMail Cloud unit was configured with the access control rules illustrated in the following table.

Examples of access control rules

ID	Sender Pattern	Recipient Pattern	Sender IP/Netmask	Reverse DNS Pattern	Authentication	Action
1	-/*	-/user932@example.com	0.0.0.0/0	-/*	Any	Reject
2	R/^\s*$	-/*	0.0.0.0/0	-/*	Any	Reject
3	-/*	-/*@example.com	172.20.120.0/24	-/mail.example.org	Any	Relay

ID	Sender Pattern	Recipient Pattern	Sender IP/Netmask	Reverse DNS Pattern	Authentication	Action
4	-/*@example.org	-/*	0.0.0.0/0	-/*	Any	Reject
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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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*.

See also

Configuring access control rules

Example: Access control rules with wild cards

Controlling SMTP access and delivery

Configuring delivery rules

The Delivery tab displays a list of delivery rules that apply to SMTP sessions being **initiated** by the FortiMail Cloud unit in order to deliver email.

Delivery rules let you to require TLS for the SMTP sessions the FortiMail Cloud 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 287.

When initiating an SMTP session, the FortiMail Cloud 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 Cloud 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 Cloud 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 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 234.
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 237.

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 Cloud 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 Cloud 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 235.
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 237 and Configuring certificate bindings on page 292. For information about content action profiles, see Configuring content action profiles on page 195.

GUI item	Description
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 blocklisted 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 80). 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.
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.
Restrict the number of recipients per message	Specify to limit the number of email recipients per message. 0 means no limit.

See also

What is a policy?

How to use policies

Incoming versus outgoing email messages

Which policy/profile is applied when an email has multiple recipients?

Controlling email based on IP addresses

The IP Policies section of the Policies tab lets you create policies that apply profiles to SMTP connections based on the IP addresses of SMTP clients and/or servers.

Due to the nature of relay in SMTP, an SMTP client is not necessarily always located on an email user's computer. The SMTP client is the connection initiator; it could be, for example, another email server or a mail relay attempting to deliver email. The SMTP server, however, is always a mail relay or email server that receives the connection.

For example, if computer A opened a connection to computer B to deliver mail, A is the client and B is the server. If computer B later opened a connection to computer A to deliver a reply email, B is now the client and A is now the server.

Like access control rules, IP-based policies can reject connections based on IP address.

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 121.

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 118.

If SMTP traffic does not match any IP-based or recipient-based policy, it is allowed. However, no antivirus or antispam protection may be applied.
If you are certain that you have configured policies to match and allow all required traffic, you can tighten security by adding an IP policy at the bottom of the policy list to reject all other, unwanted connections.
To do this, create a new IP policy, enter `0.0.0.0/0` as the client IP/netmask, and set the action to Reject. See the following procedures about how to configure an IP policy. Then, move the policy to the very bottom of the IP policy list. Because this policy matches any connection, all connections that do not match any other policy will match this final policy, and be rejected.

Profiles used by the policy, if any, are listed in the policy table, and appear as linked text. To modify profile settings, click the name of the profile.

Domain administrators can create and modify IP-based policies. Because they can affect any IP address, a domain administrator could therefore create a policy that affects another domain. If you do not want to allow this, do **not** grant Read-Write permission to the Policy category in domain administrators' access profiles.

For details, see About administrator account permissions and domains on page 44.

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

GUI item	Description
	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 119 and Which policy/profile is applied when an email has multiple recipients? on page 120
Source	Displays the IP address, IP group, GeoIP, or Internet Service Database (ISDB) entry of the SMTP source to which the policy applies. The ISDB is a comprehensive public IP address database that combines IP address range, IP owner, port number, and IP security credibility. The data comes from the FortiGuard service system. Information is regularly added to this database, for example, geographic location, IP reputation, popularity, DNS, and so on. All this information helps users define Internet security more effectively. You can use the contents of the database as criteria for inclusion or exclusion in a policy.
Destination	Displays the IP address of the destination IP to which the policy applies. **Note**: For FortiMail Cloud users, this field doesn't take effect.
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 144.
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 160.
AntiVirus	Displays the name of the antivirus profile applied by this policy. To modify the or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring antivirus profiles, file signatures, and antivirus action profiles on page 181.
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 186.
DLP (if DLP is enabled on GUI)	Displays the name of the DLP profile applied by this policy. To modify the or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring DLP profiles on page 298.
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 202

GUI item	Description
Exclusive	Indicates whether or not Take precedence over recipient based policy match on page 137 is enabled in this policy. See Order of execution of policies on page 119 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 240. • GeoIP group. See Configuring GeoIP groups on page 241. • ISDB To match all clients, enter `0.0.0.0/0`.
Destination	**Note**: **For FortiMail Cloud users, this field doesn't take effect**. 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 240. To match all servers, enter `0.0.0.0/0`. If the FortiMail unit runs in gateway or server mode, the destination will be the FortiMail unit itself. But if you use virtual hosts on the FortiMail unit, you can specify which virtual host (IP/subnet or IP group) the email is destined to. Otherwise, you do not have to specify the destination address. If you use virtual hosts, you must also configure the MX record to direct email to the virtual host IP addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well.
Action	Select whether to: • Scan: Accept the connection and perform any scans configured in the profiles selected in this policy. • Reject: Reject the email and respond to the SMTP client with SMTP reply code 550, indicating a permanent failure. • Fail Temporarily: Reject the email and respond to the SMTP client with SMTP reply code 451, indicating to try again later. • *Proxy Bypass*: Bypass the FortiMail proxy without scanning. Note that this action is for

GUI item	Description
	transparent only.
Comment	Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.
Profiles	
Session	Select the name of a session profile to have this policy apply. This option is applicable only if Action on page 135 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 135 is Scan.
AntiVirus	Select the name of an antivirus profile to have this policy apply. This option is applicable only if Action on page 135 is Scan.
Content	Select the name of a content profile to have this policy apply. This option is applicable only if Action on page 135 is Scan.
DLP (if DLP is enable on GUI)	Select the name of a DLP profile to have this policy apply. This option is applicable only if Action on page 135 is Scan.
Authentication and Access (not available in server mode)	This section appears only if the FortiMail unit is operating in gateway or transparent mode. For server mode, select a resource profile instead. For more information on configuring authentication, see Workflow to enable and configure authentication of email users on page 201.
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 142 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 23.
Authentication profile	Select an existing authentication profile to use with this policy. Click New to create on or Edit to modify the selected profile.
Allow SMTP authentication	Enable to allow the SMTP client to use the SMTP `AUTH` command, and to use the server defined in Authentication profile on page 142 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile on page 142.

		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 121.
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 118. Note that if there is no authentication profile in a recipient based policy, but there is an authentication profile in an IP-based policy, SMTP authentication can still succeed without this feature enabled. This option is applicable only if Action on page 135 is Scan. **Note:** Enabling this option also causes the FortiMail unit to ignore the option Configuring protected domains on page 71 in the protected domain.

See also

Example: Strict and loose IP-based policies

Example: Strict and loose IP-based policies

You have a FortiMail unit running in gateway mode to protect your internal mail server (192.168.1.1). The FortiMail unit receives email incoming to, and relays email from, the internal mail server.

You can create two IP-based policies:

- Policy 1: Enter `192.168.1.1/32` as the source IP address and `0.0.0.0/0` as the destination to match outgoing email connections from the mail server, and select a **loose** session profile, which may have sender

reputation and other similar restrictions disabled, since the sender (that is, source IP) will always be your mail server.

- Policy 2: Enter `0.0.0.0/0` as the source IP address and `0.0.0.0/0` as the destination IP address to match incoming email connections from all other mail servers, and select a **strict** session profile, which has all antispam options enabled.

You would then move policy 1 above policy 2, as policies are evaluated for a match with the connection in order of their display on the page.

See also

Controlling email based on IP addresses

Controlling SMTP access and delivery

Controlling email based on sender and recipient addresses

Go to *Policy* > *Recipient Policy* to create recipient-based policies based on the incoming or outgoing directionality of an email message with respect to the protected domain.

Recipient-based policies have precedence if an IP-based policy is also applicable but conflicts. Exceptions include IP-based policies where you have enabled Take precedence over recipient based policy match on page 137. 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 118.

If the FortiMail Cloud 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 132.
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 71)
- 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 83 or Configuring LDAP profiles on page 205)
- at least one PKI user, if you will allow or require email users to access their per-recipient quarantine using PKI authentication (see Managing users on page 83)

About the default system policy

Starting from FortiMail 5.4.0, an inbound and outbound default system-level recipient policy has been added. If enabled, the default system policy will be checked before any other policies. If the email matches the default system policy, no other policies will be checked.

The default system policy provides the following conveniences:

- If many domains will be using identical policies, you can just modify the default system policy for the domains to use.
- When troubleshooting profiles and policies, you can temporarily use the system policy for all domains while disabling other policies, so that you can examine the profiles and policies.

If the system policies are not visible, turn on the *Show system policy* switch.

To view recipient-based policies

Go to *Policy* > *Recipient Policy* > *Inbound* or *Policy* > *Recipient Policy* > *Outbound* to view a list of applicable policies.

GUI item	Description
Move (button)	FortiMail Cloud units match the policies for each domain in sequence, from the top of the list downwards. Therefore, you must put the more specific policies on top of the more generic ones. To move a policy in the policy list: 1. Select a domain. **Note**: If *Domain* is set to *All*, the *Move* button is disabled. When *Domain* is set to a particular domain, *Show system policy* must be disabled in order to move domain policies. 2. Click a policy to select it. 3. Click Move, then select either: • the direction in which to move the selected policy (Up or Down), or • After or Before, then in Move right after or Move right before indicate the policy's new location by entering the ID of another policy.
Domain (dropdown list)	• All: Select to display both system-level and domain-level policies. • System: Select to display system-level policies. • <domain>: Select one domain to display this domain's policies. Use the *Show system policy* switch to display or hide the system-level policies when you view all policies or domain-level policies. If you are a domain administrator, you can only see the domains that are permitted by your administrator profile.
Enabled	Select whether or not the policy is currently in effect.
ID	Displays the number identifying the policy. If a comment is added to this rule when the rule is created, the comment will show up as a mouse-over tool-tip in this column. **Note:** This may be different from the order in which they appear on the page, which indicates order of evaluation. FortiMail Cloud units evaluate policies in sequence. More than one policy may be applied. For details, see Order of execution of policies on page 119 and Which policy/profile is applied when an email has multiple recipients? on page 120
Domain Name (column)	Indicates which part the policy is used for: either system wide or a specific protected domain.
Sender Pattern	A sender email address (`MAIL FROM:`) as it appears in the envelope or a regular expression pattern to match sender email addresses. See also Syntax on page 1.

GUI item	Description
Recipient Pattern	A recipient email address (`RCPT TO:`) as it appears in the envelope or a regular expression pattern to match recipient email addresses. See also Syntax on page 1.
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 160.
AntiVirus	Displays the antivirus profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring antivirus profiles, file signatures, and antivirus action profiles on page 181.
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 186.
DLP (if DLP is enable on GUI)	Displays the DLP profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring data loss prevention on page 295.
Resource (server mode and gateway mode)	Displays the resource profile selected for the matching recipients. To modify or view a profile, click its name. The profile appears in a pop-up window. For details, see Configuring resource profiles on page 199.
Authentication (not in server mode; inbound only)	Displays the authentication profile selected for the matching recipients. To modify or view a profile, click its name.The profile appears in a pop-up window. For details, see Configuring authentication profiles on page 202 or Configuring LDAP profiles on page 205.

To configure recipient-based policies

1. Go to *Policy* > *Recipient Policy* > *Inbound* or *Policy* > *Recipient Policy* > *Outbound*, either click New to add a policy or double-click a policy to modify it.
   A multisection dialog appears.
2. Select Enable to determine whether or not the policy is in effect.
3. For *Domain*, select either *System* or the domain name that this profile will be used for.
4. Enter a comment if necessary. The comment will appears as a mouse-over tool-tip in the ID column of the rule list.
5. Configure the following sections, as applicable:
   - Configuring the sender and recipient patterns on page 140
   - Configuring the profiles section of a recipient policy on page 141
   - Configuring authentication for inbound email on page 142
   - Configuring the advanced settings of inbound policies on page 142

Configuring the sender and recipient patterns

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 (wildcard)*: Enter a sender email address. • *User (regex)*: Enter a sender as a regular expression pattern, such as `*@example.com`. Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. See also Syntax on page 1. • *Local group (server mode only)*: Select the name of a protected domain in the second dropdown list, then select the name of a user group in the first dropdown list. • *LDAP group*: Select an LDAP profile in which you have enabled and configured a group query, then enter either the group's full or partial membership attribute value as it appears in the LDAP directory. Depending on your LDAP directory's schema, and whether or not you have enabled Use group name with base DN as group DN, this may be a value such as `1001`, `admins`, or `cn=admins,ou=Groups,dc=example,dc=com`. • *Email address group*: Select an email group from the dropdown list. For details about creating an email group, see Configuring email groups on page 240. 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 dropdown lists is the domain profile, not the system profile. Thus, only the domain profile will be selected.

GUI item	Description
AntiSpam	Select which antispam profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Managing antispam profiles on page 160. **Tip:** You can use an LDAP query to enable or disable antispam scanning on a per-user basis.
AntiVirus	Select which antivirus profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring antivirus profiles, file signatures, and antivirus action profiles on page 181.
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 186.
DLP	Select which DLP profile, if any, to apply to email matching the policy.

GUI item	Description
(if enabled)	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 298.
Resource (server mode and gateway mode)	Select which resource profile, if any, to apply to email matching the policy. If you have not yet configured the profile that you want to apply, click New to add the profile in a pop-up dialog. If you need to modify an existing profile before applying it, click Edit. For details, see Configuring resource profiles on page 199.

Configuring authentication for inbound email

The Authentication and Access section appears only for inbound policies.

When FortiMail authenticates a user, it checks the authentication profile in the matching recipient policy.

Note that for outbound email, when FortiMail requires authentication with the sender, FortiMail will lookup authentication profiles for the defined recipient patterns within inbound policies.

For more information on configuring an authentication profile, see Workflow to enable and configure authentication of email users on page 201.

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 142 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 23.
Authentication profile	Select an existing authentication profile to use with this policy.
Allow SMTP authentication (gateway and transparent mode only)	Enable to allow the SMTP client to use the SMTP `AUTH` command, and to use the server defined in Authentication profile on page 142 to authenticate the connection. Disable to make SMTP authentication unavailable. This option is available only if you have selected an Authentication profile on page 142. **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 121.

Configuring the advanced settings of inbound policies

The Advanced Setting section appears for both inbound and outbound policies.

GUI item	Description
Reject different SMTP sender identity for authenticated user	Enable to require that the sender uses the same identity for: authentication name, SMTP envelope `MAIL FROM:`, and header `FROM:`. Disable to remove such requirements on sender identities. By default, this feature is disabled.
Sender identity verification with LDAP server for authenticated user	In some cases, while you do not want to allow different SMTP sender identities for an authenticated user, you still want to: • allow users to authenticate with their identities (for example, user1@example.com) and send email from their proxy email addresses (for example, user1.name@example.com and user1name@example.com) • or to allow users in an alias group to authenticate with their own identities (for example, salesperson1@example.com) and send email from their alias group address (for example, sales@example.com) Then you can choose to verify the sender identity with the LDAP server. If the verification is successful, the sender will be allowed to send email with different identities. **Note**: When the above rejection option is enabled, even though the authentication identity can be different from the sender identity upon successful LDAP verification. the envelope (`MAIL FROM:`) address is never allowed to be different from the header `FROM:`) address. And the two addresses cannot be empty either.
Enable PKI authentication for web mail access (Inbound policy only)	Enable if you want to allow web mail users to log in by presenting a certificate rather than a user name and password. Also configure Certificate validation is mandatory on page 143. For more information on configuring PKI users and what defines a valid certificate, see Managing users on page 83.
Certificate validation is mandatory (Inbound policy only)	If the email user's web browser does not provide a valid personal certificate, the FortiMail Cloud unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enable this option.

Configuring profiles

The *Profile* menu lets you configure many types of profiles. These are a collection of settings for antispam, antivirus, authentication, or other features.

After creating and configuring a profile, you can apply it either directly in a policy, or indirectly by inclusion in another profile that is selected in a policy. Policies apply each selected profile to all email messages and SMTP connections that the policy governs.

Creating multiple profiles for each type of policy lets you customize your email service by applying different profiles to policies that govern different SMTP connections or email users. For instance, if you are an Internet service provider (ISP), you might want to create and apply antivirus profiles only to policies governing email users who pay you to provide antivirus protection.

Configuring session profiles

Session profiles focus on the connection and envelope portion of the SMTP session. This is in contrast to other types of profiles that focus on the message header, body, or attachments.

To configure session profiles

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to add a profile or double-click a profile to modify it.
3. For a new session profile, type the name in Profile name. The profile name is editable later.
4. Configure the following sections:
   - Configuring connection settings on page 144
   - Configuring sender reputation options on page 145
   - Configuring endpoint reputation options on page 148
   - Configuring sender validation options on page 148
   - Configuring session settings on page 150
   - Configuring unauthenticated session settings on page 152
   - Configuring SMTP limit options on page 154
   - Configuring error handling options on page 155
   - Configuring header manipulation options on page 156
   - Configuring list options on page 156
   - Configuring advanced MTA control settings on page 157

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 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Expand the Connection Setting section if needed. The options vary with the operation mode.
4. Configure the following options to restrict the number and duration of connections to the FortiMail Cloud unit. When any of these limits are exceeded, the FortiMail Cloud 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 Cloud unit to the protected SMTP server. Disable to replace the SMTP client's IP addresses or domain names with that of the FortiMail Cloud unit. **Note:** Unless you enabled Take precedence over recipient based policy match in the IP-based policy, the Hide the transparent box option in the protected domain supersedes this option, and may prevent it from applying to incoming email messages. **Note:** For full transparency, also enable Configuring protected domains on page 71.
Restrict the number of connections per client per 30 minutes to	Specify the maximum connections per client IP address in a period of 30 minutes. 0 means no limit.
Restrict the number of messages per client per 30 minutes to	Specify the maximum email messages (number of MAIL FROM) a client can send in a period of 30 minutes. 0 means no limit.
Restrict the number of recipients per client per 30 minutes to	Specify the maximum recipients (number of RCPT TO) a client can send email to for a period of 30 minutes. 0 means no limit.
Maximum concurrent connections for each client	Enter the maximum number of concurrent connections per client. 0 means no limit.
Connection idle timeout (seconds)	Enter a limit to the number of seconds a client may be idle before the FortiMail Cloud unit drops the connection. Set the value between 5-1200.
Do not let client connect to blocklisted SMTP servers (transparent mode only)	Enable to prevent clients from connecting to SMTP servers that have been blocklisted in antispam profiles or, the FortiGuard AntiSpam service if enabled. **Note:** This option applies only if you have enabled "Use client-specified SMTP server to send email" on page 259, and only for outgoing connections.

Configuring sender reputation options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

You can also view the sender reputation statuses by going to *Monitor* > *Sender Reputation*. See Viewing sender reputation statuses on page 38.

To configure sender reputation options

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click to expand Sender Reputation.
   Sender reputation is a predominantly automatic antispam feature, requiring little or no maintenance. For each connecting SMTP client (sometimes called a sender), the sender reputation feature records the sender IP address and the number of good email and bad email from the sender.
   In this case, bad email is defined as:
   - Spam
   - Virus-infected
   - Unknown recipients
   - Invalid DKIM
   - Failed SPF check

   
   Sender reputation scores can be affected by sender validation results.

   
   Enabling sender reputation can improve performance by rejecting known spammers before more resource-intensive antispam scans are performed.
4. Configure the following:

GUI item	Description
Enable sender reputation	Enable to accept or reject email based upon sender reputation scores. The following options have no effect unless this option is enabled. This option may not function well for SMTP clients with dynamic IP addresses. Instead, consider “Enable Endpoint Reputation” on page 316.
Throttle client at	Enter a sender reputation score over which the FortiMail Cloud unit will rate limit the number of email messages that can be sent by this SMTP client. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increases or decreases the sender reputation scores accordingly. The enforced rate limit is either Restrict number of emails per hour to n or Restrict email to n percent of the previous hour, whichever value is greater. After the sender reaches the limit, no more incoming email will be accepted.
Restrict number of emails per hour to	Enter the maximum number of email messages per hour that the FortiMail Cloud unit will accept from a throttled SMTP client.
Restrict email to ... percent of the previous hour	Enter the maximum number of email messages per hour that the FortiMail Cloud 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.

GUI item	Description
Temporarily fail client at	Enter a sender reputation score over which the FortiMail Cloud unit will return a temporary failure error when the SMTP client attempts to initiate a connection. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increase or decrease the sender reputation scores accordingly.
Reject client at	Enter a sender reputation score over which the FortiMail Cloud unit will reject the email and reply to the SMTP client with SMTP reply code 550 when the SMTP client attempts to initiate a connection. Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increase or decrease the sender reputation scores accordingly.

FortiGuard IP reputation check	If you want the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted, enable this option. If the SMTP client IP address is a private one, the FortiMail unit will query the FortiGuard Antispam service to determine if the first public IP address in the header is blocklisted.
	• *Use AntiSpam profile settings*: In an antispam profile, you can also enable or disable FortiGuard IP reputation checking. This action happens after the entire message has been received by FortiMail. For details, see Configuring FortiGuard options on page 164.
	• *Use AntiSpam profile settings (no authentication)*: Use antispam profile settings but disable SMTP authentication when the client IP reputation score triggers the threshold.
	• *When client connects*: Enable to query the FortiGuard Antispam Service to determine if the IP address of the SMTP server is blocklisted. And this action will happen during the connection phase. Therefore, if this feature is enabled in a session profile and the action is reject, the performance will be improved.
	FortiGuard categorizes the blocklisted IP addresses into three levels -- level 3 has bad reputation; level 2 has worse reputation; and level 1 has the worst reputation. To help prevent false positives, you can choose which level to block with the following CLI commands:
	`config system fortiguard antispam`
	`set threshold-ip-connect <integer>`
	`end`
	<integer> is the level number: 1, 2, or 3. The default setting is 3, which means all levels will be blocked. If you want to block level 1 and level 2 but not level 3, then you set it to 2.
	• *Disable*: Skip FortiGuard IP reputation check, even this is enabled in an antispam profile.

Configuring endpoint reputation options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand Endpoint Reputation.
   The Endpoint Reputation settings let you restrict, based upon its endpoint reputation score, the ability of an MSISDN or subscriber ID to send email or MM3 multimedia messaging service (MMS) messages from a mobile device. The MSISDN reputation score is similar to a sender reputation score.
   For more on endpoint reputation-based behavior, see About endpoint reputation.

Enabling endpoint reputation can improve performance by rejecting known spammers before more resource-intensive antispam scans are performed.

4. Configure the following:

GUI item	Description
Enable Endpoint Reputation	Enable to accept, monitor, or reject email based upon endpoint reputation scores. This option is designed for use with SMTP clients with dynamic IP addresses. It requires that your RADIUS server provide mappings between dynamic IP addresses and MSISDNs/subscriber IDs to the FortiMail Cloud unit. If this profile governs sessions of SMTP clients with static IP addresses, instead see Configuring sender reputation options on page 145.
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 Cloud unit will add the MSISDN/subscriber ID to the automatic blocklist. The trigger score is relative to the period of time configured as the automatic blocklist window. For more information on the automatic blocklist window, see Configuring the endpoint reputation score window.
Auto blocklist duration	Enter the number of minutes that an MSISDN/subscriber ID will be prevented from sending email or MMS messages after they have been automatically blocklisted.

Configuring sender validation options

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 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.

3. Click the arrow to expand Sender Validation. Configure the settings to confirm sender and message.
   DomainKeys validation is a predecessor of DKIM and works in the same way. Because some domains still use DomainKeys validation, it is provided for backward compatibility.
   Failure to validate does not guarantee that an email is spam, just as successful validation does not guarantee that an email is not spam, but it may help to indicate spam. Validation results are used to adjust the sender reputation scores, MSISDN reputation scores, and deep header scans.

Enabling sender validation can improve performance by rejecting invalid senders before more resource-intensive antispam scans are performed.

4. Configure the following:

GUI item	Description
SPF check	If the sender domain DNS record lists SPF authorized IP addresses, use SPF check to compare the client IP address to the IP addresses of authorized senders in the DNS record (RFC 4408). An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score. If the DNS record for the domain name of the sender does not publish SPF information, the FortiMail Cloud unit omits the SPF client IP address validation. **Note:** No SPF check is performed for direct connections from RFC 1918 private IP addresses. **Note:** If you select to *Bypass* SPF checking in the session profile, SPF checking will be bypassed even though you enable it in the antispam profile. **Note:** Before FortiMail 4.3.1 release, only SPF hardfailed (-all) email is treated as spam. Starting from 4.3.2 to 6.0.2 release, you can use a CLI command (`set spf-checking {strict | aggressive}` under `config antispam settings`) to control if the SPF softfailed (~all) email should also be treated as spam. For details, see the FortiMail CLI Guide. Starting from 6.0.3, this command is removed.
Enable DKIM check	If a DKIM signature is present (RFC 4871), enable this to query the DNS server that hosts the DNS record for the sender's domain name to retrieve its public key to decrypt and verify the DKIM signature. An invalid signature increases the client sender reputation score and affects the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DKIM information or the message is not signed, the FortiMail Cloud 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 and ARC Setting on page 77.

GUI item	Description
	Before 6.2.0 release, Envelope From domain is used for DKIM signatures. After 6.2.0 release, Header From domain is used instead. If there is no DKIM key for the Header From domain, then the key for the Envelope From domain will be used. ***Note***: Outbound quarantined email messages will not be DKIM signed when they are released.
Enable DKIM signing for authenticated senders only	Enable to sign outgoing email with a DKIM signature only if the sender is authenticated.
Enable domain key check	If a DomainKey signature is present, use this option to query the DNS server for the sender's domain name to retrieve its public key to decrypt and verify the DomainKey signature. An invalid signature increases the client sender reputation score and affects the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DomainKey information or the message is not signed, the FortiMail Cloud 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 272.
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 205.

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 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand Session Setting.
4. Configure the following:

GUI item	Description
Session action	Select an action profile or click *New* to create a new one. The session action profile uses the content action profile. For more information about actions, see Configuring content action profiles on page 195.
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 Cloud unit will not be sources of viruses or spam. FortiMail Cloud 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 Cloud unit.
Allow pipelining for the session	Enable to allow SMTP command pipelining. This lets multiple SMTP commands to be accepted and processed simultaneously, improving performance for high-latency connections. Disable to allow the SMTP client to send only a single command at a time during an SMTP session.
Enforce strict RFC compliance (transparent mode only)	Enable to limit pipelining support to strict compliance with RFC 2920, SMTP Service Extension for Command Pipelining. This option is effective only if *Allow pipelining for the session* is enabled.

GUI item	Description

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 Cloud 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 Cloud unit does not complete antispam scanning within 4 minutes, it returns SMTP reply code `451 (Try again later)`, resulting in no permanent problems, since according to RFC 2821, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail Cloud 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 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand Unauthenticated Session Setting.
4. Configure the following:

GUI item	Description

Check HELO/EHLO domain	Enable to return SMTP reply code 501, and reject the SMTP command, if the domain name accompanying the SMTP greeting is not a domain name that exists in either MX or A records.In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT`
	`EHLO example.com`
	The following example shows the invalid command in bold italics:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 20 Nov 2013 10:42:07 -0500`
	`ehlo abc.qq`

GUI item	Description
	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.
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

GUI item	Description

	`550 5.5.0 Empty EHLO/HELO domain.`
	`quit`
	`221 2.0.0 FortiMail-400.localdomain closing connection`

Prevent open relaying (transparent mode only)	Enable to prevent clients from using open relays to send email by blocking sessions that are unauthenticated (Unauthenticated sessions are assumed to be occurring to an open relay). If you permit SMTP clients to use open relays to send email, email from your domain could be blocklisted by other SMTP servers. This option is effective only if you have enabled Configuring mail settings on page 49 for outgoing mail. Otherwise, the FortiMail Cloud unit forces clients to use the gateway you have defined as a relay server (see Configuring mail settings on page 49), if any, or the MTA of the domain name in the recipient email address (`RCPT TO:`), as determined using an MX lookup, so it is not possible for them to use an open relay.
Reject if recipient and helo domain match but sender domain is different	Enable to reject the email if the domain name in the SMTP greeting (`HELO`/`EHLO`) and recipient email address (`RCPT TO:`) match, but the domain name in the sender email address (`MAIL FROM:`) does not. Mismatching domain names is sometimes used by spammers to mask the true identity of their SMTP client. ***Note***: This option should not be used if you have Microsoft 365 and would like to send email to other MS365 tenants (private or business).

Configuring SMTP limit options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand SMTP Limits.
   Setting any of these values to 0 disables the limit.
4. Configure the following:

GUI item	Description
Restrict number of EHLO/HELOs per session to	Enter the limit of SMTP greetings that a connecting SMTP server or client can perform before the FortiMail Cloud 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.

GUI item	Description
Restrict number of recipients per email to	Enter the limit of recipients to prevent mass mailing.
Cap message size (KB) at	Enter the limit of the message size. Messages over the threshold size are rejected. **Note:** When you configure domain settings under *Domain & User* > *Domain*, you can also set the message size limit. Here is how the two settings work together: • For outgoing email (for information about email directions, see Inbound versus outbound email on page 117), only the size limit in the session profile will be matched. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be used. • For incoming email, the size limits in both the session profile and domain settings will be checked. If there is no session profile defined or no IP-based policy matched, the default size limit of 10 MB will be compared with the size limit in the domain settings. FortiMail will use the smaller size.
Cap header size (KB) at	Enter the limit of the message header size. Messages with headers over the threshold size are rejected.
Maximum number of NOOPs allowed for each connection	Enter the limit of `NOOP` commands permitted per SMTP connection. Some spammers use `NOOP` commands to keep a long connection alive. Legitimate connections usually require few `NOOP`s.
Maximum number of RSETs allowed for each connection	Enter the limit of `RSET` commands permitted per SMTP connection. Some spammers use `RSET` commands to try again after receiving error messages such as unknown recipient. Legitimate connections should require few `RSET`s.

Configuring error handling options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand Error Handling.
   Configure Error Handling to specify how the FortiMail Cloud unit should handle connections from SMTP clients that are error-prone. Errors sometime indicate attempts to misuse the server. You can impose delays or drop connections if there are errors. Setting any of these values to `0` disables the limit.

Configuring error handling can improve performance by dropping connections with error-prone SMTP clients.

4. Configure the following:

GUI item	Description
Number of 'free' errors allowed for each client	Enter the number of errors permitted before the FortiMail Cloud unit imposes a delay.
Delay for the first non-free error (seconds)	Enter the delay time for the first error after the number of **free** errors is reached.
Delay increment for subsequent errors (seconds)	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.
Maximum number of errors allowed for each connection	Enter the total number of errors the FortiMail Cloud unit accepts before dropping the connection. By default, five errors are permitted before the FortiMail Cloud unit drops the connection.

Configuring header manipulation options

Email processing software can add lines to the message header of each email message. When multiple lines are added, this can significantly increase the size of the email message. You can configure FortiMail Cloud to delete message headers that are not needed. This can improve the speed of email throughput and reduce disk space usage.

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Expand the *Header Manipulation* section.
4. Configure the following:

GUI item	Description
Received:	Enable to remove all `Received:` message headers that have been inserted by other MTAs (not this FortiMail Cloud). Alternatively, you can remove this header with a per-domain setting. For details, see Remove received header of outgoing email on page 82.
Custom	Enable to remove other headers that have been inserted by other MTAs (not this FortiMail Cloud), then click Edit to configure which headers should be removed.
Headers inserted by this unit	Enable to remove the headers that are inserted by this FortiMail Cloud unit, except `DKIM-Signature:`. **Note**: For backwards compatibility, if you upgrade the firmware and both of the related settings *Received:* and *Custom* were enabled, then this setting will be enabled by default.

Configuring list options

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

1. Go to *Profile* > *Session* > *Session*.
2. Click *New* to create a new session profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Lists*.
   Configure the sender and recipient block lists and safe lists, if any, to sue with the session profile. Block and safe lists are separate for each session profile, and apply only to traffic controlled by the IP-based policy to which the session profile is applied.
   Email addresses in each block list or safe list are arranged in alphabetical order. For more information on how blocklisted email addresses are handled, see Order of execution of block lists and safe lists on page 257.

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 103.

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 Cloud unit's other antispam scans, including SPF validation.

4. Configure the following:

GUI item	Description
Enable sender safe list checking	Enable to check the sender addresses in the email envelope (`MAIL FROM:`), email header (`From:`) and (`Reply-to:`) against the safe list in the SMTP sessions to which this profile is applied, then click Edit to define the safelisted email addresses.
Enable sender block list checking	Enable to check the sender addresses in the email envelope (`MAIL FROM:`), email header (`From:`) and (`Reply-to:`) against the block list in the SMTP sessions to which this profile is applied, then click Edit to define the blocklisted email addresses.
Allow recipients on this list	Enable to check the recipient addresses in the email envelope (`RCPT TO:`) against the safe list in the SMTP sessions to which this profile is applied, then click Edit to define safelisted email addresses.
Disallow recipients on this list	Enable to check the recipient addresses in the email envelope (`RCPT TO:`) against the block list in the SMTP sessions to which this profile is applied, then click Edit to define blocklisted email addresses.

Configuring advanced MTA control settings

This procedure is part of the session profile configuration process. For general procedures about how to configure a session profile, see Configuring session profiles on page 144.

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.

This feature requires a valid license and is hidden by default. To use this feature, go to *System* > *FortiGuard* > *Licensed Feature* > *Advanced Management* and select *Enable MTA advanced control*.

You may also enable the feature by entering 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* > *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 settings on page 49.
Rewrite sender address	Select an Address Rewrite profile to rewrite the sender address and specify which sender address to rewrite: *Envelope From*, *Header From*, or *Header Reply-to*. Select *Use Envelope From value for selected headers* if you want to use the sender email address in the SMTP envelope (`MAIL FROM:`) to rewrite the sender in the message header (`From:` and/or `Reply-to:`). Click *New* to create a new profile. For details about configuring Address Rewrite profiles, see Configuring address rewrite profiles in the session profile on page 159.
Rewrite recipient address	Select an Address Rewrite profile to rewrite the recipient address and specify which recipient address to rewrite: *Envelope recipient* or *Header To and CC*. Note that if you set to deliver or quarantine the unmodified copy of email when you configure the action profile preferences, the recipient (`RCPT TO:`) in the SMTP envelope will still be rewritten. Click *New* to create a new profile. For details about configuring Address Rewrite profiles, see Configuring address rewrite profiles in the session profile on page 159.
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 159.
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 160.
DSN	Select a DNS profile or click *New* to create one. For details, see Configuring DSN profiles in a session profile on page 160.
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 on page 306.

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 157), the *Address Rewrite* tab will appear.

To configure an address rewrite profile to be used in a session profile

1. Go to *Profile* > *Session* > *Address Rewrite*.
2. Click *New*.
3. Enter a profile name.
4. Click *New* to enter the address rewrite rules.
   - For *Rewrite type*, select *Local* if you are configuring direct rewrite from the original address to another specific address. Then specify the original address and the address you want to rewrite to. If you want to keep the local part or the domain part of the original address, click *Insert Variable* to insert the variable for the local part or the domain part.
   - Select *LDAP* if you want to rewrite the original address to the user's external email address and display name that are stored on an LDAP server when the `MAIL FROM:` in the SMTP envelope or `From:` or `Reply-To:` in the message header matches a sender rewrite pattern. Then specify the original address and the LDAP profile. For information about LDAP server configuration, see Configuring address mapping options on page 215.
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 157), the *Mail Routing* tab will appear.

To configure a mail routing profile to be used in a session profile

1. Go to *Profile* > *Session* > *Mail Routing*.
2. Click *New*.
3. Enter a profile name.
4. Click *New* to configure the mail routing settings.
5. In the popup window, specify the sender pattern, recipient pattern, and the relay type:
   - *Host*: Relay the matched sessions to the specified SMTP server.
   - *MX Record (alternative domain):* Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail Cloud unit will load balance between them. Also specify the alternate domain name.
   - *MX Record (this domain)*: Query the DNS server's MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail Cloud unit will load balance between them.
   - *Relay Host*: Relay to a pre-defined relay host.
6. Enter the SMTP port number. See also Appendix C: Port Numbers on page 1.
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 157), 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 121.
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 157), the *DSN* tab will appear. Configure this setting to overwrite the global setting configured in Configuring mail settings on page 49.

To configure a DSN profile to be used in a session profile

1. Go to *Profile* > *Session* > *DSN*.
2. Click *New*.
3. Enter a profile name.
4. Specify if you want to send DSN email and the maximum number of retries.
5. Click *Create*.

Configuring antispam profiles and antispam action profiles

The *AntiSpam* submenu lets you configure antispam profiles and related 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.

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 205 and Configuring scan override options on page 216.

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 174.
Domain (dropdown list)	Select System to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile. 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.
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 44.
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 178.
FortiGuard	See Configuring FortiGuard options on page 164.
Greylist	Enable to apply greylisting. For more information, see Configuring greylisting on page 264. **Note:** Enabling greylisting can improve performance by blocking most spam before it undergoes other resource-intensive antispam scans.
SPF	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.

GUI item	Description
	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. • **Soft Fail**: The host is not authorized to send messages but not a strong statement. • **Permanent Error**: The SPF records are invalid. • **Temporary Error**: Processing 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:** If you select to *Bypass* SPF checking in the session profile (see Configuring sender validation options on page 148), 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 Reference. Starting from 6.0.3, this command is removed.
DKIM	DomainKeys Identified Mail (DKIM) checking utilizes public and private keys to digitally sign outbound emails to prove that email has not been tampered with in transit. Starting from 7.2.1 release, you can set different actions according to different DKIM check results: • **Fail**: DKIM invalid body hash or invalid signature. • **None**: No DKIM DNS record found or the record could not be correctly parsed. • **Pass**: DKIM check passed. • **Temporary Error**: DNS server returned Temp error when querying DKIM DNS record.
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. FortiMail also conducts DMARC alignment, whereby at least one of the domains authenticated by SPF or DKIM must align with the `header-from` domain. If alignment check fails, DMARC check will fail. For more information, see RFC 7489. Starting from 7.2.1 release, you can set different actions according to different DMARC check results: • **Fail**: DMARC check failed. • **None**: No DMARC DNS record found, or the record could not be correctly parsed. • **Pass**: DMARC check passed. • **Temporary Error**: DNS server returned `Temp error` when querying DMARC DNS

GUI item	Description

	record.
	 
	FortiMail combines non-final actions set in the antispam profile with the actions set in the DMARC DNS record policy.
	If the antispam profile DMARC actions are non-final, such as "Tag subject" and "Notify", then they are combined with the actions in the DMARC DNS record policy: none, reject, or quarantine.
	This happens when either the FortiMail Cloudconfiguration is either:
	`config antispam settings`
	`set dmarc-failure-action use-policy-action`
	or, if the policy option in the sender's DMARC record is `p=none`:
	`config antispam settings`
	`set dmarc-failure-action use-profile-action-with-none`
	You can generate DMARC reports with the following CLI command, from the system level and domain level, respectively:
	• `config antispam dmarc-report`
	• `config domain-setting`
	For more details, see the FortiMail CLI Reference.

ARC	Authenticated Received Chain (ARC) permits intermediate email servers (such as mailing lists or forwarding services) to sign an email's original authentication results. This allows a receiving service to validate an email, in the event the email's SPF and DKIM records are rendered invalid by an intermediate server's processing. For more information, see RFC 8617. Enable the service, and enable ARC to override SPF, DKIM, and/or DMARC.

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.
Business email compromise	Expand to specify a profile and an action for each category. See Configuring Business Email Compromise on page 166.
Heuristic	See Configuring heuristic options on page 167.
SURBL	See Configuring SURBL options on page 168.

GUI item	Description
DNSBL	See Configuring DNSBL options on page 169.
Banned word	See Configuring banned word options on page 169.
Safelist word	See Configuring safelist word options on page 170.
Dictionary	See Configuring dictionary options on page 171.
Image spam	See Configuring image spam options on page 171.
Bayesian	See Configuring Bayesian options on page 172.
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 Options	See Configuring scan options on page 173.

Configuring FortiGuard options

The *FortiGuard* section of antispam profiles lets you configure the FortiMail Cloud 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.
- **URL category**: This option determines if any uniform resource identifiers (URL) in the message body are associated with spam. FortiGuard URL filter groups URL into various categories, such as hacking, drug abuse and so on. You can configure the FortiGuard URL filter to check for certain categories only. If a URL 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 FortiGuard URL filter on page 243.
  To take different actions towards different URL filters or categories, you can specify a primary and a secondary filter, and specify different actions for each filter. If both URL 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 (configurable with CLI command `config profile antispam set spam-outbreak-protection` and `config system fortiguard antispam set outbreak-protection-period`) if the enabled FortiGuard antispam check (block IP and/or URL filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs. To view the email on hold, go to *Monitor* > *Mail Queue* > *Spam Outbreak*.

When set to *Monitor only*, email is not deferred. Instead, it logs the email and inserts this header:
`X-FEAS-Spam-outbreak: monitor-only`

- 
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 fall back to "system quarantine" if spam is detected afterward.

- 
Email from some sources, such as safelisted IP addresses and ACL relay rules, will be exempted from FortiGuard spam outbreak protection scan.

When FortiGuard detects spam for both IP reputation and URL category in an email, the URL category action will be taken and logged. For example, if the IP reputation action is *Tag* while the URL category action is *Reject*, then the email will be rejected.

FortiGuard URL filter and URL scanning have two levels of control: strict or aggressive. For details see URL types on page 244.

Aggressive scans also example the domain part of envelope `MAIL FROM:`, header `From:`, and `Reply-To:` addresses. If the domains are identified as spam, then the configured antispam actions will be applied.


If the *FortiGuard*option is enabled, you may improve performance and the spam catch rate by also enabling *Block IP*.

To configure FortiGuard scan options

1. Before enabling *FortiGuard*, you must enable and configure FortiGuard Antispam rating queries.
2. When configuring an antispam profile, select the *FortiGuard* check box in the *AntiSpam Profile* dialog. This is the main switch to turn on/off all the sub items. If disabled, all the sub items under the FortiGuard category are also disabled.
3. 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, URL filter, and spam outbreak protection.

   
   If the action is set to *None* for FortiGuard, FortiGuard Antispam checks are still performed and logged, but no action will be taken. IP Reputation and WebFilter checks are still performed as well and the specified action will be applied.

   For more information about action profiles, see Configuring antispam action profiles on page 178.
4. 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.

FortiGuard categorizes the blocklisted IP addresses into three levels -- level 3 has bad reputation; level 2 has worse reputation; and level 1 has the worst reputation. To help prevent false positives, you can choose to take different actions towards different IP reputation levels. Usually you should take strict actions, such as reject or discard, towards level 1 IP addresses while take loose actions, such as quarantine or tag, towards level 3 IP addresses. Using default actions for level 1, 2, and 3 means to use the IP Reputation action; using the default action for IP reputation means to use the FortiGuard action; and using the FortiGuard default action means to use 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.

5. If you want to use the FortiGuard URL filter service, select a URL category profile from the *Primary* or *Secondary URL Category* list. For details, see Configuring the FortiGuard URL filter on page 243. Then select an action profile. The default action means to use the FortiGuard action, not the antispam profile action.

   Note: If the secondary URL category is matched, the email will be deferred in the spam outbreak queue if the spam outbreak protection is enabled.
6. If you want to 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.
7. Continue to the next section, or click *Create* to save the antispam profile.

Configuring Business Email Compromise

To better protect against business email compromise (BEC) spam attacks, FortiMail can scan for the most common BEC attack types, such as cousin domains, suspicious characters, sender alignment, action keywords, and URL categories. To avoid false positives and false negatives, you can adjust ("weight") the scores of each type of suspicious behavior, and the total score threshold that an email must reach to be categorized as spam.

BEC is configurable in antispam profiles. For details about antispam profiles, see Managing antispam profiles on page 160.

To configure Business Email Compromise

1. Go to *Profile* > *AntiSpam* > *AntiSpam*.
2. Either click *New* to add a profile or double-click an existing profile to modify it. You can also select multiple profiles and batch edit them.
3. Select a domain or *System* from the dropdown list. The profile will be applied to your selection.
4. Enter a *Profile name*.
5. Enter a *Comment*.

6. Under *Scan Configurations*, enable *Business email compromise*, and configure the following:

GUI item	Description
Weighted analysis	Enable to apply a weighted analysis profile and assign an appropriate action. For more information, see Configuring weighted analysis profiles on page 177.
Impersonation analysis	Enable to automatically learn and track the mapping of display names and internal email addresses to prevent spoofing attacks. Select the action if the addresses do not match. For more information, see Configuring impersonation profiles on page 174.
Cousin domain	Enable to scan for domain names that are deliberately misspelled in order to appear to come from a trusted domain. Additionally, enable *Header Detection*, *Body Detection*, and/or *Auto Detection* if you wish to scan for cousin domain names either within the email header, the email body, and/or automatically (respectively). Select the action if the cousin domain scan is triggered. For more information, see Configuring cousin domain profiles on page 176.
Sender alignment	Enable to scan for sender email address mismatches. Sender alignment compares the domain name of the sender email address in the message header (`From:` or `Reply-To:`) and SMTP envelope (`MAIL FROM:`) to look for a mismatch, which is typical of spam. Select the action if a mismatch occurs.

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.

To configure heuristic scan options

1. When configuring an antispam profile, enable *Heuristic* under *Scan Configurations*.
2. Click the plus 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 details, see Configuring antispam action profiles on page 178.
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 options on page 173.

Configuring SURBL options

In addition to supporting Fortinet's FortiGuard Antispam SURBL service, the FortiMail unit supports third-party Spam URL Realtime Block Lists (SURBL) servers. You can specify which public SURBL servers to use as part of an antispam profile. Consult the third-party SURBL service providers for any conditions and restrictions.

The SURBL section of antispam profiles lets you configure the FortiMail unit to query one or more SURBL servers to determine if any of the uniform resource identifiers (URL) in the message body are associated with spam. If a URL is blocklisted, the FortiMail unit treats the email as spam and performs the associated action. There are two types of URLs. For details, see URL types on page 244.

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 178.
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 dropdown 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.

Closing the pop-up window does **not** save the antispam profile and its associated SURBL server list. To save changes to the SURBL server list, in the antispam profile, click *OK* before navigating away to another part of the GUI.

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.

Carefully select your DNSBL providers and review their operations. Fortinet recommends that all email administrators utilize services which have clearly defined and rational listing policies and do not charge for delisting. Services that block whole subnets and AS numbers and have a business model which charges for delisting should be viewed with heavy caution. Fortinet cannot delist IP addresses blocklisted by other vendors.

DNSBL scans examine the IP address of the SMTP client that is currently delivering the email message. If the *Enable Block IP to query for the blocklist status of the IP addresses of all SMTP servers appearing in the Received: lines of header lines.* option 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 164.

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 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 178.
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 dropdown 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 GUI.
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, see Appendix D: Wildcards and regular expressions on page 1.

You can also apply this scan to PDF attachments. For more information, see Configuring scan options on page 173.

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 178.
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.
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, see Appendix D: Regular expressions.

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.
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 231.

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 plus 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 178.
4. From the With dictionary group dropdown list, select the name of a group of dictionary profiles to use with the dictionary scan. Or, from the With dictionary profile dropdown 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 spam 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 details, see Configuring antispam action profiles on page 178.

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 options on page 173.
4. Continue to the next section, or click Create or OK to save the antispam profile.

See also

Managing antispam profiles

Configuring antispam action profiles

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 279.

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 plus 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 details, see Configuring antispam action profiles on page 178.
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 255.

GUI item	Description
	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 options

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 options

1. When configuring an antispam profile, Click the plus to expand Scan Options 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. This option is enabled by default. **Note:** If you can trust that authenticating SMTP clients are not a source of spam, consider enabling this option to improve performance.
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.

GUI item	Description
	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 167, Configuring banned word options on page 169, and Configuring image spam options on page 171.
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, hold Ctrl and select the profiles you want to edit.
   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 160, changing only those settings that you want to apply to all selected profiles.
5. Click Apply To All to save the changes and remain on the dialog, or click OK to save the changes and return to the AntiSpam tab.

Configuring impersonation profiles

Email impersonation is 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 `From: CEO ABC <ceo@external.com>` in the email header, and send such email to a user(`victim@company.com`). If FortiMail has been configured with a manual entry "`CEO ABC`"/"`ceo@company.com`" in an impersonation analysis profile to indicate the correct display name/email pair, or it has learned display name/email pair through the dynamic process, then such email will be detected by impersonation analysis, because the spammer uses an external email address and an internal user's display name.

There are two ways to map entries:

- **Manual**: 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 160). Eventually, you will apply the antispam profile in the IP-based or recipient-based policies (Controlling email based on IP addresses

on page 132 and Controlling email based on sender and recipient addresses on page 138).

- **Dynamic**: FortiMail Cloud Mail Statistics Service can automatically learn the mapping. See details below.

Impersonation analysis checks both the header `From:` and `Reply-To:` fields.

You can also add exempt entries so that FortiMail Cloud will skip the impersonation analysis check.

To avoid false positives, impersonation analysis also follows some other 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*, select *Match Rule* or *Exempt Rule*.
6. 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 a wildcard or regular expression.
Pattern type	Either wildcard or regular expression. See Appendix D: Wildcards and regular expressions on page 1.
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, dynamically learn and track the mapping of display names and internal email addresses.

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
```

After the service is enabled, you can search the dynamic database by going to *Profile* > *AntiSpam* > *Impersonation* and clicking *Impersonation Lookup*. If the record exists in the database, after you enter the email address, the corresponding display name will be displayed.

Configuring cousin domain profiles

Similar to impersonation profiles, cousin domain profiles help to mitigate domain impersonation risks. Similar to impersonation profiles that map display names, cousin domain profiles can map both inbound and outbound domain names to either be scanned or exempt from scanning. Domain names may be deliberately misspelled, either by character removal, substitution, and/or transposition, in order to make emails look as though they originate from trusted internal sources.

For example, if you configure a regular expression for the sender domain `f?rtinet.com`, it will match `f0rtinet.com`, but the legitimate and trusted sender domain `fortinet.com` will also be detected as a cousin domain. To avoid this, you can add `fortinet.com` into the exempt rules setting to avoid detecting it as spam.

Cousin domain scan options, such as auto detection, are configured within antispam profiles. See Managing antispam profiles on page 160 for more information.

To create a cousin domain profile

1. Go to *Profile* > *AntiSpam* > *Cousin Domain*.
2. Either click New to add a profile or double-click an existing profile to modify it. You can also select multiple profiles and batch edit them.
3. Select a domain or System from the dropdown list. The profile will be applied to your selection.
4. Enter a profile name.
5. Under *Domain Pattern*, select *From*, *To*, or *Exempt*.
6. Click *New* to add an entry.

GUI item	Description
Domain name pattern	Enter the domain name to be mapped to the email address. You can use wildcard or regular expression.
Pattern type	Either wildcard, regular expression, or look-alike. A look-alike pattern can be configured to specifically check for instances of recipient domain typos. For example, if a domain such as `fortinet.com` is configured with pattern type set to look-alike, any similar misspelled domains, such as `fort1net.com`, are caught. See also Syntax on page 1.  Since auto-detection is not applicable to outgoing policies, look-alike patterns are best suited for catching misspelled domains.

7. Click Create or OK.

Configuring weighted analysis profiles

The Weighted Analysis tab in the AntiSpam submenu allows you to create weighted analysis profiles containing of one or more score weighted rules configured to scan for various categories, including intelligent analysis.

To create a weighted analysis profile

1. Go to *Profile* > *AntiSpam* > *Weighted Analysis*.
2. Either click New to add a profile or double-click an existing profile to modify it.
3. From *Domain*, select if the weighted analysis profile will be system-wide or apply only to a specific domain. You can see only the domains that are permitted by your administrator profile.
4. In *Name*, enter a unique name for the profile.
5. Optionally, in the *Comment* field, enter a descriptive comment.
6. Under *Rule*, click *New*.
   A dialog appears.
7. Configure the following:

GUI item	Description
Status	Enable or disable the rule.
Name	Enter the name of the rule.
Action (dropdown list)	Specify an action for the rule.
Threshold	Enter the threshold at which the current rule is to be triggered. This score will be allocated to the seven categories below.

Score Weight	Enter the score weight thresholds of the following factors:
	• *Intelligent analysis*: Multiple factors contribute to intelligent analysis in order to reduce false positives, including:
	  • SPF
	  • DKIM
	  • DMARC
	  • matching of sender addresses in the message headers (`From:` and `Reply-To:`)
	  • newly registered domain names that do not have a FortiGuard Antispam rating yet
	  • header analysis
	  • malformed email detection
	• *Cousin domain*: Detects domain impersonation. See Configuring cousin domain profiles on page 176.
	• *Suspicious character*: Detects internationalized domain name (IDN) homograph attacks. If domain names in URLs, sender email addresses, or recipient email addresses have Unicode characters that are from different languages yet look similar (for example, `A` looks similar in Cyrillic, Greek, and Latin alphabets), then an attacker could trick the user

GUI item	Description
	into using a fraudulent website or email. FortiMail Cloud detects these as suspicious. • *Sender alignment*: Compares the domain name of the sender email address in the message header (`From:`) and SMTP envelope (`MAIL FROM:`) to look for a mismatch, which is typical of spam. • *Action keyword*: Select the name of a dictionary profile that contains words or phrases that typically only spam has. Keywords are often a "call to action" that motivates the user to reply or click a hyperlink. For example, "Click here", "transfer", "money", "dollars", "bank account", "conference attendee", etc. • *Dictionary profile*: Select the dictionary profile. See Configuring dictionary profiles on page 231. • *Minimum dictionary score*: Enter the threshold for dictionary profile matches. When the dictionary profile scans an email, it counts the number of matching words or phrases, and adjusts this total according to the pattern weight and maximum pattern weight in the dictionary profile. If the result equals or exceeds this threshold, then FortiMail Cloud applies the weighted score defined in *Action keyword*. • *URL category*: Detects spam or phishing URLs in the email. • *Malformed email*: Detects malformed data in the email structure, header, or body. For more information, see RFC 7103.

8. Click Create or OK.

To apply a weighted analysis profile, select it in one or more antispam profiles under Business email compromise. For details, see Managing antispam profiles on page 160.

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 view and configure antispam action profiles

1. Go to *Profile* > *AntiSpam* > *Action*.

GUI item	Description
Domain (dropdown list)	Select System to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain (column)	Displays either System or a domain name.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click New to add a profile or double-click an existing profile to modify it. You can also select multiple profiles and batch edit them.
   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]`. 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.

GUI item	Description
Insert disclaimer	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System* > *Mail Setting* > *Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email. **Note:** If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile and ignores Relay server name and Use this domain's SMTP server to deliver the mail.
Deliver to original host	Enable to deliver email to the original host.
FortiGuard spam outbreak protection	Enable to manually defer emails and place email in the spam defer queue. **Note:** The *Spam outbreak protection* option in the FortiGuard settings under *Profile* > *AntiSpam* > *AntiSpam* does not affect this feature.
Defer delivery	Enable to defer delivery of emails that may be resource intensive and reduce performance of the mail server, such as large email messages, or lower priority email from certain senders (for example, marketing campaign email and mass mailing).
BCC	Enable to send a blind carbon copy (BCC) of the email. You can specify an *Envelope from address* so that, in the case the email is not deliverable and bounced back, it will be returned to the specified envelope from address, instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. Click *New* to add BCC recipients.
Notify with profile	Enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification email is customizable and will tell the users what happened to the email message. For details about notification profiles and email templates, see Configuring notification profiles on page 242 and Customizing email templates on page 59.
Final action	For details about final and non-final actions, see Order of execution.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
Reject	Enable to reject the email and reply to the SMTP client with SMTP reply code 550. However, if email messages are held for FortiGuard spam outbreak protection or FortiGuard virus outbreak protection, or sent to FortiSandbox, the actual action will fallback to "system quarantine".
Personal quarantine	For incoming email, enable to redirect the email to the recipient's personal quarantine. For more information, see Managing the personal quarantines on page 22. 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	Enable to redirect spam to the system quarantine folder. For more information, see Managing the system quarantine on page 25. You can choose to quarantine the original email or the modified email.
	Domain quarantine	Enable to redirect spam to the domain quarantine folder. For more information, see Managing the domain quarantines on page 27.
	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 160.

Configuring antivirus profiles, file signatures, and antivirus action profiles

The *AntiVirus* submenu lets you configure antivirus profiles and related action profiles.

Managing antivirus profiles

Go to *Profile* > *AntiVirus* > *AntiVirus* to create antivirus profiles that you can select in a policy in order to scan email for viruses.

The FortiMail unit scans email header, body, and attachments (including compressed files, such as ZIP, PKZIP, LHA, ARJ, and RAR files) for virus infections. If the FortiMail Cloud 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 184.

FortiMail keeps its antivirus scan engine and virus signature database up-to-date by connecting to Fortinet FortiGuard Distribution Network (FDN) antivirus services.

To configure an antivirus profile

1. Go to *Profile* > *AntiVirus* > *AntiVirus*.
2. Either click *New* to add a profile or double-click a profile to modify it.
   A dialog appears.
3. Click the arrows to expand each section 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 184.
AntiVirus	Enable to perform antivirus scanning.
Malware/virus Outbreak	Instead of using virus signatures, malware outbreak protection uses data analytic from the FortiGuard Service. For example, if a threshold volume of previously unknown attachments are being sent from known malicious sources, they are treated as suspicious viruses. This feature can help quickly identify new threats. Because the infected email is treated as virus, the virus replacement message will be used, if the replacement action is triggered.
Heuristic	Enable to use real-time malware analysis, or heuristic antivirus scan, when performing antivirus scanning.
File signature check	Enable to scan for file signatures. For details, see Adding file signatures on page 183.
Grayware	Enable to scan for grayware, such as mail bomb detection.
FortiNDR	Enable this option to send potentially harmful attachments, such as executables, PDF, and OCX files, to FortiNDR for further malware analysis. For details about FortiNDR configuration, see Using FortiNDR malware inspection on page 61.
Malicious/Virus **High risk** **Medium risk** **Low risk**	Specify the action to take if the FortiNDR analysis determines that the email messages have malware or other threat qualities. You can specify different actions according to the threat levels.
FortiSandbox	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 62.
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.
URL analysis		Enable to send the URLs to FortiSandbox. If desired, configure different actions for different scan results.
	Email selection	Specify to scan URLs in all email or the suspicious email only.
	Malicious/Virus **High risk** **Medium risk** **Low risk** **No Result**	Specify the action to take if the FortiSandbox analysis determines that the email messages have virus or other threat qualities. You can specify different actions according to the threat levels.

Adding file signatures

If you already have the SHA-1or 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, file signatures, and antivirus action profiles on page 181.

You can manually add the SHA-1or SHA-256 checksums individually. You can also import a list ofchecksums in CSV (comma-separated values) or plain text file 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, .docx, .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 *Profile* > *AntiVirus* > *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 CSV format

1. Go to *Profile* > *AntiVirus* > *File Signature* and select a signature profile and click Import.
2. Browse to the CSVfile and click *OK*. The CSVfile must contain the hash values, and the type must be SHA1 or SHA256. The list will be imported into the profile.

To export the file signatures

1. Go to *Profile* > *AntiVirus* > *File Signature*. Select a signature profile and click Export.
2. Click *Save File* to save the file in CSVformat to your local machine.

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 view and configure antivirus action profiles

1. Go to *Profile* > *AntiVirus* > *Action*.

GUI item	Description
Domain (dropdown list)	Select System to see profiles for the entire FortiMail Cloud 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 `[virus]`. The FortiMail Cloud 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 Cloud unit adds this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.

GUI item	Description
	Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as virus by profile 22.` If you enter a header line that does not include a colon, the FortiMail Cloud 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	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System* > *Mail Setting* > *Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email. **Note:** If you enable this setting, the FortiMail Cloud unit uses this destination for all email that matches the profile and ignores Relay server name and Use this domain's SMTP server to deliver the mail.
Deliver to original host	Enable to route the email back to its original source destination.
BCC	Enable to send a blind carbon copy (BCC) of the email. You can specify an Envelope from address so that, in the case the email is not deliverable and bounced back, it will be returned to the specified envelope from address, instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. Click New to add BCC recipients.
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 Configuring custom messages and email templates on page 51.
Remove URL detected by FortiSandbox	Removes suspicious URLs from email, as detected by ForttiSandox.
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 242 and Customizing email templates on page 59.
Final action	Select one of the following actions:

GUI item	Description
	• *Discard*: Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • *Reject*: Enable to reject the email and reply to the SMTP client with SMTP reply code 550. However, if email messages are held for FortiGuard spam outbreak protection or FortiGuard virus outbreak protection, or sent to FortiSandbox, the actual action will fallback to "system quarantine". • *System quarantine*: Enable to redirect email to the system quarantine. For more information, see Managing the system quarantine on page 25.You can choose to quarantine the original email or the modified email. • *Domain quarantine*: Enable to redirect email to the domain quarantine folder. For more information, see Managing the domain quarantines on page 27. • *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 cusotmized 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 59. • *Repackage email with original text content*: Enable to forward the infected email as an attachment but the original email body will still be used without modification.

Configuring content profiles and content action profiles

The *Content* sub-menu lets you configure content profiles for incoming and outgoing content-based scanning. The available options vary depending on the chosen directionality.

Configuring content profiles

The *Content* tab lets you create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

Unlike antispam profiles, which deal primarily with spam, content profiles match any other type of email.

You can use content profiles to apply content-based encryption to email, or to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. You can apply content profiles to email that you want to protect and email that you want to prevent.

To view and configure content profiles

1. Go to *Profile* > *Content* > *Content*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone.* A single-field dialog appears. Enter a name for the new profile. Click *OK*.
Domain (dropdown list)	Select *System* to see profiles for the entire FortiMail Cloud unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain Name (column)	Displays either *System* or the name of a protected domain.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new profile, from the *Domain* dropdown, select either *System* to see profiles that apply to the entire FortiMail Cloud unit, or select the name of a protected domain.
4. For a new profile, enter its name. The profile name is editable later.
5. In *Action*, select a content action profile to use. For details, see Configuring content action profiles on page 195.
6. Configure the following sections:
   - Configuring attachment scan rules on page 187
   - Configuring scan options on page 188
   - Configuring content disarm and reconstruction (CDR) on page 189
   - Configuring archive handling on page 190
   - Configuring password decryption options on page 191
   - Configuring content monitor and filtering on page 192
7. Click *Create* or *OK* to save the content profile.

Configuring attachment scan rules

The attachment scan rules define what actions will be taken if the specified files types are found in email attachments.

Before you can configure the scan rule, you must configure the file filters. See Configuring file filters on page 193.

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 186.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Attachment Scan Rules* section.
4. Click *New* to add a rule:

GUI item	Description
Enabled	Select to enable the rule.

GUI item	Description
File filter	Select the file filter. See Configuring file filters on page 193.
Operator	Select *Is* or *Is Not*. If *Is* is selected, the below action will be taken. If *Is Not* is selected, the below action will not be taken. You can use the *Is Not* option to safelist some attachment types. For example, if you want to reject all file types except for the PDF files, you can specify that *PDF Is Not Reject*.
Action	Specify the action. Or click *New* to create a new action profile.

Configuring scan options

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 186.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Scan 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 Microsoft Outlook, can fragment big emails into multiple sub-messages. This is used to bypass oversize limits and scanning.
Detect password protected Office/PDF document	Enable to apply the block action configured in the content action profile if an attached Microsoft Office, OpenOffice, or PDF document is password-protected, and therefore cannot be decompressed in order to scan its contents.
Attempt to decrypt Office/PDF document	Enable to decrypt Microsoft Office, Open Office, or PDF attachments using the predefined or user-defined passwords. For details, see Configuring file passwords on page 194.
Detect embedded component	Specify which option(s) to use when scanning documents with embedded files such as Microsoft Office, Microsoft Visio, OpenOffice.org , and PDF documents. Similar to an archive, documents can sometimes contain video, graphics, sounds, and other files that are used by the document. By wrapping files within a document instead of linking to the file on a separate, external location, a document becomes more portable. However, it also means that documents with other files embedded can be used to hide infected files.
Policy match	Enable to defer mail delivery from specific senders configured in the policy. By sending low-priority, bandwidth-consuming email such as newsletter digest or marketing campaigns at scheduled times, you can conserve bandwidth at peak time so that high priority email can be sent more quickly.

GUI item	Description
	For information on policy, see How to use policies on page 118. For information on scheduling deferred delivery, see Configuring mail settings on page 49.
Maximum number of attachment	Enter how many attachments are allowed in one email message. The valid range is from 1 to 100.
Maximum size	Enter the maximum size threshold in kilobytes for email or attachments.
Adult image analysis	If you have 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. Go to *System* > *FortiGuard* > *Adult Image Analysis*. For details, see Configuring FortiGuard services on page 64.

Configuring content disarm and reconstruction (CDR)

Configure these settings to sanitize email that contains hyperlinks and scripts, including in attachments, in order to reduce risk of spam, malware, and tracking. For more information about CDR, see Configuring content disarming and reconstruction on page 244.

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 186.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *Content Disarm and Reconstruction* and configure the following:

GUI item	Description
Action	Select an action. See Configuring content action profiles on page 195.

HTML content	Enable to detect risky hypertext markup language (HTML) tags in an HTML email body, and then select how FortiMail Cloud will sanitize the email:
	• *Convert to text*: Convert the HTML email to plain text.
	• *Modify content*: Modify the HTML content, using the following settings:
	  • *Active content*: Select to either *Keep* or *Remove*active content such as JavaScript.
	  • *URL*: Select whether to:
	  • *Keep*: Keep the URL or script. Do not remove or modify it.
	  • *Remove*: Remove the URL or script.
	  • *Redirect to FortiIsolator*: Redirect the user to FortiIsolator so that the user will be browsing indirectly, protected through FortiIsolator. To view the settings for URL click protection and FortiIsolator, click *View settings*.
	  • *Redirect to Click Protection*: Rewrite the URL. If the user clicks on the URL, scan the URL and then perform click protection action configured in Configuring CDR URL click protection and removal options on page 245.
	  • *Redirect to Click Protection + FortiIsolator*: Rewrite the URL and if the user clicks on it, redirect the URL to FortiMail for scanning. If the URL is malicious, it will be blocked; if the URL passes the scan, then it is rewritten to point to FortiIsolator, and the user will browse through FortiIsolator.

GUI item	Description

	• *Neutralize*: Modify the URL to make it inactive when clicked, but still easy to determine what the original URL was. For example, a link to:
	`https://www.example.com`
	is changed to:
	`hxxps:\\www[.]example[.]com`
	Then in *Apply to*, select whether CDR modifications should apply to either *Tag attribute* (for example, the `href` attribute in hyperlinks such as `<a href="https://example.com">`), *Tag text content*, or both.
	FortiMail Cloud will also add:
	`X-FEAS-ATTACHMENT-FILTER: Contains HTML tags.`
	to the message headers.

Text content	Enable to detect risky URLs in a plain text email body, and then in *URL*, select how FortiMail Cloud will sanitize the email (the options are similar to *URL* for HTML email).
MS Office	Enable to disarm and reconstruct Microsoft Office attachments. This also includes ZIP files that are compressed (nested compression is not supported).
PDF	Enable to disarm and reconstruct the PDF attachments. This also includes ZIP files that are compressed (nested compression is not supported).

Configuring archive handling

For email with archive attachments, you can decide what to do with them. Currently, FortiMail supports ZIP, PKZIP, GZIP, BZIP, TAR, RAR, JAR, CAB, 7Z, and EGG for content inspection.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 186.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *Archive Handling* and configure the following:

GUI Item	Description
Check archive content	Enable to determine which action to perform with the archive attachments. • blocking password protected archives if you have selected *Detect Password Protected Archive* • blocking archives that could not be successfully decompressed if you have selected *Detect on Failure to Decompress* • passing/blocking by comparing the depth of nested archives with the nesting depth threshold configured in *Max Level of Compression* By default, archives with less than 10 levels of compression will be blocked if they cannot be successfully decompressed or are password-protected. Depending on the nesting depth threshold and the attachment's depth of nested archives, the FortiMail Cloud unit may **also** consider the file types of files within the archive when determining which action to perform. For details, see the section below.

GUI Item	Description
	If disabled, the FortiMail Cloud unit will perform the *Block*/*Pass* action solely based upon whether an email contains an archive. It will disregard the depth of nesting, password protection, successful decompression, and the file types of contents within the archive.
Detect archive bomb and decompression failure	Enable to apply the block action configured in the content action profile if an attached archive cannot be successfully decompressed, such as if the compression algorithm is unknown, and therefore cannot be decompressed in order to scan its contents. This option is available only if *Check archive content* is enabled.
Detect password protected archive	Enable to apply the block action configured in the content action profile if an attached archive is password-protected, and therefore cannot be decompressed in order to scan its contents. This option is available only if *Check archive content* is enabled.
Attempt to decrypt archive	Enable to decrypt and scan the archives, using the passwords configured in Configuring password decryption options on page 191. If it fails, the email will be passed. This option is available only if *Check archive content* is enabled.
Max level of compression	Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail Cloud unit uses one of the following methods to determine if it should block or pass the email. • *Max Level of Compression* is 0, or attachment's depth of nesting equals or is less than *Max Level of Compression*: If the attachment contains a file that matches one of the other file types, perform the action configured for that file type, either block or pass. • Attachment's depth of nesting is greater than *Max Level of Compression*: Apply the block action, unless you have deselected the check box for *Max Level of Compression*, in which case it will pass the file type content filter. Block actions are specified in the content action profile. The specified compression value is always considered if *Check Archive Content* is enabled, but has an effect only if the threshold is exceeded. This option is available only if *Check archive content* is enabled.

Configuring password decryption options

For password-protected PDF and archive attachments, if you want to decrypt and scan them, you can specify what kind of passwords you want to use to decrypt the files.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 186.

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Expand *File Password Decryption Options*.
4. Specify the type of passwords to use:
   - *Words in email content*: Enable and enter the *Number of adjacent word to keyword* to specify how many words before and after the keywords to try as the password for file decryption. For example, in an email, there could be a sentence such as: "To open the document, please use password 123456. If you cannot open it, please contact us." If you specify to use two words before and after the keyword, then "please", "use" (two

words before the keyword “password”), “123456”, and “If” (two words after the keyword “password”) would be used as one by one as the password to decrypt the attachments. If no keyword exists, any words in the email body may be tried as the password.

- *Built-in password list*: Enable this option to use the predefined passwords.
- *User-defined password list*: Enable this option to use the passwords defined under *Profile* > *Content* > *File Password*. For details, see Configuring file passwords on page 194.

Configuring content monitor and filtering

The monitor profile uses the dictionary profile to determine matching email messages, and the actions that will be performed if a match is found.

You can also select to scan Microsoft Office, PDF, or archived email attachments.

The following procedure is part of the content profile configuration process. For general procedures about how to configure a content profile, see Configuring content profiles on page 186.

To configure a content monitor profile

1. Go to *Profile* > *Content* > *Content*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Content Monitor and Filtering*.

GUI item	Description
Move (button)	Mark a check box to select a content monitor profile, then click this button. Choose *Up* or *Down* from the pop-up menu. Content monitor profiles are evaluated for a match in order of their appearance in this list. Usually, content monitor profiles should be ordered from most specific to most general, and from accepting or quarantining to rejecting.
Delete (button)	Mark a check box to select a content monitor profile, then click this button to remove it. **Note:** Deletion does not take effect immediately; it occurs when you save the content profile.

4. Click *New* for a new monitor profile or double-click an existing profile to modify it.
   A dialog appears.

5. Configure the following:

GUI item	Description
Enable	Enable to use the content monitor to inspect email for matching email and perform the configured action.
Dictionary	Select either *Profile* or *Group*, then select the name of a dictionary profile or group from the dropdown list next to it. If no profile or group exists, click *New* to create one, or select an existing profile or group and click *Edit* to modify it. A dialog appears. For information on creating and editing dictionary profiles and groups, see Configuring dictionary profiles on page 231.
Minimum score	Displays the number of times that an email must match the dictionary profile before it will receive the action configured in *Action*. Note that the score value is based on individual dictionary profile matches, not the dictionary group matches.
Action	Displays action that the FortiMail Cloud 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 195.

Scan Condition	Select the content type(s) to scan:
	• *PDF files*
	• *Microsoft Office files*
	• *Archived PDF and MS Office files*. If you select this option, you can also use the following CLI commands to specify the maximum levels to decompress and the maximum file size to decompress:
	`config mailsetting mail-scan-options`
	`set decompress-max-level <level_1-16>`
	`set decompress-max-size <MB_int>`
	`end`

6. Click *Create* or *OK*.

Configuring file filters

File filters are used in the attachment scan rules (see Configuring attachment scan rules on page 187. File filters defines the email attachment file types and file extensions to be scanned.

Wildcards can be used in file filters. For details, see Appendix D: Wildcards and regular expressions on page 1.

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 186.

1. Go to *Profile* > *Content* > *File Filter*.
2. Click *New* to create a new filter or double click on an existing filter to edit it.

GUI item	Description
Domain	The new filter can applied to a domain or system wide.
Name	Enter a name for the filter.
Description	Optionally enter a description.
File Type	Either select from the predefined types and/or specify your own.
File Extension	Either select from the predefined extensions and/or specify your own.

Encrypted email content cannot be scanned for spam, viruses, or banned content.

Unlike other attachment types, archives may receive an action other than your *Block*/*Pass* selection, depending on your configuration in the *Scan Conditions* (see Action on page 148).

For each file type, you can use an action profile to overwrite the default action profile used by the content profile. For example, if you want to redirect encrypted email to a third party server (such as a PGP Universal Server) for decryption, You can:

1. Create a content action profile and enable the Send to alternate host option in the action profile. Enter the PGP server as the alternate host. For details about how create a content action profile, see Configuring content action profiles on page 195.
2. Select to block the `encrypted/pgp` file type under `document/encrypted`. “Block” means to apply an action profile.
3. Select the action profile for the `document/encrypted` file type. This action profile will overwrite the action profile you select for the entire content profile.

Configuring file passwords

When you configure a content profile, you can choose to decrypt documents (see Configuring scan options on page 188) and archived files (see Configuring archive handling on page 190). To decrypt the documents, you need passwords. See also Configuring password decryption options on page 191.

To configure user-defined passwords

1. Go to *Profile* > *Content* > *File Password*.
2. Click *New*.
3. Enter the password that will be used to decrypt documents.
4. Click *Create*.

Configuring content action profiles

The *Action* tab in the *Content* submenu lets you define content action profiles. Use these profiles to apply content-based encryption.

Alternatively, content action profiles can define one or more things that the FortiMail unit should do if the content profile determines that an email contains prohibited words or phrases, file names, or file types.

For example, you might have configured most content profiles to match prohibited content, and therefore to use a content action profile named `quar_profile` which quarantines email to the system quarantine for review.

However, you have decided that email that does not pass the dictionary scan named `financial_terms` is **always** prohibited, and should be rejected so that it does not require manual review. To do this, first configure a second action profile, named `rejection_profile`, which rejects email. You would then override `quar_profile` specifically for the dictionary-based content scan in each profile by selecting `rejection_profile` for content that matches `financial_terms`.

To view and manage the list of content action profiles

1. Go to *Profile* > *Content* > *Action*.

GUI item	Description
Domain (dropdown list)	Select *System*to see profiles for the entire FortiMail Cloud 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 Cloud unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter its name.
Tag subject	Enable and enter the text that will appear in the subject line of the email, such as `[PROHIBITED-CONTENT]`. FortiMail Cloud prepends this text to the subject line of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client.

GUI item	Description
Insert header	Enable and click New to enter a message header key. The FortiMail Cloud 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 Cloud unit will automatically append a colon, causing the entire text that you enter to be the key. You can add multiple headers by adding them to the header table. You can also insert the predefined variables to the header value. **Note**: Do not enter spaces in the key portion of the header line. These are forbidden by RFC 2822.
Remove header	Enable and click *New* to enter the message header name to be removed.
Insert disclaimer	Insert disclaimer as an action, and select whether you want to insert the disclaimer at the start of the message, end of the message, or at the location of the custom message. You can modify the default disclaimer or add new disclaimers by going to *System* > *Mail Setting* > *Disclaimer*.
Deliver to alternate host	Enable to route the email to a specific SMTP server or relay, then type the fully qualified domain name (FQDN) or IP address of the destination. You can choose to deliver the original email or the modified email.
Deliver to original host	Enable to route the email to the original SMTP server or relay. Note the you can deliver email to both the original and alternate hosts. You can choose to deliver the original email or the modified email.
FortiGuard spam outbreak protection	Enable to send incoming email to the deferred mail queue. See also Configuring mail settings on page 49.
Defer delivery	Enable to defer delivery of emails that may be resource intensive and reduce throughput of the mail server, such as large email messages, or mass email such as marketing campaign email and newsletter digest. See also. See also Configuring mail settings on page 49.
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 Configuring custom messages and email templates on page 51.

GUI item	Description
Notify with profile	Enable and select a notification profile to send a notification email to the sender, recipient, or any other people as you configure in the notification profile. The notification email is customizable and will tell the users what happened to the email message. For details about notification profiles and email templates, see Configuring notification profiles on page 242 and Customizing email templates on page 59.
Final action	Select one of the following final actions listed below for the content action profile.
Discard	Enable to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.
Reject	Enable to reject the email and reply to the SMTP client with SMTP reply code 550.
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 22. 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	Enable to redirect the email to the system quarantine and specify the quarantine folder. For more information, see Managing the system quarantine on page 25. You can choose to quarantine the original email or the modified email.
Domain quarantine	Enable to redirect email to the domain quarantine folder. For more information, see Managing the domain quarantines on page 27.
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 237. 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 129.
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 178.

4. To apply a content action profile, select it in the *Action* dropdown list of one or more antispam profiles. For details, see Managing antispam profiles on page 160.

Configuring replacement message profiles and variables

Starting from v7.2.0, replacement message customization for content and DLP actions and variable customization has been moved from *System* > *Customization* > *Custom Message* to *Profile* > *Replacement Message*.

The replacement messages are used in the content/DLP action profiles when specifying the "Replace with message" action (see Configuring content profiles and content action profiles on page 186), and in the antivirus action profiles when you specifying the "Replace infected/suspicious body or attachment" action (see Configuring antivirus profiles, file signatures, and antivirus action profiles on page 181).

You can customize replacement messages for the subject, body, or attachment part, depending on which part triggers the content/DLP scanning. For virus-infected email, you can replace either the email body or attachments.

Modifying replacement messages

You can modify the text and HTML code within a replacement message to suit your requirements.

You can change the content of the replacement message by editing the text and HTML codes and by working with replacement message variables.

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

To customize replacement messages

1. Go to *Profile* > *Replacement Message* > *Replacement Message*.
2. Click New to add a message or click edit to modify an existing message.
3. Enter a name for the message.
4. Enter a description.
5. Under Replacement Message, click New.
6. Select a type.
7. In the Replacement massage area, enter the content. There is a limit of 8191 characters for each replacement message.
8. Click Insert Variables to include any other existing variables, if needed.
9. Place your mouse cursor in the text message at the insertion point for the variable.
10. Click the name of the variable to add. It appears at the insertion point.
    For example, you may enter :
    `The file %%FILE%% has been detected containing virus %%VIRUS%%, and has been removed. File type is %%FILE_TYPE%%.`
    where `%%FILE%%` is the file name, `%%VIRUS%%` provides the virus name, and `%%FILE_TYPE%%` is the file type of the infected file.
11. To add a color code, use HTML tags, such as `<tr bgcolor="#3366ff">`. You can select a color code, such as `"#3366ff"` in the HTML tag, from the color palette after selecting Insert Color Code.

    Some message types include predefined variables.
12. Click OK, or click Reset To Default to revert the replacement message to its default text.

Creating variables

In addition to the predefined variables, you can create new ones to customize replacement messages and email templates. Typically, these variables represent messages that you will use frequently. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

To create a new variable

1. To create new variables to be used in the replacement messages, go to *Profile* > *Replacement Message* > *Variable*.
2. Click New.
   A dialog appears.
3. Configure the following:
   - In Name, enter the variable name to use in the replacement message. Its format is: `%%<variable_name>%%`. For example, if you enter the word `virus`, this variable will appear as `%%virus%%` in the replacement message if you select to insert it. This is usually a simple and short form for a variable.
   - In Display Name, enter words to describe the variable. For example, use `virus name` for the variable `virus`. The display name appears in the variable list when you select Insert Variables while customizing a message or creating a variable.
   - In Content, enter the variable's content.
4. Click Create.

Configuring resource profiles

Go to *Profile* > *Resource* > *Resource* to configure miscellaneous aspects of the email user accounts, such as disk space quota.

For more information on settings that can be applied to email user accounts, see Configuring local user accounts (server mode only) on page 84 and Configuring user preferences on page 88.

To view and configure resource profiles

1. Go to *Profile* > *Resource* > *Resource*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Domain (dropdown list)	Select System to see profiles for the entire FortiMail unit, or select a protected domain name to see profiles for that domain. You can see only the domains that are permitted by your administrator profile.
Profile Name	Displays the name of the profile.
Domain Name (column)	Displays either System or a domain name.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

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

GUI item	Description
Domain	For a new profile, select either System to apply the profile to the entire FortiMail unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter the name of the profile. The profile name is editable later.
Disk quota (MB)	Enter the disk space quota in Megabytes for this profile (set the value between 0-60000; default value is 1000). Note that this option is only available in server mode.
User account status	Enable email user accounts using this resource profile. If not enabled, the user will have no access to FortiMail system, including webmail, address book, quarantine, or any other functions.
Webmail access	Enable to allow email users to access FortiMail webmail and other webmail features, such as auto reply and address books: • *User preference access*: Determine whether users can access user preference options, including idle timeout and ability to automatically check for new messages. • *Address book access*: Determine whether users can access the domain address book and system address book. • *Quarantine attachment download*: Enable or disable attachment download for quarantined email. Note this option is only available for Server and Gateway mode. When disabled, all email within the *Bulk* folder (including subfolders) will have attachment download disabled.

GUI item	Description
	• *Mobile device access*: Enable for disable user mail access via mobile device.
Email Continuity	Enable to enforce email continuity for instances where the SMTP server is inaccessible. **Note:** This feature is license based, and must be enabled under FortiGuard services. See Configuring FortiGuard services on page 64 for more information. When the SMTP server is detected as inaccessible, recipient verification is skipped and emails are put into the email continuity queue. When the SMTP server is accessible again, the email is delivered. Note there is no DSN if the email is from an unknown user. Additionally, expand *Email continuity* and enable *BCC self*. When enabled, customers who log on to the webmail portal and who send email during a service disruption will have a copy of the mail sent back to them once service is restored.
Personal Quarantine	Specify the personal quarantine options, such as release method and safelisting.
Email Retention	Enter the number of days after which the FortiMail unit will automatically delete email that is locally hosted in each folder. 0 means not to delete email.

To apply the resource profile, you must select it in a policy. For details, see Controlling email based on sender and recipient addresses on page 138 and Controlling email based on IP addresses on page 132.

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 121.
2. For secure (SSL/TLS) authentication:
   - Upload a local certificate. For details, see Managing local certificates.
   - Enable *SMTP over SSL/TLS*. For details, see Configuring mail settings on page 49.
   - 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 235 and Configuring access control rules on page 121.
   - 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 Managing users on page 83, Managing certificate authority certificates, and Managing OCSP server certificates on page 1.
3. If authentication will occur by querying an external authentication server rather than email user accounts locally defined on the FortiMail unit, configure the appropriate profile type, either:
   - SMTP, IMAP, or POP3 (gateway mode or transparent mode only; see Configuring authentication profiles on page 202)
   - LDAP (see Configuring LDAP profiles on page 205)
   - RADIUS (see Configuring authentication profiles on page 202)

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 84 and Configuring resource profiles on page 199.
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 138 and Controlling email based on IP addresses on page 132.
   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 138.

Configuring authentication profiles

FortiMail Cloud units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS
- LDAP
- SSO

LDAP profiles can configure many features other than authentication. For details, see Configuring LDAP profiles on page 205.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine, and when authenticating with another SMTP server to deliver email.

For the general procedure of how to enable and configure authentication, see Workflow to enable and configure authentication of email users on page 201.

To configure an SMTP, IMAP, or POP3 authentication profile

1. Go to *Profile* > *Authentication* > *SMTP*, *IMAP*,or *POP3*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. Configure the following settings:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail Cloud 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.

GUI item	Description
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of a server that will be queried to authenticate email users if they authenticate to send email, or when they are accessing their personal quarantine.
Server port	Enter the port number on which the authentication server listens. See also Appendix C: Port Numbers on page 1.
Use generic LDAP mail host if available (SMTP authentication only)	For gateway and transparent mode, select this option if your LDAP server has a mail host entry for the generic user. For more information, see Domain Lookup Query on page 217. If you select this option, the FortiMail Cloud unit will query the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail Cloud 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 Cloud unit and this server, and if the server supports it.
STARTTLS	Enable if you want to upgrade the existing insecure connection to the secure connection using SSL/TLS.
Secure authentication	Enable if you want to use secure authentication to encrypt the passwords of email users when communicating with the server, and if the server supports it.
Server requires domain	Enable if the authentication server requires that email users authenticate using their full email address (such as `user1@example.com`) and not just the user name (such as `user1`).

4. To apply the authentication profile, depending on the mode in which your FortiMail Cloud unit is operating, you may be able to select the profile in incoming recipient-based policies, IP-based policies, and email user accounts. For details, see Controlling email based on sender and recipient addresses on page 138, Controlling email based on IP addresses on page 132, and Configuring local user accounts (server mode only) on page 84.

To configure a RADIUS authentication profile

1. Go to *Profile* > *Authentication* > *RADIUS*.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. Configure the following settings:

GUI item	Description
Domain	For a new profile, select either *System* to apply the profile to the entire FortiMail Cloud unit, or select a protected domain name to apply it to that domain. You can see only the domains that are permitted by your administrator profile.
Profile name	For a new profile, enter the name of the profile.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of a server that will be queried to authenticate email users if they authenticate to send email, or when they are accessing their personal quarantine.
Server port	Enter the port number on which the authentication server listens.

GUI item	Description
	See also Appendix C: Port Numbers on page 1.
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 Cloud interface uses to communicate with the RADIUS server will be applied.
Server secret	Enter the secret required by the RADIUS server. It must be identical to the secret that is configured on the RADIUS server.
Server requires domain	Enable if the authentication server requires that email users authenticate using their full email address (such as `user1@example.com`) and not just the user name (such as `user1`).

Advanced Setting	When you add a FortiMail Cloud administrator (see Configuring administrator accounts on page 47), 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 Cloud. 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 Cloud. The default ID is `3`, which is `Fortinet-Vdom-Name`.

4. To apply the authentication profile, depending on the mode in which your FortiMail Cloud unit is operating, you may be able to select the profile in incoming recipient-based policies, IP-based policies, and email user accounts. For details, see Controlling email based on sender and recipient addresses on page 138, Controlling email based on IP addresses on page 132, and Configuring local user accounts (server mode only) on page 84.

Configuring LDAP profiles

The *LDAP* submenu lets you configure LDAP profiles which can query LDAP servers such as FortiAuthenticator, Microsoft Active Directory, Red Hat Directory Server, or Google Cloud Identity for authentication, email address mappings, and more.

Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server. When LDAP queries do not match with the server's schema and/or contents, unintended mail processing behaviors can result, including bypassing antivirus scans. For details on preparing an LDAP directory for use with FortiMail Cloud LDAP profiles, see Preparing your LDAP schema for FortiMail Cloud LDAP profiles on page 220.

LDAP profiles each contain one or more queries that retrieve specific configuration data, such as user groups, from an LDAP server. The LDAP profile list indicates which queries you have enabled in each LDAP profile.

To view the list of LDAP profiles, go to *Profile* > *LDAP* > *LDAP*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click *Clone*. A single-field dialog appears. Enter a name for the new profile. Click *OK*.
Comment	Displays the comment in the profile.
Name	Displays the name of the profile.
Server	Displays the domain name or IP address of the LDAP server.
Port	Displays the listening port of the LDAP server.
Group	Indicates whether *Group Query Options* is enabled.
Auth	Indicates whether *User Authentication Options* is enabled.
Alias	Indicates whether *User Alias Options* is enabled.
Routing	Indicates whether *Mail Routing Options* is enabled.
Address Map	Indicates whether *Address Mapping Options* is enabled.
Cache	Indicates whether query result caching is enabled.
Ref.	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

You can add an LDAP profile to define a set of queries that the FortiMail Cloud 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 Cloud 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 Cloud unit itself. These other configuration areas will only allow you to select applicable LDAP profiles — that is, those LDAP profiles in which you have enabled the query required by that feature. For example, if a feature requires a definition of user groups, you can select only from those LDAP profiles where *Group Query Options* are enabled.

To configure an LDAP profile

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to add a profile or double-click a profile to modify it.
   A dialog appears.
3. Configure the following settings:

GUI item	Description
Name	For a new profile, enter a unique name.
Comment	Optional. Enter a descriptive comment.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. *Port*: Enter the port number where the LDAP server listens. The default port number varies by your selection in Use secure connection. See also Appendix C: Port Numbers on page 1.
Fallback server name/IP	Optional. Enter the fully qualified domain name (FQDN) or IP address of an alternate LDAP server that the FortiMail Cloud unit can query if the primary LDAP server is unreachable. *Port*: Enter the port number where the fallback LDAP server listens. The default port number varies by your selection in Use secure connection. See also Appendix C: Port Numbers on page 1.
Use secure connection	Select whether or not to connect to the LDAP servers using an encrypted connection. • *none*: Use a non-secure connection. • *SSL*: Use an SSL/TLS-secured (LDAPS) connection. If the LDAP server requires that clients such as the FortiMail Cloud unit present a client certificate to identify themselves during secure connections, then select the certificate from the *Client certificate* dropdown. Optionally,to authenticate using the selected certificate, enable *Use client certificate for TLS authentication*.This can be used instead of, or in addition to, a bind DN and password. See also Managing local certificates on page 1. Click *Test LDAP Query* to test the connection. A pop-up window appears. For details, see To verify user query options on page 227. **Note:** If your FortiMail Cloud unit is deployed in server mode, and you want to enable *Enable webmail password change* using an LDAP server that uses a Microsoft Active Directory-style schema, then you must select *SSL*. Active Directory servers require a secure connection for queries that change user passwords. **Note:** The certificate that FortiMail Cloud uses for client authentication must: • not be expired • not be revoked • be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail Cloud unit and that the server trusts (directly or indirectly, proven via a signing chain) Otherwise the secure connection will fail. Servers may have their own certificate validation requirements in addition to FortiMail Cloud requirements. For example, client certificates may require that `Key Usage` field allow client authentication. See your LDAP server's documentation.
Default Bind Options	

GUI item	Description
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail Cloud will search for user objects, such as: `ou=People,dc=example,dc=com` User objects should be child nodes of this location.
Bind DN	Enter the bind DN of an LDAP user account with permissions to query the *Base DN*, such as: `cn=fortimail,dc=example,dc=com`
Bind password	Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in Base DN, or, if you have not yet entered a Base DN, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your Base DN, or need to look up attribute names. For example, if the Base DN is unknown, browsing can help you to locate it. **Note:** Before you click *Browse*, you must configure Server name/IP, Use secure connection, Bind DN, Bind password, and Protocol version, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.

4. Configure the following sections:
   - Configuring user query options on page 207
   - Configuring group query options on page 209
   - Configuring user authentication options on page 210
   - Configuring user alias options on page 211
   - Configuring mail routing on page 214
   - Configuring address mapping options on page 215
   - Configuring scan override options on page 216
   - Configuring domain lookup options on page 217
   - Configuring remote access override options on page 218
   - Configuring LDAP chain query on page 219
   - Configuring advanced options on page 219

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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *User Query Options* section.
4. Configure the query to retrieve the distinguished names (DN) of user objects by their email addresses:

GUI item	Description
Schema	Click *Schema* to select a schema style. Then you can edit the schema or select *User Defined* and write your own schema.
User query	Enter an LDAP query filter that selects a set of user objects from the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects. For details, see Example: LDAP user query on page 208. 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.

Example: LDAP user query

For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:

```
(& (objectClass=inetOrgPerson) (mail=$m))
```

where `$m` is the FortiMail Cloud 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 Cloud 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 Cloud variable for the tag to remove before performing the query.

For some schemas, such as Microsoft Active Directory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure *User Alias Options* to resolve aliases. For details, see Configuring user alias options on page 211.

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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand *Group Query Options* section.

   For more information on determining user group membership by LDAP query, see Controlling email based on sender and recipient addresses on page 138 or Controlling email based on IP addresses on page 132.
4. Configure the following:

GUI item	Description
Use LDAP tree node as group	Enable to use objects within the Base DN of *User Query Options* as if they were members of a user group object. For example, your LDAP directory might not contain user group objects. In that sense, groups do not really exist in the LDAP directory. However, you could mimic a group's presence by enabling this option to treat all users that are child objects of the Base DN in *User Query Options* as if they were members of such a group.
Group membership attribute	Enter the name of the attribute, such as `memberOf` or `gidNumber`, whose value is the group number or DN of a group to which the user belongs. This attribute must be present in user objects. Whether the value must use common name, group number, or DN syntax varies by your LDAP server schema. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`.
Use group name with base DN as group DN	Enable to specify the base distinguished name (DN) portion of the group's full DN in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query. For example, you might find it more convenient in each recipient-based policy to type only the group name, `admins`, rather than typing the full DN, `cn=admins,ou=Groups,dc=example,dc=com`. In this case, you could enable this option, then configure Group base DN (`ou=Groups,dc=example,dc=com`) and Group name attribute (`cn`). When performing the query, the FortiMail Cloud unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the Group name attribute and the Group base DN configured in the LDAP profile. **Note:** Enabling this option is appropriate **only if** your LDAP server's schema specifies that the group membership attribute's value must use DN syntax. It is **not** appropriate if this value uses another type of syntax, such as a number or common name. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`. Because a group ID number does not use DN syntax, you would not enable this option.
Group base DN	Enter the base DN portion of the group's full DN, such as:

GUI item	Description
	`ou=Groups,dc=example,dc=com` This option is available only if Use group name with base DN as group DN is enabled.
Group name attribute	Enter the name of the attribute, such as `cn`, whose value is the group name of a group to which the user belongs. This option is available only if Use group name with base DN as group DN is enabled.
Max group expansion level	Enter how many levels of nested groups will be expanded for lookup. Valid range is 1-6. Default value is 1.
Lookup group owner	Enable to query the group object by its distinguished name (DN) to retrieve the DN of the group owner, which is a user that will receive that group's quarantine reports. Using that user's DN, the FortiMail Cloud 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 75 and Managing the personal quarantines on page 22.
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 Cloud 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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *User Authentication Options* section.
   For more information on authenticating users by LDAP query, see Controlling email based on sender and recipient addresses on page 138.
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 Cloud 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.

GUI item	Description
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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *User Alias Options* section.

   Resolving aliases to real email addresses enables the FortiMail Cloud 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 Cloud units operating in server mode, this means that users need only log in to their primary account in order to manage their spam quarantine, rather than logging in to each alias account individually.
4. Configure the following:

GUI item	Description
Schema (dropdown list)	Click *Schema* to select a schema style. Then you can edit the schema or select *User Defined* and write your own schema.
Alias member attribute	Enter the name of the attribute, such as `mail` or `rfc822MailMember`, whose value is an email address to which the email alias resolves, such as `user@example.com`. This attribute must be present in either alias or user objects, as determined by your schema and whether it resolves aliases directly or indirectly. For more information, see Base DN on page 207. 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 objects that are not user/alias objects. For details, see Example: Alias member query on page 213. For more information on required object types and their attributes, see Preparing your LDAP schema for FortiMail Cloud LDAP profiles on page 220.

GUI item	Description
	For details on query syntax, refer to any standard LDAP query filter reference manual.
User group expansion In advance	Enable if your LDAP schema resolves email aliases indirectly. For more information on direct versus indirect resolution, see Base DN on page 207. When this option is **disabled**, alias resolution occurs using **one** query. The FortiMail Cloud 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 Cloud 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 Cloud 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 Cloud unit must first "expand" the alias object into its constituent user objects before it can resolve the alias email address. This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*.
Group member attribute	Enter the name of the attribute, such as `member`, whose value is the DN of a user object. This attribute must be present in alias objects only if they do not contain an email address attribute specified in Alias member attribute. This option is preconfigured and read-only if you have selected from Schema any schema style other than *User Defined*. If you have selected *User Defined*, this option is available only if User group expansion In advance is enabled.
Group member query	Enter an LDAP query filter that selects a set of alias objects, represented as a group of member objects in the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all alias objects but also exclude non-alias objects. For example, if alias objects in your directory have two distinguishing characteristics, their `objectClass` and `proxyAddresses` attributes, the query filter might be: `(&(objectClass=group) (proxyAddresses=smtp:$m))` where `$m` is the FortiMail Cloud 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	Specify the maximum number of alias nesting levels that will be expanded for lookup. Valid range is 1-12 and the default value is 1.
Scope	Select which level of depth to query, starting from Base DN. • *One level*: Query only the one level directly below the base DN in the LDAP directory tree.

GUI item	Description
	• *Subtree:* Query recursively all levels below the base DN in the LDAP directory tree.
Derefer	Select the method to use, if any, when dereferencing attributes whose values are references. • *Never*: Do not dereference. • *Always*: Always dereference. • *Search*: Dereference only when searching. • *Find*: Dereference only when finding the base search object.
Use separate bind (configure the following if Default Bind Options on page 206 is not what you want)	
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail Cloud will search for either alias or user objects. User or alias objects should be child nodes of this location. Whether you should specify the base DN of either user objects or alias objects varies by your LDAP schema style. Schema may resolve alias email addresses directly or indirectly (using references). • With a direct resolution, alias objects directly contain one or more email address attributes, such as `mail` or `rfc822MailMember`, whose values are user email addresses such as `user@example.com`, and that resolves the alias. The Base DN, such as `ou=Aliases,dc=example,dc=com`, should contain alias objects. • With an indirect resolution, alias objects do **not** directly contain an email address attribute that can resolve the alias; instead, in the style of LDAP group-like objects, the alias objects contain only references to user objects that are “members” of the alias “group.” User objects’ email address attribute values, such as `user@example.com`, actually resolve the alias. Alias objects refer to user objects by possessing one or more “member” attributes whose value is the DN of a user object, such as `uid=user,ou=People,dc=example,dc=com`. The FortiMail Cloud unit performs a first query to retrieve the distinguished names of “member” user objects, then performs a second query using those distinguished names to retrieve email addresses from each user object. The Base DN, such as `ou=People,dc=example,dc=com`, should contain user objects.
Bind DN	Enter the bind DN of an LDAP user account with permissions to query the Base DN, such as: `cn=FortiMail CloudA,dc=example,dc=com`
Bind password	Enter the password of the Bind DN.

Example: Alias member query

For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:

```
(& (objectClass=alias) (mail=$m))
```

where `$m` is the FortiMail Cloud 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 Cloud 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 Cloud 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 207.

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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Mail Routing Options* section.

The *Mail Routing Options* section query occurs after recipient tagging processing. If you have enabled recipient tagging, the *Mail Routing Options* section query will then be based on the tagged recipient address. If the tagged email address does not exist for the user in the LDAP directory, you may prefer to transform the recipient address by using the *User Alias Options*.

4. Configure the following:

GUI item	Description
Mail host attribute	Enter the name of the attribute, such as `mailHost`, whose value is the fully qualified domain name (FQDN) or IP address of the email server that stores email for the user's email account. 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.

GUI item	Description
	For example, a user may have many aliases and external email addresses that are not necessarily known to the email server. These addresses would all map to a real email account (mail routing address) on the email server (mail host) where the user's email is actually stored. A user's recipient email address located in the envelope or header portion of each email will be rewritten to this address. This attribute must be present in user objects.

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 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Address Mapping Options* section.

   Mappings usually should not translate an email address into one that belongs to an unprotected domain. However, unlike locally defined address mappings, this restriction is not enforced for mappings defined on an LDAP server.

   After configuring a profile with this query, you must select it in order for the FortiMail Cloud unit to use it.

   Alternatively, you can configure email address mappings on the FortiMail Cloud unit itself.
4. Configure the following:

GUI item	Description
Internal address attribute	Enter the name of the LDAP attribute, such as `internalAddress`, whose value is an email address in the same or another protected domain. This email address will be rewritten to the value of the external address attribute according to the match conditions and effects. The name of this attribute may vary by the schema of your LDAP directory.
External address attribute	Enter the name of the attribute, such as `externalAddress`, whose value is an email address in the same or another protected domain. This email address will be rewritten to the value of the internal address attribute according to the match conditions and effects. The name of this attribute may vary by the schema of your LDAP directory.
Display name attribute	Enter the name of the attribute, such as `displayName`, whose value is the display name of the user. This display name will be inserted into the sender message header before the external email address, such as: `From: Display Name<externalAddress@example.com>` The name of this attribute may vary by the schema of your LDAP directory.

Configuring scan override options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Scan Override Options* section.

If the *Scan Override Options* query fails, then the FortiMail Cloud unit will instead use the antispam, antivirus, and content processing settings defined in the profile for that policy.

4. Configure the following:

GUI item	Description
AntiSpam attribute	Enter the name of the attribute, such as `antispam`, whose value indicates whether or not to perform antispam processing for that user, and which antispam profile to use. Multiple syntax values are permissible. For details, see LDAP directory requirements for each FortiMail Cloud LDAP profile query on page 222. 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 217). 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 Cloud LDAP profile query on page 222. 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 217). 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 Cloud LDAP profile query on page 222. 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 217). 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 205.

When configuring domain settings in gateway and transparent mode, if you set the *Relay Type* to *LDAP Domain Mail Host*, FortiMail will query the LDAP server to look up the domain and apply the antispam, antivirus, and content profiles assigned to this domain. If you set the Relay Type to other methods, the following settings will not apply.

If the LDAP server does not find a user matching the domain, the user is considered as unknown, and the mail will be rejected unless it has a specific access list entry.

For this option to work, your LDAP directory should contain a single generic user for each domain such as `generic@example.com` because the FortiMail unit will only look at the domain portion of the generic user's mail address, such as `example.com`.

When an SMTP session is processed, the FortiMail unit will query the LDAP server for the domain portion retrieved from the recipient email address. If the LDAP server finds a user entry, it will reply with the domain objects defined in the LDAP directory, including parent domain attribute, generic mail host attribute, generic antispam attribute, and generic antivirus attribute. The FortiMail unit will remember the mapping domain, mail routing, and antispam and antivirus profiles information to avoid querying the LDAP server again for the same domain portion retrieved from a recipient email address in the future.

If there are no antispam and antivirus profiles for the user, the FortiMail unit will use the antispam and antivirus profiles from the matching IP policy.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Domain Lookup Options* section.
4. Configure the following:

GUI item	Description
Domain Lookup Query	Enter an LDAP query filter that selects a set of domain objects, whichever object class contains the attribute you configured for this option, from the LDAP directory. Since each domain needs a generic user in the LDAP directory, you can specify the query filter as the following: `mail=generic@$d` Where the value of $d is the domain name.
Parent domain attribute	Enter the name of the attribute, such as `parentDomain`, whose value is the name of the parent domain from which a domain inherits the specific `RCPT TO:` check settings and quarantine report settings. The name of this attribute may vary by the schema of your LDAP directory.
Mail host attribute	Enter the name of the attribute, such as `mailHost`, whose value is the IP address of the backend mail server hosting the mailboxes of the domain. The name of this attribute may vary by the schema of your LDAP directory.
AntiSpam attribute	Enter the name of the attribute, such as `genericAntispam`, whose value is the name of the antispam profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory.

GUI item	Description
	If you do not specify this attribute (that is, leave this field blank), the antispam profile in the matched recipient-based policy will be used.
AntiVirus attribute	Enter the name of the attribute, such as `genericAntivirus`, whose value is the name of the antivirus profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute (that is, leave this field blank), the antivirus profile in the matched recipient-based policy will be used.
Content attribute	Enter the name of the attribute, such as `genericContent`, whose value is the name of the content profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute (that is, leave this field blank), the content profile in the matched recipient-based policy will be used.

Configuring remote access override options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 205.

When you add a FortiMail administrator (see Configuring administrator accounts on page 47), you must specify an access profile (the access privileges) for the administrator. You must also specify a domain (either system or a protected domain) that the administrator is allowed to access.

If you are adding an LDAP account, you can override the access profile and domain setting with the values of the remote attributes returned from the LDAP server.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Remote Access Override Options* section.
4. Configure the following:

GUI item	Description
Enable remote access override	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing access profile. If there is no match, the specified access profile will still be used. Also specify the access profile attribute.
Enable remote domain override	Enable to override the domain you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing protected domain. If there is no match, the specified domain will still be used. Also specify the domain name attribute.

Configuring LDAP chain query

If you use different attributes for similar or same values on different LDAP servers, you may want to query all of the LDAP servers one by one (a chain query).

You can do this by grouping several LDAP profiles into one LDAP profile. The order of the profiles determines the sequential order of the queries.

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *LDAP Profile Chain.*
4. From the LDAP profile list, select the profile you want to add to the chain and click the plus sign.
5. Repeat the above step to add more profiles.

Configuring advanced options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 205.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Advanced Options* section.
4. Configure the following:

GUI item	Description
Timeout	Enter the maximum amount of time in seconds that the FortiMail Cloud unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server.
Referrals chase	Enable to use the LDAP server's function of referral chasing, that is, instead of returning a result, it will return a referal to another LDAP server, which may contain further information.
Enable cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiMail Cloud unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of `0` effectively disables caching.
Clear Cache	Select to empty the FortiMail unit's LDAP query cache. This can be useful if you have updated the LDAP directory, and want the FortiMail unit to refresh its LDAP query cache with the new information.

GUI item	Description
TTL	Enter the amount of time, in minutes, that the FortiMail Cloud unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail Cloud 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 Cloud webmail users to change their password. This option does not appear for FortiMail Cloud units operating in gateway or transparent mode. *Active Directory* appears only if Use secure connection is *SSL*.
Password schema	Select your LDAP server's user schema style, either *Openldap* or *Active Directory*.
Bypass user verification if server is unavailable	If you have selected using LDAP server to verify recipient or sender address and your LDAP server is not accessible, then you can enable this option to bypass the address verification process. **Note:** This option only takes effect in gateway and transparent mode. For more information about recipient address verification, see Configuring recipient address verification on page 72.

Preparing your LDAP schema for FortiMail Cloud LDAP profiles

FortiMail Cloud units can be configured to consult an LDAP server for many things that you might otherwise normally have to configure on the FortiMail Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud units can perform antivirus processing, which can be switched off or on depending on the results from an LDAP query. The FortiMail Cloud unit expects the query to return a value that may use Boolean syntax (`TRUE` or `FALSE`) that reflects whether or not, respectively, to perform antivirus processing. In this case, you would add to user objects in your LDAP directory an antivirus attribute whose value is a Boolean value.

The following table indicates expected object types, attribute names, and value syntax, as well as query results, for each LDAP profile query. Attributes listed should be present, but their names may vary by schema. Attributes that do not have a default name require that you configure them in both your LDAP profile and your LDAP directory's schema.

LDAP directory requirements for each FortiMail Cloud LDAP profile query

Object type	Attribute	Value	Query result
User Query Options			

Object type	Attribute	Value	Query result
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			
(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 207.	`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 207.

Object type	Attribute	Value	Query result
User group object classes such as `group` or `groupOfNames`. User groups are not inherently associated with email aliases, but for some schemas, such as Microsoft Active Directory, group objects play the role of email alias objects, and are used to indirectly resolve email aliases. For details, see Base DN on page 207.	`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 207.
Mail Routing Options			
(Objects from *User Query Options*.)	`mailHost`	A fully qualified domain name (FQDN) or IP address.	Query retrieves the fully qualified domain name (FQDN) or IP address of the mail server — sometimes also called the mail host — that stores email for any user defined by *User Query Options*.
	`mailRoutingAddress`	A user's email address for a user account whose email is physically stored on `mailHost`.	Query retrieves the email address for a real account physically stored on `mailHost` for any user defined by *User Query Options*.
Scan Override Options			
(Objects from *User Query Options*.)	No default attribute name.	Varies by schema. May be: • `TRUE`, `YES`, `1`, `ENABLE` or `ENABLED` (on) • `FALSE`, `NO`, `0`, `DISABLE`, or `DISABLED`, or any other value not associated with "on" (off) • the name of an antivirus profile	Query retrieves whether or not to perform **antivirus** processing, or which profile to use, for any user defined by *User Query Options*.

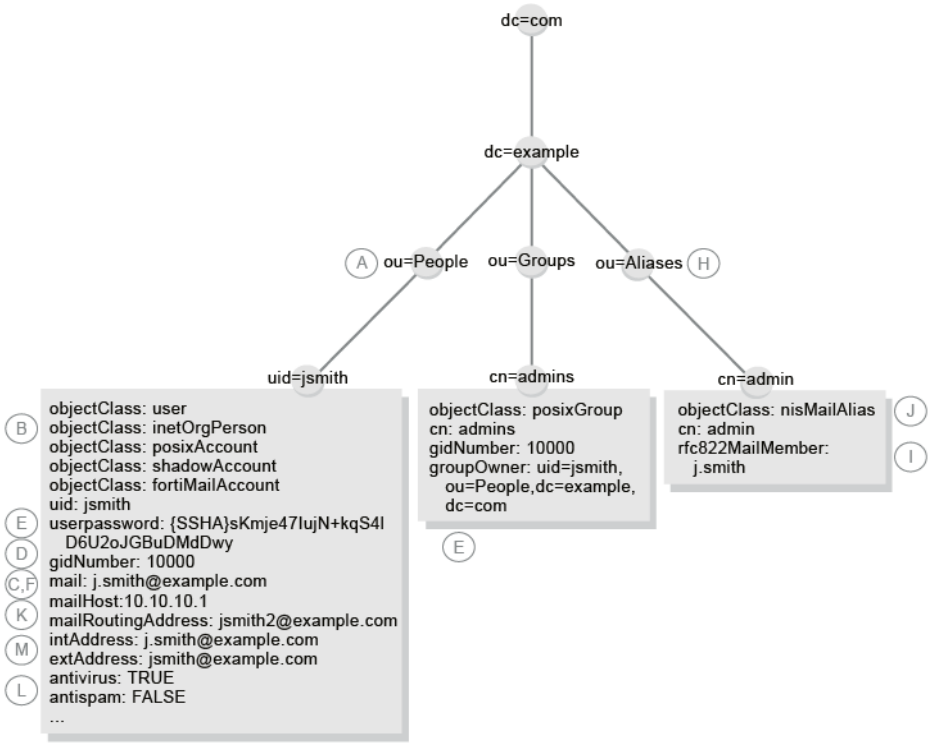
Object type	Attribute	Value	Query result
	No default attribute name.	Varies by schema. May be: • `TRUE`, `YES`, `1`, `ENABLE` or `ENABLED` (on) • `FALSE`, `NO`, `0`, `DISABLE`, or `DISABLED`, or any other value not associated with “on” (off) • the name of an antivirus profile	Query retrieves whether or not to perform **antispam** processing, or which profile to use, for any user defined by *User Query 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 Cloud 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.

Example: Compatible LDAP directory and LDAP profile



Testing LDAP profile queries

After you have created an LDAP profile, you should test each enabled query in the LDAP profile to verify that the FortiMail unit can connect to the LDAP server, that the LDAP directory contains the required attributes and values, and that the query configuration is correct.

When testing a query in an LDAP profile, you may encounter error messages that indicate failure of the query and how to fix the problem.

LDAP Query Failure Message	Meaning and Solution
Empty input	The query cannot be performed until you provide the information required by the query.
Connection Failed	The FortiMail Cloud unit could not connect to the LDAP server. The LDAP server may be unreachable, or the LDAP profile may be configured with an incorrect IP address, port number, or secure connection setting.
Failed to bind with bind DN and password	The FortiMail Cloud unit successfully connected to the LDAP server, but could not authenticate in order to perform the query. If the server permits anonymous queries, the Bind DN and Bind password you specified in *User Query Options* section should be blank. Otherwise, you must enter a valid bind DN and its password.

LDAP Query Failure Message	Meaning and Solution
Unable to found user DN that matches mail address	The FortiMail Cloud 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 Cloud unit successfully located a user with that email address, but their group membership attribute did not match your supplied value. The group membership attribute you specified in *Group Query Options* may not exist, or the value of the group membership attribute may not match the value that you supplied in Group base DN. If the value does not match, verify that you have supplied the Group base DN according to the syntax expected by both your LDAP server and your configuration of *Group Query Options*.
Group owner query failure	The FortiMail unit successfully connected to the LDAP server, but could not find a group whose distinguished name matched that value. The group may not exist on the LDAP server, or the value of the group's distinguished name attribute does not match the value that you entered in Group base DN.
Authentication failure	
Failed to bind	The FortiMail Cloud unit successfully located a user with that email address, but the user's bind failed and the FortiMail Cloud unit was unable to authenticate the user. Binding may fail if the value of the user's password attribute does not match the value that you supplied in *Old password*. If this error message appears when testing Enable webmail password change, it also implies that the query failed to change the password.
Unable to find mail alias	The FortiMail Cloud unit was unable to find the email alias. The email address alias may not exist on the LDAP server in the Base DN and using the query filter you specified in *User Alias Options*, or the value of the alias' email address attribute does not match the value that you supplied in *Mail address*.
Error for LDAP user profile ID	The FortiMail Cloud unit failed to change the email user's password. Verify that you have entered the correct existing password in *Old password*.

To verify user query options

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose *User Query Options section* query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *User*.
5. In *Mail address*, enter the email address of a user on the LDAP server, such as `test@example.com`.
6. Click *Test*.
   The FortiMail Cloud 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 Cloud configuration, such as for a recipient-based policy.
7. Click *Test*.

   The FortiMail Cloud 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 Cloud configuration, such as for a recipient-based policy.
6. Click *Test*.

   The FortiMail Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud 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 Cloud unit to query the updated LDAP server, refreshing the cache.

1. Go to *Profile* > *LDAP* > *LDAP*.
2. Double-click the LDAP profile whose query cache you want to clear.
3. Click *Test LDAP Query*.
4. From *Select query type*, select *Clear Cache*.
   A warning appears at the bottom of the window, notifying you that the cache for this LDAP profile will be cleared if you proceed. All queries will therefore be new again, resulting in decreased performance until the query results are again cached.
5. Click *OK*.
   The FortiMail Cloud 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 160 and Configuring content profiles and content action profiles on page 186.

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 287.

Predefined patterns

Canadian SIN	Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666.
US SSN	United States Social Security number. The format is a nine digit number, such as 078051111.
Credit Card	Major credit card number formats.
ABA Routing	A routing transit number (RTN) is a nine digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which it was drawn.
CUSIP	CUSIP typically refers to both the Committee on Uniform Security Identification Procedures and the 9-character alphanumeric security identifiers that they distribute for all North American securities for the purposes of facilitating clearing and settlement of trades.
ISIN	An International Securities Identification Number (ISIN) uniquely identifies a security. Securities for which ISINs are issued include bonds, commercial paper, equities and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at trading and settlement.

To view the list of dictionary profiles

1. Go to *Profile* > *Dictionary* > *Dictionary*.

GUI item	Description
Export (button)	Select one dictionary check box and click Export. Follow the prompts to save the dictionary file. Note that you can only export one dictionary at a time.
Import (button)	Select one dictionary check box and then click the import button to import dictionary entries into the existing dictionary. In the dialog, click Browse to locate a dictionary in text format. Click OK to upload the file. Note that you can only select one dictionary at a time and you can only import dictionary entries into an existing dictionary.
Name	Displays the dictionary name.

2. Click New to create a new profile or double-click a profile to modify it.
   A two-part page appears.
3. For a new profile, type its name. The profile name is editable later.
4. To enable or edit a predefined pattern:
   - Double-click a pattern in Smart Identifiers.
   - A dialog appears.
   - Select Enable to add the pattern to the dictionary profile.
   - To edit a predefined pattern, do the same as for a user-defined pattern in Step 5
   - Click OK.
5. To add or edit a user-defined pattern:
   - Click *New* under Dictionary Entries to add an entry or double click an entry to modify it.
   - A dialog appears.
6. Configure a custom entry.

GUI item	Description
Enable	Select to enable a pattern.

Pattern	Type a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression. Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text.
	Regular expressions do not require slash (`/`) boundaries. For example, enter:
	`v[i1]agr?a`
	Matches are not case sensitive and can occur over multiple lines as if the word were on a single line (that is, Perl-style match modifier options `i` and `s` are in effect).
	The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, **not** the originally encoded string. For example, if the original encoded string is:
	`=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=`
	then the pattern must match:
	`Se trata del spam.`
	Entering the pattern `*iso-8859-1*` would **not** match.

GUI item	Description
	This option is not editable for predefined patterns.
Pattern type	For a new dictionary entry, select either: • Wildcard: Pattern is verbatim or uses only simple wild cards (`?` or `*`). • Regex: Pattern is a Perl-style regular expression. See also Syntax on page 1. 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 171. For more information about content monitor profiles, see Configuring content monitor and filtering on page 192.
Pattern max weight	Enter the maximum by which matches of this pattern can contribute to an email's dictionary match score. This option applies only if Enable pattern max weight limit is enabled.
Enable pattern max weight limit	Enable if the pattern must not increase an email's dictionary match score more than the amount configured in Pattern max weight.
Search header	Enable to match occurrences of the pattern when it is located in an email's message headers, including the subject line. The FortiMail unit uses the full header string, including the header name and value, to match the pattern. Therefore, when you define the pattern, you can specify both the header name and value. For example, such a pattern entry as `from: .*@example.com.*` will block all email messages with the From header as `xxx@example.com`.
Search body	Enable to match occurrences of the pattern when it is located in an email's message body.

To apply a dictionary, in an antispam profile or content profile, either select it individually or select a dictionary group that contains it. For more information, see Configuring dictionary groups on page 233, Managing antispam profiles on page 160, and Configuring content profiles on page 186.

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 231.

To view and configure a dictionary group

1. Go to *Profile* > *Dictionary* > *Group*.

GUI item	Description
Create New	Select the name of a protected domain from Select Domain, then click Create New to add a dictionary for that protected domain. **Note:** If you have not yet configured a protected domain, new dictionary groups will by default be assigned to the system domain. For more information on protected domains, see “Configuring protected domains” on page 229.
Select Domain	Select the name of a protected domain to display dictionary groups belonging to that protected domain, or select system to display system-wide dictionary groups. This option is not available if you have not yet configured a protected domain. For more information on protected domains, see “Configuring protected domains” on page 229.
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Group Name	Displays the name of the dictionary group or dictionary group item.
Domain	The entire FortiMail unit (System) or name of a protected domain to which the profile is assigned. Which dictionary groups are visible and modifiable by the administrator varies by whether a FortiMail administrator account is assigned to specific protected domain. For more information, see “About administrator account permissions and domains” on page 143.
Description	The description of the dictionary group.

2. Either click New to add a profile or double-click a profile to modify it.
3. For a new group, enter the name of the dictionary group in Group name.
4. In the Available dictionaries area, select one or more dictionaries that you want to include in the dictionary group, then click ->.
   The dictionaries move to the Members area.
5. Click Create or OK.

To apply a dictionary group, select it instead of a dictionary profile when configuring an antispam profile or content profile. For details, see Managing antispam profiles on page 160 and Configuring content profiles on page 186.

Configuring security profiles

Go to *Profile* > *Security* to create transport layer security (TLS) profiles and encryption profiles.

This section includes:

Configuring TLS security profiles

The TLS tab lets you create TLS profiles, which contain settings for TLS-secured connections.

TLS profiles, unlike other types of profiles, are applied through access control rules and message delivery rules, not policies. For more information, see Controlling SMTP access and delivery on page 121.

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. • **Secure**: Requires a certificate-authenticated TLS connection. CA certificates must be installed on the FortiMail Cloud unit before they can be used for secure TLS connections. For information on installing CA certificates, see Managing certificate authority certificates.
Action On Failure	Indicates the action the FortiMail Cloud unit takes when a TLS connection cannot be established, either: • **Temporarily Fail**: Reply to the SMTP client with a code indicating temporary failure. • **Fail**: Reject the email and reply to the SMTP client with SMTP reply code 550.  Optionally, you can choose to select the *IBE on TLS failure* option when configuring an encryption profile. For more information, see Configuring encryption profiles on page 237.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

To configure a TLS profile

1. Go to *Profile* > *Security* > *TLS*.
   A dialog appears.
2. Either click *New* to add a profile or double-click a profile to modify it.
3. For a new profile, enter the *Profile name*.
4. From *TLS option*, select the security level of the TLS profile.
5. Configure the following, as applicable:
   The availability of the following options varies by your selection in TLS option.

GUI item	Description
Check TLS version	Enable to select a *Minimum TLS version* to apply for the TLS profile.

GUI item	Description
	 The connection will be refused if the *Minimum TLS version* is not met, regardless of whether *TLS option* is set to *Preferred* or *Secure*. • SSL 3.0 • TLS 1.0 • TLS 1.1 • TLS 1.2 • TLS 1.3
DANE	Assign a DNS-based Authentication of Named Entities (DANE) support level: • None • Opportunistic • Mandatory (only available when TLS option is set to Secure) For more information, see RFC 7929.

MTA-STS	Assign an MTA Strict Transport Security (MTA-STS) domain checking level.
	Note that the MTA-STS feature may only take effect when enabled under *System* > *Mail Setting* > *Mail Server Settings*, or via the CLI Console:
	`config system mailserver`
	`set smtp-mtasts-status {check-all-domain | check-external-domain | disable}`
	`end`
	For more information, see Configuring mail settings on page 49

Action on failure	Select whether to fail or temporarily fail if a TLS connection with the parameters described in the TLS profile cannot be established.
Check encryption strength	Enable to require a minimum level of encryption strength. Also configure *Minimum encryption strength*. This option appears only if *TLS option* is *Secure*.
Minimum encryption strength	Enter the bit size of the encryption key. Greater key size results in stronger encryption, but requires more processing resources.
Check CA issuer	Enable and enter a string on the CA issuer field. The FortiMail Cloud unit will compare the string in the CA issuer field with the field with that same name in the installed CA certificates.  The CA issuer string format must use **no** spaces, and must use slashes "/" to separate the certificate components. For example: /CN=Fortinet/O=Fortinet Ltd. This option appears only if TLS level is Secure.
CA issuer	Select the type of match required when the FortiMail Cloud unit compares the string in the `CA Issuer` field and the same field in the installed CA certificates. For more information on CA certificates, see Managing certificate authority certificates. Check CA issuer must be enabled for CA issuer to have any effect.

GUI item	Description
	This option appears only if TLS level is Secure.
Lookup CA	To populate the CA issuer field with text from a CA certificate's `CA Issuer`, select the name of a CA certificate that you have uploaded to the FortiMail Cloud unit.
Check certificate subject	Enable and enter a string in the Certificate subject field. The FortiMail Cloud unit will compare the string in the Certificate subject field with the field with that same name in the installed CA certificates.  The certificate subject string format must use **no** spaces, and must use slashes "/" to separate the certificate components. For example: /CN=Fortinet/O=Fortinet Ltd. This option appears only if TLS level is Secure.
Certificate subject	Select the type of match required when the FortiMail Cloud unit compares the string in the Certificate subject and the same field in the installed CA certificates. Check certificate subject must be enabled for Certificate subject to have any effect. This option appears only if TLS level is Secure.

Configuring encryption profiles

The Encryption tab lets you create encryption profiles, which contain encryption settings for secure MIME (S/MIME), identity-based encryption (IBE), and fallback to IBE if TLS delivery fails.

The ability to fallback automatically to IBE if TLS encryption fails ensures that all email is sent encrypted, even in instances where encryption keywords are used.

Encryption profiles are applied through either message delivery rules or content action profiles used in content profiles which are included in policies. For more information, see Configuring delivery rules on page 129 and Configuring content action profiles on page 195.

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 292.

For more information about using S/MIME encryption, see Using S/MIME encryption on page 239.

For more information about using IBE, see Configuring IBE encryption on page 287.

To view or configure encryption profiles

1. Go to *Profile* > *Security* > *Encryption*.

GUI item	Description
Clone (button)	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click Clone. A single-field dialog appears. Enter a name for the new profile. Click OK.
Profile Name	Displays the name of the profile.
Protocol	Displays the protocol used for this profile, S/MIME, IBE, or IBE on TLS failure.
TLS profile	Select the TLS profile for FortiMail to use first before falling back to the IBE profile, when necessary.
Encryption algorithm	Displays the encryption algorithm that will be used to encrypt the email (AES 128, AES 192, AES 256, CAST5 128, or Triple DES).
Action	For S/MIME, the actions are Encrypt, Sign, or Encrypt and Sign. For IBE, the action will be Encrypt only.
Action on failure	Indicates the action the FortiMail Cloud unit takes when S/MIME or IBE cannot be used: • Drop and send DSN: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable. • Send plain message: Deliver the email without encryption. • Enforce TLS: If the message delivery rule has no TLS profile or the TLS level in its profile is Preferred, the FortiMail unit will enforce the TLS Secure level. If the TLS level in its profile is None, then the email will temp fail because it contradicts with Enforce TLS. For more information, see Configuring delivery rules on page 129 and Configuring TLS security profiles on page 235.
Access method	Displays the action used by the mail recipients to retrieve IBE messages. • Push: A notification and a secure mail is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit does not store the message. • Pull: A notification is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit stores the message.
Maximum size (KB) for Push method	Displays the settings of the maximum message size (KB) of the secure mail delivered (or pushed) to the recipient. If the message exceeds the size limit, it will be delivered with the Pull method.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click New to add a profile or double-click a profile to modify it.
   A dialog appears.
3. For a new profile, enter the name of the profile in Profile name.
4. In Protocol, select S/MIME or IBE.
   The availability of the following options varies by your selection in Protocol.
5. If you selected IBE as the protocol:

- Select the Action method (Push or Pull) for the mail recipients.
- For Push, specify the maximum message size (KB) for the Push method (messages exceeding the size limit will be delivered with the Pull method).

6. If you select S/MIME as the protocol, select an action: Encrypt, Sign, or Encrypt and Sign. To use S/MIME encryption, you must also configure certificate binding. For details, see Using S/MIME encryption on page 239 and Configuring certificate bindings on page 292.
7. From Encryption algorithm, select the encryption algorithm that will be used to encrypt email (AES 128, AES 192, AES 256, CAST5 128, or Triple DES).
8. From Action on failure, select the action the FortiMail Cloud 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 Cloud 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 Cloud 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.
   - 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 292.
   - create an S/MIME encryption profile. For details, see Configuring encryption profiles on page 237.
   - 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 129), 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 138, Controlling email based on IP addresses on page 132, Configuring content action profiles on page 195, and Configuring content profiles on page 186).

If the email to be encrypted is matched both by the message delivery rule and the policy, the email will be encrypted based on the content profile in the policy.

2. On FortiMail unit B:
   - import the CA certificate. For details, see Managing certificates.
   - create a certificate binding for the incoming email and import both FortiMail unit B's private key and certificate to decrypt the email encrypted by FortiMail unit A using FortiMail unit B's public key.

Configuring email, IP and GeoIP groups

The *Profile* > *Group* tab displays the list of email and IP group and override profiles.

This sections includes:

- Configuring email groups
- Configuring IP groups
- Configuring GeoIP groups
- Configuring GeoIP override

Configuring email groups

Email groups include groups of email addresses that can be used when configuring access control rules and recipient-based policies. For information about access control rules and polices, see Configuring access control rules on page 121 and Controlling email based on sender and recipient addresses on page 138.

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 and IP-based policies. For information about access control rules and polices, see Configuring access control rules on page 121 and Controlling email based on IP addresses on page 132.

To configure an IP group

1. Go to *Profile* > *Group* > *IP Group*.
2. Either click New to add a profile or double-click a profile to modify it.
   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.
6. Click Create.

Configuring GeoIP groups

Starting from 6.2 release, FortiMail utilizes the GeoIP database to map the geolocations of client IP addresses. You can use GeoIP groups in access control rules and IP-based policies to geo-targeting spam and virus devices. For information about access control rules and polices, see Configuring access control rules on page 121 and Controlling email based on IP addresses on page 132.

You can also override geolocation mappings that may not be correct in the GeoIP database. For details, see Configuring GeoIP override.

To configure a GeoIP group

1. Go to *Profile* > *Group* > *GeoIP Group*.
2. Either click New to add a profile or double-click a profile to modify it.
   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. Optionally enter a comment.
5. If you want to create a group to include all countries and regions, enable this option and click Create. Otherwise, disable this option and move the available countries, regions, or override groups to the member list, and click Create. You can have a maximum of 30 countries and regions in one group.

Configuring GeoIP override

GeoIP service looks up the IP address geographic locations in the GeoIP database. However, in some cases, the lookup might not be accurate, for example, when clients use proxies.

With FortiMail, you can override the GeoIP lookup by manually specifying the geographic locations of some IP addresses and ranges. When you create GeoIP groups (see Configuring GeoIP groups on page 241), you can use the override geographic locations in the groups.

When entering IP addresses for GeoIP overrides, only IPv4 addresses are supported.

To configure a GeoIP override

1. Go to *Profile* > *Group* > *GeoIP Override*.
2. Click *New*.
3. Specify a geographic location name for the client IP addresses.
4. Optionally enter a description.
5. Click *New* to specify the IPv4 addresses that you want to include in the geographic location.
6. Click *Create*.
   To test a lookup, click *IP Geography Query*.

Configuring notification profiles

When FortiMail takes actions against email messages, you may wan to inform email senders, recipients, or any other users of the actions, that is, what happened to the email.

To achieve this purpose, you need to create such kind of notification profiles and then use them in antispam, antivirus, and content action profiles. For details, see Configuring antispam action profiles on page 178, Configuring antivirus action profiles on page 184, and Configuring content action profiles on page 195.

To create a notification profile

1. Go to *Profile* > *Notification* > *Notification*. If you have created some notification profiles, you can view, clone, edit, or delete them there.
2. Click *New* to create a profile.
3. For *Name*, enter a profile name. The profile name is editable later.
4. From *Type*, select:
   - *Generic*: this type of notification profile can be used in the antispam, antivirus and content profiles to notify the sender, recipient, or other email accounts.
   - *Sender Address Rate Control*: When you configure sender address rate control notification in domain settings (see Other advanced domain settings on page 81), you can also choose a notification profile. In this case, you only need to notify the senders, not the recipients. You do not need to include the original message as attachment either. Therefore, these two options are greyed out.
   - *Attachment Filtering*: this type of notification profile most probably be used in the content profiles where attachment filtering is implemented.
5. Choose whom you want to send notification to: sender, recipient, or other users. If you choose *Others*, you can manage the email list by using the *Add* and *Remove* buttons.
6. Select an email template to use. You can also click New to create a new template or click Edit to modify an existing template. For details about email templates, see Customizing email templates on page 59.
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 160.

This section contains the following topics:

Configuring the FortiGuard URL filter

The FortiGuard URL filter service allows you choose which categories of URL in the email body you want to scan, rewrite, or block.

To configure a URL rating category profile

1. Go to *Security* > *URL Filter* > *Profile*.
2. Click *New*.
3. Enter a profile name.
4. Select which URL rating categories to examine in the email body.
5. Click *Create*.
6. To apply the URL rating category profile, select it in antispam profiles (see Configuring FortiGuard options on page 164) and/or click protection settings (see Configuring CDR URL click protection and removal options on page 245).

Configuring local URL rating categories

You can configure custom URL rating categories for URL rating override profiles. For most exemptions, you may want to use the pre-defined *local-exempt* category instead.

1. Go to *Security* > *URL Filter* > *Local Category*.
2. Click *New*.
3. Enter a *Name* and an optional *Comment* for the new custom local category.
4. Click *Create*.

Configuring URL rating overrides

To specify which URLs will have overrides of their URL rating category, you can configure patterns (either wildcard or regular expressions) . During configuration of other features, the URL rating override pattern can be selected instead of the usual FortiGuard web filter categories.

1. Go to *Security* > *URL Filter* > *Override Rating*.
2. Click *New*.
3. Enable *Status*, and enter a URL pattern.The pattern can use wildcards (default) or regular expressions. Optionally, before entering a regular expression, click *Validate* to test regular expressions and string text. See URL types on page 244 and Syntax on page 1.
4. Under *Override To*, select a *Group* and a group-approriate *Category*.

To exempt URLs from FortiGuard URL and web filter (see Configuring FortiGuard options on page 164), FortiGuard URL protection (see Configuring CDR URL click protection and removal options on page 245), FortiSandbox scanning (see Using FortiSandbox antivirus inspection on page 62), select the *Local Category* group and *local-exempt* category.

5. Click *Create*.

URL types

There are two types of URLs:

- **Absolute URLs** strictly follow the URL syntax and include the URL scheme names, such as `http`, `https`, and `ftp`. The often only include a domain name, such as `http://www.example.com`.
- **Reference URLs** do not contain the scheme names. Example: `example.com`

By default, FortiMail scans for absolute URLs.

You can use the following CLI command to change the default setting:

```
config antispam settings
   set url-checking {aggressive | strict}
end
```

- `strict`: Choose this option to scan for absolute URLs only. Websites with no `http` or `https` but with `www`, such as `www.example.com`, are also treated as absolute URLs.
- `aggressive`: Choose this option to scan for both the absolute and reference URLs. Sender domains are also checked against FortiGuard.
- `extreme`: Choose this option to scan for all URLs with or without schemes, including absolute URLs, reference URLs, URLs in text format, and sender domains.

For more information about this command, see FortiMail CLI Reference.

Configuring content disarming and reconstruction

System-wide attachment and URL sanitization settings that are used by all content profiles are configured in *Security* > *Disarm & Reconstruction*.

About content disarming and reconstruction (CDR)

In an email and attachments, there may be risky URLs and HTML tags such as hyperlinks and JavaScript. Similarly, Microsoft Office and PDF attachments may have macros, links, and other active content that also can be used by spyware or malware. Zero-day or spear phishing attacks that have been specially crafted initially do not have matching virus signatures or URL ratings yet. Some email clients automatically display HTML and attachments, increasing the risk.

Content disarming and reconstruction (CDR) in content profiles (see Configuring content disarm and reconstruction (CDR) on page 189) allows you to remove or mitigate risky content and then reconstruct and still deliver the sanitized email, without affecting the integrity of the text in the email.

For example, HTML email, you could select an action in the content action profile to warn email users by tagging email that contains potentially dangerous HTML content. Alternatively, if you select to remove the HTML tags, then users can safely read the email to decide whether or not it is legitimate.

Configuring CDR attachment settings

For each CDR that content profiles can perform on attached files, configure how FortiMail Cloud should disarm or remove the files.

1. Go to *Security* > *Disarm & Reconstruction* > *Attachment*.
2. Configuring the following:

GUI item	Description

Attachment handling for deferred email	Configure the following:
	• *Send notification:* Enable for the recipient to receive a notification if an email attachment is subjected to deferred scanning.
	  • *Remove all*: Send the notification with all the attachments removed.
	  • *Disarm Office/PDF and remove others*: Send notification with the disarmed Microsoft Office or PDF attachments. Remove all other attachments that are not supported by CDR.
	• *Verdict threshold to disarm on delivery*: Enter the threshold at which attachments will be disarmed. For example, if set to *Medium*, the attachments with *Medium*, *High*, and *Malicious* verdicts will all be disarmed.

Attachment scan by FortiSandbox	By default, if content disarmament succeeds, then the FortiSandbox scan is bypassed. Enable *Continue FortiSandbox scan on successful content disarm* if you want to allow FortiSandbox to scan the attachment even after successful CDR.

3. Click *Apply*.
4. To use these settings as actions, select it in a content profile. See Configuring content disarm and reconstruction (CDR) on page 189.

Configuring CDR URL click protection and removal options

If you do not configure CDR in the content profile to remove URLs, then users can click them. To protect users from malicious or spam URLs, such as phishing or advertising web sites, you can configure FortiMail Cloud to use the

FortiGuard URL filter service and FortiSandbox to scan the URLs when users click them. Depending on the results from FortiGuard and FortiSandbox, you can decide if you want to allow users to go to the URLs or block them.

You can also integrate with FortiIsolator to isolate threats. FortiIsolator is a browser isolation solution, which protects users against zero day malware and phishing threats that are delivered over the web and email. These threats may result in data loss, compromise, or ransomware. To protect users, FortiIsolator creates a virtual air gap between users' browsers and websites. Web content is executed in a remote disposable container and displayed to users visually, without running code from the website on their computer.

For each CDR action that content profiles can perform on URLs, configure how FortiMail Cloud should change or remove the URLs.

To configure URL click protection options

1. Go to *Security* > *Disarm & Reconstruction* > *URL*.
2. Configure the following:

GUI item	Description
URL Click Protection Option	
URL Rewrite	
Category	Select which URL rating category a URL must match in order to be rewritten. See also Configuring the FortiGuard URL filter on page 243.
Base URL	Enter the prefix `https://` and then the FQDN or IP address of FortiMail Cloud. When users click a hyperlink, they will be directed to the rewritten URL on FortiMail Cloud first. **Note:** The `https://` protocol prefix is required. **Tip:** The URL is rewritten in the format: `https://example.com/fmlurlsvc/?fewReq/baseValue&url=originalUrlEscaped` where `originalUrlEscaped` is the original URL in URL-encoded format. If you want to convert it back to see the original URL, you can use a text editor or online service such as: https://www.urldecoder.org
URL Click Handling	
Category	Select which URL rating category a URL must match in order to receive click handling. See also Configuring the FortiGuard URL filter on page 243.
Action	Select how the link will behave when click handling applies, and a user clicks a link: either *Block* or *Allow with Confirmation*.
FortiSandbox Scan	For all other URL categories not selected in *Category*, enable this setting if you want to send them to FortiSandbox for scanning (see Using FortiSandbox antivirus inspection on page 62). • *Enable*: Enable or disable the FortiSandbox scan. • *Action*: Select how the link will behave when a link is clicked during a FortiSandbox scan, either: • *Allow with Confirmation* : Allow access with warning.

GUI item	Description
	• *Block*: Block access. • *Submit only*: Allow access while sending the URLs for scanning. • *Timeout*: When the URLs are sent to FortiSandbox for scanning, it can take some time to get the results. Enter how long (in seconds) to wait for FortiSandbox scan results. If FortiMail Cloud does not get a reply in this time, then click handling instead uses the action in *Timeout action*. • *Timeout action*: Select how the link will behave when a user clicks a link after a FortiSandbox scan timeout, either: • *Allow* • *Allow with Confirmation* • *Block*
FortiIsolator Integration	
Category	Select which URL rating category a URL must match in order to be reached through FortiIsolator. See Configuring the FortiGuard URL filter on page 243.
Base URL	Enter the prefix `https://` and then the FQDN or IP address of FortiIsolator. **Note:** The `https://` protocol prefix is required.
URL Removal	
Category	Select which URL rating category a URL must match in order to be removed. See Configuring the FortiGuard URL filter on page 243.
URL Neutralization	
Category	Select which URL rating category a URL must match in order to be neutralized. See Configuring the FortiGuard URL filter on page 243.
Include image source attribute	Enable to neutralize URLs of images that are stored on remote web servers. Newsletters often do not embed images in email in order to keep the email file size small so that email can be sent to many people quickly. Instead, the image files are stored on a web server or CDN. Email clients download and display the image later, when each person reads their email. Normal newsletters often include a plain text version or a link to a web page to fall back if the images cannot be displayed in the email. Spammers and malware, however, can abuse remotely stored images to detect valid recipient addresses even when SMTP recipient verification is disabled, and to bypass email antispam and antivirus scans by transmitting the content over HTTPS instead of SMTP. **Note:** When you update FortiMail Cloud firmware from a previous version, default values are applied to any new settings. If this setting is new, the default results in a change in behavior. If you prefer the previous behavior, then enable this setting.

3. Click *Apply*.
4. To use these settings as actions, select it in a content profile. See Configuring content disarm and reconstruction (CDR) on page 189.

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 178) and content action profiles (see Configuring content action profiles on page 195).
- Configure the system quarantine administrator account who can manage the system quarantine. See Configuring the system quarantine setting on page 255.
- 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 255.
- 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 248.
- Configure domain-wide quarantine report settings for specific domains. See Quarantine Report Setting on page 75.
- View and manage personal quarantines and system quarantines. See Managing the quarantines on page 21.
- 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 324.

See also

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 178 and Configuring content action profiles on page 195. For general steps about how to use email quarantine, see Configuring email quarantines and quarantine reports on page 248.

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 75.

Starting from v4.1, domain-wide quarantine report settings are independent from the system-wide quarantine report settings.

For information on the contents of the plain text and HTML format quarantine report, see About the plain text formatted quarantine report on page 250 and About the HTML formatted quarantine report on page 252.

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 59.
Webmail Access Setting		
	Time limited access without authentication	Enable to allow user access without authentication for the following period of time.
	Expiry period	Specify the time limit for the above setting. 0 means unlimited.
	Web release host name/IP	Enter a host name for the FortiMail unit that will be used for web release links in quarantine reports (but not email release links). If this field is left blank: • If the FortiMail unit is operating in gateway mode or server mode, web release and delete links in the quarantine report will use the fully qualified domain name (FQDN) of the FortiMail unit. • If the FortiMail unit is operating in transparent mode, web release and delete links in the quarantine report will use the FortiMail unit's management IP address. For more information, see About the management IP. Configuring an alternate host name for web release and delete links can be useful if the local domain name or management IP of the FortiMail unit is not resolvable from everywhere that email users will use their quarantine reports. In that case, you can override the web release link to use a globally resolvable host name or IP address.

3. In the *Quarantine Report Recipient Setting* section, double-click a domain name to modify its related settings.

A dialog appears.

4. Configure the following and click *OK*.

Quarantine report recipient settings

GUI item		Description
Domain name		Displays the name of a protected domain. For more information on protected domains, see Configuring protected domains on page 71.
	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 209. 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 253.

Release instructions in a plain text quarantine report may use either the management IP address or local domain name.

The contents of quarantine reports are customizable. For more information, see Configuring custom messages and email templates on page 51.

Sample plain text quarantine report

Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00]
From: release-ctrl@example.com
Date: 12:00 PM
To: user1@example.com

Date: Thu, 04 Sep 2008 11:52:51
Subject: [SPAM] information leak
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzU3MS43NDJfNTk5ODcuRm9ydGlNYWlsLTQwMCwjRiNTIzYzMyNFLFU4OjIsUw==

Date: Thu, 04 Sep 2008 11:51:10
Subject: [SPAM] curious?
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsI0YjUyM2MjUjRSxVNzoyLA==

Date: Thu, 04 Sep 2008 11:48:50
Subject: [SPAM] Buy now!!!! lowest prices
From: User 1 <user1@example.com>
Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsI0YjUyM2NDIjRSxVNToyLA==

Actions:

o) Release a message: Send an email to <release-ctrl@example.com> with subject line set to "user1@example.com:Message-Id".
o) Delete a message: Send an email to <delete-ctrl@example.com> with subject line set to "user1@example.com:Message-Id".
o) Delete all messages: Send an email to <delete-ctrl@example.com> with subject line set to "delete all:user1@example.com:e4d46814:ac146004:05737c7c111d68d0111d68d0111d68d0".

Sample plain text quarantine report

	Report content
Message header of quarantine report	Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00] From: release-ctrl@example.com Date: Thu, 04 Sep 2008 12:00:00 To: user1@example.com
Quarantined email #1	Date: Thu, 04 Sep 2008 11:52:51 Subject: [SPAM] information leak From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzU3MS43NDJfNTk5ODcuRm9ydGlNYWlsLTQwMCwjRiNTIzYzMyNFLFU4OjIsUw==
Quarantined email #2	Date: Thu, 04 Sep 2008 11:51:10 Subject: [SPAM] curious? From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzQ3MC43NDFfOTA0MjcxLkZvcnRpTWFpbC00MDAsI0YjUyM2MjUjRSxVNzoyLA==
Quarantined email #3	Date: Thu, 04 Sep 2008 11:48:50 Subject: [SPAM] Buy now!!!! lowest prices From: User 1 <user1@example.com> Message-Id: MTIyMDU0MzMzMC43NDBfNjkwMTUwLkZvcnRpTWFpbC00MDAsI0YjUyM2NDIjRSxVNToyLA==
Instructions for deleting or releasing quarantined email	Actions: o) Release a message: Send an email to <release-ctrl@example.com> with subject line set to "user1@example.com:Message-Id". o) Delete a message: Send an email to <delete-ctrl@example.com> with subject line set to "user1@example.com:Message-Id". o) Delete all messages: Send an email to <delete-ctrl@example.com> with subject line set to "delete_ all:user1@example.com:e4d46814:ac146004:05737c7c111d68d0111d68d0111d68d0".

About the HTML formatted quarantine report

HTML quarantine reports:

- notify email users about email messages that have been quarantined to their per-recipient quarantine
- contain links to delete one or all quarantined email messages (see Sample HTML quarantine report on page 252)
- contain links to release individual email messages (see Sample HTML quarantine report on page 252)

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 253.

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 249.

The contents of quarantine reports are customizable. For more information, see Configuring custom messages and email templates on page 51.

If option to auto add to personal safe list when releasing spam is enabled, default HTML report now seems to include notification of that setting. From replacement message:

```
<**SPAM_CONFIG_NOTE**><b>Note: %%SPAM_SAFE_LIST%%.</b>
<**/SPAM_CONFIG_NOTE**>
```

Sample HTML quarantine report

Sample HTML quarantine report

	Report content
Message header of quarantine report	`Subject: Quarantine Summary: [ 3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00 ]` `From: release-ctrl@example.com`

	Date: Thu, 04 Sep 2008 12:00:00 To: user1@example.com
Quarantined email #1	**Date**: Thu, 04 Sep 2008 11:52:51 **From**: User 1 <user1@example.com> **Subject**: [SPAM] information leak **Web Actions**: Release Delete **Email Actions**: Release Delete
Quarantined email #2	**Date**: Thu, 04 Sep 2008 11:51:10 **From**: User 1 <user1@example.com> **Subject**: [SPAM] curious? **Web Actions**: Release Delete **Email Actions**: Release Delete
Quarantined email #3	**Date**: Thu, 04 Sep 2008 11:48:50 **From**: User 1 <user1@example.com> **Subject**: [SPAM] Buy now!!!! lowest prices **Web Actions**: Release Delete **Email Actions**: Release Delete
Instructions for deleting or releasing quarantined email	Web Actions: Click on Release link to send a http(s) request to have the message sent to your inbox. Click on Delete link to send a http(s) request to delete the message from your quarantine. Click Here to send a http(s) request to Delete all messages from your quarantine. Email Actions: Click on Release link to send an email to have the message sent to your inbox. Click on Delete link to send an email to delete the message from your quarantine. Click here to send an email to Delete all messages from your quarantine. Other: To view your entire quarantine inbox or manage your preferences, Click Here

Releasing and deleting email via quarantine reports

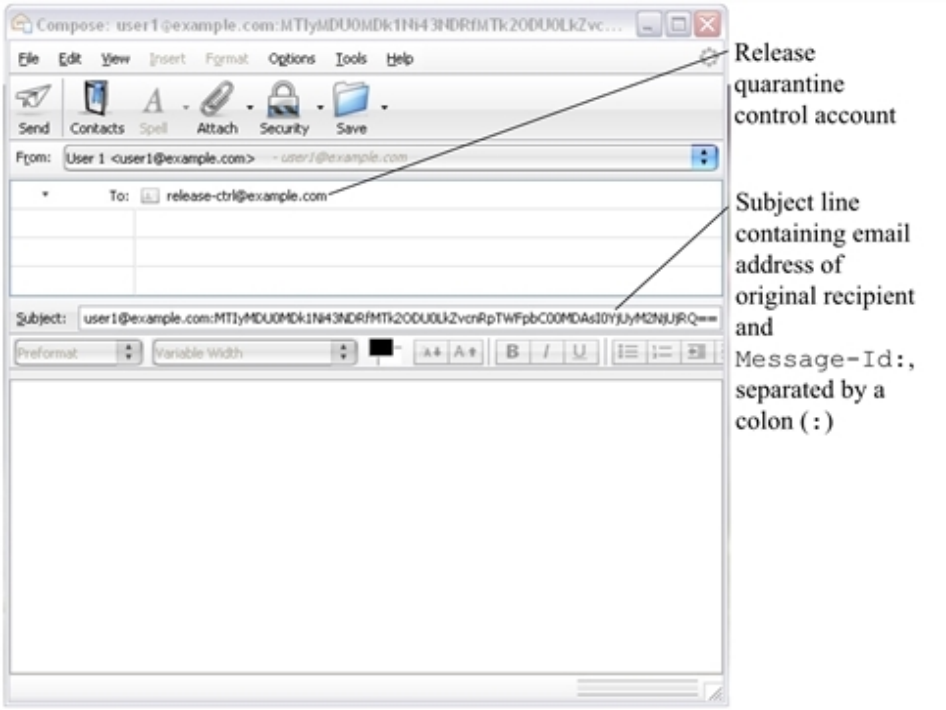
Quarantine reports enable recipients to remotely monitor and delete or release email messages in the per-recipient quarantine folders.

Depending on whether the quarantine report is sent and viewed in plain text or HTML format, a quarantine report recipient may use either or both web release and email release methods to release or delete email from a per-recipient quarantine.

- *Web release*: To release or delete an email from the per-recipient quarantine, the recipient must click the *Release* or *Delete* web action link which sends an HTTP or HTTPS request to the FortiMail unit. Available for HTML format quarantine reports only.

- *Email release*: To release or delete an email from the per-recipient quarantine, the recipient must either:
  - Click the *Release* or *Delete* email action link which creates a new email message containing all required information, then send it to the quarantine control account of the FortiMail unit. Available for HTML format quarantine reports only.
  - Manually send an email message to the quarantine control account of the FortiMail unit. The `To:` address must be the quarantine control email address, such as `release-ctrl@example.com` or `delete-ctrl@example.com`. The subject line must contain both the recipient email address and `Message-Id:` of the quarantined email, separated by a colon (`:`), such as:
    `user1@example.com:MTIyMDU0MDk1Ni43NDRfMTk2ODU0LkZvcnRpTWFpbC00MDAsI0YjUyM2NjUjRQ==`

Releasing an email from the per-recipient quarantine using email release



Quarantine control email addresses are configurable. For information, see Configuring the quarantine control options on page 255.

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 248.

For more information on the differences between plain text and HTML format quarantine reports, see About the plain text formatted quarantine report on page 250 and About the HTML formatted quarantine report on page 252.

See also

Configuring global quarantine report settings

Managing the personal quarantines

About the plain text formatted quarantine report

About the HTML formatted quarantine report

Configuring the system quarantine setting

Go to *Security* > *Quarantine* > *System Quarantine Setting* to configure the system quarantine account, quarantine folder, and other system quarantine settings.

The system quarantine can be accessed through either:

- IMAP -- use an IMAP email client to access the FortiMail unit with the system quarantine account name (without any domain name) and password.
- Administrative GUI -- create an administrator account with the quarantine access privilege in the access profile and access the GUI using this administrator account.

The system quarantine cannot be accessed through POP3 or webmail.

To configure the system quarantine account and quarantine folders

1. Go to *Security* > *Quarantine* > *System Quarantine Setting*.
2. Configure the following:

GUI item	Description
Account Setting	
Account	Enter the user name of the system quarantine account. You can use this account to view the system quarantine via an IMAP email client.
Password	Enter the password for the system quarantine account.
Forward to	Enter an email address to which the FortiMail unit will forward a copy of each email that is quarantined to the system quarantine.
Quarantine Folders	
Enable folder rotation	Enable to rotate the folders according to the interval settings below.
Rotation interval (days)	Enter the maximum amount of time that the current system quarantine mailbox (Inbox) will be used. When the mailbox reaches this time, the FortiMail unit renames the current mailbox based on its creation date and rename date, and creates a new Inbox mailbox.
New	Click to create a new folder. When creating a folder, also specify the retention time (in days) and the administrators who are allowed to access the quarantine folder. The retention time determines how long the quarantined email will saved in the folder before it get deleted.

See also

Managing the system quarantine

Configuring the quarantine control options

Go to *Security* > *Quarantine* > *Quarantine Control* to configure quarantine release and delete control accounts. You can also specify whether to re-scan the quarantined email for virus infections before they are released. This can be useful if the email messages are quarantined due to antispam reasons, or if the antivirus signatures are updated later.

For email messages in the Virus folder of the system quarantine, they will not be rescanned when they are released. Otherwise, you may never be able to release them. For email messages in other quarantine folders, they will be rescanned when they are released for the first time. In case they are quarantined again and you still want to release them, they will be released without rescan.

Email users can remotely release or delete email messages in their per-recipient quarantine by sending email to quarantine control email addresses.

For example, if the Release account is `release-ctrl` and the local domain name of the FortiMail unit is `example.com` and `example.com` is not a protected domain, an email user could release an email message from their per-recipient quarantine by sending an email to `release-ctrl@example.com`. If the FortiMail unit's local domain name happens to be a protected domain name, the Release account address would be `release-ctrl@hostname.example.com`. The FortiMail unit's host name and local domain name are configured under *System* > *Mail Setting* > *Mail Server Setting*.

For more information on releasing and deleting quarantined items through email, see Releasing and deleting email via quarantine reports on page 253.

To configure the quarantine control settings

1. Go to Security > Quarantine > Quarantine Control.
2. Under *Quarantine Release Re-scan Setting*, specify whether to re-scan the quarantined email with the FortiMail AV engine and/or FortiSandbox before the email is released. Also specify whether to scan the personal quarantine and/or system quarantine.
3. For Release account, enter the user name portion (also known as the local-part) of the email address on the FortiMail unit that will receive quarantine release commands; for example: such as `release-ctrl`.
4. For Delete account, enter the user name portion (also known as the local-part) of the email address on the FortiMail unit that will receive quarantine delete commands; such as `delete-ctrl`.
5. Click Apply.

See also

Managing the personal quarantines

Configuring global quarantine report settings

Configuring the block lists and safe lists

The *Security* > *Block/Safe List* submenu lets you reject, discard, or allow email messages based on email addresses, domain names, and IP addresses. It also lets you back up and restore the block lists and safe lists.

Multiple types of block lists and safe lists exist: system-wide, per-domain, per-user, and per-session profile. There are several places in the GUI where you can configure these block lists and safe lists.

- For system-wide, per-domain, and per-user block lists and safe lists, go to *Security* > *Block/Safe List*. For details, see Managing the global block and safe list on page 260, Managing the per-domain block lists and safe lists on page 261, and Managing the personal block lists and safe lists on page 262.

- For per-user block lists and safe lists, you can alternatively go to *Domain & User* > *User* > *User Preference*. For details, see Configuring user preferences on page 88.
- 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 144.

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 257.

All block and safe list entries are automatically sorted into alphabetical order, where wildcard characters (* and ?) and numbers sort before letters.

See also

Order of execution of block lists and safe lists

About block list and safe list address formats

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution of block lists and safe lists

As one of the first steps to detect spam, FortiMail units evaluate whether an email message matches a block list or safe list entry.

Generally, safe lists take precedence over block lists. If the same entry appears in both lists, the entry will be safelisted. Similarly, system-wide lists take precedence over session lists, session lists over per-domain lists, and per-domain lists over per-user lists.

The following table is the sequence in which the FortiMail unit evaluates email for matches with block list and safe list entries. If the FortiMail unit finds a match, it does not look for any additional matches, and cancels any remaining antispam scans of the message (but not the antivirus and content scans).

Block and safe list order of operations

Order	List	Examines	Action taken if match is found
1	System safe list	Sender address, Client IP	Accept message
2	System block list	Sender address, Client IP	Invoke block list action
3	Session recipient safe list	Recipient address	Accept message for matching recipients
4	Session recipient block list	Recipient address	Invoke block list action
5	Session sender safe list	Sender address, Client IP	Accept message for all recipients

Order	List	Examines	Action taken if match is found
6	Session sender block list	Sender address, Client IP	Invoke block list action
7	Domain safe list	Sender address, Client IP	Accept message
8	Domain block list	Sender address, Client IP	Invoke block list action
9	User safe list	Sender address, Client IP	Accept message for this recipient
10	User block list	Sender address, Client IP	Discard message

When the sender email address or domain is examined for a match:

- email addresses and domain names in the list are compared to the sender address in the email envelope (`MAIL FROM:`), email header (`From:`) and (`Reply-to:`)
- IP addresses are compared to the IP address of the SMTP client delivering the email, also known as the last hop address

When the recipient is examined for a match, email addresses and domain names in the list are compared to the recipient address in both the envelop and header. An IP address in a recipient safe or block list is not a valid entry, because IP addresses are not used.

System-wide, per-domain, and per-user block lists and safe lists are executed before any policy match. In contrast, per-session profile block lists and safe lists require that the traffic first match a policy. When configuring a session profile (see Configuring session profiles on page 144), 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.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution

About block list and safe list address formats

Since the release of 7.0.0, FortiMail supports three block and safe list entry types:

1. **Email:** Matches email address, supporting wildcard entries. Matches both header from and envelope from.
   Email entries must be entered in the following format:
   "user@example.com"

Email entries prior to upgrading to 7.0.0 or higher utilize the following format
"example.com"
Such entries are automatically updated once FortiMail is upgraded to 7.0.0 or higher, in this example, "*@example.com".

2. **IP/Netmask:** Matches IP/Netmasks, entered in the following format:
   "172.20.0.1/32"

Prior to 7.0.0, only IP address was supported. Any such entries are automatically updated to those with a netmask, for example "172.20.0.1/32" once FortiMail is upgraded to 7.0.0 or higher.

Supports CIDR notation.

3. **Reverse DNS:** Enter the hostname/FQDN which will match reverse DNS lookup (PTR) results for connecting client MTA IPs.

Acceptable input for block and safe list entries may vary by the type of the block or safe list, but may be:

- an IP address or subnet (CIDR notation is supported)
- all or part of an email address using wildcards

Domain name portions (for example, example.com) and user name portions (for example, user1) may use wild cards (`?` and `*`).

Examples of valid block/safe list entries

Type	Example	Description
Email	**spammer@example.com**	Email from the sender spammer@example.com.
	?ser1@example.com	Email from any sender with any character preceding and including “ser1” at example.com.
	***@example.com**	Email from any sender at example.com.
	***@*.example.com**	Email from any sender at any subdomain of example.com.
	hostname.example.com	Email from client MTA IP which has PTR record resolving to hostname.example.com.
	user1@ex?mple.com	Email from the sender user1 in domains such as example.com, exemple.com, or exumple.com.
	user1@*.com	Email from the sender user1 at any .com domain.
IP/Netmask	**172.16.1.0/24**	Email from the IP subnet 172.16.1.0/24.
	172.16.1.1/32	Email from client IP matching 172.16.1.1.
Reverse DNS	**hostname.example.com**	Hostname/FQDN matching reverse DNS lookup results for connecting client MTA IPs.

The following formats are **not** valid:

- 172.168.1
- example.com
- @spam. example.com

See also

Order of execution of block lists and safe lists

Configuring the block lists and safe lists

Managing the global block and safe list

The *System* tab lets you configure system-wide block and safe lists to block or allow email by sender. It also lets you back up and restore the system-wide block and safe lists.

System-wide block lists and safe lists can also be tracked in terms of when they were created, when they last had a match or hit, and hit count. See To configure block list settings on page 263 for more information.

You can alternatively back up all system-wide, per-domain, and per-user block and safe lists together. For details, see Backup and restore on page 1.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans, including SPF validation.

Domain administrators can access the global block list and global safe list, and therefore could affect domains other than their own. If you do not want to permit this, do **not** provide Read-Write permission to the Block/Safe List category in domain administrators' access profile.

To view the global block list or safe list, go to *Security* > *Block/Safe List* > *System*. The page displays two links:

- Block List
- Safe List

To add an entry to the system-wide block list or safe list

1. Go to *Security* > *Block/Safe List* > *System*.
2. Do one of the following:
   - To block email by sender, select *Block* from the *List* dropdown.
   - To allow email by sender, select *Safe* from the *List* dropdown.
3. Click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 258.
4. Click *Create*.
5. From the safe/block lists, you can also select *Backup* to back up the list or *Restore* to restore a backup list.

Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.

See also

Configuring the block lists and safe lists

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution of block lists and safe lists

About block list and safe list address formats

Backup and restore

Managing the per-domain block lists and safe lists

The Domain tab lets you configure block and safe lists that are specific to a protected domain in order to block or allow email by sender. It also lets you back up and restore the per-domain block lists and safe lists.

You can alternatively back up all system-wide, per-domain, and per-user block lists and safe lists together. For details, see Backup and restore.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans.

To view and edit per-domain block or safe lists

1. Go to *Security* > *Block/Safe List* > *Domain*.

GUI item	Description
Show domain association	Enable to filter by domain association in the domain block/safe list.
Domain	Displays the name of the protected domain to which the block list and safe list belong. For more information on protected domains, see Configuring protected domains on page 71.
Block List	Click the List icon to display, modify, back up, or restore the block list for the protected domain.
Safe List	Click the List icon to display, modify, back up, or restore the safe list for the protected domain.

2. Click the Block List or Safe List icon.
3. Click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 258.

Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the personal block lists and safe lists

Configuring block list settings

Order of execution of block lists and safe lists

About block list and safe list address formats

Backup and restore

Managing the personal block lists and safe lists

Security > *Block/Safe List* > *Personal* lets you add or modify email users' personal block or safe lists in order to block or allow email by sender. It also lets you back up and restore the per-user block lists and safe lists.

In addition to FortiMail administrators configuring per-user block lists and safe lists, email users can configure their own per-user block list and safe list by going to the Preferences tab in FortiMail webmail. For more information, see the online help for FortiMail webmail.

Use block and safe lists with caution. They are simple and efficient tools for fighting spam and enhancing performance, but can also cause false positives and false negatives if not used carefully. For example, a safe list entry of `*.edu` would allow all email from the `.edu` top level domain to bypass the FortiMail unit's other antispam scans.

To view and add to personal block lists or safe lists

1. Go to *Security* > *Block/Safe List* > *Personal*.
2. Users in the selected domain will be displayed. In the Search box, type the user name of the email user whose per-user block list or safe list you want to modify, and click Enter to search the user.
3. Select a use and click *New* to add an email address, domain name, or IP address of the sender you wish to add to the block or safe list. For information on valid formats, see About block list and safe list address formats on page 258.
4. Click *Backup* to back up the list or *Restore* to restore a backup list.

Back up the block list and safe list before restoring a list. Restoring the block list and safe list overwrites any existing block or safe list.

If you add the user's email address to the same user's personal safe list, the FortiMail unit will ignore this entry. This is a precautious measure taken to guard against spammers from sending spam in disguise of that user's email address as the sender address.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Configuring block list settings

Order of execution of block lists and safe lists

About block list and safe list address formats

Backup and restore

Configuring block list settings

The *Setting* tab lets you configure the action to take if an email message arrives from a blocklisted domain name, email address, or IP address. You may also enable or disable block/safe list tracking.

The FortiMail unit will apply this action to email matching system-wide, per-domain, and per-session profile block lists.

Domain administrators can configure the block list action, and therefore could affect domains other than their own. If you do not want to permit this, do **not** provide Read-Write permission to the Block/Safe List category in domain administrators' access profile.

To configure block list settings

1. Go to *Security* > *Block/Safe List* > *Setting*.
2. Select one of the following actions:
   - *Reject*: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (`Relaying denied`).
   - *Discard*: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client.
   - *Use AntiSpam profile settings*: Use the actions configured in the antispam profile that you selected in the policy that matches the email message. For more information on actions, see Configuring antispam action profiles on page 178.
3. Enable *Block/Safe list tracking* to track various blocklist and safelist statistics, including creation time, last hit time, and hit count. These statistics are tracked under *Security* > *Block/Safe List* > *System* and *Security* > *Block/Safe List* > *Domain*.
4. Additionally, enable *Status* under *Auto Aging Of List Entries* to apply automatic purging of system and domain

block and safe lists that are listed for a defined *Retention period* (up to a maximum of 365 days).

Once *Auto Aging Of List Entries* is enabled and a *Retention period* is applied, you may manually remove any expired entries on-demand by using the *Cleanup* option from the System and Domain block/safe lists.

5. Click *Apply*.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Managing the per-domain block lists and safe lists

Managing the personal block lists and safe lists

Order of execution of block lists and safe lists

Configuring greylisting

Go to *Security* > *Greylist* to configure greylisting and to view greylist-exempt senders.

This section contains the following topics:

- About greylisting
- Viewing the pending and individual automatic greylist entries
- Manually exempting senders from greylisting
- Viewing the consolidated automatic greylist exemptions
- Configuring the greylist TTL and initial delay

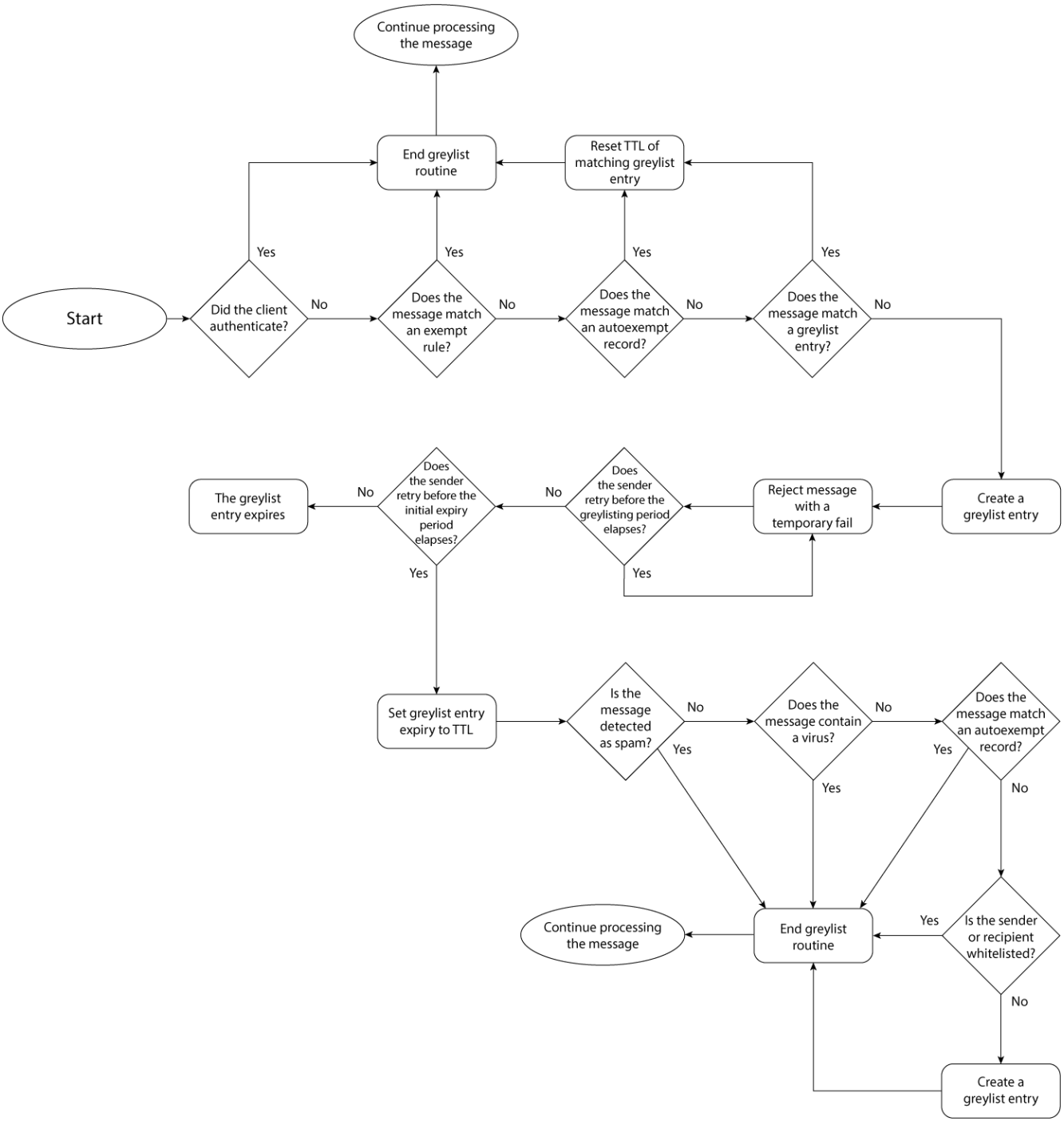
About greylisting

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.

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.

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 268)
2. consolidated automatic greylist entries, also known as autoexempt entries (see Automatic greylist entries on page 267)
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 267 and Automatic greylist entries on page 267.

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 35) to note that combination of sender, recipient, and client addresses, then replies to the SMTP client with a temporary failure code. During the greylist delay period after the initial delivery attempt, the FortiMail unit continues to reply to delivery attempts with a temporarily failure code. To confirm the pending automatic greylist entry and successfully send the email message, the SMTP client must retry delivery during the greylist window: after the delay period, but before the expiry of the pending entry.

Subsequent email messages matching a greylist entry are accepted by the greylist scanner without being subject to the greylisting delay.

For information on how the greylist scanner matches email messages, see Matching automatic greylist entries on page 266. For information on configuring the greylisting delay, window, and entry expiry/TTL, see Configuring the greylist TTL and initial delay on page 268.

Matching automatic greylist entries

While the email addresses in the message envelope must match exactly, the IP address of the SMTP client is a less specific match: any IP address on the /24 network will match.

For example, if an email server at 192.168.1.99 is known to the greylist scanner, its greylist entry contains the IP address `192.168.1.0` where `0` indicates that any value will match the last octet, and that any IP address starting with `192.168.1` will match that entry.

This greylist IP address matching mechanism restricts the number of IP addresses which can match the greylist entry while also minimizing potential issues with email server farms. Some large organizations use many email servers with IP addresses in the same class C subnet. If the first attempt to deliver email receives a temporary failure response, the second attempt may come from an email server with a different IP address. If an exact match were required, the greylist

scanner would treat the second delivery attempt as a new delivery attempt unrelated to the first. Depending on the configuration of the email servers, the email message might never be delivered properly. Approximate IP address matching often prevents this problem.

For very large email server farms that require greater than a /24 subnet, you can manually create greylist exemptions. For more information, see Manual greylist entries on page 268.

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 35)
- individual (see Viewing the pending and individual automatic greylist entries on page 35)
- consolidated (see Viewing the consolidated automatic greylist exemptions on page 37)

Pending entries are created on the initial delivery attempt, and track the email messages whose delivery attempts are currently experiencing the greylist delay period. They are converted to confirmed individual entries if a delivery attempt occurs after the greylist delay period, during the greylist window.

The automatic greylisting process can reduce the number of individual automatic greylist entries by consolidating similar entries after they have been confirmed during the greylisting window. Consolidation improves performance and greatly reduces the possibility of overflowing the maximum number of greylist entries.

Consolidated automatic greylist entries include only:

- the domain name portion of the sender email address
- the IP address of the SMTP client

They do not include the recipient email address, or the user name portion of the sender email address. By containing only the domain name portion and not the entire sender email address, a consolidated entry can match all senders from a single domain, rather than each sender having and matching their own individual automatic greylist entry. Similarly, by not containing the recipient email address, any recipient can share the same greylist entry. Because consolidated entries have broader match sets, they less likely to reach the time to live (TTL) than an individual automatic greylist entry.

For example, example.com and example.org each have 100 employees. The two organizations work together and employees of each company exchange email with many of their counterparts in the other company. If each example.com employee corresponds with 20 people from example.org, the FortiMail unit used by example.com will have 2000 greylist entries for the email received from example.org alone. By consolidating, these 2000 greylist entries are replaced by a single entry.

Not all individual automatic greylist entries can be consolidated. Because consolidated entries have fewer message attributes, more email messages may match each entry, some of which could contain different recipient email addresses and sender user names than those of the originally greylisted email messages. To prevent spam from taking advantage of the broader match sets, requirements for creation of consolidated entries are more strict than those of individual automatic greylist entries. FortiMail units will create a consolidated (autoexempt) entry only if the email:

- does not match any manual greylist entry (exemption)
- passes the automatic greylisting process
- passes all configured antispam scans
- passes all configured antivirus scans

- passes all configured content scans
- does not match any safe lists

If an email message fails to meet the above requirements, the FortiMail unit instead maintains the individual automatic greylist entry.

If an email message matches a manual greylist entry, it is not subject to automatic greylisting and the FortiMail unit will not create an entry in the individual or consolidated automatic greylist or autoexempt list.

After an individual automatic greylist entry is consolidated, both the consolidated autoexempt entry and the original greylist entry will coexist for the length of the greylist TTL. Because email messages are compared to the autoexempt list before the greylist, subsequent matching email will reset only the expiry date of the autoexempt list entry, but not the expiry date of the original greylist entry. Eventually, the original greylist entry expires, leaving the automatic greylist entry.

Manual greylist entries

In some cases, you may want to manually configure some greylist entries. Manual greylist entries are exempt from the automatic greylisting process, and are therefore not subject to the greylist delay period and confirmation.

For example, a manual greylist entry can be useful when email messages are sent from an email server farm whose network is larger than /24. For very large email server farms, if a different email server attempts the delivery retry each time, the greylist scanner could perceive each retry as a first attempt, and automatic greylist entries could expire before the same email server retries delivery of the same email. To prevent this problem, you can manually create an exemption using common elements of the host names of the email servers.

For more information on creating manual greylist entries, see Manually exempting senders from greylisting on page 269.

Configuring the greylist TTL and initial delay

The Setting tab lets you configure time intervals used during the automatic greylisting process.

For more information on the automatic greylisting process, see About greylisting on page 264.

To configure greylisting intervals

1. Go to *Security* > *Greylist* > *Setting*.
2. Configure the following:

GUI item	Description
TTL	Enter the time to live (TTL) that determines the maximum amount of time that unused automatic greylist entries will be retained. Expiration dates of automatic greylist entries are determined by the following two factors: • Initial expiry period: After a greylist entry passes the greylist delay period and its status is changed to PASSTHROUGH, the entry's initial expiry time is determined by the time you set with the CLI command `set greylist-init-expiry-period` under `config antispam settings`.

GUI item	Description
	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 34.
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 35.

You can use the CLI to change the default 4 hour greylist window. For more information, see the CLI command `set greylist-init-expiry-period` under `config antispam settings` in the FortiMail CLI Reference.

Manually exempting senders from greylisting

The Exempt tab displays manual greylist entries, which exempt email messages from the automatic greylisting process and its associated greylist delay period.

Greylisting is omitted if the matching access control rule's Action is RELAY. For more information on antispam features' order of execution, see Order of execution.

For more information on the automatic greylisting process, see About greylisting on page 264. For more information on manual greylist entries, see Manual greylist entries on page 268.

To view and configure manual greylist entries

1. Go to *Security* > *Greylist* > *Exempt*.

GUI item	Description
Sender Pattern	Displays the pattern that defines a matching sender address in the message envelope (`MAIL FROM:`). The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 1. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).
Recipient Pattern	Displays the pattern that defines a matching recipient address in the message envelope (`RCPT TO:`). The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 1. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).
Sender IP/Netmask	Displays the IP address and netmask that defines SMTP clients (the last hop address) that match this entry. `0.0.0.0/0` matches all SMTP client IP addresses.
Reverse DNS Pattern	Displays the pattern that defines a matching result when the FortiMail unit performs the reverse DNS lookup of the IP address of the SMTP client. The prefix to the pattern indicates whether or not the Regular expression option is enabled for the entry. • **R/**: Regular expressions are enabled. See also Syntax on page 1. • **-/**: Regular expressions are not enabled, but the pattern may use wild cards (`*` or `?`).

2. Click New to add an entry or double-click an entry to modify it.
   A dialog appears.
3. Configure the following:

GUI item	Description
Sender pattern	Enter the pattern that defines a matching sender email address in the message envelope (`MAIL FROM:`). To match any sender email address, enter either `*`, or, if Regular expression is enabled, `.*`. You can create a pattern that matches multiple addresses either by: • including wild card characters (`*` or `?`). An asterisk (`*`) matches one or more characters; a question mark (`?`) matches any single character. • using regular expressions. You must also enable the Regular expression option.
Regular expression	For any of the pattern options, select the accompanying Regular expression check box if you entered a pattern using regular expression syntax. See also Syntax on page 1.
Recipient pattern	Enter the pattern that defines a matching recipient address in the message envelope (`RCPT TO:`). To match any recipient email address, enter either `*`, or, if Regular expression is enabled, `.*`. See also Syntax on page 1.
Sender IP/Netmask	Enter the IP address and netmask that defines SMTP clients that match this entry.

GUI item	Description
	To match any SMTP client IP address, enter `0.0.0.0/0`. You can create a pattern that matches multiple addresses by entering any bit mask other than `/32`. For example, entering `10.10.10.10/24` would match the 24-bit subnet of IP addresses starting with 10.10.10, and would appear in the list of manual greylist entries as `10.10.10.0/24`.
Reverse DNS pattern	Enter the pattern that defines valid host names for the IP address of the SMTP client (the last hop address). Since the SMTP client can use a fake self-reported host name in its SMTP greeting (`EHLO`/`HELO`), you can use a reverse DNS lookup of the SMTP client's IP address to get the real host name of the SMTP client. Then the FortiMail greylist scanner can compare the host name resulting from the reverse DNS query with the pattern that you specify. If the query result matches the specified pattern, the greylist exempt rule will apply, Otherwise, the rule will not apply. You can create a pattern that matches multiple addresses either by: • including wild card characters (`*` or `?`). An asterisk (`*`) matches one or more characters; a question mark (`?`) matches any single character. • using regular expressions. You must also enable the Regular expression option. See also Syntax on page 1.

No pattern can be left blank in a greylist exempt rule. To have the FortiMail unit ignore a pattern, enter an asterisk (`*`) in the pattern field. For example, if you enter an asterisk in the Recipient Pattern field and do not enable Regular Expression, the asterisk matches all recipient addresses. This eliminates the recipient pattern as an item used to determine if the rule matches an email message.

See also

Configuring the block lists and safe lists

Managing the global block and safe list

Example: Manual greylist entries (exemptions)

Example Corporation uses a FortiMail unit that is operating in gateway mode, and uses greylisting to reduce the quantity of spam they receive at their protected domain, example.com.

Example Corporation wants to exempt some email from the initial greylist delay period by creating manual greylist entries (exemptions to the automatic greylisting process) that match trusted combinations of SMTP client IP addresses and recipient email addresses.

Rule 1

Example Corporation has a number of foreign offices. Email from these offices does not need to be greylisted.The IP addresses of email servers in the foreign offices vary, though their host names all begin with “mail” and end with “example.com”.

Rule 1 uses the recipient pattern and the reverse DNS pattern to exempt from the automatic greylisting process all email messages that are sent to recipients at example.com, and are being delivered by an email server with a host name beginning with “mail” and ending with “example.com”.

Rule 2

Example Corporation works closely with a partner organization, Example Org, whose email domain is example.org. Email from the example.org email servers does not need to be greylisted. The IP addresses of email servers for example.org are within the 172.20.120.0/24 subnet, and have a host name of mail.example.org.

Rule 2 uses the recipient pattern, sender IP/ netmask, and reverse DNS pattern to exempt from the automatic greylisting process all email messages that are sent to recipients at example.com by any email server whose IP address is between 172.20.120.1 and 172.20.120.255 and whose host name is mail.example.org.

Configuring bounce verification and tagging

The Bounce Verification submenu lets you configure bounce address tagging and verification.

Spammers sometimes fraudulently use others' email addresses as the sender email address in the message envelope (`MAIL FROM:`) when delivering spam. When an email cannot be delivered, email servers often return a a delivery status notification (DSN) message, sometimes also known as a bounce message, to the sender email address located in the message envelope.

While DSNs are normally useful in notifying email users when an email could not be delivered, in this case, it could result in delivery of a DSN to an email user who never actually sent the original message. Because the invalid bounce message is from a valid email server, it can be difficult to detect as invalid.

You can combat this problem with bounce address tagging and verification. If the FortiMail unit tags outgoing email, it can verify the tags of incoming bounce messages to guarantee that the bounce message is truly in reply to a previous outgoing email.

For a FortiMail unit to perform bounce address tagging, the following must be true:

- bounce verification is enabled
- a bounce address key must exist and be activated
- in the protected domain to which the sender belongs, the "Bypass bounce verification" option is disabled (see Configuring protected domains on page 71)
- 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 71)
- in the session profile, the Bypass Bounce Verification check option is disabled (see Configuring session profiles on page 144)
- the sender email address (`MAIL FROM:`) in the message envelope is empty
- the DSN sender is not in the verification example list

The sender email address is typically empty for bounce messages. The sender email address may also be empty for some types of spam that are not bounce messages. Because the sender email addresses of those types of spam will not have a proper tag, similar to bounce message spam, these spam will fail the bounce verification process. Email sent from email clients or webmail will not have an empty sender email address, and therefore will not be subject to the bounce verification process.

If the tag is successfully verified, the bounce verification scan removes the tag, restoring the recipient email address to one known by the protected domain, and allows the bounce message.

If the tag is **not** successfully verified, the bounce verification scan will perform the action that you have configured for invalid bounce messages.

To configure bounce verification settings

1. Go to *Security* > *Bounce Verification* > *Setting*.
2. Configure the following as required:

GUI item	Description
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.

GUI item	Description
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 71 and Configuring session profiles on page 144.
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.
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 178.

To configure a bounce address tagging and verification key

1. Go to *Security* > *Bounce Verification* > *Setting*.
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 verification exempt list

1. Go to *Security* > *Bounce Verification* > *Verification Exempt List*.
2. Click *New*.
3. Add the host name. FortiMail will use reverse DNS to resolve the client's IP address into host name. You can use wildcard to include all hosts within a domain, for instance, *.example.com.
4. Click *Create*.

Configuring sender rewriting scheme

Go to *Security* > *Sender Rewriting Scheme* to configure sender rewriting scheme (SRS) settings, and maintain a domain name exempt list.

SRS is used to rewrite the envelope sender of an email address, so that emails may be forwarded by an MTA if necessary without being rejected by the receiving server which may have a strict SPF policy in place.

To configure SRS settings

1. Go to *Security* > *Sender Rewriting Scheme* > *Setting*.
2. Configure the following as required:

GUI item	Description
Domain for rewrite	Select which domains to rewrite for external senders sending emails. • None: No domains are rewritten. • Protected Domains: Only protected domains are rewritten. • All Domains: All domains are rewritten.

GUI item	Description
Rewritten address handling	Select which action to take for rewritten addresses. • None: Deny any recipient that is previously rewritten. • Reverse: Reverse the recipient address and send the email to the original sender, for those recipients that are previously rewritten senders.

- If *Default domain for authentication* (under *System* > *Mail Setting* > *Mail Server Setting*) is not enabled, SRS rewrite will not work.
- If there are multiple domains, the default domain will be used for SRS rewrite.

Excluding domains from SRS

If you want to exempt certain domain names from SRS, you can do so by adding the recipient domain name to the exempt list.

To configure the domain name exempt list

1. Go to *Security* > *Sender Rewriting Scheme* > *Exempt List*.
2. Click *New*.
3. Add the recipient domain name.
4. Click *Create*.

Configuring preferences

Go to *Security* > *Option* > *Preference* to configure a few global settings for action profile, mail scan, and antispam preferences.

GUI item	Description
Action Profile	When you configure action profiles (see Configuring antispam action profiles on page 178, Configuring antivirus action profiles on page 184, and Configuring content action profiles on page 195), you may use the following actions: • Deliver to alternate host • Deliver to original host • System quarantine • Personal quarantine • Disclaimer insertion • Subject tag location • Replacement message location

GUI item	Description
	For the delivery and quarantine 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. For the disclaimer insertion action, you can choose to insert the disclaimer in the selected messages or all messages. For the subject tagging action, you can choose to insert the tag at the beginning or the end of the subject.
Enforce delivery action if 'delivery to original/alternate host' is enabled	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 this option to overwrite the final action.
Execute attachment scan on spam email under personal quarantine	For spam email that is sent to personal quarantine, you have the option to continue or stop further scanning the email attachments.
Mail Scan	Specify the following: • *Maximum level to decompress archive file*: Specify how many levels to decompress the archived files for antivirus and content scan. Valid range is 1 to 36. Default value is 12. • *Maximum archive file size to decompress (MB):* Specify the maximum file size to scan after the archived files are decompressed. This applies to every single file after decompression. Bigger files will not be scanned. Default value is 10MB. • *Maximum compression ratio for archive bomb:* Specify the maximum compression ratio for FortiMail to decompress. Valid range is 1 to 1000. Default value is 200.
AntiSpam	
DMARC failure action	Select either: • *Action profile*: Use the action specified in the antispam profile. • *Action profile with none*: If the policy option in the sender's DMARC record is `p=none`, use that action. Else use the action in the antispam profile. • *DMARC record policy*: Use the actions specified in the `policy` option of the sender's DMARC record. The default setting is *Action profile with none*. This system-wide setting can be overridden by a per-domain setting. For details, see the FortiMail Cloud CLI Reference.

GUI item	Description
Impersonation analysis	Email impersonation is one of the email spoofing attacks. It forges the email header to deceive the recipient because the message appears to be from a different source than the actual address. To fight against email impersonation, you can map display names with email addresses and check email for the mapping. You can choose whether the impersonation analysis uses manual mapping entries or dynamic entries. You can also use both types of entries. • *Manual*: Use the entries you manually entered under *Profile* > *AntiSpam* > *Impersonation*. • *Dynamic*: Use the entries automatically learned by the FortiMail mail statistics service. To enable this service, enable `mailstat-service` under `config system global`. The default setting is *Manual*.
QR code URL scan	Select which location(s) to scan for QR code images that contain known spam URLs. • *Inline image*: Embedded inline, in the email body. • *Attachment image*: Email attachments.

Training and maintaining the Bayesian databases

Bayesian scanning uses databases to determine if an email is spam. For Bayesian scanning to be effective, the databases must be trained with known-spam and known-good email messages so the scanner can learn the differences between the two types of email. To maintain its effectiveness, false positives and false negatives must be sent to the FortiMail unit so the Bayesian scanner can learn from its mistakes.

Be aware that, without ongoing training, Bayesian scanning will become significantly less effective over time and thus Fortinet does not recommend enabling the Bayesian scanning feature.

The *Security* > *Option* > *Bayesian* submenu lets you manage the databases used to store statistical information for Bayesian antispam processing, and to configure the email addresses used for remote control and training of the Bayesian databases.

To use a Bayesian database, you must enable the Bayesian scan in the antispam profile. For more information, see Managing antispam profiles on page 160.

This section contains the following topics:

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 279.

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 82.

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 82.

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 82.

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 283.
   By uploading mailbox files, you can provide initial training more rapidly than through the Bayesian control email addresses. Training the global database ensures that outgoing antispam profiles in which you have enabled Bayesian scanning, and incoming antispam profiles for protected domains that you have configured to use the global database, can recognize spam.

   If you have configured the FortiMail unit for email archiving, you can make mailbox files from archived email and spam. For details, see Managing archived email.

   You can leave the global database untrained if both these conditions are true:
   - no outgoing antispam profile has Bayesian scanning enabled
   - no protected domain is configured to use the global Bayesian database
2. Train the per-domain databases by uploading mailbox (.mbox) files. For details, see Backing up, batch training, and monitoring the Bayesian databases on page 283.
   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 285, Accept training messages from users on page 172, and Training Bayesian databases on page 323.

   Before instructing email users to train the Bayesian databases, verify that you have enabled the FortiMail unit to accept training messages. If you have not enabled the “Accept training messages from users” option in the antispam profile for policies which match training messages, the training messages will be discarded without notification to the sender, and no training will occur.

FortiMail units apply training messages to either the global or per-domain Bayesian database, whichever is enabled for the sender's protected domain.

Example: Bayesian training

In this example, Company X has set up a FortiMail unit to protect its email server. With over 1,000 email users, Company X plans to enable Bayesian scanning for incoming email. You, the system administrator, have been asked to configure Bayesian scanning, perform initial training of the Bayesian databases, and configure Bayesian control email addresses for ongoing training.

The local domain name of the FortiMail unit itself is example.com.

Company X has email users in two existing protected domains:

- example.net
- example.org

Each protected domains receives email with slightly different terminology, which could be considered spam to the other protected domain, and so will use separate per-domain Bayesian databases.

To facilitate initial training of each per-domain Bayesian database, you have used your email client software to collect samples of spam and non-spam email from each protected domain, and exported them into mailbox files:

- example-net-spam.mbox
- example-net-not-spam.mbox
- example-org-spam.mbox
- example-org-not-spam.mbox

After initial training, email users will use the default Bayesian control email addresses to perform any required ongoing training for each of their per-domain Bayesian databases.

To enable use of per-domain Bayesian databases

1. Go to *Domain & User* > *Domain* > *Domain*.
2. Select the row corresponding to example.net and click Edit.
3. Click the arrow to expand Advanced Setting and click Other.
4. Disable *Use global bayesian database*.
5. Click OK.
   Repeat the above steps for the protected domain example.org.

To initially train each per-domain Bayesian database using mailbox files

1. Go to *Security* > *Option* > *Bayesian.*
2. Under Database Training, from Select a domain, select a domain.
   This example uses example.net and example.org.
3. In the Operations area, click Train group Bayesian database with email samples.
   A dialog appears.
4. In Clean emails, click Browse and locate example-net-not-spam.mbox.
5. In Spam emails, click Browse and locate example-net-spam.mbox.
6. Click OK.
   Repeat the above steps for the protected domain example.org and its sample Bayesian database files.

To enable Bayesian scanning

1. Go to *Profile* > *AntiSpam* > *AntiSpam*.
2. In the row corresponding to an antispam profile that is selected in a policy that matches recipients in the protected domain example.net, click Edit.
3. Enable Bayesian.
4. Click the arrow to expand Bayesian.
5. Enable the option Accept training messages from user.
6. Click OK.
   Repeat the above steps for all incoming antispam profiles that are selected in policies that match recipients in the protected domain example.org.

To perform ongoing training of each per-domain Bayesian database

1. Notify email users that they can train the Bayesian database for their protected domain by sending them an email similar to the following:

   This procedure assumes the default Bayesian control email addresses. To configure the Bayesian control email addresses, go to *Security* > *Bayesian* > *Control Account*.

   ```
   All employees,
   We have enabled a new email system feature that can be trained to recognize the differences
        between spam and legitimate email. You can help to train this feature. This message
        describes how to train our email system.
   If you have old email messages and spam...
   ```
   - `Forward the old spam to learn-is-spam@example.com from your company email account.`
   - `Forward any old email messages that are not spam to learn-is-not-spam@example.com from your company email account.`

   ```
   If you receive any new spam, or if a legitimate email is mistakenly classified as spam...
   ```
   - `Forward spam that was not recognized to is-spam@example.com from your company email account.`
   - `Forward legitimate email that was incorrectly classified as spam to is-not-spam@example.com from your company email account.`
2. Notify other FortiMail administrators that they can train the per-domain Bayesian databases for those protected domains by forwarding email to the Bayesian control accounts, described in the previous step. To do so, they must configure their email client software with the following sender addresses:
   - default-grp@example.net
   - default-grp@example.org

   For example, when forwarding a training message from the sender (`From:`) email address `default-grp@example.net`, the FortiMail unit will apply the training message to the per-domain Bayesian database of example.net.

See also

Training the Bayesian databases

Types of Bayesian databases

Backing up, batch training, and monitoring the Bayesian databases

Configuring the Bayesian training control accounts

Configuring global quarantine report settings

Backing up, batch training, and monitoring the Bayesian databases

You can train, back up, restore, and reset the global and per-domain Bayesian databases. You can also view a summary of the number of email messages that have been used to train each Bayesian database.

You can alternatively train Bayesian databases by forwarding spam and non-spam email to Bayesian control email addresses. For more information, see Training the Bayesian databases on page 279.

You can alternatively back up, restore, and reset all Bayesian databases at once. For more information, see Backup and restore.

Domain administrators cannot access the global Bayesian settings.

For details, see About administrator account permissions and domains on page 44.

To individually train, view and manage Bayesian databases

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database:
   - For the global Bayesian database, from Select a domain, select System. For more information, see Use global Bayesian database on page 82.
   - 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 283
   - To back up a Bayesian database on page 284
   - To restore a Bayesian database on page 284
   - To reset a Bayesian database on page 285

To train a Bayesian database using mailbox files

Uploading mailbox files trains a Bayesian database with many email messages at once, which is especially useful for initial training of the Bayesian database until it reaches maturity. Because this method appends to the Bayesian database rather than overwriting, you may also perform this procedure periodically with new samples of spam and non-spam email for batch maintenance training.

If you have configured the FortiMail unit for email archiving, you can make mailbox files from archived email and spam. For details, see Managing archived email.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Train global Bayesian database with mbox files
   - Train group Bayesian database with mbox files

   A pop-up window appears enabling you to specify which mailbox files to upload.
4. In the Innocent mailbox field, click Browse, then select a mailbox file containing email that is not spam.
5. In the Spam mailbox field, click Browse, then select a mailbox file containing email that is spam.
   For best results, the mailbox file should contain a representative sample of spam for the specific FortiMail unit, protected domain, or email user.
6. Click OK.
   Your management computer uploads the file to the FortiMail unit to train the database, and the pop-up window closes. Time required varies by the size of the file and the speed of your network connection. To update the training summary display in the Summary area with the new number of learned spam and non-spam messages, refresh the page by selecting the tab.

To back up a Bayesian database

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Backup global Bayesian database
   - Backup group Bayesian database

   A pop-up window appears enabling you to download the database backup file.
4. Select a location in which to save the database backup file and save it.
   The Bayesian database backup file is downloaded to your management computer. Time required varies by the size of the file and the speed of your network connection.

To restore a Bayesian database

Back up the Bayesian database before beginning this procedure. Restoring a Bayesian database replaces all training data stored in the database. For more information on backing up Bayesian database files, see To back up a Bayesian database on page 284 or Backup and restore.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Restore global Bayesian database
   - Restore group Bayesian database

   A pop-up window appears enabling you to upload a database backup file.
4. Click Browse to locate and select the Bayesian database backup file, then click OK.
5. Click OK.

   The Bayesian database backup file is uploaded from your management computer, and a success message appears. Time required varies by the size of the file and the speed of your network connection.

   If a database operation error message appears, you can attempt to repair database errors. For more information, see Backup and restore.

To reset a Bayesian database

Back up the Bayesian database before beginning this procedure. Resetting a Bayesian database deletes all training data stored in the database. For more information on backing up Bayesian database files, see To back up a Bayesian database on page 284 or Backup and restore.

1. Go to *Security* > *Option* > *Bayesian*.
2. Select the type of the Bayesian database that you want to train.
   - For the global Bayesian database, from Select a domain, select System.
   - For a per-domain Bayesian database, from Select a domain, select the name of the protected domain, such as example.com.
3. In the Operation area, click the link appropriate to the type that you selected in the previous step, either:
   - Reset global Bayesian database
   - Reset group Bayesian database

   A pop-up window appears asking for confirmation.
4. Click Yes.

   A status message notifies you that the FortiMail unit has emptied the contents of the Bayesian database.

See also

Training the Bayesian databases

Types of Bayesian databases

Configuring the Bayesian training control accounts

Configuring the Bayesian training control accounts

The Control Account tab lets you configure the email addresses used for remote training of the Bayesian databases.

To train the Bayesian databases through email, email users and FortiMail administrators forward spam and non-spam email (also called training messages) to the appropriate Bayesian control email address. Bayesian control email addresses consist of the user name portion (also known as the local-part) of the email address configured on this tab and the local domain name of the FortiMail unit. For example, if the local domain name of the FortiMail unit is example.com, you might forward spam to `learn-is-spam@example.com`.

If the FortiMail unit is configured to accept training messages, it will use the email to train one or more Bayesian databases. To accept a training message:

- The training message must match a recipient-based policy.
- The matching recipient-based policy must specify use of an antispam profile in which *Accept training messages from users* is enabled.

If either of these conditions is not met, the FortiMail unit will silently discard the training message without using them for training.

If these conditions are both met, the FortiMail unit accepts the training message and examines the user name portion and domain name portion of the sender address.

Depending on whether the sender's protected domain is configured to use the global or per-domain Bayesian database (the option *Use global Bayesian database*), the FortiMail Cloud unit trains that Bayesian database.

To configure the Bayesian control email addresses, go to *Security* > *Option* > *Bayesian*.

GUI item	Description
"is really spam" user name	Enter the user name portion of the email address, such as `is-spam`, to which email users will forward spam false negatives. Forwarding false negatives corrects the Bayesian database when it inaccurately classifies spam as being legitimate email.
"is not really spam" user name	Enter the user name portion of the email address, such as `is-not-spam`, to which email users will forward spam false positives. Forwarding false positives corrects the Bayesian database when it inaccurately classifies legitimate email as being spam.
"learn is spam" user name	Enter the user name portion of the email address, such as `learn-is-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
"learn is not spam" user name	Enter the user name portion of the email address, such as `learn-is-not-spam`, to which email users will forward spam that the Bayesian scanner has not previously scanned.
training group	Enter the user name portion of the email address, such as `default-grp`, that FortiMail administrators can use as their sender email address when forwarding email to the "learn is spam" email address or "learn is not spam" email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain).

See also

Training the Bayesian databases

Types of Bayesian databases

Backing up, batch training, and monitoring the Bayesian databases

Configuring 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* > *IBE Encryption* submenu lets you configure the Identity Based Encryption (IBE) service. With IBE, you can send secured email through the FortiMail unit.

This section contains the following topics:

- About FortiMail IBE
- FortiMail IBE configuration workflow
- Configuring IBE services

IBE is a type of public-key encryption. IBE uses identities (such as email addresses) to calculate encryption keys that can be used for encrypting and decrypting electronic messages. Compared with traditional public-key cryptography, IBE greatly simplifies the encryption process for both users and administrators. Another advantage is that a message recipient does not need any certificate, key pre-enrollment, or specialized software to access the email.

About FortiMail IBE

The FortiMail unit encrypts an email message using the public key generated with the recipient's email address. The email recipient does not need to install any software or generate a pair of keys in order to access the email.

When an email reaches the FortiMail unit, the FortiMail unit applies its IP-based policies and recipient-based policies containing IBE-related content profiles as well as the message delivery rules to the email. If a policy or rule match is found, the FortiMail unit encrypts the email using the public key before sending a notification to the recipient. Sample secure message notification on page 288 shows a sample notification.

The notification email contains an HTML attachment, which contains instructions and links telling the recipient how to access the encrypted email.

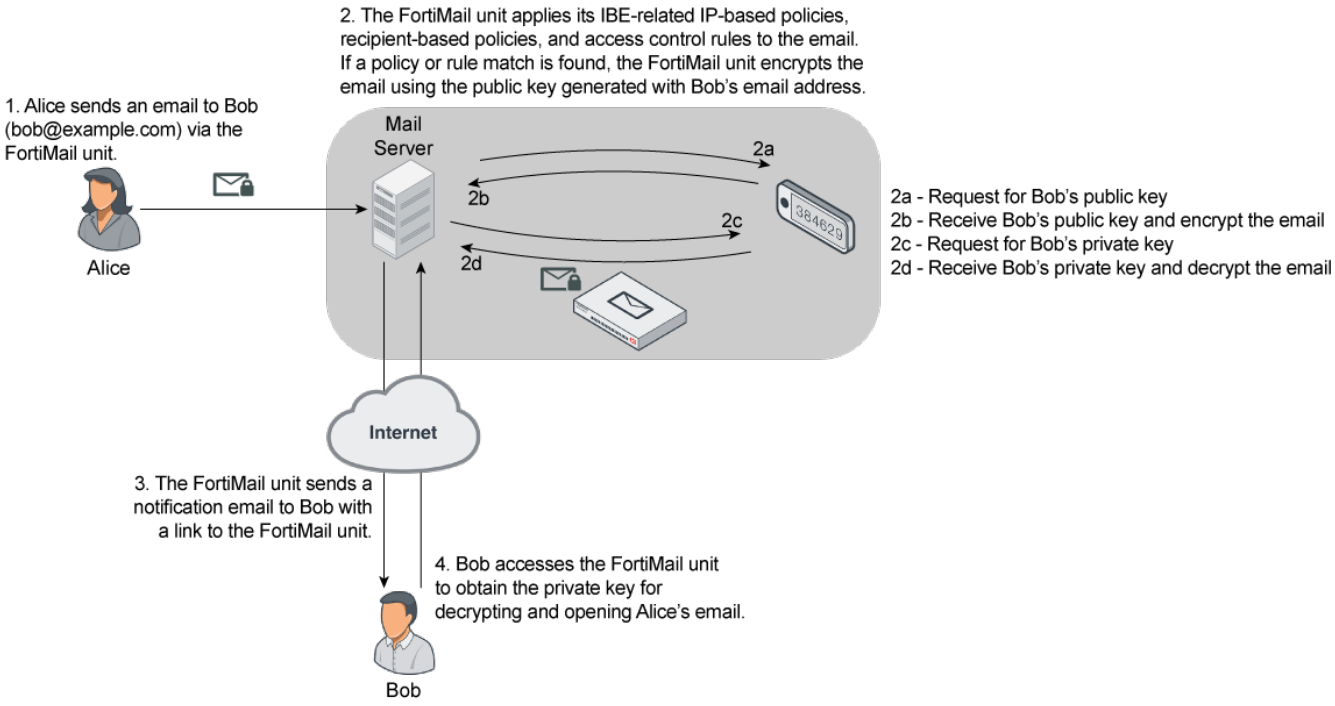
If this is the first time the recipient receives such a notification, the recipient must follow the instructions and links to register on the FortiMail unit before reading email.

If this is not the first time the recipient receives such a notification and the recipient has already registered on the FortiMail unit, the recipient only needs to log in to the FortiMail unit to read email.

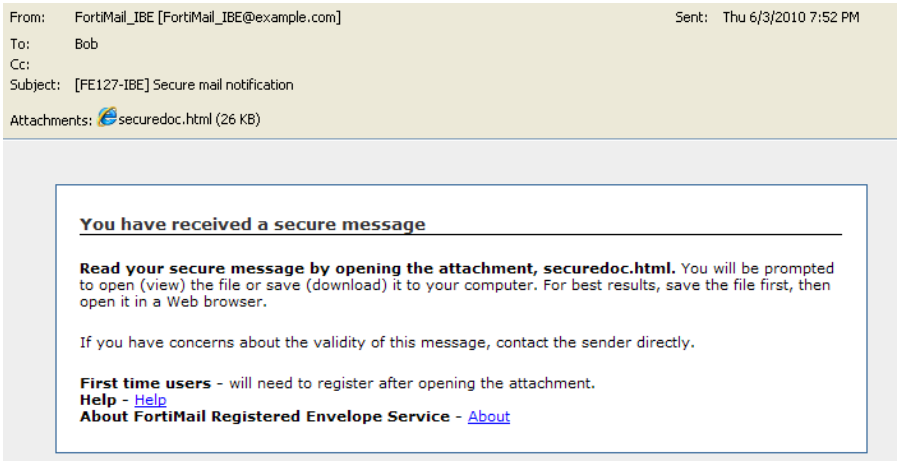
When the recipient opens the mail on the FortiMail unit, the email is decrypted automatically.

Due to more confining security restrictions imposed by the iOS system, email attachments included in IBE PUSH (for details about IBE PUSH and PULL methods, see Configuring encryption profiles on page 237) notification messages can no longer be opened properly on iOS 10 and later. Therefore, users cannot view the encrypted email messages on these iOS devices. Users should download and open the attachments on their PCs as a workaround.

How FortiMail works with IBE



Sample secure message notification



External IBE users can only access their secure messages via the link in the IBE notification email, while internal users (protected domain users) can also access their secure messages via webmail login.

See also

About FortiMail IBE

FortiMail IBE configuration workflow

Configuring IBE services

FortiMail IBE configuration workflow

Follow the general steps below to use the FortiMail IBE function:

- Configure and enable the IBE service. See Configuring IBE services on page 290.
- Manage IBE users. See Configuring IBE users on page 98.
- Configure an IBE encryption profile. See Configuring encryption profiles on page 237.

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 195.
- 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 186.
- 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 138, and Controlling email based on IP addresses on page 132.

  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 231)
  - added the dictionary profile to a content profile which also includes a content action profile that has an encryption profile in it
  - included the content profile to IP and recipient policies

  You then notify your email users on how to mark the email subject line and header if they want to send encrypted email.

  For example, Alice wants to send an encrypted email to Bob through the FortiMail unit. She can add “Confidential” in the email subject line, or “Confidential” in the header (in Microsoft Outlook, when compiling a new mail, go to Options > Message settings > Sensitivity, and select Confidential in the list). The FortiMail unit will apply the policies you configured to the email by checking the email’s subject line and header. If one of them matches the patterns defined in the dictionary profile, the email will be encrypted.
- Configure IBE email storage.
- Configure log settings for IBE encryption. See Configuring logging on page 306.
- View logs of IBE encryption. See Viewing log messages on page 14.

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 129.
- Configure IBE email storage.

- Configure log settings for IBE encryption. See Configuring logging on page 306.
- View logs of IBE encryption. See Viewing log messages on page 14.

For full configuration and procedural details, depending on your environment's requirements, see the Cookbook recipes Encrypting confidential emails in FortiMail and How to encrypt emails sent from a designated source in FortiMail.

See also

About FortiMail IBE

Configuring IBE services

Configuring IBE services

You can configure, enable, or disable IBE services which control how secured mail recipients use the FortiMail IBE function. For details about how to use IBE service, see FortiMail IBE configuration workflow on page 289.

To configure IBE service

1. Go to *Encryption* > *IBE* > *IBE Encryption*.
2. Configure the following:

GUI item	Description
Enable IBE service	Select to enable the IBE service you configured.
IBE service name	Enter the name for the IBE service. This is the name the secure mail recipients will see once they access the FortiMail unit to view the mail.
Activation is required for account registration	When enabled, IBE users receive a validation email that contains an activation link to complete the account registration. When disabled, IBE users are redirected to the IBE account after registration. Note that if the IBE user registered by clicking the registration link inside the reset notification email, they will not be redirected, and will need to login to their account.
Account registration expiry time (days)	Enter the number of days that the secure mail recipient has to register on the FortiMail unit to view the mail before the registration expires. The starting date is the date when the FortiMail unit sends out the first notification to a mail recipient.
Account inactivity expiry time (days)	Enter the number of days the secure mail recipient can access the FortiMail unit without registration. For example, if you set the value to 30 days and if the mail recipient did not access the FortiMail unit for 30 days after the user registers on the unit, the recipient will need to register again if another secure mail is sent to the user. If the recipient accessed the FortiMail unit on the 15th days, the 30-day limit will be recalculated from the 15th day onwards.
Account password reset expiry time (hours)	Enter the password reset expiry time in hours. This is for the recipients who have forgotten their login passwords and request for new ones. The secured mail recipient must reset the password within this time limit to access the FortiMail unit.

GUI item	Description
Encrypted email retention period (days)	Enter the number of days that the secured mail will be saved on the FortiMail unit.
Allow secure replying	Select to allow the secure mail recipient to reply the email with encryption.
Allow secure forwarding	Select to allow the secure mail recipient to forward the email with encryption.
Allow secure composing	Select to allow the secure mail recipient to compose an email. The FortiMail unit will use policies and mail delivery rules to determine if this mail needs to be encrypted. For encrypted email, the domain of the composed mail's recipient must be a protected one, otherwise an error message will appear and the mail will not be delivered.
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.
"About" content URL	You can create a file about the FortiMail IBE encryption and enter the URL for the file. The mail recipient can click the "About" link from the secure mail notification to view the file. If you leave this field empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification.
Allow custom user control	If your corporation has its own user authentication tools, enable this option and enter the URL. **"Custom user control" URL**: This is the URL where you can check for user existence. **"Custom forgot password" URL**: This is the URL where users get authenticated.
Authentication Setting	FortiMail supports the customization of IBE authentication settings, supporting two-factor authentication through the use of one-time password (OTP) tokens and passwords. Users may authenticate themselves through either SMS or email. Additionally, authenticated sessions may be time limited, to ensure historical emails are not accessed from the encrypted mailbox. Use this section to define the authentication mode, email and SMS secure token delivery options, and secure token and maximum attempt timeouts and limits. See the User registration process with two-factor authentication on page 101 for more information on the user workflow.
Notification Setting	Under *Account Status Notification*, enable the types of account notifications you wish to be sent to users. For *Expiration*, also define when the expiration notification should be sent. Under *Email Status Notification*, you can choose to send a notification to the sender or recipient when the secure email is read or remains unread for a specified period of time. Click the *Edit* link to modify the email template. For details, see Customizing email templates on page 59. Depending on the IBE email access method (either PUSH or PULL) you defined in Configuring encryption profiles on page 237, the notification settings behave differently.

GUI item	Description
	• If the IBE message is stored on FortiMail (PULL access method), the “read” notification will only be sent the first time the message is read. • If the IBE message is not stored on FortiMail (PUSH access method), the “read” notification will be sent every time the message is read, that is, after the user pushes the message to FortiMail and FortiMail decrypts the message. • There is no “unread” notification for IBE PUSH messages.

Configuring certificate bindings

Go to *Encryption* > *S/MIME* > *Certificate Binding* to create certificate binding profiles, which establish the relationship between an email address and the certificate that:

- proves an individual’s identity
- provides their keys for use with encryption profiles

Use this relationship and that information for secure MIME (S/MIME) according to RFC 2634.

If an incoming email message is encrypted, FortiMail Cloud compares the recipient’s identity with the list of certificate bindings to determine if it has a key that can decrypt the email. If there is a matching **private key**, FortiMail Cloud will decrypt the email before delivering it. If there is **not**, then FortiMail Cloud forwards the still-encrypted email to the recipient.

If you have selected an encryption profile (see Configuring encryption profiles on page 237) with an encryption action in the message delivery rule that applies to the session, then FortiMail Cloud compares the recipient’s identity with the list of certificate bindings to determine if it has a certificate and **public key**. If there is a matching public key, then FortiMail Cloud will encrypt the email using the algorithm specified in the encryption profile. If there is **not**, then FortiMail Cloud performs the failure action indicated in the encryption profile.

If an incoming email message is digitally signed, FortiMail will **not** verify the signature. Instead, it will deliver the message unmodified. Email clients usually do the verification.

If you have selected an encryption profile with signing action in the message delivery rule that applies to the session, then FortiMail Cloud compares the sender’s identity with the list of certificate bindings to determine if it has a certificate and **private key**. If there is a matching private key, it will add a digital signature using the algorithm specified in the encryption profile. If there is **not**, then FortiMail Cloud performs the failure action indicated in the encryption profile.

FortiMail Cloud does **not** check if an outgoing email is already encrypted. Email clients optionally can apply their own additional layer of S/MIME encryption (such as if they require non-repudiation) before they submit email for delivery through FortiMail Cloud.

The destination of an S/MIME email can be another FortiMail Cloud, for gateway-to-gateway S/MIME, but it could alternatively be any email gateway or server, as long as one of the following supports S/MIME and possesses the sender’s certificate and public key, either the:

- destination’s mail relay or mail server
- recipient’s email client

This is necessary to decrypt the email; otherwise, the recipient cannot read the email.

Before any personal certificate that you upload will be valid for use, you must upload the certificate of its signing certificate authority (CA). For details, see Managing certificate authority certificates.

To view and configure certificate binding

1. Go to *Encryption* > *S/MIME* > *Certificate Binding*.

GUI item	Description
Profile ID	Displays the name of the profile.
Address Pattern	Displays the email address or domain associated with the identity represented by the personal or server certificate.
Key Usage	Displays if the key is for encryption, signing, or encryption and signing.
Identity	Displays the identity, often a first and last name, included in the common name (CN) field of the Subject line of the personal or server certificate.
Private Key	Displays the private key associated with the identity, used to decrypt and sign email from that identity.
Valid From	Displays the beginning date of the period of time during which the certificate and its keys are valid for use by signing and encryption.
Valid To	Displays the end date of the certificate's period of validity. After this date and time, the certificate expires, although the keys may be retained for the purpose of decrypting and reading email that was signed and encrypted previously.
Status	Indicates whether the certificate is currently not yet valid, valid, or expired, depending on the current system time and the certificate's validity period.
(Green dot in column heading)	Indicates whether or not the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

2. Either click *New* to add a profile or double-click a profile to modify it.
3. In *Address Pattern*, enter the email address or email domain that you want to use the certificate in this binding.

   For example, you might bind a personal certificate for `User1` to the email address, `user1@example.com`.
4. From Key type, select what kind of keys you want to upload. If you only have a public key, you can only use it to encrypt email. If you have a public key and private key pair, you can use them to encrypt email (with a public key), decrypt email (with a private key), or digitally sign email (with a private key).
5. Select one of the following ways to either import and bind a personal certificate, or to bind an existing server certificate:
   - *Import PKCS12 file*: Upload and bind a personal certificate-and-key file that uses the public key cryptography standard #12 (PKCS #12), stored in a password-protected file format (.p12).
   - *Import PEM files*: Upload and bind a pair of personal certificates and public and private keys that use privacy-enhanced email (PEM), a password-protected file format (.pem).
   - *Choose from local certificate list*: Bind a certificate that you have previously uploaded to the FortiMail unit. For details, see Managing local certificates on page 1.
6. Depending on your selection in *Import key from*, either upload the personal certificate files and enter their password, or select the name of a local certificate from *Select local certificate*list.

   If a certificate import does not succeed and event logging is enabled, to determine the cause of the failure, you can examine the event log messages. Log messages may indicate errors such as an unsupported password-based encryption (PBE) algorithm:

   ```
   PKCS12 Import: err=0x6074079: digital envelope routines / EVP_PBE_CipherInit / unknown pbe
       algorithm
   ```

For best results, use 3DES with SHA1. RC2 is not supported.

7. Click *Create*.
   Certificate bindings will be used automatically as needed for matching message delivery rules in which you have selected an encryption profile. For details, see Using S/MIME encryption on page 239, Configuring encryption profiles on page 237, and Configuring delivery rules on page 129. It will also be used in the content profile and then in the policies which use the content profile.

See also

Configuring encryption profiles

Configuring data loss prevention

The FortiMail data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. After you define sensitive data patterns, you can take actions against the email containing data matching these patterns. You configure the DLP system by creating individual rules based on document fingerprint, file filters or sensitive information in a DLP profile and assign the profile to a policy.

This section describes how to configure the DLP settings.

- DLP configuration workflow
- Defining the sensitive data
- Configuring DLP rules
- Configuring DLP profiles

DLP configuration workflow

DLP is enabled by default on high-end platforms. For performance reasons, it is disabled by default on low-end platforms.

To use the DLP feature

1. Enable the DLP feature using the following hidden command.
```
config system global
   set data-loss-prevention enable
end
```
2. Define the sensitive data first. See Defining the sensitive data on page 295.
3. Define the DLP scan rules which specify the information to be checked in the email traffic. See Configuring DLP rules on page 297.
4. Define DLP profiles, which use one or more rules. See Configuring DLP profiles on page 298. 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 195.
5. Apply the DLP profiles to the IP or recipient based policies. See Controlling email based on sender and recipient addresses on page 138 and Controlling email based on IP addresses on page 132.

Defining the sensitive data

Sensitive data can be any of the following types:

- **User-defined**: You specify what information should be checked, such as a word, a phrase, or a regular expression. See also Syntax on page 1.
- **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 296.
- **File filters**: Also used in the content profiles. See Configuring file filters on page 193.

DLP document fingerprinting

One of the DLP techniques to detect sensitive data is fingerprinting (also called document fingerprinting). Most DLP techniques rely on you providing a characteristic of the file you want to detect, whether it's the file type, the file name, or part of the file contents. Fingerprinting is different in that you provide the file itself. The FortiMail unit then generates a checksum fingerprint and stores it. The FortiMail unit generates a fingerprint for all email attachments, and compares it to all of the fingerprints stored in its fingerprint database. If a match is found, the configured action is taken.

Currently, Microsoft Office, Open Office, PDF and text files can be detected by DLP fingerprinting and fingerprints can be saved for each revision of your files as they are updated.

The FortiMail unit must have access to the documents for which it generates fingerprints. There are two methods to generate fingerprints:

- One method is to manually upload documents to be fingerprinted directly to the FortiMail unit.
- The other is to allow the FortiMail unit to access a network share that contains the documents to be fingerprinted.

If only a few documents are to be fingerprinted, a manual upload may be the easiest solution. If many documents require fingerprinting, or if the fingerprinted documents are frequently revised, using a network share makes user access easier to manage.

When you generate document fingerprints, only Microsoft Office, Open Office, PDF and text files with a minimum of 50 characters are supported.

To configure manual document fingerprints

1. Go to *Data Loss Prevention* > *Sensitive Data* > *Fingerprint*.
2. Click *New* and configure the following:

GUI item	Description
Name	Enter a descriptive name for the fingerprint.
Description	Optionally enter a description.
File list	Click *New* to browse to the file and generate a fingerprint for it. In the Fingerprint Status column, one of the following status will be displayed: • To be generated - The status when you've uploaded the file to the Fingerprint list before clicking the Create button. • Being generated: The status when the fingerprint generating process is executing. • Generated - The fingerprint has been generated. • Not generated - No fingerprint has been generated for the file because there is not enough text or the fingerprint is being generated • File type not supported - The file type is not supported to generated fingerprint.

To configure a fingerprint document source

1. Go to *Data Loss Prevention* > *Sensitive Data* > *Fingerprint Source*.
2. Click *New* and configure the following:

GUI item	Description
Name	Enter a descriptive name for the document source.
Server type	This refers to the type of server share that is being accessed. The default is SMB/CIFS (Windows Share protocol) but this will also work on Samba shares.
Server address	Enter the IP address of the server.
User name	Enter the user name of the account the FortiMail unit uses to access the server network share.
Password	Enter the password of the account the FortiMail unit uses to access the server network share.
Path	Enter the path to the document folder.
File pattern	You may enter a filename pattern to restrict fingerprinting to only those files that match the pattern. To fingerprint all files, enter an asterisk (“*”).
Checking period	Check the files document source daily if the files are added or changed regularly.
Advanced	
Fingerprint files in subdirectories	By default, only the files in the specified path are fingerprinted. Files in subdirectories are ignored. Select this option to fingerprint files in subdirectories of the specified path.
Remove fingerprints for detected files	Select this option to retain the fingerprints of files deleted from the document source. If this option is disabled, fingerprints for deleted files will be removed when the document source is scanned next time.
Keep previous fingerprints for modified files	Select this option to retain the fingerprints of previous revisions of updated files. If this option is disabled, fingerprints for previous version of files will be deleted when a new fingerprint is generated.

See also

Configuring DLP rules

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring DLP rules

DLP scan rules specify what to look for in what part of the email. For example, you can specify to scan for some sensitive data in email bodies and attachments.

To configure DLP rules

1. Go to *Data Loss Prevention* > *Rule & Profile* > *Rule*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Name	Enter a descriptive name for the rule.
Description	Optionally enter a description.
Conditions	Select either Match all conditions or Match any condition. Click *New* to add conditions. Depending on what email part you select, you can specify different conditions.
Exceptions	Click *New* to add exceptions. Email matching the exceptions will not be scanned.

Configuring DLP profiles

After you configure the scan rules/conditions, you add them to the DLP profiles. In the profiles, you also specify what actions to take (for details about action profiles, see Configuring content action profiles on page 195). Then you apply the DLP profiles to the IP or recipient based policies.

To configure a DLP profile

1. Go to *Data Loss Prevention* > *Rule & Profile* > *Profile*.
2. Click *New*.
3. Configure the following:

GUI item	Description
Name	Enter a descriptive name for the profile.
Action	Select a default action to use when the specified scan rules match the email. Click *New* to create a new action profile. See Configuring content action profiles on page 195.
Comment	Optionally enter a comment.
Content Scan Setting	Click *New* to configure the following settings: • Enabled: check this box to enable the settings. • Scan rule: select a scan rule from the dropdown list. Or click *New* to create a new rule. • Action: select an action profile from the dropdown list. Or click New to create a new profile. If no action profile is selected, the default one will be used.

Log and report

FortiMail provides 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 Cloud logging

FortiMail Cloud units can log many different email activities and traffic to FortiAnalyzer Cloud:

- system-related events
- 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 302.

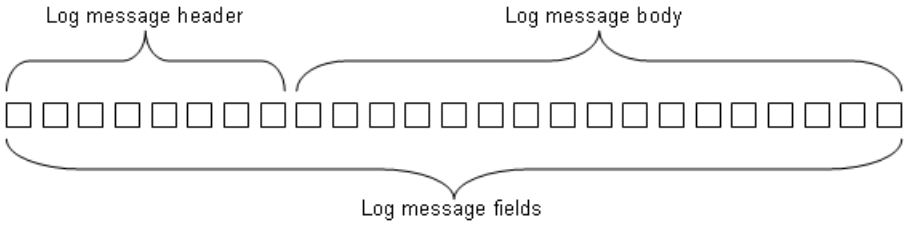
If you need remote logging, please contact Fortinet Support.

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 Cloud appliance took to respond to it. **These fields may vary by log type.**

Log message header and body



For example, in the following event log, the bold section is the header and the italic section is the body.

date=2012-08-17 time=12:26:41 device_id=FE100C3909600504 log_id=0001001623 type=kevent subtype=admin pri=information*user=admin ui=GUI(172.20.120.26) action=login status=success reason=none msg="User admin login successfully from GUI (172.20.120.26)"*

Device ID field

Depending on where you view log messages, log formats may vary slightly. For example, if you view logs on the FortiMail GUI or download them to your 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

FortiMail 5.0 added two new fields -- policy ID and domain -- to history logs.

The policy ID is in the format of x:y:z, where:

- x is the ID of the global access control policy.
- y is the ID of the IP-based policy.
- z is the ID of the recipient-based policy.

If the value of x, y, and z is 0, it means that no policy is matched.

If the matched recipient-based policy is incoming, the protected domain will be logged in the domain field.

If the matched recipient-based policy is outgoing, the domain field will be empty.

Endpoint field

FortiMail 4.0 MR3added a field called `endpoint` to the history and antispam logs. This field displays the endpoint's subscriber ID, MSISDN, login ID, or other identifiers. This field is empty if the sender IP is not matched to any endpoint identifier or if the endpoint reputation is not enabled in the session profiles.

Log_part field

In FortiMail 3.0 MR3 and newer, the log header of some log messages may include an extra field, `log_part`, which provides numbered identification (such as 00, 01, and 02) when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length was reduced.

Hex numbers in history logs

If you view the log messages on the FortiMail GUI or send the logs to a Syslog server, the dispositions and classifiers are described. However, if you download log files from FortiMail GUI to your computer and open them, the dispositions and classifiers are displayed in hex numbers. For explanation of these numbers, see the Classifiers and dispositions in history logs on page 303.

See also

FortiMail log types

Configuring logging

Log message severity levels

Viewing log messages

Viewing generated reports

FortiMail log types

FortiMail Cloud units can record the following types of log messages. Event logs also include several subtypes. You can view and download these logs from the Log submenu of the Monitor tab.

Log types

Log Types	Default File Name	Description
History (statistics)	alog	Records all email traffic going through the FortiMail unit (SMTP relay or proxy).
System Event (kevent)	klog	Records system management activities, including changes to the system configuration as well as administrator and user log in and log outs.
Mail Event (event)	elog	Records webmail, SMTP, POP3, and IMAP events.
Antispam (spam)	slog	Records spam detection events.
Antivirus (virus)	vlog	Records virus detection events.
Encryption (encrypt)	nlog	Records detection of IBE-related events. See also.Configuring encryption profiles on page 237.

Email related logs contain a session identification (ID) number, which is located in the session ID field of the log message. The session ID corresponds to all the relevant log types so that the administrator can get all the information about the event or activity that occurred on their network.

For more information about these specific log types, see the FortiMail Log Reference.

Avoid recording highly frequent log types to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

See also

Log message severity levels

Viewing log messages

Configuring logging

About FortiMail Cloud logging

Subtypes

FortiMail logs are grouped into categories by log type and subtype as shown in the table below:

Log Type	Subtype
kevent	admin config config-user dns ha system update
event	imap pop3 smtp webmail
virus	infected malware-outbreak file-signature
spam	default admin user
statistics	(no subtype)
encrypt	(no subtype)

Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `pri=warning`.

Log severity levels

Levels (0 is highest)	Name	Description
0	Emergency	The system has become unstable
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notice	Information about normal events.
6	Information	General information about system operation.

For each location where the FortiMail Cloud 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 Cloud unit stores all log messages equal to or exceeding the severity level you select. For example, if you select Error, the FortiMail Cloud unit stores log messages whose severity level is Error, Critical, Alert, or Emergency.

Classifiers and dispositions in history logs

Each history log contains one field called Classifier and another called Disposition.

The Classifier field displays which FortiMail scanner applies to the email message. For example, “Banned Word” means the email messages was detected by the FortiMail banned word scanner. The Disposition field specifies the action taken by the FortiMail unit.

If you view the log messages on the FortiMail GUI or send the logs to a Syslog server, the dispositions and classifiers are displayed in English terms. However, if you download log files from FortiMail GUI to your computer and open them, the dispositions and classifiers are displayed in hex numbers.

The following tables map the hex numbers for classifiers with their description.

Classifiers

Hex Number	Classifier	Hex Number	Classifier
0x00	Undefined	0x2A	Message Cryptography

Hex Number	Classifier	Hex Number	Classifier
0x01	User Safe	0x2B	Delivery Control
0x02	User Discard	0x2C	Encrypted Content
0x03	System Safe	0x2D	SPF Failure as Spam
0x04	System Discard	0x2E	Fragmented Email
0x05	RBL	0x2F	Email Contains Image
0x06	SURBL	0x30	Content Requires Encryption
0x07	FortiGuard AntiSpam	0x31	FortiGuard AntiSpam Block IP
0x08	FortiGuard AntiSpam-Safe	0x32	Session Remote
0x09	Bayesian	0x33	FortiGuard Phishing
0x0A	Heuristic	0x34	AntiVirus
0x0B	Dictionary Scanner	0x35	Sender Address Rate Control
0x0C	Banned Word	0x36	SMTP Auth Failure
0x0D	Deep Header	0x37	Access Control List Reject
0x0E	Forged IP (before v5.2 release)	0x38	Access Control List Discard
0x0F	Quarantine Control	0x39	Access Control List Bypass
0x10	Tagged virus (before v4.3 release)	0x3A	FortiGuard Antispam Webfilter
0x11	Attachment Filter (see note above)	0x3B	Newsletter Suspicious
0x12	Grey List	0x3C	TLS Streaming
0x13	Bypass Scan On Auth	0x3D	Policy Match
0x14	Disclaimer	0x3E	Dynamic Safe List
0x15	Defer Delivery	0x3F	Sender Verification
0x16	Session Domain	0x40	Behavior Analysis
0x17	Session Limits	0x41	FortiGuard Spam Outbreak
0x18	Session Safe	0x42	Newsletter
0x19	Session Block	0x43	DMARC
0x1A	Content Monitor and Filter	0x44	File Signature
0x1B	Content Monitor as Spam	0x45	Sandbox
0x1C	Attachment as Spam	0x46	Malware Outbreak
0x1D	Image Spam	0x47	DLP Filter
0x1E	Sender Reputation	0x48	DLP Treated as Spam
0x1F	Access Control List Relay Denied	0x49	DLP Requires Encryption
0x20	Safelist Word	0x4A	Access Control List Safe

Hex Number	Classifier	Hex Number	Classifier
0x21	Domain Safe	0x4B	Virus Outbreak
0x22	Domain Block	0x4C	FortiGuard Antispam Webfilter
0x23	SPF (not in use)	0x4D	Impersonation Analysis
0x24	Domain Key (not in use)	0x4E	Session Action
0x25	DKIM (not in use)	0x4F	SPF Sender Alignment
0x26	Recipient Verification	0x50	SPF Check
0x27	Bounce Verification	0x51	Sandbox URL
0x28	Endpoint Reputation	0x52	Sandbox No Result
0x29	SSL Profile Check	0x53	Content Modification
		0x54	DKIM Failure

When the classifier is “Attachment Filter”, a new field “atype” (attachment type) is also displayed. This field is for debug purpose only.

Dispositions

Hex number	Disposition	Hex Number	Disposition
0x00	Undefined	0x10000	Encryption
0x01	Accept the message	0x20000	Decryption
0x02	Move to a specified folder	0x40000	Deliver the message to an alternate host
0x04	Send a reject to the SMTP client	0x80000	Deliver the message to a set of recipients
0x08	Add a header to the message	0x100000	Archive the message
0x10	Modify the subject line	0x200000	Encase the original message with customizable text
0x20	Quarantine the message	0x400000	Wrap the original message
0x40	Insert disclaimer content	0x800000	Notification
0x80	Block the message	0x1000000	Sign the message using SMIME/CMS
0x100	Replace banned attachments	0x2000000	Defer the message disposition
0x200	Delay and greylist the message	0x4000000	Convert HTML attachment to text
0x400	Forward the message to a review account	0x8000000	Remove active HTML content
0x800	Added a disclaimer to the body	0x10000000	Remove URLs from processed HTML attachments

Hex number	Disposition	Hex Number	Disposition
0x1000	Added a disclaimer to the headers	0x20000000	Deliver to original host
0x2000	Defer message delivery	0x40000000	Content Disarm and Reconstruction
0x4000	Quarantine for review	0x80000000	URL Click Protection
0x8000	Treat as spam	0x100000000	Domain quarantine

The disposition field in a log message may contain one or more dispositions or actions. For example, “Accept” and “Defer” dispositions may appear in the same message. Defer disposition is added when an email message is deferred for either of the following two reasons: FortiGuard antispam outbreak and FortiSandbox scan.

The "Accept" disposition is logged when any other actions are not taken.

See also

FortiMail log types

Viewing log messages

Configuring logging

About FortiMail Cloud logging

Configuring logging

The Log Setting submenu allows you to:

- set the severity level
- configure which types of log messages to record
- specify where to store the logs

You can configure the FortiMail Cloud unit to store log messages to the FortiAnalyzer Cloud (license required).

If you need remote logging, please contact Fortinet Support.

Logging to FortiAnalyzer Cloud

If you have the FortiAnalyzer Cloud Storage Subscription license, you can log to the Cloud service. In addition to the following procedures, you must configure FortiAnalyzer Cloud to accept FortiMail logs. For information about how to

configure FortiAnalyzer Cloud, see the FortiAnalyzer Cloud Deployment Guide.

Logs stored remotely cannot be viewed from the GUI of the FortiMail Cloud unit. If you require the ability to view logs from the GUI, also enable local storage. For details, see Configuring logging on page 306.

Before you can log to a remote location, you must first enable logging. For logging accuracy, you should also verify that the FortiMail Cloud unit's system time is accurate. For details, see Configuring system time on page 49.

To configure logging to FortiAnalyzer Cloud

1. Go to to *Dashboard* > *Status*.
2. Under *License Information*, for FortiCloud, click *Activate*.
3. Enter your FortiCare license information.
4. Go to *Log & Report* > *Log Setting* > *FortiAnalyzer Cloud*.
5. Enable the status and click *Apply*. If FortiMail has the correct license registered with FortiCare, then a connection is established with FortiAnalyzer Cloud. You can also use the *Test connection* button to test and troubleshoot network connections.
6. From Log level, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.
   For information about severity levels, see Log message severity levels on page 302.
7. In Logging Policy Configuration, enable the types of logs you want to record to this storage location.
8. Click Apply.

See also

Log message severity levels

Downloading log files

You can download log files to your management computer. Downloading log files can be useful if you want to view log messages on your management computer, or if you want to download a backup copy of log files to another location before deleting them from the FortiMail Cloud unit's hard disk.

To download a log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as History.
3. Select the row(s) corresponding to the log file(s) that you want to download and click Export > Export Selected. You can select multiple non-contiguous rows by holding Ctrl while selecting the log files.
   The log file downloads in comma-separated value (CSV) format with a file extension of `.csv`. You can view this format in a spreadsheet application such as Microsoft Excel.
4. If your web browser prompts you for the location to save the file, browse to select or enter the name of the folder.

To download all log files

1. Go to *Monitor* > *Log*.
2. Click a log type tab.
3. Click Export > Export All.

The log file downloads in comma-separated value (CSV) format with a file extension of `.csv`.

4. If your web browser prompts you for the location to save the file, browse to select or enter the name of the folder.

See also

Configuring logging

Viewing log messages

Emptying the current log file

You can empty the current log file to remove all of the log messages contained in that file, without deleting the log file itself.

This can be useful in cases such as when you want to delete all old log messages from the FortiMail Cloud unit's hard disk, because rolled log files can be deleted but the current log file cannot.

Only the current log file can be emptied. Rolled log files cannot be emptied, but may be deleted instead. For more information, see Deleting rotated log files on page 308.

Back up the current log file before emptying the current log file. When emptying the log file, log messages are permanently removed, and cannot be recovered. For instructions on how to download a backup copy of the current log file, see Downloading log files on page 307.

To empty the current log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as History.
3. In the row corresponding to the current log file, click Empty Log.
   A confirmation dialog appears, such as:
   ```
   Are you sure you want to delete: alog?
   ```
4. Click OK.

See also

Configuring logging

Viewing log messages

Deleting rotated log files

You can delete rotated (also called "rolled") log files. This can be useful if you want to free disk space used by old log files to make disk space available for newer log files.

Only rolled log files can be deleted. Current log files cannot be deleted, but may be emptied instead. For more information, see Emptying the current log file on page 308.

Back up the current log file before deleting a log file. When deleting a log file, log messages are permanently removed, and cannot be recovered. For instructions on how to download a backup copy of a log file, see Downloading log files on page 307.

To delete a rolled log file

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as History.
3. In the Action column, in the row corresponding to the log file that you want to delete, click Delete.
   A confirmation dialog appears, such as:
   ```
   Are you sure you want to delete: 2008-06-16-14:45:15_2007-10-16-22:52:20.alog?
   ```
4. Click OK.

To delete multiple rolled log files

1. Go to *Monitor* > *Log*.
2. Click a log type tab, such as History.
3. If you want to delete selected log files, mark the checkbox in each row corresponding to a log file that you want to delete.
4. If you want to delete all rolled log files, mark the checkbox in the column heading for the column that contains checkboxes. This automatically marks all other checkboxes.
5. Click Delete Selected Items.
   A dialog appears:
   ```
   Are you sure you want to delete: selected log files?
   ```
6. Click OK.

See also

Viewing log messages

Configuring logging

Configuring report profiles and generating mail statistic reports

The *Log & Report* > *Report Setting* > *Mail Statistics* 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 311.

To view and configure report profiles

1. Go to *Log & Report* > *Report Setting* > *Mail Statistics*.

GUI item	Description
Generate (button)	Select a report and click this button to generate a report immediately. See Generating a report manually on page 312.
Report Name	Displays the name of the report profiles.
Recipient Domain	Displays the name of the recipient domain.
Sender Domain	Displays the name of the sender domain.
Schedule	Displays the frequency with which the FortiMail unit generates a scheduled report. If the report is 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 310.
   - Configuring the report query selection on page 310.
   - Configuring the report schedule on page 311.
   - Selecting the protected domains to report on page 312.
   - Configuring report conditions on page 312.
   - Configuring report email notification on page 312.
5. Click Create or OK.

Configuring the report time period

When configuring a report profile, you can select the time span of log messages from which to generate the report.

- 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 “Last N hours”, another field appears that requires more information.

Configuring the report query selection

When configuring a report profile, you can select one or more queries or query groups that define the subject matter of the report.

Each query group contains multiple individual queries, each of which correspond to a chart that will appear in the generated report. You can select all queries within the group by marking the check box of the query group, or you can expand the query group and individually select each query to include.

For example:

- If you want the report to include charts about spam, select both the Spam by Sender and Spam by Recipient query groups.

- If you want the report to specifically include only a chart about top virus senders by date, expand the query group Virus by Sender and select only the individual query Top Virus Sender By Date.

GUI item	Description
Mail Filtering Statistics	Select to include high-level categories, such as mail, spam, non-spam, and virus.
Mail High Level	Select to include all top level and summary information for all queries, such as Top Client IP By Date.
Mail Statistics	Select to include information on daily, hourly or weekly email message statistics, such as Mail Stat Messages By Day.
Mail by Recipient	Select to include information on email messages by each recipient, such as Top Recipient By Date.
Mail by Sender	Select to include information on email messages by each sender, such as Top Sender By Date.
Spam by Recipient	Select to include information on spam by each recipient, such as Top Spam Recipient By Date.
Spam by Sender	Select to include information on spam by each sender, such as Top Spam Sender By Date.
Statistics	Select to include information on generalized email message statistics (less granular than Mail Statistics).
Total Summary	Select to include summary information, such as Total Sent And Received.
Virus by Sender	Select to include information on infected email messages by each sender, such as Top Virus Sender By Date.
Virus by Recipient	Select to include information on infected email messages by each recipient, such as Top Virus Recipient By Date.

Configuring the report schedule

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 312.

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 312.
Daily	Select to generate the report each day. Also configure At hour.

GUI item	Description
These days	Select to generate the report on specific days of each week, then select those days. Also configure At hour.
These dates	Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. For example, to generate a report on the first and 30th day of every month, enter `1,30`. Also configure At hour.

Selecting the protected domains to report

When configuring a report profile, you must specify at least one protected domain as the recipient domain or sender domain whose log messages are used when generating the report. You can select more than one domain.

1. Disable *All domains* to 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

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

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 & Report* > *Report Setting* > *Mail Statistics*.
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 42.

Configuring mailbox statistics

The FortiMail unit can generate reports on the total number of active mailboxes during a particular time period, as specified in the report profile creation. Mailbox statistic reports can be configured based on schedule, domain, and email address notification. After configuration, historical active mailbox counts over the last 30 days and 12 months can be viewed under *FortiView* > *Mail Statistics* > *Active Mailbox*.

The configuration of mailbox statistic reports is license based. If you do not purchase the advanced management license, this feature is not available.

To view and configure report profiles

1. Go to *Log & Report* > *Report Setting* > *Mailbox Statistics*.

GUI item	Description
Generate (button)	Select a report and click this button to generate a report immediately. See Generating a report manually on page 312.
Report Name	Displays the name of the report profiles.
Domain	Displays the domain name(s).
Schedule	Displays the frequency with which the FortiMail unit generates a scheduled report. If the report is designed for manual generation, Not Scheduled appears in this column.

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. Enable *Include mailbox list* to include information about the active mailboxes per domain and their last delivery time.
5. Expand your desired option and configure the following as needed:
   - Configuring the report time period on page 313
   - Configuring the report schedule on page 314
   - Selecting the protected domains to report on page 314
   - Configuring report email notification on page 314
6. Click Create or OK.

Configuring the report time period

When configuring a report profile, you can select the time span of log messages from which to generate the report.

Select from either Today, Yesterday, This month, or Last month. This sets the range of log data to include in the report.

Configuring the report schedule

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 312.

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 315.
Daily	Select to generate the report each day. Also configure At hour.
Weekly	Select to generate the report on specific days of each week, then select those days. Also configure At hour.
Monthly	Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. For example, to generate a report on the first and 30th day of every month, enter `1,30`. Also configure At hour.

Selecting the protected domains to report

When configuring a report profile, you must specify at least one protected domain whose log messages are used when generating the report. You can select more than one domain.

1. Disable *All domains* to 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 email notification

When configuring a report profile, you can have the FortiMail unit email an attached copy of the generated report to designated recipients.

1. In the Email address field, enter the email address of a recipient. Click >> to add the email address to the list of recipients.
2. 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 & Report* > *Report Setting* > *Mailbox Statistics*.
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 42.

Microsoft 365 and Google Workspace threat remediation

Microsoft 365 and Google Workspace email messages can now be scanned in real-time, whereby email is scanned immediately after the email arrives in the user's mailbox.

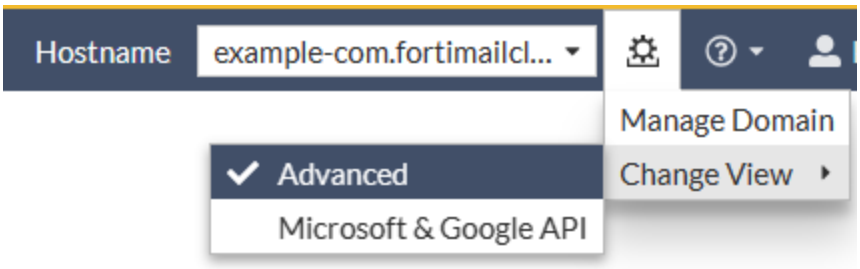
You can also conduct on-demand search and scan of email messages already delivered to the user's inbox. Once scanned, you can decide what to do with the infected or spam email. You can also manually apply actions directly to the email messages you specify.

Both Microsoft 365 and Google Workspace protection features are license based. If you have not purchased the required licenses, then this feature does not display on the GUI.

The real-time scan feature requires the following:

- A valid CA-signed certificate
- The FortiMail Cloud unit must be reachable by hostname (not IP address)

Note that Microsoft 365 and Google API management settings are available from the *Settings*dropdown menu in the top right corner of the GUI.



Microsoft 365 and Google Workspace protection workflow

To use this feature, do the following:

1. Connect to Microsoft 365 or Google Workspace by creating an account on FortiMail Cloud with the Microsoft 365 or Google Workspace domain administrator's credentials. See Configuring accounts on page 317.
2. Create antivirus, antispam, content, DLP, and action profiles to be used to scan the email. See Configuring profiles on page 321.
3. Conduct real-time scans or scheduled scans and searches for email according to your criteria. See Microsoft 365 and Google Workspace protection workflow on page 316.
4. View the history, antivirus, and antispam logs. See Monitoring log messages on page 322.
5. View and generate mail statistic reports in FortiView, based on mail count, size, scan and transfer speed, and notification delay and by received notifications. See Microsoft 365 and Google Workspace notification statistics.

See also

Configuring accounts

Configuring email archiving policies

Configuring email archiving exemptions

Managing archived email

Configuring accounts

Before you can scan email in Microsoft 365 or Google Workspace mailboxes, you must connect to a respective server.

Adding a Microsoft 365 account in FortiMail requires your Tenant ID, Application ID, and Application Secret. Adding a Google Workspace account in FortiMail requires an email address designated for the administrator, and the account's JSON content.

When acquiring the Tenant ID and Application ID from Microsoft 365, you must also grant consent permissions for the admin.

Add the following permissions for the administrator in Microsoft 365:

- User.Read.All
- Mail.ReadWrite
- Mail.Send
- GroupMember.Read.All

By default, *User.Read* is added.

To create a Microsoft 365 account

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *System* > *Account* > *Account*.
3. Click *New*.
4. Leave *Status* enabled.
5. Set *Type* to *Microsoft 365*.
6. Enter the *Tenant ID*, *Application ID*, and the *Application Secret*.
   You receive log on credentials when you create the custom application on Microsoft Azure. For details, see the Azure documentation.
7. Select a regional *Service Endpoint* appropriate to your geographical location.
8. Enable *Real-time Scan* if you wish to conduct real-time scanning of emails that match certain criteria specified in a real-time scan policy. For more information, see Enabling and configuring real-time scanning on page 318.
9. Optionally, click *New* under *User Filter Setting* to configure user filter settings.
   Enable *Status*, select the appropriate user *Type*, and specify additional options depending upon the filter type

selected, then click *Create*.

FortiMail supports the importation of Azure AD user group memberships, which can subsequently be applied to domain level recipient policies.

To use this feature, select *Azure AD Group* from the *Type* dropdown when configuring *User Filter Settings*.

This feature is currently only available when configuring Microsoft 365 accounts.

10. When finished configuring the account, click *Create*.

To create a Google Workspace account

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *System* > *Account* > *Account*.
3. Click *New*.
4. Leave *Status* enabled.
5. Set *Type* to *Google Workspace*.
6. Enter the *Admin email* and the *JSON content*.

   You receive JSON credentials when you create the custom application on Google Workspace. For details, see the Google documentation.
7. Enable *Real-time Scan* if you wish to conduct real-time scanning of emails that match certain criteria specified in a real-time scan policy. For more information, see Enabling and configuring real-time scanning on page 318.
8. Optionally, click *New* under *User Filter Setting* to configure user filter settings.

   Enable *Status*, select the appropriate user *Type*, and specify additional options depending upon the filter type selected, then click *Create*.
9. When finished configuring the account, click *Create*.

   If successful, your account will appear in the account list, showing FortiMail connected to Microsoft 365 or Google Workspace.
10. Click *View User List* to view the following email user information under the selected account:
    - *Status*: Displays whether the user is subscribed or not.
    - *Email*: User names of the email users on the Microsoft 365 or Google Workspace account.
    - *Expiry Date*: Subscription expiry date and time to notifications of the user's real-time email.

Configuring scanning policies

After you connect to Microsoft 365 or Google Workspace and create profiles, you can scan certain email according to the criteria you specify. These can be real-time scans, or on-demand scheduled scans and searches.

Enabling and configuring real-time scanning

Real-time scanning allows you to apply security profiles and their actions to only those emails that match certain criteria specified in a real-time scan policy. These criteria are based on source, sender, and recipient information.

Before you can configure real-time scan policies, you must first enable the feature, and define the base URL for the FortiMail unit to receive notifications from Microsoft 365 or Google Workspace.

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *Policy* > *Real-time Scan* > *Setting*.
3. Select *Enable*.
4. Verify the *Base URL to receive notification* field, which is based on the local host and domain name of the FortiMail unit. To define this URL:
   a. Go to *View* > *Advanced View*.
   b. Go to *System* > *Mail Setting* > *Mail Server Settings*.
   c. Under *Local Host*, enter the *Host name* and *Local domain name* of the FortiMail unit, and click *Apply*. This displays the FortiMail unit's fully qualified domain name (FQDN) in the format:
5. Select an appropriate Service endpoint from the dropdown menu, depending on your geographic location.
6. Determine whether you want to *Log* all email, or only those emails that match a policy.

To configure real-time scan policy:

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *Policy* > *Real-time Scan* > *Policy*.
3. Click *New* and configure the following:

GUI item	Description
Enable	Enter a descriptive name.
Account	Select a Microsoft 365 or Google Workspace account.
Source	Select either **IP/Netmask**, **IP Group**, or **GeoIP Group**, and enter the appropriate source information.
Sender	Define the sender type, entering the type's settings as required.
Recipient	Define the recipient type, entering the type's settings as required.
Profiles	Select profile(s) to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profiles.

4. Click *Create*.

For full configuration and procedural details, see the Cookbook recipe Real-time scanning of Microsoft 365 email in FortiMail.

Hide email on arrival (Microsoft 365 only)

With real-time scanning, there is still a small risk that users may open dangerous emails in Microsoft 365 before the FortiMail unit can finish scanning the email, especially if the email contains large attachments. To mitigate this risk, you can enable a feature that automatically moves email to a hidden folder on arrival for it to be subjected to real-time scanning. After the email is scanned and deemed safe, it is then removed from the hidden folder and put into the user's mailbox.

This feature (disabled by default) can only be enabled using the *CLI Console*.

To enable this feature, open the *CLI Console* and enter the following:

```
config cloud-api setting
   set hide-email-on-arrival enable
end
```

Release system quarantine email (Microsoft 365 only)

You can enable a feature that automatically stores FortiMail system quarantined email, both original and modified copies, in Microsoft 365. All the tenant, user, and message GUIDs are stored in the FortiMail system quarantine. After the email is scanned and deemed safe, it is then released and redelivered to the user.

This feature (enabled by default) can only be enabled using the *CLI Console*.

To enable this feature, open the *CLI Console* and enter the following:

```
config cloud-api setting
   set system-quarantine-release-original enable
end
```

Configuring scheduled scan

To scan email on demand for Microsoft 365 or Google Workspace:

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *Policy* > *Scheduled Scan & Search* > *Scan*.
3. Click *New* and configure the following:

GUI item	Description
Description	Enter a descriptive name.
Account	Select to scan **All** accounts, or specify specific accounts to scan.
Mailbox	Select to scan **All** mailboxes, or specify specific mailboxes to scan.
Schedule	Specify a scheduled time and email start and end time range.
Profiles	Select profile(s) to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profiles.
Condition	Specify the search criteria.

4. If *Schedule* is set to *Now*, click *Scan*. If *Schedule* is set to *Later*, *Daily*, or *Weekly*, click *OK*.
5. The scanning status of all the scan tasks will be displayed: either Running, Done, Scheduled, or Stopped.
6. After the scan process is done, you can double click on the scan task to view the details.

In addition to automatic scanning, you can also search for specific email on Microsoft 365 or Google Workspace and manual apply actions.

Configuring scheduled search

To search for email and take manual actions:

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *Policy* > *Scheduled Scan & Search* > *Search*.
3. Click *New* and configure the following:

GUI item	Description
Description	Enter a descriptive name.
Account	Select to search **All** accounts, or specify specific accounts to search.
Mailbox	Select to search **All** mailboxes, or specify specific mailboxes to search.
Schedule	Specify a scheduled time and email start and end time range.
Search Action	Select an action profile to be applied for emails meeting the search criteria. Actions will be taken against the infected email with the actions you specified in the profile.
Condition	Specify the search criteria.

4. If *Schedule* is set to *Now*, click *Scan*. If *Schedule* is set to *Later*, *Daily*, or *Weekly*, click *OK*.
5. The search status of all the search tasks will be displayed: either Running, Done, Scheduled, or Stopped.
6. After the search process is done, you can double click on the search task to view the details.
7. To take any action towards a specific email (if the search task has not already applied an action), from the search result list, select the email and select the action from the *Apply Action* dropdown list. For action definitions, see Configuring action profiles on page 321.

Configuring profiles

Before you can scan the email on Microsoft 365 or Google Workspace, you must configure the antivirus, antispam, content, DLP, and action profiles to use.

The antivirus, antispam, content, and DLP profile configurations are almost identical to the regular profile configurations, except for some settings that do not apply to this situation. For details about these profiles, see the following sections:

- Managing antivirus profiles
- Managing antispam profiles
- Configuring content profiles
- Configuring DLP profiles

Configuring action profiles

When you scan email on Microsoft 365 or Google Workspace, you can apply action profiles towards the infected email. Note that since you are applying actions on Microsoft 365 or Google Workspace, the action definitions are different from the actions performed on FortiMail itself.

To configure an action profile

1. Go to *View* > *Microsoft 365 & Google Workspace*.
2. Go to *Profile* > *Action* > *Action*.
3. Click *New* and configure the following:

GUI item	Description
Profile name	Enter a name for the action profile.
Replace attachment with message	Select to replace the email attachment that triggers a scanner (such as the content and antivirus attachment filters) with a custom message. For more information about custom replacement message, see Configuring custom messages on page 51.
Notify with profile	Select to send out notifications to the recipients specified in the notification profile. For more information about notification profiles, see Configuring notification profiles on page 242.
Action	Specify one of the following final actions: • ***None***: No action will be taken. • ***Discard***: Delete the email message from the user's inbox on Microsoft 365 or Google Workspace. • ***Personal quarantine***: Move the email message from the user's inbox to the junk folder on Microsoft 365, or to the spam folder on Google Workspace. • ***System quarantine***: Send a copy to FortiMail system quarantine folder, and move the email message from the user's inbox to the Deleted Items folder on Microsoft 365 or Google Workspace. If desired, the user can view the deleted email by clicking Recover Deleted Items. • ***Move to folder***: Move the email message from the user's inbox to a specified folder on Microsoft 365 or Google Workspace.

Monitoring log messages

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

- *History*: Where you can view the log of scanned and searched email messages.
- *Mail Event*: Where you can view the log of all and/or SMTP mail events.
- *AntiVirus*: Where you can view the log of email messages detected as infected by a virus.
- *AntiSpam*: Where you can view the log of email messages detected as spam.
- Log Search Task: Where you can create and view a log of search tasks.

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

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

For more information about how to use FortiMail logs, see Viewing log messages on page 14.

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

Bayesian scanning can be used by antispam profiles to filter email for spam. In order to be accurate, the Bayesian databases that are at the core of this scan must be trained. This is especially important when the databases are empty.

Be aware that, without ongoing training, Bayesian scanning will become significantly less effective over time and thus Fortinet does not recommend enabling the Bayesian scanning feature.

Administrators can provide initial training. For details, see Training the Bayesian databases on page 279. If you have enabled it (see Configuring the Bayesian training control accounts on page 285 and Accept training messages from users on page 172),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 Cloud 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 178.

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 248, Configuring protected domains on page 71, and Using quarantine reports on page 325). 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 the personal quarantine and webmail
- 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 FortiMail webmail (server mode)

Unlike gateway mode and transparent mode, server mode does not require that the administrator create an authentication profile. However, he or she must still configure an incoming recipient-based policy that matches the email user's address, where webmail access to the quarantine is enabled through a resource profile.

Once this is configured, the administrator informs email users of the FortiMail webmail URL. When they log in, email users will immediately see their mailbox folders, including their *Inbox*, in addition to their *Bulk* folder.

For additional instructions related to their personal quarantine, email users can click the *Help* button in FortiMail webmail.

Accessing mailboxes through POP3 or IMAPv4 (server mode)

To allow email users to access their *Inbox*, *Bulk*, and other folders through an email client, the administrator must configure an incoming recipient-based policy that matches the email user's address, where POP3/IMAPv4 access to the quarantine is enabled.

Once this is configured, the administrator tells email users about the IP address and POP3/IMAPv4 port number of the FortiMail unit (see also Appendix C: Port Numbers on page 1), 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 178) 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 248)
- the quarantine control email addresses (see Configuring the quarantine control options on page 255)

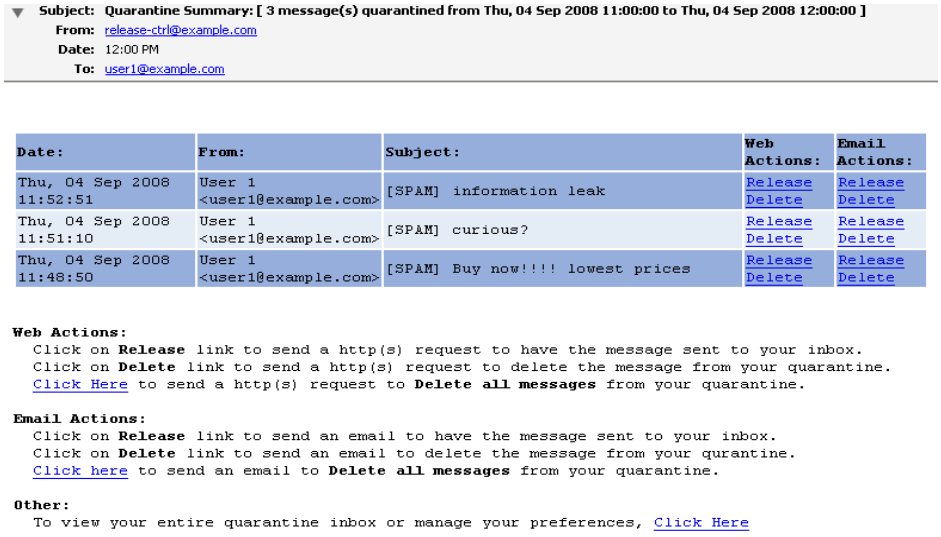
When email is added to their personal quarantine, email users will periodically receive an email similar to one of the samples below.

Email users can follow the instructions in the quarantine report to release or delete email from their personal quarantine. Quarantine reports can be used from with FortiMail webmail, or from an email client with POP3 access.

Example: Quarantine report (HTML)

The following sample report in HTML format informs the email user about how many messages are in quarantine, and explains how to delete one or all quarantined messages, and how to release an individual email. Email users can make decisions to release or delete an email based on a message's subject and sender information contained in the body of the report.

Sample quarantine report in HTML format



Subject: Quarantine Summary: [3 message(s) quarantined from Thu, 04 Sep 2008 11:00:00 to Thu, 04 Sep 2008 12:00:00]
From: release-ctrl@example.com
Date: 12:00 PM
To: user1@example.com

Date:	From:	Subject:	Web Actions:	Email Actions:
Thu, 04 Sep 2008 11:52:51	User 1 <user1@example.com>	[SPAM] information leak	Release Delete	Release Delete
Thu, 04 Sep 2008 11:51:10	User 1 <user1@example.com>	[SPAM] curious?	Release Delete	Release Delete
Thu, 04 Sep 2008 11:48:50	User 1 <user1@example.com>	[SPAM] Buy now!!!! lowest prices	Release Delete	Release Delete

Web Actions:
Click on **Release** link to send a http(s) request to have the message sent to your inbox.
Click on **Delete** link to send a http(s) request to delete the message from your quarantine.
Click Here to send a http(s) request to **Delete all messages** from your quarantine.

Email Actions:
Click on **Release** link to send an email to have the message sent to your inbox.
Click on **Delete** link to send an email to delete the message from your qurantine.
Click here to send an email to **Delete all messages** from your quarantine.

Other:
To view your entire quarantine inbox or manage your preferences, Click Here

Example: Quarantine report (plain text)

The following sample report in plain text format informs email users about how many messages are in quarantine, and explains how to delete one or all quarantined messages, and how to release an individual email. Email users can make decisions to release or delete an email based on a message's subject and sender information contained in the body of the report.

Note that email users cannot access their personal quarantines through POP3 or IMAP.

Sample quarantine report in plain text format

```
To: user1@example.com
      From: release-ctrl@fm3.example.com
      Subject: Quarantine Summary: [3 message(s) quarantined from Wed, 11 Jul 2007 11:00:01 to
      Wed, 11 Jul 2007 12:00:01]
      Date: Wed, 11 Jul 2007 12:00:01 -0400
Date: Wed, 11 Jul 2007 11:11:25
      Subject: Sign up for FREE offers!!!
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166681.16BFAj5100093800000@fm3.example.com
Date: Wed, 11 Jul 2007 11:14:16
      Subject: Buy cheap stuff!
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166854.16BFDchG0009440000@fm3.example.com
Date: Wed, 11 Jul 2007 11:15:46
      Subject: Why pay more?
```

```
      From: "Spam Sender" <spamsender@example.org>
      Message-Id: 1184166944.l6BFF7HI0009460000@fm3.example.com
Actions:
o) Release a message:
      Send an email to <release-ctrl@fm3.example.com> with subject line set to
      "user1@example.com:Message-Id".
o) Delete a message:
      Send an email to <delete-ctrl@fm3.example.com> with subject line set to
      "user1@example.com:Message-Id".
o) Delete all messages:
      Send an email to <delete-ctrl@fm3.example.com> with subject line set to "delete_
      all:user1@example.com:ea809095:ac146004:05737c7c111d68d0111d68d0111d68d0".
```

Sending email from an email client (gateway 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 121.
- Create an authentication profile to authenticate the users. For details, see Configuring authentication profiles on page 202.
- Enable SMTP authentication in the incoming recipient-based policy. For details, see Controlling email based on sender and recipient addresses on page 138.

The email user must configure their email client with:

- outgoing SMTP email server that is either the FortiMail unit (gateway 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`

www.fortinet.com

Copyright© 2024 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.