FortiMail™ Secure Messaging Platform

Version 4.0 MR1 Patch 2

CLI Reference

FORTINET

FortiMail™ Secure Messaging Platform CLI Reference

Version 4.0 MR1 Patch 2

Revision 1

10 December 2010

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

FortiMail™ Secure Messaging Platforms (FortiMail units) are an integrated hardware and software solution that provides powerful and flexible logging and reporting, antispam, antivirus, and email archiving capabilities to incoming and outgoing email traffic. FortiMail units have reliable and high performance features for detecting and blocking spam messages and malicious attachments. Built on Fortinet's FortiOS™, FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.

This chapter contains the following topics:

Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article Technical Support Requirements.

Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email them at training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document to techdoc@fortinet.com.

Scope

This document describes how to use the command line interface (CLI) of the FortiMail unit. It assumes that you have already successfully installed the FortiMail unit by following the instructions in the *FortiMail Installation Guide*.

At this stage:

- You have administrative access to the web-based manager and/or CLI.
- The FortiMail unit is integrated into your network.
- The operation mode has been configured.
- The Quick Start Wizard has been completed. The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- DNS records for your mail domains have been updated.
- For transparent mode or gateway mode, you have verified that the network routes all email through the FortiMail unit.
- For server mode, you have verified that the network allows the FortiMail unit access to and from other email servers and MTAs, typically including those on the Internet, and from email users with IMAP, POP3 or webmail access.

Once that basic installation is complete, you can use this document. This document explains how to use the CLI to:

- maintain the FortiMail unit, including backups
- reconfigure basic items that were configured during installation
- configure advanced features, such as customized antispam scans, email archiving, logging, and reporting

This document does ***not*** cover the web-based manager. For information on the web-based manager, see the *FortiMail Administration Guide*.

This document is intended for administrators, not end users. If you are an email user, please click the *Help* link in FortiMail webmail to see the webmail online help instead, or contact your administrator.

Conventions

Fortinet technical documentation uses the following conventions:

- IP addresses
- Notes, Tips and Cautions
- Typographical conventions
- Command syntax conventions

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.

Tip: Highlights useful additional information, often tailored to your workplace activity.

Note: Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographical conventions

Fortinet documentation uses the following typographical conventions.

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.

CLI input*	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system settings`
	`comments  : (null)`
	`opmode  : nat`

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>` `<BODY><H4>You must authenticate to use this service.</H4>`
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN* > *IPSEC* > *Auto Key (IKE)*.
Publication	*FortiMail Administration Guide*.

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

For command syntax conventions such as braces, brackets, and command constraints such as `<address_ipv4>`, see “Notation” on page 21.

What's new

The table below lists the CLI commands that are changed in v4.0 MR1 Patch 2 release.

Command	Change
config domain edit <protected-domain_name> config domain-setting set smtp-recipient-verification-accept-reply-string <accept_string>	New field. Configure the string to match the reply string from recipient verification.

Using the CLI

The command line interface (CLI) is an alternative to the web-based manager.

Both can be used to configure the FortiMail unit. However, to perform the configuration, in the web-based manager, you would use buttons, icons, and forms, while, in the CLI, you would either type lines of text that are commands, or upload batches of commands from a text file, like a configuration script.

If you are new to Fortinet products, or if you are new to the CLI, this section can help you to become familiar.

This section contains the following topics:

Connecting to the CLI

You can access the CLI in two ways:

- **Locally** — Connect your computer directly to the FortiMail unit's console port.
- **Through the network** — Connect your computer through any network attached to one of the FortiMail unit's network ports. The network interface must have enabled Telnet or SSH administrative access.

Local access is required in some cases.

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

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

This section includes the following:

Connecting to the CLI using a local console

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

Requirements

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiMail package
- terminal emulation software such as HyperTerminal for Microsoft Windows

Note: The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1 Using the null modem or RJ-45-to-DB-9 cable, connect the FortiMail unit's console port to the serial communications (COM) port on your management computer.

2 On your management computer, start HyperTerminal.

3 On *Connection Description*, enter a *Name* for the connection, and select *OK*.

4 On *Connect To*, from *Connect using*, select the communications (COM) port where you connected the FortiMail unit.

5 Select *OK*.

6 Select the following *Port* settings and select *OK*.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7 Press Enter to connect to the CLI.

The login prompt appears.

8 Type a valid administrator account name (such as `admin`) and press Enter.

9 Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

The CLI displays the following text:

```
Welcome!
Type ? to list available commands.
```

You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 16.

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

SSH or Telnet access to the CLI is formed by connecting your computer to the FortiMail unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

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

You can do this using either:

- a local console connection (see the following procedure)
- the web-based manager (see the *FortiMail Install Guide*)

Requirements

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

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

1 Using the network cable, connect the FortiMail unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiMail unit.

2 Note the number of the physical network port.

3 Using a local console connection, connect and log into the CLI. For details, see "Connecting to the CLI using a local console" on page 15.

4 Enter the following command:

```
set system interface <interface_str> config allowaccess
<protocols_list>
```

where:

- `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
- `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
set system interface port1 config allowaccess ssh telnet
```

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

5 To confirm the configuration, enter the command to display the network interface settings.

```
get system interface
```

The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

To connect to the CLI through the network interface, see "Connecting to the CLI using SSH" on page 17 or "Connecting to the CLI using Telnet" on page 18.

Connecting to the CLI using SSH

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

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI.

Note: FortiMail units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 16.

Note: The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1 On your management computer, start an SSH client.

2 In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.

3 In *Port*, type `22`.

4 From *Connection type*, select *SSH*.

5 Select *Open*.

The SSH client connects to the FortiMail unit.

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

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

The CLI displays a login prompt.

7 Type a valid administrator account name (such as `admin`) and press Enter.

Note: You can alternatively log in using an SSH key. For details, see "system admin" on page 159.

8 Type the password for this administrator account and press Enter.

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

The FortiMail unit displays a command prompt (its host name followed by a `#`).

You can now enter CLI commands.

Connecting to the CLI using Telnet

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

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

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 16.

To connect to the CLI using Telnet

1 On your management computer, start a Telnet client.
2 Connect to a FortiMail network interface on which you have enabled Telnet.
3 Type a valid administrator account name (such as `admin`) and press Enter.
4 Type the password for this administrator account and press Enter.

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

The FortiMail unit displays a command prompt (its host name followed by a `#`).

You can now enter CLI commands.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the following conventions to describe valid command syntax.

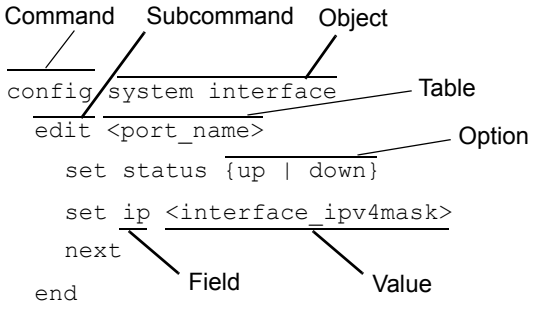
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Figure 1: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiMail unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line.

  Valid command lines must be unambiguous if abbreviated. (See "Command abbreviation" on page 29.) Optional words or other command line permutations are indicated by syntax notation. (See "Notation" on page 21.)

  Note: This CLI Reference is organized alphabetically by object for the `config` command, and by the name of the command for remaining top-level commands.

- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands. (See "Indentation" on page 21.)

  Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope. (See "Sub-commands" on page 23.)
- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See "Notation" on page 21.)
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiMail unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See "Notation" on page 21.)
- **option** — A kind of value that must be one or more words from of a fixed set of options. (See "Notation" on page 21.)

Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope.

For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
    next
  end
```

For information about available sub-commands, see "Sub-commands" on page 23.

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 2: Command syntax notation

Convention	Description

Square brackets `[ ]`	A non-required word or series of words. For example:
	`[verbose {1 | 2 | 3}]`
	indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:
	`verbose 3`

Table 2: Command syntax notation

Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: <retries_int> indicates that you should enter a number of retries, such as 5. Data types include: • <xxx_name>: A name referring to another part of the configuration, such as policy_A. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as mail.example.com. • <xxx_email>: An email address, such as admin@mail.example.com. • <xxx_url>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as http://www.fortinet./com/. • <xxx_ipv4>: An IPv4 address, such as 192.168.1.99. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as 192.168.1.99/24. • <xxx_ipv4range>: A hyphen (-)-delimited inclusive range of IPv4 addresses, such as 192.168.1.1-192.168.1.255. • <xxx_ipv6>: A colon(:)-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234. • <xxx_v6mask>: An IPv6 netmask, such as /96. • <xxx_ipv6mask>: An IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is ***not*** another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See "Special characters" on page 29. • <xxx_int>: An integer number that is ***not*** another data type, such as 15 for the number of minutes.
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].

Table 2: Command syntax notation

	Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

	Options delimited by spaces	Non-mutually exclusive options. For example:
		`{http https ping snmp ssh telnet}`
		indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
		`ping https ssh`
		Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
		`ping https snmp ssh`
		If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Sub-commands

Once you have connected to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands.When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
    next
  end
```

Note: Sub-command scope is indicated in this CLI Reference by indentation. See "Indentation" on page 21.

Available sub-commands vary by command.From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Note: Syntax examples for each top-level command in this CLI Reference do not show all available sub-commands. However, when nested scope is demonstrated, you should assume that sub-commands applicable for that level of scope are available.

Table 3: Commands for tables

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
purge	Remove all tables in the current object. For example, in `config forensic user`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiMail unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see `execute backup`. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiMail unit to be formatted and restored.
rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Table 4: Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set passwd newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the <`new-value`> rather than appending <`new-value`> to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset passwd` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set passwd my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `passwd` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

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

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

The domain to which an administrator is assigned can be either:

- *System:* Can access areas regardless of whether an item pertains to the FortiMail unit itself or to a protected domain. The administrator's permissions are restricted only by his or her access profile.

- a protected domain: Can ***only*** access areas that are specifically assigned to that protected domain. The administrator ***cannot*** access system-wide settings, files or statistics, nor most settings that can affect other protected domains, regardless of whether access to those items would otherwise be allowed by his or her access profile. The administrator ***cannot*** access the CLI, nor the basic mode of the web-based manager. (For more information on the display modes of the GUI, see the *FortiMail Administration Guide*.)

Note: IP-based policies, the global black list, and the global white list, the blacklist action, and the global Bayesian database are exceptions to this rule. Domain administrators can configure them, regardless of the fact that they could affect other domains. If you do not want to allow this, do ***not*** provide *Read-Write* permission to those categories in domain administrators' access profiles.

Table 5: Areas of the GUI (advanced mode) that cannot be accessed by domain administrators

Maintenance
Monitor ***except*** for the *Personal quarantine* tab
System ***except*** for the *Administrator* tab
Mail Settings ***except*** for the domain, its subdomains, and associated domains
User > User > PKI User
Policy > Access Control > Receive *Policy > Access Control > Delivery*
Profile > Authentication
AntiSpam ***except*** for *AntiSpam > Bayesian > User and AntiSpam > Black/White List*
Email Archiving
Log and Report

Access profiles assign either read, write, or no access to each area of the FortiMail software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an access profile that administrator accounts can use, see `config system accprofile`.

Table 6: Areas of control in access profiles

Access control area name		**Grants access to**
In the web-based manager	**In the CLI**	(For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires read permission.)

Table 6: Areas of control in access profiles

Policy	`policy`	*Monitor > Mail Queue ...* *Monitor > Greylist ...* *Monitor > Sender Reputation > Display* *Mail Settings > Domains > Domains* *Mail Settings > Proxies > Proxies* *User > User ...* *Policy ...* *Profile ...* *AntiSpam > Greylist ...* *AntiSpam > Bounce Verification > Settings* *AntiSpam > Endpoint Reputation ...* *AntiSpam > Bayesian ...*

		`config antispam greylist exempt`
		`config antispam bounce-verification key`
		`config antispam settings`
		`config domain`
		`config mailsetting proxy-smtp`
		`config policy ...`
		`config profile ...`
		`config user ...`

Black/White List	`black-white-list`	*Monitor > Endpoint Reputation > Auto Blacklist* *Maintenance > AntiSpam > Black/White List Maintenance* *AntiSpam > Black/White List ...*
		N/A
Quarantine	`quarantine`	*Monitor > Quarantine ...* *AntiSpam > Quarantine > Quarantine Report* *AntiSpam > Quarantine > System Quarantine Setting* *AntiSpam > Quarantine > Control Account*
		`config antispam quarantine-report` `config mailsetting systemquarantine`
Others	`others`	*Monitor > System Status ...* *Monitor > Archive > Email Archives* *Monitor > Log ...* *Monitor > Report ...* *Maintenance* ... ***except*** the *Black/White List Maintenance* tab *System ...* *Mail Settings > Settings ...* *Mail Settings > Address Book > Address Book* *User > User Alias > User Alias* *User > Address Map > Address Map* *Email Archiving ...* *Log and Report ...*

		`config archive ...`
		`config log ...`
		`config mailsetting relayserver`
		`config mailsetting storage`
		`config report`
		`config system ...`
		`config user alias`
		`config user map`
		`diagnose ...`
		`execute ...`
		`get system status`

Unlike other administrator accounts whose *Access profile* is *super_admin_prof* and *Domain* is *System*, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiMail configuration options, including viewing and changing ***all*** other administrator accounts. It is the only administrator account that can reset another administrator's password without being required to enter the existing password. As such, it is the ***only*** account that can reset another administrator's password if that administrator forgets his or her password. Its name, permissions, and assignment to the *System* domain cannot be changed.

Caution: Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiMail unit.

For complete access to all commands, you must log in with the administrator account named `admin`. For access to the CLI, you must log in with a *System*-level administrator account.

Tips and tricks

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

This section includes:

- Help
- Shortcuts and key commands
- Command abbreviation
- Special characters
- Language support
- Baud rate
- Editing the configuration file on an external host

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Table 7: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines.	Ctrl + C

Command abbreviation

In most cases, you can abbreviate words in the command line to their smallest number of non-ambiguous characters. For example, the command `get system status` could be abbreviated to `g sy st`.

Some commands may not be abbreviated. See the notes in the specific commands.

Special characters

The characters <, >, (,), #, ', and “ are not permitted in most CLI fields. These characters are special characters, sometimes also called reserved characters.

You may be able to enter a special character as part of a string’s value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\ ) character.

Table 8: Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: `"Security Administrator"`. Enclose the string in single quotes: `'Security Administrator'`. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured.

For example, the host name must not contain special characters, and so the web-based manager and CLI will not accept most symbols and non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. But dictionary profiles support terms encoded in UTF-8, and therefore support a number of languages.

It is simplest to use only US-ASCII characters when configuring the FortiMail unit using the web-based manager or CLI. Using only ASCII, you do not need to worry about:

- mail transfer agent (MTA) encoding support
- mail user agent (MUA) language support
- web browser language support
- Telnet and/or SSH client support
- font availability
- compatibility of your input's encoding with the encoding/language setting of the web-based manager
- switching input methods when entering a command word such as `get` in ASCII but a setting that uses a different encoding

Note: If you choose to configure parts of the FortiMail unit using non-ASCII characters, verify that all systems interacting with the FortiMail unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

Baud rate

You can change the default baud rate of the local console connection. For more information, see the *FortiMail Administration Guide*.

Editing the configuration file on an external host

You can edit the FortiMail configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiMail unit.

Editing the configuration on an external host can be time-saving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1 Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.

2 Edit the configuration file using a plain text editor that supports Unix-style line endings.

Caution: Do not edit the first line. The first line(s) of the configuration file (preceded by a `#` character) contains information about the firmware version and FortiMail model. If you change the model number, the FortiMail unit will reject the configuration file when you attempt to restore it.

3 Use `execute restore config` to upload the modified configuration file back to the FortiMail unit.

The FortiMail unit downloads the configuration file and checks that the model information is correct. If it is, the FortiMail unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiMail unit ignores the command. If the configuration file is valid, the FortiMail unit restarts and loads the new configuration.

config

`config` commands configure your FortiMail unit's settings.

This chapter describes the following commands:

antispam bounce-verification key

Use this command to configure bounce address tagging and verification (BATV) keys.

Syntax

```
config antispam bounce-verification key
  edit <key_str>
    set status {active | inactive}
  next
end
```

Variable	Description	Default
<key_str>	Enter a new or existing key.	No default.
status {active | inactive}	Enable or disable usage of the key.	inactive

History

FortiMail v4.0 New.

Related topics

- config antispam deepheader-analysis
- config antispam greylist exempt
- config antispam quarantine-report
- config antispam settings
- config antispam trusted

antispam deepheader-analysis

Use this command to configure global deepheader-analysis scan settings used by antispam profiles.

Deepheader analysis examines the entire message header for spam characteristics.

Not all headers may be checked, depending on your configuration of “config antispam trusted” on page 46.

Syntax

```
config antispam deepheader-analysis
  set confidence <percent_float>
  set greyscale-level <level_int>
end
```

Variable	Description	Default
`confidence <percent_float>`	Type the confidence percentage above which a message will be considered spam. The deep header scan examines each message and calculate a confidence value based on the results of the decision-tree analysis. The higher the calculated confidence value, the more likely the message is really spam. The deep header scan adds an `X-FEAS-DEEPHEADER:` line to the message header that includes the message’s calculated confidence value.	`95.000000`
`greyscale-level <level_int>`	Type the grey scale threshold above which the deepheader scan will be skipped. FortiGuard antispam service uses the grey scale of 1-9 to determine spam. 1-4 means the email is a spam for sure, while 9 is not a spam for sure. Therefore, increasing this grey scale level will increase the probability to scan the email. This may increase spam catch rate but also increase false positives.	`7`

History

FortiMail v4.0 New.

Related topics

- config profile antispam
- config antispam trusted
- config antispam greylist exempt
- config antispam settings

antispam greylist exempt

Use this command to configure the greylist exempt list.

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. Spam senders rarely attempt a retry.

Syntax

```
config antispam greylist exempt
  edit <entry_index>
    set recipient-pattern <recipient_pattern>
    set recipient-pattern-regexp {enable | disable}
    set reverse-dns-pattern <reverse-dns_pattern>
    set reverse-dns-pattern-regexp {enable | disable}
    set sender-ip <client_ipv4/mask>
    set sender-pattern <sender_pattern>
    set sender-pattern-regexp {enable | disable}
  next
end
```

Variable	Description	Default
<entry_index>	Greylist exempt rule ID.	No default.
recipient-pattern <recipient_pattern>	Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as \'*\').	No default.
recipient-pattern-regexp {enable | disable}	• Enter enable if you used regular expression syntax to define the pattern. • Enter disable if you did ***not*** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable
reverse-dns-pattern <reverse-dns_pattern>	Enter a pattern that defines reverse DNS query responses which match this rule, surrounded in slashes and single quotes (such as \'*\').	No default.
reverse-dns-pattern-regexp {enable | disable}	• Enter enable if you used regular expression syntax to define the pattern. • Enter disable if you did ***not*** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable
sender-ip <client_ipv4/mask>	Enter the IP address and netmask of the SMTP client. To match SMTP sessions from any SMTP client, enter 0.0.0.0/0.	No default.
sender-pattern <sender_pattern>	Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as \'*@example.com\').	No default.
sender-pattern-regexp {enable | disable}	• Enter enable if you used regular expression syntax to define the pattern. • Enter disable if you did ***not*** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable

History

FortiMail v4.0 New.

Related topics

- config antispam bounce-verification key
- config antispam deepheader-analysis
- config antispam quarantine-report
- config antispam settings
- config antispam trusted

antispam quarantine-report

Use these commands to configure global settings for quarantine reports.

Quarantine reports notify email users of email added to their per-recipient quarantine, and allow them to release or delete email from the quarantine.

Alternatively, you can configure quarantine report settings specifically for each protected domain. For details, see "config domain-setting" on page 51.

Syntax

```
config antispam quarantine-report
  set schedule-days <days_str>
  set schedule-hours <hour_int>
  set web-release-hostname <FortiMail_fqdn>
  set web-release-https {enable | disable}
  set web-release-https {enable | disable}
  set web-release-unauth-expiry <hour_int>
end
```

Variable	Description	Default
`schedule-days <days_str>`	Enter a comma-delimited list of days off the week on which the FortiMail unit will generate spam reports.	No default.
`schedule-hours <hour_int>`	Enter a comma-delimited list of numbers corresponding to the hours of the day on which the FortiMail unit will generate spam reports. For example, to generate spam reports on 1:00 AM, 2:00 PM, and 11:00 PM, you would enter `1,14,23`. Valid numbers are from 0 to 23, based upon a 24-hour clock.	No default.
`web-release-hostname <FortiMail_fqdn>`	Enter an alternate resolvable fully qualified domain name (FQDN) to use in web release hyperlinks that appear in spam reports.	No default.
`web-release-https {enable | disable}`	Enable to redirect HTTP requests for FortiMail webmail and per-recipient quarantines to secure access using HTTPS. **Note**: For this option to function properly, you must also enable both HTTP and HTTPS access protocols on the network interface to which the email user is connecting.	`enable`
`web-release-unauth-expiry <hour_int>`	Enter the period of time after the spam report is generated during which the email user can access the per-recipient quarantine without authenticating. To require the user enter a user name and password, enter `0`. Valid values are from 0 to 720. **Note:** If you require email users to authenticate, in order to define their user name and password, you must configure either local user accounts, or authentication profiles applied through an incoming recipient-based policy.	`0`

History

FortiMail v4.0 New.

Related topics

- config antispam bounce-verification key
- config antispam deepheader-analysis
- config antispam greylist exempt

- config antispam settings
- config antispam trusted

antispam settings

Use these commands to configure global antispam settings.

Syntax

```
config antispam settings
  set backend_verify <time_str>
  set bayesian-is-not-spam <local-part_str>
  set bayesian-is-spam <local-part_str>
  set bayesian-learn-is-not-spam <local-part_str>
  set bayesian-learn-is-spam <local-part_str>
  set bayesian-training-group <local-part_str>
  set blacklist-action {as-profile | discard | reject}
  set bounce-verification-action {as-profile | discard | reject}
  set bounce-verification-auto-delete-policy {never | one-month | one-year |
     six-months | three-months}
  set bounce-verification-status {enable | disable}
  set bounce-verification-tagexpiry <days_int>
  set carrier-endpoint-acct-response {enable | disable}
  set carrier-endpoint-acct-secret <password_str>
  set carrier-endpoint-acct-validate {enable | disable}
  set carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific)
  set carrier-endpoint-blacklist-window-size {quarter | half-hour | one-hour
     | two-hours | four-hours | six-hours | one-day}
  set carrier-endpoint-framed-ip-attr <attribute_number>
  set carrier-endpoint-framed-ip-order {host-order | network-order}
  set carrier-endpoint-radius-port <port_int>
  set carrier-endpoint-status {enable | disable}
  set delete-ctrl-account <local_part_str>
  set greylist-capacity <maximum_int>
  set greylist-delay <1-120 minutes>
  set greylist-init-expiry-period <window_int>
  set greylist-ttl <ttl_int>
  set release-ctrl-account <local-part_str>
  set session-profile-rate-control-type {connection | message}
end
```

Variable	Description	Default
`backend_verify <time_str>`	Enter the time of day at which the FortiMail unit will automatically remove invalid per-recipient quarantines. Use the format `hh:mm:ss`, where `hh` is the hour according to a 24-hour clock, `mm` is the minute, and `ss` is the second. For example, to begin automatic invalid quarantine removal at 5:30 PM, enter `17:30:00`.	`4:0:0`
`bayesian-is-not-spam <local-part_str>`	Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that correct false positives. For example, if the local domain name of the FortiMail unit is example.com and you want to correct the assessment of a previously scanned spam that was actually legitimate email by sending control messages to is-not-spam@example.com, you would enter `is-not-spam`.	`is-not-spam`

Variable	Description	Default
bayesian-is-spam <local-part_str>	Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that correct false negatives. For example, if the local domain name of the FortiMail unit is example.com and you want to correct the assessment of a previously scanned email that was actually spam by sending control messages to is-spam@example.com, you would enter `is-spam`.	is-spam
bayesian-learn-is-not-spam <local-part_str>	Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that train it to recognize legitimate email. Unlike the `is-not-spam` email address, this email address will receive email that has ***not*** been previously seen by the Bayesian scanner. For example, if the local domain name of the FortiMail unit is example.com and you want to train the Bayesian database to recognize legitimate email by sending control messages to learn-is-not-spam@example.com, you would enter `learn-is-not-spam`.	learn-is-not-spam
bayesian-learn-is-spam <local-part_str>	Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that train it to recognize spam. Unlike the `is-spam` email address, this email address will receive spam that has ***not*** been previously seen by the Bayesian scanner. For example, if the local domain name of the FortiMail unit is example.com and you want to train the Bayesian database to recognize spam by sending control messages to learn-is-spam@example.com, you would enter `learn-is-spam`.	learn-is-spam
bayesian-training-group <local-part_str>	Enter the local-part portion of the email address 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) but will ***not*** train any per-user Bayesian database. In contrast, if a FortiMail administrator were to forward email using their own email address (rather than the training group email address) as the sender email address, and per-user Bayesian databases were enabled in the corresponding incoming antispam profile, the FortiMail unit would also apply the training message to their own per-user Bayesian database.	default-grp
blacklist-action {as-profile | discard | reject}	Use these commands to select the action that the FortiMail unit performs when an email message arrives from or, in the case of per-session profile recipient black lists, is destined for a blacklisted email address, mail domain, or IP address. This setting affects email matching any system-wide, per-domain, per-session profile, or per-user blacklist. For email messages involving a blacklisted email address, domain, or IP address, select one of the following options: • `as-profile`: Apply the action selected in the antispam profile being applied to the email message. For details, see “profile antispam-action” on page 113. • `discard`: Accept the message but delete and do not deliver it, without notifying the SMTP client. • `reject`: Reject the message, returning an SMTP error code to the SMTP client.	reject
bounce-verification-action {as-profile | discard | reject}	Enter the action that the FortiMail unit will perform if it receives a bounce address tag that is invalid. • `as-profile`: Perform the action selected in the antispam profile. • `discard`: Accept the message but then delete it without notifying the SMTP client. • `reject`: Reject the message, replying to the SMTP client with an SMTP rejection code.	as-profile

Variable	Description	Default
bounce-verification-auto-delete-policy {never | one-month | one-year | six-months | three-months}	Inactive keys will be removed after being unused for the selected time period. • never: Never automatically delete an unused key. • one-month: Delete a key when it hasn't been used for 1 month. • three-months: Delete a key when it hasn't been used for 3 months. • six-months: Delete a key when it hasn't been used for 6 months. • one-year: Delete a key when it hasn't been used for 12 months. The active key will not be automatically removed.	never
bounce-verification-status {enable | disable}	Enable to activate bounce address tagging and verification. Tag verification can be bypassed in IP profiles and protected domains.	disable
bounce-verification-tagexpiry <days_int>	Enter the number of days an email tag is valid. When this time elapses, the FortiMail unit will treat the tag as invalid. Valid range is from 3 to 30 days.	7
carrier-endpoint-acct-response {enable | disable}	Enable/disable endpoint account validation on the RADIUS server.	disable
carrier-endpoint-acct-secret <password_str>	Type the shared secret for RADIUS account response/request validation.	
carrier-endpoint-acct-validate {enable | disable}	Enable/disable validating shared secret of account request.	disable
carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific)	Type the RADIUS account attribute associated with the endpoint user. A carrier end point is any device on the periphery of a carrier's or Internet service provider's (ISP) network. It could be a subscriber's GSM cellular phone, wireless PDA, or computer using DSL service. Unlike MTAs, computers in homes and small offices and mobile devices such as laptops and cellular phones that send email may not have a static IP address. Cellular phones' IP addresses especially may change very frequently. After a device leaves the network or changes its IP address, its dynamic IP address may be reused by another device. Because of this, a sender reputation score that is directly associated with an SMTP client's IP address may not function well. A device sending spam could start again with a clean sender reputation score simply by rejoining the network to get another IP address, and an innocent device could be accidentally blacklisted when it receives an IP address that was previously used by a spammer.	Calling-Station-Id (RADIUS attribute 31)
carrier-endpoint-blacklist-window-size {quarter | half-hour | one-hour | two-hours | four-hours | six-hours | one-day}	Enter the amount of previous time, in minutes, whose score-increasing events will be used to calculate the current endpoint reputation score. For example, if the window is a quarter (15 minutes), detections of spam or viruses 0-15 minutes ago would count towards the current score; detections of spam or viruses older than 15 minutes ago would not count towards the current score.	quarter
carrier-endpoint-framed-ip-attr <attribute_number>	Enter the RADIUS attribute number whose attribute value will be used as the endpoint user IP address. By default, the endpoint user IP address uses the value of RADIUS attribute 8 (framed IP address). However, if the endpoint IP address uses the value from different RADIUS attribute/number other than attribute 8, you can specify the corresponding attribute number with this command. You can use the "diagnose debug application msisdn" command to capture RADIUS packets and find out what attribute name/number is used to hold the IP address value. For details, see "Related topics" on page 220.	8

Variable	Description	Default
carrier-endpoint-framed-ip-order {host-order | network-order}	Select one of the following methods for endpoint IP address formatting: • **host-order**: format an IP address in host order, that is, the host portion is at the beginning. For example, 1.1.168.192. • **network-order**: sorts IP addresses in the network order, that is, the network portion is at the begging. For example, 192.168.1.1.	host-order
carrier-endpoint-radius-port <port_int>	Type the RADIUS server port for carrier endpoint account requests.	1813
carrier-endpoint-status {enable | disable}	Enable endpoint reputation scan for traffic examined by the session profile. This command starts the endpoint reputation daemon. You must start this daemon for the endpoint reputation feature to work.	enable
delete-ctrl-account <local_part_str>	Use this command to configure the email addresses through which email users can delete email from their per-recipient quarantines. Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines. For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter quar_delete.	delete-ctrl
greylist-capacity <maximum_int>	Enter the maximum number of greylist items in the greylist. New items that would otherwise cause the greylist database to grow larger than the capacity will instead overwrite the oldest item. To determine the default value and acceptable range for your FortiMail model, enter a question mark (?).	Varies by model
greylist-delay <1-120 minutes>	Enter the length in minutes 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 initial_expiry_period, also known as 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. The valid range between 1 and 120 minutes.	20
greylist-init-expiry-period <window_int>	Enter the period of time in hours after the greylistperiod, during which pending greylist entries will be confirmed and converted into automatic greylist entries if the SMTP client retries delivery. The valid range is from 4 to 24 hours.	4
greylist-ttl <ttl_int>	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 adding the TTL to the date and time of the previous matching delivery attempt. 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 and the greylist scanner removes the entry. The valid range is between 1 and 60 days.	10

Variable	Description	Default
`release-ctrl-account <local-part_str>`	Use this command to configure the email addresses through which email users can release email from their per-recipient quarantines. Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines. For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter `quar_delete`.	No default.
`session-profile-rate-control-type {connection | message}`	The rate control option enables you to control the rate at which email messages can be sent, either by the number of SMTP connections or the number of email messages. Enter which unit of measure will be used for traffic control, either: • `connection`: Restrict rates by the number of connections from each SMTP client IP address per specified number of minutes. • `message`: Restrict rates by the number of email messages from each SMTP client IP address per specified number of minutes.	

History

v4.0 New

Related topics

- config antispam bounce-verification key
- config antispam deepheader-analysis
- config antispam greylist exempt
- config antispam quarantine-report
- config antispam trusted

antispam trusted

Use these commands to configure both the IP addresses of mail transfer agents (MTAs) that are trusted to insert genuine `Received:` message headers, and the IP addresses of MTAs that perform antispam scans before the FortiMail unit.

`Received:` message headers are inserted by each mail transfer agent (MTA) that handles an email message in route to its destination. The IP addresses in those headers can be used as part of FortiGuard Antispam and DNSBL antispam checks, and SPF and DKIM sender validation. However, they should only be used if you trust that the `Received:` header added by an MTA is not fake — spam-producing MTAs sometimes insert fake headers containing the IP addresses of legitimate MTAs in an attempt to circumvent antispam measures.

If you trust that `Received:` headers containing specific IP addresses are always genuine, you can add those IP addresses to the `mta` list.

Note: Private network addresses, defined in RFC 1918, are never checked and do not need to be excluded using `config antispam trusted mta`.

Relatedly, if you can trust that a previous mail hop has already scanned the email for spam, you can add its IP address to the `antispam-mta` list to omit deep header scans for email that has already been evaluated by that MTA, thereby improving performance.

Syntax

```
config antispam trusted {mta | antispam-mta}
  edit <smtp_ipv4/mask>
end
```

Variable	Description	Default
`<smtp_ipv4/mask>`	Enter the IP address and netmask of an MTA.	No default.

History

FortiMail v4.0 New.

Related topics

- config antispam bounce-verification key
- config antispam deepheader-analysis
- config antispam greylist exempt
- config antispam quarantine-report
- config antispam settings

archive exempt-policy

Use this command to configure the exemptions to email archiving.

This command applies only if email archiving is enabled.

Syntax

```
config archive exempt-policy
  edit <policy_id>
    set pattern <string>
    set status {enable | disable}
    set type {attachment | body | recipient | sender | subject}
end
```

Variable	Description	Default
<policy_id>	Enter the index number of the exemption policy. To view a list of existing entries, enter a question mark (?).	No default.
pattern <string>	Enter a pattern, such as user*@example.com, that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this exemption will apply.	*
status {enable | disable}	Enable to activate the email archiving exemption.	enable
type {attachment | body | recipient | sender | subject}	Enter one of the following exemption match types: • attachment: The attachment file name will be evaluated for matches with pattern. • body: The body text will be evaluated for matches with pattern. • recipient: The recipient email address will be evaluated for matches with pattern. • sender: The sender email address will be evaluated for matches with pattern. • subject: The email subject will be evaluated for matches with pattern.	

History

FortiMail v4.0 New.

Related topics

- config archive policy
- config archive setting

archive policy

Use this command to configure email archiving policies.

This command applies only if email archiving is enabled.

Syntax

```
config archive policy
  edit <policy_id>
    set pattern <string>
    set status {enable | disable}
    set type {attachment | body | recipient | sender | subject}
end
```

Variable	Description	Default
<policy_id>	Enter the index number of the policy. To view a list of existing entries, enter a question mark (?).	No default.
pattern <string>	Enter a pattern, such as user*@example.com, that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this policy will apply.	*
status {enable | disable}	Enable to activate the email archiving policy.	enable
type {attachment | body | recipient | sender | subject}	Enter one of the following match types: • attachment: The attachment file name will be evaluated for matches with pattern. • body: The body text will be evaluated for matches with pattern. • recipient: The recipient email address will be evaluated for matches with pattern. • sender: The sender email address will be evaluated for matches with pattern. • subject: The email subject will be evaluated for matches with pattern.	

History

FortiMail v4.0 New.

Related topics

- config archive exempt-policy
- config archive setting

archive setting

Use this command to configure email archiving policies.

This command applies only if email archiving is enabled.

Syntax

```
config archive setting
  set account <account_str>
  set destination {local | remote}
  set forward-address <recipient_email>
  set local-quota <quota_int>
  set local-quota-cache <cache_int>
  set password <password_str>
  set quota-full {overwrite | noarchive}
  set remote-directory <path_str>
  set remote-ip <ftp_ipv4>
  set remote-password <password_Str>
  set remote-protocol {ftp | sftp}
  set remote-username <user_str>
  set rotation-size <size_int>
  set rotation-time <time_int>
  set status {enable | disable}
end
```

Variable	Description	Default
account <account_str>	Enter the email archiving account name.	archive
destination {local | remote}	Select whether to archive to the local disk or remote server.	local
forward-address <recipient_email>	Enter the email address to which all archived messages will also be forwarded. If no forwarding address exists, the FortiMail unit will not forward email when it archives it.	No default.
local-quota <quota_int>	Enter the local disk quota for email archiving in gigabytes (GB). The valid range depends on the amount of free disk space.	5
local-quota-cache <cache_int>	Enter the local disk quota for caching in gigabytes (GB). The valid range depends on the amount of free disk space.	5
password <password_str>	Enter the archiving account's password.	forti12356net
quota-full {overwrite | noarchive}	Enter either: • noarchive: Discard the email message if the hard disk space is consumed and a new email message arrives. • overwrite: Replace the oldest email message if the hard disk space is consumed and a new email message arrives.	overwrite
remote-directory <path_str>	Enter the directory path on the remote server where email archives will be stored.	No default.
remote-ip <ftp_ipv4>	Enter the IP address of the remote server that will store email archives.	0.0.0.0
remote-password <password_Str>	Enter the password of the user account on the remote server.	No default.
remote-protocol {ftp | sftp}	Enter either ftp or sftp to use that protocol when transferring email archives to the remote server.	sftp

Variable	Description	Default
`remote-username <user_str>`	Enter the name of a user account on the remote server.	No default.
`rotation-size <size_int>`	Enter the maximum size of the current email archiving mailbox in megabytes (MB). When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 10 to 200 MB.	`100`
`rotation-time <time_int>`	Enter the maximum age of the current email archiving mailbox in days. When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 1 to 365 days.	`7`
`status {enable | disable}`	Enable to activate email archiving.	`disable`

History

FortiMail v4.0 New.

Related topics

- config archive exempt-policy
- config archive policy

domain

Use these commands to configure a protected domain.

For more information on protected domains and when they are required, see the *FortiMail Administration Guide*.

Syntax

This command contains many sub-commands. Each sub-command, linked below, is documented in subsequent sections.

```
config domain
  edit <domain_name>
    config domain-setting...
    config policy recipient...
    config profile antispam...
    config profile antispam-action...
    config profile antivirus...
    config profile authentication...
    config profile content...
    config profile content-action...
    config user mail...
    config user group...
  next
end
```

Variable	Description	Default
<domain_name>	Type the fully qualified domain name (FQDN) of the protected domain. For example, to protect email addresses ending in “@example.com”, type example.com.	No default.

History

FortiMail v4.0 New.

Related topics

- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group

config domain-setting

Use this sub-command to configure the basic settings of a protected domain.

Syntax

This sub-command is available from within the command config domain.

```
config domain-setting
  set bypass-bounce-verification {enable | disable}
  set fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>}
  set fallback-port <port_int>
  set fallback-use-smtps {enable | disable}
  set global-bayesian {enable | disable}
  set greeting-with-host-name {enable | disable}
  set host <host_name>
  set ip-pool <pool_name>
  set ip-pool-direction {outgoing | incoming | both}
  set is-sub-domain {enable | disable}
  set ldap-asav-profile <ldap-profile_name>
  set ldap-asav-status {enable | disable}
  set ldap-domain-routing-port <port_int>
  set ldap-domain-routing-profile <ldap-profile_name>
  set ldap-domain-routing-smtps {enable |disable}
  set ldap-groupowner-profile <ldap-profile_name>
  set ldap-routing-profile <ldap-profile_name>
  set ldap-routing-status {enable | disable}
  set max-message-size <limit_int>
  set port <smtp-port_int>
  set quarantine-report-schedule-status {enable | disable}
  set quarantine-report-status {enable | disable}
  set quarantine-report-to-alt {enable | disable}
  set quarantine-report-to-alt-addr <recipient_email>
  set quarantine-report-to-individual {enable | disable}
  set quarantine-report-to-ldap-groupowner {enable | disable}
  set recipient-verification {disable | ldap | smtp}
  set recipient-verification-background {disable | ldap | smtp}
  set relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-
     lookup-alt-domain}
  set remove-outgoing-received-header {enable | disable}
  set smtp-recipient-verification-command {rcpt | vrfy}
  set smtp-recipient-verification-accept-reply-string <accept_string>
  set tp-hidden {no | yes}
  set tp-server-on-port <port_int>
  set tp-use-domain-mta {yes | no}
  set use-stmps {enable | disable}
  set webmail-language <language_name>
end
```

Variable	Description	Default
`bypass-bounce-verification {enable | disable}`	Enable to omit bounce address tag verification of email incoming to this protected domain. This bypass does not omit bounce address tagging of outgoing email.	`disable`
`fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>}` (transparent mode and gateway mode only)	Enter the fully qualified domain name (FQDN) or IP address of the secondary SMTP server for this protected domain. This SMTP server will be used if the primary SMTP server is unreachable.	No default.
`fallback-port <port_int>` (transparent mode and gateway mode only)	Enter the port number on which the failover SMTP server listens. If you enable Use SMTPS, Port automatically changes to the default port number for SMTPS, but can still be customized. The default SMTP port number is 25; the default SMTPS port number is 465.	`25`
`fallback-use-smtps {enable | disable}` (transparent mode and gateway mode only)	Enable to use SMTPS for connections originating from or destined for this protected server.	`disable`
`global-bayesian {enable | disable}`	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. This option does not apply if you have enabled use of personal Bayesian databases in an incoming antispam profile, and if the personal Bayesian database is mature. Instead, the FortiMail unit will use the personal Bayesian database.	`disable`
`greeting-with-host-name {enable | disable}`	Specify how the FortiMail unit will identify itself during the `HELO` or `EHLO` greeting of outgoing SMTP connections that it initiates. Disable: The FortiMail unit will identify itself using the domain name for this protected domain. If the FortiMail unit will handle internal email messages (those for which both the sender and recipient addresses in the envelope contain the domain name of the protected domain), to use this option, you must also configure your protected SMTP server to use its host name for SMTP greetings. Failure to do this will result in dropped SMTP sessions, as both the FortiMail unit and the protected SMTP server will be using the same domain name when greeting each other. Enable: The FortiMail unit will identify itself using its own host name. By default, the FortiMail unit uses the domain name of the protected domain. If your FortiMail unit is protecting multiple domains and using IP pool addresses, select Use system host name instead. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.	`disable`
`host <host_name>` (transparent mode and gateway mode only)	The host name or IP address and port number of the mail exchanger (MX) for this protected domain. If Relay Type is MX Record (this domain) or MX Record (alternative domain), this information is determined dynamically by querying the MX record of the DNS server, and this field will be empty.	No default.

Variable	Description	Default
ip-pool <pool_name>	You can use a pool of IP addresses as the source IP address when sending email from this domain, or as the destination IP address when receiving email destined to this domain, or as both the source and destination IP addresses. • If you want to use the IP pool as the source IP address for this protected domain, according to the sender's email address in the envelope (MAIL FROM:), select the IP pool to use and select *outgoing* as the ip-pool-direction. • If you want to use the IP pool as the destination IP address (virtual host) for this protected domain, according to the recipient's email address in the envelope (RCPT TO:), select the IP pool to use and select *incoming* as the ip-pool-direction. You must also configure the MX record to direct email to the IP pool addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be saperated as well. • If you want to use the IP pool as both the destination and source IP address, select the IP pool to use and select *Both* as the ip-pool-direction. Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.	No default.
ip-pool-direction {outgoing | incoming | both}	Sets the direction for the ip-pool option. See description above.	
is-sub-domain {enable | disable}	Enable to indicate the protected domain you are creating is a subdomain of an existing protected domain, then also configure Main domain. Subdomains, like their parent protected domains, can be selected when configuring policies specific to that subdomain. Unlike top-level protected domains, however, subdomains will be displayed as grouped under the parent protected domain when viewing the list of protected domains. This option is available only when another protected domain exists to select as the parent domain.	disable
ldap-asav-profile <ldap-profile_name>	Specify the name of an LDAP profile which you have enabled and configured.	No default.
ldap-asav-status {enable | disable}	Enable to query an LDAP server for an email user's preferences to enable or disable antispam and/or antivirus processing for email messages destined for them.	disable
ldap-domain-routing-port <port_int>	Enter the port number on which the SMTP servers in the LDAP profile listen. If you enable ldap-domain-routing-smtps, this setting automatically changes to the default port number for SMTPS, but can still be customized. The default SMTP port number is 25; the default SMTPS port number is 465. This option is valid when relay-type is ldap-domain-routing.	25
ldap-domain-routing-profile <ldap-profile_name>	Select the name of the LDAP profile that has the FQDN or IP address of the SMTP server you want to query. Also configure *ldap-domain-routing-port <port_int>* and *ldap-domain-routing-smtps {enable |disable}*. This option is valid when relay-type is set to ldap-domain-routing.	
ldap-domain-routing-smtps {enable |disable}	Enable to use SMTPS for connections originating from or destined for this protected server. This option is valid when relay-type is ldap-domain-routing.	disable

Variable	Description	Default
`ldap-groupowner-profile <ldap-profile_name>`	Select an LDAP profile to send the quarantine report to a group owner, rather than individual recipients.	No default.
`ldap-routing-profile <ldap-profile_name>`	Select an LDAP profile for mail routing.	No default.
`ldap-routing-status {enable | disable}`	Enable/disable LDAP mail routing.	`disable`
`max-message-size <limit_int>`	Enable then type the limit in kilobytes (KB) of the message size. Email messages over the threshold size are rejected. **Note:** If both this option and `limit-max-message-size <limit_int>` in the session profile are enabled, email size will be limited to whichever size is smaller.	`10240`
`port <smtp-port_int>`	Set the SMTP port number of the mail server.	`25`
`quarantine-report-schedule-status {enable | disable}`	Enable or disable domain-level quarantine report schedule setting. The quarantine report settings for a protected domain are a subset of the system-wide quarantine report settings. For example, if the system settings for schedule include only Monday and Thursday, when you are setting the schedule for the quarantine reports of the protected domain, you will only be able to select either Monday or Thursday.	`disable`
`quarantine-report-status {enable | disable}`	Enable or disable domain-level quarantine report.	`disable`
`quarantine-report-to-alt {enable | disable}`	Enable or disable sending domain-level 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.	`disable`
`quarantine-report-to-alt-addr <recipient_email>`	Enter the recipient's email address.	No default.
`quarantine-report-to-individual {enable | disable}`	Enable to send quarantine reports to all recipients.	`enable`
`quarantine-report-to-ldap-groupowner {enable | disable}`	Enable to send quarantine reports to the LDAP group owner of the specified LDAP profile.	`disable`

Variable	Description	Default
`recipient-verification {disable | ldap | smtp}`	Select a method of confirming that the recipient email address in the message envelope (`RCPT TO:`) corresponds to an email user account that actually exists on the protected email server. If the recipient address is invalid, the FortiMail unit will reject the email. This prevents quarantine email messages for non-existent accounts, thereby conserving quarantine hard disk space. • `disable`: Do not verify that the recipient address is an email user account that actually exists. • `smtp`: Query the SMTP server using the SMTP RCPT command to verify that the recipient address is an email user account that actually exists. You can also choose to use the SMTP VRFY command to do the verification. This feature is avaible on the GUI when you create a domain. If you want to query an SMTP server other than the one you have defined as the protected SMTP server, also enable Use alternative server, then enter the IP address or FQDN of the server in the field next to it. Also configure Port with the TCP port number on which the SMTP server listens, and enable Use SMTPS if you want to use SMTPS for recipient address verification connections with the server. • `ldap`: 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. **Note**: This option can cause a performance impact that may 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. **Note**: Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or the periodic removal of invalid quarantine accounts.	`disable`

Variable	Description	Default
`recipient-verification-background {disable | ldap | smtp}`	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. • `disable`: Do not verify that the recipient address is an email user account that actually exists. • `smtp`: Query the SMTP server to verify that the recipient address is an email user account that actually exists. • `ldap`: 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. If you select either Use SMTP server or Use LDAP server, at 4:00 AM daily (unless configured for another time, using the CLI), the FortiMail unit queries the server to verify the existence of email user accounts. If an email user account does not currently exist, the FortiMail unit removes all spam quarantined for that email user account. **Note**: If you have also enabled `recipient-verification`, the FortiMail unit is prevented from forming quarantine accounts for email user accounts that do not really exist on the protected email server. In that case, invalid quarantine accounts are never formed, and this option may not be necessary, except when you delete email user accounts on the protected email server. If this is the case, you can improve the performance of the FortiMail unit by disabling this option. **Note**: Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or verification of recipient addresses.	No default.

Variable	Description	Default
`relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain}` (transparent mode and gateway mode only)	Select from one of the following methods of defining which SMTP server will receive email from the FortiMail unit that is destined for the protected domain: • `host`: Configure the connection to one protected SMTP server or, if any, one fallback. • `ldap-domain-routing`: Query the LDAP server for the FQDN or IP address of the SMTP server. For more information about domain lookup, see "domain-query <query_str>" on page 140. • `mx-lookup`: Query the DNS server's MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. • `mx-lookup-alt-domain`: Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. • `ip-pool`: Configure the connection to rotate among one or many protected SMTP servers. **Note**: If an MX option is used, you may also be required to configure the FortiMail unit to use a private DNS server whose MX and/or A records differ from that of a public DNS server. Requirements vary by the topology of your network and by the operating mode of the FortiMail unit. • **Gateway mode:** A private DNS server is required. On the private DNS server, configure the MX record with the FQDN of the SMTP server that you are protecting for this domain, causing the FortiMail unit to route email to the protected SMTP server. This is different from how a public DNS server should be configured for that domain name, where the MX record usually should contain the FQDN of the FortiMail unit itself, causing external SMTP servers to route email through the FortiMail unit. Additionally, if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall, on the private DNS server, configure the protected SMTP server's A record with its private IP address, while on the public DNS server, configure the FortiMail unit's A record with its public IP address. • **Transparent mode:** A private DNS server is required if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall. On the private DNS server, configure the protected SMTP server's A record with its private IP address. On the public DNS server, configure the protected SMTP server's A record with its public IP address. Do not modify the MX record.	`host`
`remove-outgoing-received-header {enable | disable}`	Enable to remove the `Received:` message headers from email whose: • sender email address belongs to this protected domain • recipient email address is outgoing (that is, does not belong to this protected domain); if there are multiple recipients, only the first recipient's email address is used to determine whether an email is outgoing You can alternatively remove this header from any matching email using session profiles.	`disable`
`smtp-recipient-verification-command {rcpt | vrfy}`	Specify the command that the FortiMail unit uses to query the SMTP server to verify that the recipient address is an email user account that actually exists. The default command that the FortiMail unit uses is `rcpt`. For information about recipient verification, see `config recipient-verification {disable | ldap | smtp}`.	`rcpt`

Variable	Description	Default
smtp-recipient-verification-accept-reply-string <accept_string>	When FortiMail queries the SMTP server for recipient verification: • If the reply code of the VRFY command is 2xx, the recipient exists. • If the reply code is non-2xx, FortiMail will try to match the accept string you specified with the reply string. If the strings match, the recipient exists. • Otherwise, the recipient is unknown. For example, if the recipient is a group or mailing list, FortiMail will receive a 550 error code and a reply string. Depending on what reply string you get, you can specify a string to match the reply string. For example, if the recipient is marketing@example.com, the reply string might say something like “marketing@example.com is a group”. In this case, if you specify “is a group” as the accept string and thus this string matches the string or part of the string in the reply string, FortiMail will deem the query successful and pass the email. This command is available only when you set SMTP recipient verification command to vrfy.	
tp-hidden {no | yes} (transparent mode only)	Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in: • the SMTP greeting (HELO/EHLO) in the envelope and in the Received: message headers of email messages • the IP addresses in the IP header This masks the existence of the FortiMail unit to the protected SMTP server. Disable to replace the SMTP client’s IP address or domain name with that of the FortiMail unit. For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in bold): Received: from 192.168.1.1 (EHLO ***172.16.1.1***) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800 Received: from smtpa ([172.16.1.2]) by [***172.16.1.1***] with SMTP id kAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT But if the option is disabled, the message headers would contain: Received: from 192.168.1.1 (EHLO ***fortimail.example.com***) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800 Received: from smtpa ([172.16.1.2]) by ***fortimail.example.com*** with SMTP id kAOFJl4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT	no
tp-server-on-port <port_int> (transparent mode only)	Select the network interface (physical port) to which the protected SMTP server is connected. Note: Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface.	0

Variable	Description	Default
tp-use-domain-mta {yes | no} (transparent mode only)	Enable to proxy SMTP clients' incoming connections when sending outgoing email messages via the protected SMTP server. For example, if the protected domain example.com has the SMTP server 192.168.1.1, and an SMTP client for user1@example.com connects to it to send email to user2@external.example.net, enabling this option would cause the FortiMail unit to proxy the connection through to the protected SMTP server. Disable to relay email using the built-in MTA to either the defined SMTP relay, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (RCPT TO:) domain. The email may not actually travel through the protected SMTP server, even though it was the relay originally specified by the SMTP client. This option does not affect incoming connections containing incoming email messages, which will always be handled by the built-in MTA. **Note:** This option will be ignored for email that matches an antispam or content profile where you have enabled alternate-host {<relay_fqdn> | <relay_ipv4>}.	no
use-stmps {enable | disable}	Enable to use SMTPS to relay email to the mail server.	disable
webmail-language <language_name>	Select the language that the FortiMail unit will to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same language as the web-based manager.	No default.

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	New variables ip-pool, ip-pool-direction, ldap-domain-routing-port, ldap-domain-routing-profile, ldap-domain-routing-smtps, and smtp-rcpt-vrfy-try-mailhost. The relay-type variable has a new option, ldap-domain-routing.

Related topics

- config domain
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group
- diagnose debug application starttls

config policy recipient

Use this sub-command to configure a recipient-based policy for a protected domain.

Syntax

This sub-command is available from within the command config domain.

```
config policy recipient
  edit <policy_index>
```

```
    set auth-access-options {pop3 smtp-auth smtp-diff-identity web}
    set certificate-required {yes | no}
    set pki-auth {enable | disable}
    set pki-user <user_name>
    set profile-antispam <antispam_name>
    set profile-antivirus <antivirus_name>
    set profile-auth-type {imap | ldap | pop3 | smtp | radius}
    set profile-content <profile_name>
    set profile-ldap <profile_name>
    set recipient-name <name_str>
    set recipient-type {ldap-group | local-group | user}
    set sender-domain <domain_name>
    set sender-name <local-part_str>
    set sender-type {ldap-group | local-group | user}
    set status {enable | disable}
  next
end
```

Variable	Description	Default
<policy_index>	Type the index number of the policy. To view a list of existing entries, enter a question mark (?).	No default.
auth-access-options {pop3 smtp-auth smtp-diff-identity web}	Type one or more of the following: • smtp-diff-identity: Allow email when the SMTP client authenticates with a different user name than the one that appears in the envelope's sender email address. You must also enter smtpauth for this option to have any effect. • web: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine. • pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine. • smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. **Note:** Entering 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.	No default.
certificate-required {yes | no} (transparent and gateway mode only)	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enable this option.	no
pki-auth {enable | disable} (transparent and gateway mode only)	Enable if you want to allow email users to log in to their per-recipient spam quarantine by presenting a certificate rather than a user name and password.	disable
pki-user <user_name> (transparent and gateway mode only)	Enter the name of the PKI user entry, or select a user you defined before. This is not required to be the same as the administrator or email user's account name, although you may find it helpful to do so. For example, you might have an administrator account named admin1.You might therefore find it most straightforward to ***also*** name the PKI user admin1, making it easy to remember which account you intended to use these PKI settings.	No default.
profile-antispam <antispam_name>	Select a antispam profile that you want to apply to the policy.	No default.
profile-antivirus <antivirus_name>	Select an antivirus profile that you want to apply to the policy.	No default.

Variable	Description	Default

`profile-auth-type {imap | ldap | pop3 | smtp | radius}`	If you want email users to be able to authenticate using an external authentication server, first specify the profile type (SMTP, POP3, IMAP, RADIUS, or LDAP), then specify which profile to use.
	For example:
	`set profile-auth-type ldap`
	`set profile-auth-ldap ldap_profile1`
		No default.

`profile-auth-imap <imap_name>`	Type the name of an IMAP authentication profile. This command is applicable only if you have enabled use of an IMAP authentication profile using `profile-auth-type {imap | ldap | pop3 | smtp | radius}`.	No default.
`profile-auth-ldap <ldap_name>`	Type the name of an LDAP authentication profile. This command is applicable only if you have enabled use of an LDAP authentication profile using `profile-auth-type {imap | ldap | pop3 | smtp | radius}`.	No default.
`profile-auth-pop3 <pop3_name>`	Type the name of a POP3 authentication profile. This command is applicable only if you have enabled use of a POP3 authentication profile using `profile-auth-type {imap | ldap | pop3 | smtp | radius}`.	No default.
`profile-auth-smtp <smtp_name>`	Type the name of an SMTP authentication profile. This command is applicable only if you have enabled use of an SMTP authentication profile using `profile-auth-type {imap | ldap | pop3 | smtp | radius}`.	No default.
`profile-auth-radius <radius_name>`	Type the name of a RADIUS authentication profile. This command is applicable only if you have enabled use of a RADIUS authentication profile using `profile-auth-type {imap | ldap | pop3 | smtp | radius}`.	No default.
`profile-content <profile_name>`	Select which content profile you want to apply to the policy.	No default.
`profile-ldap <profile_name>`	If you set the recipient type as “ldap-group", you can select an LDAP profile.	
`recipient-name <name_str>`	Enter the local part of the recipient email address or a pattern with wild cards.	No default.
`recipient-type {ldap-group | local-group | user}`	Select one of the following ways to define recipient (`RCPT TO:`) email addresses that match this policy. This setting applies to the incoming policies only. • `user`: Select this option and then use the above command to enter the local part of the recipient email address. • `local-group`: Select this option and then specify the local group under this domain. • `ldap-group`: Select this option and then select an LDAP profile.	`user`
`sender-domain <domain_name>`	Enter the domain part of the sender email address. For example, example.com.	
`sender-name <local-part_str>`	Enter the local part of the sender email address. For example, user1.	
`sender-type {ldap-group | local-group | user}`	Select one of the following ways to define which sender (`MAIL FROM:`) email addresses match this policy. • `user`: Select this option and then use the above command to enter the local part of the sender email address. • `local-group`: Select this option and then specify the local group under this domain. • `ldap-group`: Select this option and then select an LDAP profile. **Note:** This setting applies to the outgoing policies only.	`user`
`status {enable | disable}`	Enable or disable the policy.	`enable`

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group

config profile antispam

Use this sub-command to configure antispam profiles for a protected domain. To configure system-wide antispam profiles, use "config profile antispam" on page 108.

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.

Syntax

This sub-command is available from within the command config domain.

```
config profile antispam
  edit <profile_name>
    set (options)
    config (options)
```

For more information about the `set` and `config` options, see "config profile antispam" on page 108.

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action

- config user mail
- config user group

config profile antispam-action

Use this sub-command to define action profiles.

Antispam action profiles define one or more things that the FortiMail unit should do if the antispam profile determines that an email is spam.

For example, you might have configured an antispam action profile named `quar_and_tag_profile`, which both tags the subject line and quarantines email detected to be spam. In general, all antispam profiles using `quar_and_tag_profile` will therefore both quarantine and tag spam. However, you have decided that email that does not 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 would override the action profile's default action by configuring and selecting a second action profile, named `rejection_profile`, which rejects such email.

Syntax

This sub-command is available from within the command config domain.

```
config profile antispam-action
  edit <profile_name>
    set action {discard | none | quarantine | quarantine-review | reject |
       rewrite-rcpt}
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set subject-tagging-status {enable | disable}
    set subject-tagging-text <tag_str>
    set quarantine-report {enable | disable}
    set quarantine-days <days_int>
    set release-through-email {enable | disable}
    set release-through-web {enable | disable}
    set release-auto-whitelist {enable | disable}
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
  next
end
```

Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
action {discard | none | quarantine | quarantine-review | reject | rewrite-rcpt}	Type an action for the profile. • discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • none: Apply any configured header or subject line tags, if any. • quarantine: Enter to redirect spam to the per-recipient quarantine. For more information, see the *FortiMail Administration Guide*. This option is available only for incoming profiles. If you enter this option, also configure quarantine-report {enable | disable}, quarantine-days <days_int>, release-through-email {enable | disable}, release-through-web {enable | disable}, and release-auto-whitelist {enable | disable}. • quarantine-review: Enter to redirect spam to the system quarantine. For more information, see the *FortiMail Administration Guide*. • reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • rewrite-rcpt: Enter 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). If you enter this option, also configure rewrite-rcpt-local-type {none | prefix | replace | suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix | replace | suffix}, and rewrite-rcpt-domain-value <value_str>.	none
header-insertion-name <name_str>	Enter the message header key. The FortiMail unit will add 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. See header-insertion-value <header_str>.	
header-insertion-status {enable | disable}	Enable to add a message header to detected spam. See header-insertion-value <header_str>.	disable
header-insertion-value <header_str>	Enter the message header value. 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. See header-insertion-name <name_str>.	
subject-tagging-status {enable | disable}	Enable to prepend text (“tag”) defined using subject-tagging-text <tag_str> to the subject line on detected spam.	disable

Variable	Description	Default
subject-tagging-text <tag_str>	Enter the text that will appear 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.	
quarantine-report {enable | disable}	Enable to send a quarantine report.	disable
quarantine-days <days_int>	Enter the number of days you want to keep the quarantined email. Enter a small enough value that will prevent the size of the quarantine from exceeding the available disk space. If you enter 0 to prevent automatic deletion of quarantined files, you must periodically manually remove old files.	14
release-through-email {enable | disable}	Enable to allow email users to remotely release email from the quarantine by sending email to quarantine control account email addresses. For more information, see the *FortiMail Administration Guide*.	disable
release-through-web {enable | disable}	Enable to allow email users to remotely release email from the quarantine by selecting the *Release* link in a quarantine report. For more information, see the *FortiMail Administration Guide*.	disable
release-auto-whitelist {enable | disable}	Enable to, when an email user releases an email from the quarantine, automatically add the sender email address of the quarantined email to the email user's personal white list ***if*** the option is also enabled in the email user's preferences. Email users' preferences can be configured from both the *Preferences* tab of FortiMail webmail and from the web-based manager. For more information, see the *FortiMail Administration Guide*.	disable
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
rewrite-rcpt-domain-type {none-prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.	none
rewrite-rcpt-domain-value <value_str>	Type the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix | replace | suffix}.	

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group

config profile antivirus

Use this sub-command to create antivirus profiles that you can select in a policy in order to scan email for viruses.

If the FortiMail unit detects a virus, it replaces the infected file with a replacement message that notifies the email user the infected file has been removed. You can customize replacement messages. For more information, see the *FortiMail Administration Guide*.

Syntax

This sub-command is available from within the command config domain.

```
config profile antivirus
  edit <profile_name>
    set discard {enable | disable}
    set heuristic {enable | disable}
    set heuristic-discard {enable | disable}
    set heuristic-reject {enable | disable}
    set reject {enable | disable}
    set scanner {enable | disable}
  next
end
```

Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	
discard {enable | disable}	Enable to accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client.	disable
heuristic {enable | disable}	Enable to use heuristics when performing antivirus scanning.	disable
heuristic-discard {enable | disable}	Enable to accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client.	disable
heuristic-reject {enable | disable}	Enable to reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550.	disable
reject {enable | disable}	Enable to reject infected email and reply to the SMTP client with SMTP reply code 550.	disable
scanner {enable | disable}	Enable to perform antivirus scanning for this profile.	disable

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group

config profile authentication

Use this sub-command to configure the FortiMail unit to connect to an external SMTP server in order to authenticate email users.

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS

When the FortiMail unit is operating in server mode, only local and RADIUS authentication are available.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine.

Depending on the mode in which your FortiMail unit is operating, you may be able to apply authentication profiles through incoming recipient-based policies, IP-based policies, and email user accounts.

For more information, see the *FortiMail Administration Guide*.

Syntax

This sub-command is available from within the command config domain.

```
config profile authentication imap
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication pop3
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication radius
  edit <profile_name>
```

```
    set [port <port_int>]
    set secret <password_str>
    set send-domain {enable | disable}
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication smtp
  edit <profile_name>
    set [option {ssl secure tls senddomain}]
    set server {<fqdn_str> | <host_ipv4>}
    set port <port_int>
    set try-ldap-mailhost {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
option {ssl secure tls senddomain}	Enter one or more of the following in a space-delimited list: • senddomain: Enable if the IMAP server requires both the user name and the domain when authenticating. • ssl: Enables secure socket layers (SSL) to secure message transmission. • secure: Enables secure authentication. • tls: Enables transport layer security (TLS) to ensure privacy between communicating application	
port <port_int>	Enter the TCP port number of the IMAP server. The standard port number for IMAP is 143; for SSL-secured IMAP, it is 993.	
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the IMAP server.	
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: • domain: Enable if the POP3 server requires both the user name and the domain when authenticating. • ssl: Enables secure socket layers (SSL) to secure message transmission. • secure: Enables secure authentication. • tls: Enables transport layer security (TLS) to ensure privacy between communicating application	
port <port_int>	Enter the TCP port number of the POP3 server. The standard port number for POP3 is 110; for SSL-secured POP3, it is 995.	
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the POP3 server.	
[port <port_int>]	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server. The standard port number for RADIUS is 1812.	1812
secret <password_str>	Enter the password for the RADIUS server.	
send-domain {enable | disable}	Enable if the RADIUS server requires both the user name and the domain when authenticating.	
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the RADIUS server.	

Variable	Description	Default
`[option {ssl secure tls senddomain}]`	If you want to enable any of the following options, enter them in a space-delimited list: • `senddomain`: Enable if the SMTP server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application	
`server {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	
`port <port_int>`	Enter the TCP port number of the SMTP server. The standard port number for SMTP is 25; for SSL-secured SMTP, it is 465.	
`try-ldap-mailhost {enable | disable}`	Enable if your LDAP server has a mail host entry for the generic user If you select this option, the FortiMail unit will querry the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will querry the server you entered in the server field.	

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 New variable `try-ldap-mailhost` for `config profile authentication smtp`.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile content
- config profile content-action
- config user mail
- config user group

config profile content

Use this sub-command to 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.

Content profiles can be used to apply content-based encryption to email. They can also be used to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. As such, content profiles can be used both for email that you want to protect, and for email that you want to prevent.

Content profile options vary by whether the profile matches incoming or outgoing email.

Syntax

This sub-command is available from within the command config domain.

```
config profile content
  edit <profile_name>
    set action <action-profile_name>
    set archive-block-on-failure-to-decompress {enable | disable}
    set archive-block-password-protected {enable | disable}
    set archive-block-recursive {enable | disable}
    set archive-content-check {enable | disable}
    set archive-max-recursive-level <threshold_int>
    set attachment-name-disposition {block | pass}
    set attachment-type-disposition {block | pass}
    set bypass-on-auth {enable | disable}
    set defersize <threshold_int>
    set option {ssl secure tls senddomain}
    set server {<fqdn_str> | <host_ipv4>}
    set port <port_int>
    config attachment-name
      edit attachment-name-pattern <pattern_str>
        set status {enable | disable}
      next
    end
    config attachment-type
      edit attachment-type <MIME-type_str>
        set status {enable | disable}
      next
    end
    config monitor
      edit monitor <index_int>
        set action <action-profile_name>
        set dict-score <score_int>
        set dictionary-group <dictionary-group_name>
        set dictionary-profile <dictionary-profile_name>
        set dictionary-type {group | profile}
        set status {enable | disable}
      next
    end
  next
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the profile. To view a list of existing entries, enter a question mark (`?`).	No default.
`attachment-name-pattern <pattern_str>`	Enter a pattern, such as `'*.bat'`, that matches the email attachment names that you want the content profile to match. The patterns include: • *.bat • *.com • *.dll • *.doc • *.exe • *.gz • *.hta • *.ppt • *.rar • *.scr • *.tar • *.tgz • *.vb? • *.wps • *.xl? • *.zip • *.pif	No default.
`status {enable | disable}`	Enable or disable a pattern that matches the email attachment names that you want the content profile to match.	`disable`

Variable	Description	Default
attachment-type <MIME-type_str>	Enter one of the following MIME types or subtypes: • video • audio • image • image-gif • image-jpeg • image-tiff • image-png • image-other: This option includes all images not specified by the other image types. • executable • executable-activex • executable-java • executable-javascript • executable-vbs • executable-vba • executable-other: This option includes all executables not specified by the other executable types. • document • document-msoffice • document-msoffice-embedded-check • document-msoffice-vba-check • document-visio • document-visio-vba-check • document-openoffice • document-openoffice-embedded-check • document-pdf • document-other:This option includes all documents not specified by the other document types. • archive • application-other:This option includes all applications not specified by the other application types. • text • text-7bit • text-html • text-xml • text-other:This option includes all text documents not specified by the other text types. • encrypted: This option includes both the S/MIME type and PGP-encrypted email.	No default.
status {enable | disable}	Enter either: • enable: Perform the action configured in "config profile content-action" on page 76. • disable: Pass the file type filter. The email will still be subject to other content profile scans that you have configured, if any. **Note:** Unlike other MIME types, archive may receive the opposite of this action, or perform an action regardless of this setting.	disable
monitor <index_int>	Enter the index number of the monitor profile. If the monitor profile does not currently exist, it will be created.	No default.
action <action-profile_name>	Enter the action profile for this monitor profile. The FortiMail unit will perform the actions if the content of the email message matches words or patterns from the dictionary profile that the monitor profile uses.	No default.
dict-score <score_int>	Enter the number of times that an email must match the content monitor profile before it will receive the action configured in action <action-profile_name>.	1

Variable	Description	Default
dictionary-group <dictionary-group_name>	Enter the dictionary profile group that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profiles. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in action <action-profile_name>. For information on dictionary profiles, see the *FortiMail Administration Guide*.	No default.
dictionary-profile <dictionary-profile_name>	Enter the dictionary profile that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profile. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in action <action-profile_name>. For information on dictionary profiles, see the *FortiMail Administration Guide*.	No default.
dictionary-type {group | profile}	Enter `profile` to detect content based upon a dictionary profile, or `group` to detect content based upon a group of dictionary profiles. Depending on your selection, also configure either `dictionary-group <dictionary-group_name>` or `dictionary-profile <dictionary-profile_name>`.	`group`
status {enable | disable}	Enable or disable this monitor profile.	`disable`
action <action-profile_name>	Enter a content action profile to use.	No default.
archive-block-on-failure-to-decompress {enable | disable}	Enter to apply the action configured in "config profile content-action" on page 76 if an attached archive cannot be successfully decompressed in order to scan its contents.	`disable`
archive-block-password-protected {enable | disable}	Enter to apply the action configured in "config profile content-action" on page 76 if an attached archive is password-protected.	`disable`
archive-block-recursive {enable | disable}	Enable to block archive attachments whose depth of nested archives exceeds archive-max-recursive-level <threshold_int>.	`enabled`
archive-content-check {enable | disable}	Enter to enable consideration of the nesting depth threshold, password protection, and successful decompression when scanning attachments that are archives.	`enabled`
archive-max-recursive-level <threshold_int>	Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email. • `archive-max-recursive-level` **is** `0`**, or attachment's depth of nesting equals or is less than** `archive-max-recursive-level`: If the attachment contains a file that matches one of the other MIME file types, perform the action configured for that file type, either block or pass. • **Attachment's depth of nesting is greater than** `archive-max-recursive-level`: Apply the block action, unless you have disabled archive-block-recursive {enable | disable}, in which case it will pass the MIME file type content filter. Block actions are specified in "config profile content-action" on page 127. This option applies only if archive-content-check {enable | disable} is enabled.	`0`

Variable	Description	Default
attachment-name-disposition {block | pass}	Pass or block email if a file attachment matches the file name patterns enabled in attachment-name-pattern <pattern_str>. If an attachment matches a pattern not enabled, the FortiMail unit will perform the ***opposite*** action of whatever you selected, either block or pass. For example, if you enter block and have enabled the name pattern *.exe, files whose names end in .exe will be blocked. All other file names will pass attachment filtering, but will still be subject to any other filters or antispam scans that you have configured. Conversely, if you select pass and enabled *.doc, all file names other than those ending in .doc will be blocked.	block
attachment-type-disposition {block | pass}	Block or pass email if a file attachment matches the file types enabled in attachment-type <MIME-type_str>. File types that you have not enabled will receive the action opposite of your block/pass selection. Passed file types will pass attachment file type filtering only, and will still be subject to any other content filters or antispam scans that you have configured.	block
bypass-on-auth {enable | disable}	Enable to omit antispam scans when an SMTP sender is authenticated.	disable
defersize <threshold_int>	Enter the size threshold in kilobytes. Delivery of email messages greater than this size will be deferred until the period configured for oversize email. To disable deferred delivery, enter 0.	0
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: • senddomain: Enable if the SMTP server requires both the user name and the domain when authenticating. • ssl: Enables secure socket layers (SSL) to secure message transmission. • secure: Enables secure authentication. • tls: Enables transport layer security (TLS) to ensure privacy between communicating application	No default.
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	No default.
port <port_int>	Enter the TCP port number of the SMTP server. The standard port number for SMTP is 25; for SSL-secured SMTP, it is 465.	No default.

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content-action

- config user mail
- config user group

config profile content-action

Use this sub-command to define content action profiles.

Content action profiles can be used 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, you would 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`.

Syntax

This sub-command is available from within the command config domain.

```
config profile content-action
  edit <profile_name>
    set action {discard | encryption | none | quarantine | quarantine-review
       | reject | replace | rewrite-rcpt | treat-as-spam}
    set encryption-profile <encryption-profile_name>
    set rewrite-rcpt-domain-type {none | prefix | replace | suffix}
    set rewrite-rcpt-domain-value <case_str>
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set header-insertion-name <text_str>
    set header-insertion-value <value_str>
    set subject-tagging-text <text_str>
    set tagging type {insert-header | tag-subject}
  next
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
action {discard | encryption | none | quarantine | quarantine-review | reject | replace | rewrite-rcpt | treat-as-spam}	Enter the action that the FortiMail unit will perform if the content profile determines that an email contains prohibited words or phrases, file names, or file types. • discard: Accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • encryption: Apply an encryption profile. Also configure encryption-profile <encryption-profile_name>. • none: Apply any configured header or subject line tags, if any. • quarantine: Divert the email to the per-recipient quarantine. • quarantine-review: Divert the email to the system quarantine. • reject: Reject the email, replying with an SMTP error code to the SMTP client. • replace: Accept the email, but replace the content matching this profile with a replacement message. • rewrite-rcpt: Enter to change the recipient address of any email that matches the content profile. Also configure rewrite-rcpt-domain-type {none | prefix | replace | suffix}, rewrite-rcpt-domain-value <case_str>, rewrite-rcpt-local-type {none | prefix | replace | suffix}, and rewrite-rcpt-local-value <value_str>. • treat-as-spam: Apply the action selected in the incoming antispam profile.	replace
encryption-profile <encryption-profile_name>	Enter an encryption profile to use.	No default.
rewrite-rcpt-domain-type {none | prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email that matches the content profile. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.	none
rewrite-rcpt-domain-value <case_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix | replace | suffix}.	
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email that matches the content profile. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	

Variable	Description	Default
`header-insertion-name <text_str>`	Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Content-Filter: Contains banned word.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. Also configure tagging type {insert-header | tag-subject}.	
`header-insertion-value <value_str>`	Enter the message header value. The FortiMail unit will add this value to the message header of the email before forwarding it to the recipient. See header-insertion-name <text_str>. Also configure tagging type {insert-header | tag-subject}.	
`subject-tagging-text <text_str>`	Enter the text that will appear in the subject line of the email, such as "`[PROHIBITED-CONTENT]`". The FortiMail unit will prepend 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. Also configure tagging type {insert-header | tag-subject}.	
`tagging type {insert-header | tag-subject}`	Enter the type of tagging for this profile. Enter `insert-header` enables header-insertion-name <text_str> and header-insertion-value <value_str>. Enter `tag-subject` enables subject-tagging-text <text_str>.	

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config user mail
- config user group

config user mail

Use this sub-command to configure email user accounts.

Syntax

This sub-command is available from within the command config domain.

```
config user mail
  edit <user_name>
    set type {local | ldap}
    set type local
    set displayname <name_str>
    set password <pwd_str>
    set type ldap
    set displayname <name_str>
    set ldap-profile <ldap_name>
  next
end
```

Variable	Description	Default
<user_name>	Enter the user name of an email user, such as user1. This is also the local-part portion of the email user's primary email address.	
type {local | ldap}	Enter the type of email user account you want to add. See set type local and set type ldap.	ldap
displayname <name_str>	Enter the display name of the local email user, such as 'User One'.	
password <pwd_str>	Enter the password of the local email user.	
displayname <name_str>	Enter the display name of the LDAP email user, such as 'User One'.	
ldap-profile <ldap_name>	Enter the name of an LDAP profile in which authentication queries are enabled.	

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user group

config user group

Use this sub-command to group related email user accounts.

Email user groups can simplify the creation of policies: when creating policies, you can select the name of an email user group, rather than entering each email user name individually.

Syntax

This sub-command is available from within the command config domain.

```
config user group
  edit <group_name>
    set member member <user_str>
end
```

Variable	Description	Default
<group_name>	Type the name of the email user group.	No default.
member <user_str>	Type the email users that are members of this user group.	

History

FortiMail v4.0 New.

Related topics

- config domain
- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user mail

domain-association

Use this command to configure domain associations. Associated domains use the settings of the protected domains or subdomains with which they are associated.

Domain associations can be useful for saving time when you have multiple domains for which you would otherwise need to configure 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. Alternatively, you could create one protected domain, listing the nine remaining 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, saving time and reducing chances for error. Changes to one protected domain automatically apply to all of its associated domains.

Exceptions to settings that associated domains will re-use include DKIM keys and signing settings. Domain keys are by nature tied to the exact protected domain only, and cannot be used for any other protected domain, including associated domains.

Alternatively, you can configure LDAP queries to automatically add domain associations. For details, see "config system mailserver" on page 189.

This command applies only if the FortiMail unit is operating in gateway mode or transparent mode.

Syntax

```
config domain-association
  edit <domain-association_fqdn>
    set main-domain <protected-domain_name>
  next
end
```

Variable	Description	Default
<domain-association_fqdn>	Enter the fully qualified domain name (FQDN) of a mail domain that you want to use the same settings as the same protected domain	No default.
<protected-domain_name>	Enter the name of the protected domain. The associated domain will use the settings of this domain.	No default.

History

FortiMail v4.0 New.

Related topics

- config system mailserver

log setting remote

Use this command to configure storing log messages remotely, on a Syslog server or FortiAnalyzer unit.

Syntax

```
config log setting remote
  edit <log-destination_index>
    set comma-separated-value {enable | disable}
    set encryption-log-status {enable | disable}
    set event-log-category {admin configuration ha | imap pop3 smtp system
       update webmail}
    set event-log-status {enable | disable}
    set facility {alert | audit | auth | authpriv | clock | cron | daemon |
       ftp | kern | local0 | local1 | local2 | local3 | local4 | local5 |
       local6 | local7 | lpr | mail | news | ntp}
    set history-log-status {enable | disable}
    set loglevel {alert | critical | debug | emergency | error |
       information | notification | warning}
    set port <port_int>
    set server <log_ipv4>
    set spam-log-status {enable | disable}
    set status {enable | disable}
    set virus-log-status {enable | disable}
end
```

Variable	Description	Default
<log-destination_index>	Type an index number to identify which remote Syslog server or FortiAnalyzer unit you are configuring.	No default.
comma-separated-value {enable | disable}	Enable CSV format if you want to send log messages in comma-separated value (CSV) format. **Note:** Do not enable this option if the log destination is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV format logs.	disable
encryption-log-status {enable | disable}	Enable or disable IBE event logging to a remote Syslog server or FortiAnalyzer unit..	disable
event-log-category {admin configuration ha | imap pop3 smtp system update webmail}	Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space. • admin: Log all administrative events, such as logins, resets, and configuration updates. • configuration: Enable to log configuration changes. • ha: Log all high availability (HA) activity. • imap: Log all IMAP events. • pop3: Log all POP3 events. • smtp: Log all SMTP relay or proxy events. • system: Log all system-related events, such as rebooting the FortiMail unit. • update: Log both successful and unsuccessful attempts to download FortiGuard updates. • webmail: Log all FortiMail webmail events.	No default.
event-log-status {enable | disable}	Enable or disable event logging to a remote Syslog server or FortiAnalyzer unit.	disable

Variable	Description	Default
`facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kern | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp}`	Type the facility identifier that the FortiMail unit will use to identify itself when sending log messages to the first Syslog server. To easily identify log messages from the FortiWeb unit when they are stored on the Syslog server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.	`kern`
`history-log-status {enable | disable}`	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	`disable`
`loglevel {alert | critical | debug | emergency | error | information | notification | warning}`	Type one of the following severity levels: • `alert` • `critical` • `debug` • `emergency` • `error` • `information` • `notification` • `warning` This log destination will receive log messages greater than or equal to this severity level.	`information`
`port <port_int>`	If the remote host is a FortiAnalyzer unit, type `514`. If the remote host is a Syslog server, type the UDP port number on which the Syslog server listens for connections.	`514`
`server <log_ipv4>`	Type the IP address of the Syslog server or FortiAnalyzer unit.	No default.
`spam-log-status {enable | disable}`	Enable to log all antispam events.	`disable`
`status {enable | disable}`	Enable to send log messages to a remote Syslog server or FortiAnalyzer unit.	`disable`
`virus-log-status {enable | disable}`	Enable to log all antivirus events.	`disable`

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 Added `encryption-log-status` variable.

Related topics

- config log setting local
- config log alertemail recipient
- config log alertemail setting

log setting local

Use this command to configure storing log messages to the local hard disk.

Syntax

```
config log setting local
  set antispam-log-status {enable | disable}
  set antivirus-log-status {enable | disable}
  set disk-full {overwrite | nolog}
  set encryption-log-status {enable | disable}
  set event-log-category {admin configuration ha | imap pop3 smtp system
     update webmail}
  set event-log-status {enable | disable}
  set history-log-status {enable | disable}
  set loglevel {alert | critical | debug | emergency | error | information |
     notification | warning}
  set rotation-hour <hour_int>
  set rotation-size <file-size_int>
  set rotation-period <days_int>
  set status {enable | disable}
end
```

Variable	Description	Default
`antispam-log-status {enable | disable}`	Enable to log all antispam events.	`enable`
`antivirus-log-status {enable | disable}`	Enable to log all antivirus events.	`enable`
`disk-full {overwrite | nolog}`	Enter the action the FortiMail unit will perform when the local disk is full and a new log message is caused. • `overwrite`: Delete the oldest log file in order to free disk space, and store the new log message. • `nolog`: Discard the new log message.	`overwrite`
`encryption-log-status {enable | disable}`	Enable to log all IBE events.	`enable`
`event-log-category {admin configuration ha | imap pop3 smtp system update webmail}`	Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space. • `admin`: Log all administrative events, such as logins, resets, and configuration updates. • `configuration`: Enable to log configuration changes. • `ha`: Log all high availability (HA) activity. • `imap`: Log all IMAP events. • `pop3`: Log all POP3 events. • `smtp`: Log all SMTP relay or proxy events. • `system`: Log all system-related events, such as rebooting the FortiMail unit. • `update`: Log both successful and unsuccessful attempts to download FortiGuard updates. • `webmail`: Log all FortiMail webmail events.	No default.
`event-log-status {enable | disable}`	Enable or disable event logging to the local hard disk.	`enable`

Variable	Description	Default
history-log-status {enable | disable}	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	disable
loglevel {alert | critical | debug | emergency | error | information | notification | warning}	Type one of the following severity levels: • alert • critical • debug • emergency • error • information • notification • warning This log destination will receive log messages greater than or equal to this severity level.	information
rotation-hour <hour_int>	Enter the hour of the day when the rotation should start.	0
rotation-size <file-size_int>	Enter the maximum size of the current log file in megabytes (MB). When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started). The maximum allowed size is 1,000 MB	10
rotation-period <days_int>	Enter the maximum age of the current log file in days. When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started).	10
status {enable | disable}	Enable to send log types which are enabled to the local hard disk.	enable

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	Added encryption-log-status variable.
v4.0 MR1 Patch 1	Added rotation-hour <hour>, renamed rotation-time to rotation-period.

Related topics

- config log setting remote
- config log alertemail recipient
- config log alertemail setting

log alertemail recipient

Use this command to add up to 3 email addresses that will receive alerts.

Before the FortiMail unit can send alert email messages, you must configure it with one or more recipients.

You must also configure which categories of events will cause the FortiMail unit to send alert email message. For more information, see “config log alertemail setting” on page 87.

Syntax

```
config log alertemail recipient
  edit <recipient_email>
  next
end
```

Variable	Description	Default
<recipient_email>	Type an email address that will receive alert email.	No default.

Example

The following example configures alert email to be sent to three email addresses.

```
config log alertemail recipient
  edit admin@example.com
  next
  edit support@example.com
  next
  edit helpdesk@example.com
  next
end
```

History

FortiMail v4.0 New.

Related topics

- config log setting remote
- config log setting local
- config log alertemail setting

log alertemail setting

Use this command to configure which events will cause the FortiMail unit to send an alert email message.

Before the FortiMail unit can send an alert email message, you must select the event or events that will cause it to send an alert.

You must also configure alert email message recipients. For more information, see “log alertemail recipient” on page 86.

Syntax

```
config log alertemail setting
  set categories {archivefailure critical deferq dictionary diskfull ha
     incidents quotafull systemquarantine}
  set deferq-interval <interval_int>
  set deferq-trigger <trigger_int>
end
```

Variable	Description	Default
`categories {archivefailure critical deferq dictionary diskfull ha incidents quotafull systemquarantine}`	Enter a list of one or more of the following event types that will cause alert email: • `archivefailure`: Email archiving to the remote host has failed. • `critical`: The FortiMail unit has detected a system error. • `deferq`: The deferred mail queue has exceeded the number of messages during the interval specified in deferq-interval <interval_int> and deferq-trigger <trigger_int>. • `dictionary`: The dictionary database is corrupt. • `diskfull`: The FortiMail unit’s hard disk is full. • `ha`: A high availability (HA) event such as failover has occurred. • `incidents`: The FortiMail unit has detected a virus. Separate each option with a space. • `quotafull`: An email user account has reached its disk space quota. • `systemquarantine`: The system quarantine has reached its disk space quota.	`critical`
`deferq-interval <interval_int>`	Enter the interval in minutes between checks of deferred queue size. This can be any number greater than zero.	`30`
`deferq-trigger <trigger_int>`	Enter the size that the deferred email queue must reach to cause an alert email to be sent. The valid range is 1 to 99999.	`10000`

History

FortiMail v4.0 New.

Related topics

- config log setting remote
- config log setting local
- config log alertemail recipient

mailsetting proxy-smtp

Use this command to configure how the FortiMail unit will handle traffic arriving on each of its network interfaces.

Proxy and built-in MTA behaviors are configured separately based upon whether the SMTP connection is considered to be incoming or outgoing. Because a network connection considers the network layer rather than the application layer when deciding whether to intercept a connection, the concept of incoming and outgoing connections is based upon slightly different things than that of incoming and outgoing email messages: directionality is determined by IP addresses of connecting clients and servers, rather than the email addresses of recipients.

- **Incoming connections** consist of those destined for the SMTP servers that are protected domains of the FortiMail unit. For example, if the FortiMail unit is configured to protect the SMTP server whose IP address is 10.1.1.1, the FortiMail unit treats all SMTP connections destined for 10.1.1.1 as incoming. For information about configuring protected domains, see "config config domain-setting" on page 51.
- **Outgoing connections** consist of those destined for SMTP servers that the FortiMail unit has not been configured to protect. For example, if the FortiMail unit is ***not*** configured to protect the SMTP server whose IP address is 192.168.1.1, all SMTP connections destined for 192.168.1.1 will be treated as outgoing, regardless of their origin.

This command applies only if the FortiMail unit is operating in transparent mode.

Syntax

```
config mailsetting proxy-smtp
  set incoming-mode <port_name_str> {pass-through | drop | proxy}
  set local <port_name_str> {enable | disable}
  set outgoing-mode <port_name_str> {pass-through | drop | proxy}
  set proxy-original {enable | disable}auth-username <user_str>
end
```

Variable	Description	Default
`incoming-mode <port_name_str> {pass-through | drop | proxy}`	Enter the name of the network interface to configure how the FortiMail unit handles incoming connections arriving on it. Then enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are *incoming* to the IP addresses of email servers belonging to a protected domain: • `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • `drop`: Drop the connection. • `proxy`: Proxy or relay the connection. Once intercepted, policies determine any further scanning or logging actions. For more information, see "config policy ip" on page 104, "config policy recipient" on page 106, and "config config policy recipient" on page 60 **Note:** Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered `proxy` more than once for each interface and/or directionality. For an example, see the *FortiMail Administration Guide*.	`proxy`
`local <port_name_str> {enable | disable}`	Enter the name of the network interface to accept connections destined for the FortiMail unit itself, such as quarantine release or delete messages and Bayesian training messages. Then enable to allow connections destined for the FortiMail unit itself.	`disable`

Variable	Description	Default
`outgoing-mode <port_name_str> {pass-through | drop | proxy}`	Enter the name of the network interface to configure how the FortiMail unit handles outgoing connections arriving on it. Then enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are *incoming* to the IP addresses of email servers belonging to a protected domain: • `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • `drop`: Drop connections. • `proxy`: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see "config policy ip" on page 104. **Note:** Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered `proxy` more than once for each interface and/or directionality. For an example, see the *FortiMail Administration Guide*.	`pass-through`
`proxy-original {enable | disable}`	Enable to, for outgoing SMTP connections, use the outgoing proxy instead of the built-in MTA. This allows the client to send email using the SMTP server that they specify, rather than enforcing the use of the FortiMail unit's own built-in MTA. The outgoing proxy will refuse the connection if the client's specified destination SMTP server is not available. In addition, it will not queue email from the SMTP client, and if the client does not successfully complete the connection, the outgoing proxy will simply drop the connection, and will not retry. Disable to relay email using the built-in MTA to either the SMTP relay defined in "config mailsetting relayserver" on page 90, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (`RCPT TO:`) domain. The email may not actually travel through the unprotected SMTP server, even though it was the relay originally specified by the SMTP client. For details, see the *FortiMail Administration Guide*. **Caution:** If this option is enabled, consider also enabling `session-prevent-open-relay {enable | disable}`. Failure to do so could allow clients to use open relays. **Note:** If this option is disabled, and an SMTP client is configured to authenticate, you must configure and apply an authentication profile. Without the profile, authentication with the built-in MTA will fail. Also, the mail server must be explicitly configured to allow relay in this case. **Note:** If this option is enabled, you will not be able to use IP pools. For more information, see "config profile ip-pool" on page 134. **Note:** For security reasons, this option does not apply if there is no session profile selected in the applicable IP-based policy. For more information on configuring IP policies, see "config policy ip" on page 104.	`disable`

History

FortiMail v4.0 New.

Related topics

- config mailsetting relayserver
- config mailsetting storage config
- config mailsetting storage central-quarantine
- config mailsetting storage systemquarantine
- diagnose debug application smtpproxy

mailsetting relayserver

Use this command to configure the FortiMail unit's built-in MTA's connection to an SMTP relay, if any, to which the FortiMail unit will relay outgoing email.

This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.

If the SMTP relay's domain name resolves to more than one IP address, for each SMTP session, the FortiMail unit will randomly select one of the IP addresses from the result of the DNS query, effectively load balancing between the SMTP relays.

If you do not configure a relay server, for outgoing email delivered by the built-in MTA, the FortiMail unit will instead query the DNS server for the MX record of the mail domain in the recipient's email address (`RCPT TO:`), and relay the email directly to that mail gateway. For details, see the *FortiMail Administration Guide*.

Note: This option will be ignored for email that matches an antispam or content profile where you have enabled `alternate-host {<relay_fqdn> | <relay_ipv4>}`.

Syntax

```
config mailsetting relayserver
  set auth-password <password_str>
  set auth-status {enable | disable}
  set auth-type {auto | plain | login | digest-md5 | cram-md5}
  set auth-username <user_str>
  set server-name <relay_fqdn>
  set server-port <port_int>
  set smtps {enable | disable}
end
```

Variable	Description	Default
`auth-password <password_str>`	If auth-status {enable | disable} is `enable`, enter the password of the FortiMail unit's user account on the SMTP relay.	No default.
`auth-status {enable | disable}`	Enable if the SMTP relay requires authentication using the SMTP `AUTH` command. Also configure `auth-username <user_str>`, `auth-password <password_str>`, and `auth-type {auto | plain | login | digest-md5 | cram-md5}`.	`disable`
`auth-type {auto | plain | login | digest-md5 | cram-md5}`	If auth-status {enable | disable} is `enable`, enter either the SMTP authentication type required by the SMTP relay when the FortiMail unit sends the ESMTP `AUTH` command, or enter `auto` to automatically detect and use the most secure authentication type supported by the relay server.	`auto`
`auth-username <user_str>`	If auth-status {enable | disable} is `enable`, enter the name of the FortiMail unit's user account on the SMTP relay.	No default.
`server-name <relay_fqdn>`	Enter the fully qualified domain name (FQDN) of the SMTP relay.	No default.
`server-port <port_int>`	Enter the TCP port number on which the SMTP relay listens.	`25`
`smtps {enable | disable}`	Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiMail unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.	`disable`

History

FortiMail v4.0 New.

Related topics

- config mailsetting proxy-smtp
- config mailsetting storage config
- config mailsetting storage central-quarantine
- config mailsetting storage systemquarantine

mailsetting storage config

Use these commands to configure the FortiMail unit to store mail data such as queues and email user mailboxes either on its local hard disks, or on a network file storage (NFS or ISCSI) server.

If the FortiMail unit is operating in an HA group, remote storage may be required or recommended. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config mailsetting storage config
  set encryption-key
  set host <host_str>
  set iscsi-id <id_str>
  set password <password_str>
  set port <port_int>
  set protocol {nfs | iscsi_server}
  set type {local | remote}
  set username <user-name_str>
end
```

Variable	Description	Default
encryption-key	Enter the key that will be used to encrypt data stored on the ISCSI server. Valid key lengths are between 6 and 64 single-byte characters. Applies only when protocol is iscsi_server.	
folder <folder_str>	Enter the directory path of the NFS export on the NAS server where the FortiMail unit will store email. Applies only when protocol is nfs.	
host <host_str>	Enter the IP address or fully qualified domain name (FQDN) of the NFS or ISCSI server.	
iscsi-id <id_str>	Enter the ISCSI identifier in the format expected by the ISCSI server, such as an ISCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA). Applies only when protocol is iscsi_server.	
password <password_str>	Enter the password of the FortiMail unit's account on the ISCSI server.	
port <port_int>	Enter the TCP port number on which the NFS or ISCSI server listens for connections.	0
protocol {nfs | iscsi_server}	Select the type of the NAS server: nfs: A network file system (NFS) server. If you select this option, enter the following information: iscsi_server: An Internet SCSI (Small Computer System Interface), also called iSCSI, server. If you select this option, enter the following information:	nfs
type {local | remote}	Select whether to store email locally or on an NFS server.	local
username <user-name_str>	Enter the user name of the FortiMail unit's account on the ISCSI server.	

History

FortiMail v4.0 MR1 New.

Related topics

- config mailsetting proxy-smtp
- config mailsetting relayserver
- config mailsetting storage central-quarantine
- config mailsetting storage systemquarantine

mailsetting storage central-quarantine

Use this command to configure centralized storage of quarantined email.

To reduce the storage resources required on lower-end FortiMail units, you can configure them to store quarantined email on a high-end FortiMail unit that you have configured to act as a centralized quarantine server.

Syntax

```
config mailsetting storage central-quarantine
  set remote-storage-type {disable | from-client | to-server-plain
     | unknown | to-server-over-ssl}
  set client-ip <client_ipv4>
  set server-name <name_str>
  set server-host <server_ipv4>
end
```

Variable	Description	Default
`remote-storage-type {disable | from-client | to-server-plain | unknown | to-server-over-ssl}`	Enter one of the following centralized quarantine types: • `disable`: Centralized quarantine storage is disabled. The FortiMail unit stores its quarantines locally, on its own hard disks. • `from-client`: This FortiMail unit connects as a client to a high-end FortiMail unit that acts as a central quarantine server. Also configure the `client-ip <client_ipv4>` of the remote central quarantine server. • `to-server-plain`: This FortiMail unit acts as a central quarantine server. Also configure `server-name <name_str>` and `server-host <server_ipv4>` for each client that you want to allow. This option is available only on high-end model FortiMail units. • `unknown`: Centralized quarantine storage is unknown. • `to-server-over-ssl`: Same as `to-server-plain`, except the connection uses SSL.	`disable`
`client-ip <client_ipv4>`	Enter the IP address of the FortiMail unit that is acting as a client. This variable applies only if `remote-storage-type` is `from-client`.	No default.
`server-name <name_str>`	Enter the name of the FortiMail unit that is acting as the central quarantine server. This name may be the host name or any other name that uniquely identifies the central quarantine server. This variable applies only if `remote-storage-type` is `to-server`.	No default.
`server-host <server_ipv4>`	Enter the IP address of the FortiMail unit that is acting as the central quarantine server. This variable applies only if `remote-storage-type` is `to-server`.	No default.

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	The to-server option for remote-storage-type now has two variations, `to-server-plain` and `to-server-over-ssl`.

Related topics

- config mailsetting proxy-smtp
- config mailsetting relayserver
- config mailsetting storage config
- config mailsetting storage systemquarantine

- config mailsetting storage central-ibe

mailsetting storage central-ibe

Use this command to configure storage of IBE encrypted email.

To reduce the storage resources required on lower-end FortiMail units, you can configure them to store encrypted email on a high-end FortiMail unit that you have configured to act as a centralized storage server.

Syntax

```
config mailsetting storage central-ibe
  set remote-storage-type {disable | from-client | to-server-over-ssl}
  set client-ip <client_ipv4>
  set server-name <name_str>
  set server-host <server_ipv4>
end
```

Variable	Description	Default
`remote-storage-type {disable | from-client | to-server-over-ssl}`	Enter one of the following centralized IBE types: • `disable`: Centralized IBE storage is disabled. The FortiMail unit stores its IBE messages locally, on its own hard disks. • `from-client`: This FortiMail unit connects as a client to a high-end FortiMail unit that acts as a central IBE storage server. Also configure the `client-ip <client_ipv4>` of the remote central IBE storage server. • `to-server-over-ssl`: This FortiMail unit acts as a central IBE storage server. Also configure `server-name <name_str>` and `server-host <server_ipv4>` for each client that you want to allow. This option is available only on high-end model FortiMail units.	`disable`
`client-ip <client_ipv4>`	Enter the IP address of the FortiMail unit that is acting as a client. This variable applies only if `remote-storage-type` is `from-client`.	No default.
`server-name <name_str>`	Enter the name of the FortiMail unit that is acting as the central IBE storage server. This name may be the host name or any other name that uniquely identifies the central quarantine server. This variable applies only if `remote-storage-type` is `to-server`.	No default.
`server-host <server_ipv4>`	Enter the IP address of the FortiMail unit that is acting as the central IBE storage server. This variable applies only if `remote-storage-type` is `to-server`.	No default.

History

FortiMail v4.0 MR1 New.

Related topics

- config mailsetting proxy-smtp
- config mailsetting relayserver
- config mailsetting storage config
- config mailsetting storage central-quarantine
- config mailsetting storage systemquarantine

mailsetting storage systemquarantine

Use this command to configure the system quarantine disk space quota, rotation size and time, forward email address, and system quarantine administrator account.

For more information on the system quarantine administrator account, see the *FortiMail Administration Guide*.

Syntax

```
config mailsetting storage systemquarantine
  set account <name_str>
  set password <password_str>
  set forward-address <recipient_str>
  set quota <quota_int>
  set quotafull {overwrite | noquarantine}
  set rotatesize <size_int>
  set rotatetime <time_int>
end
```

Variable	Description	Default
account <name_str>	Enter the name for the system quarantine administrator account. Surround the account name with single quotes.	systemquarantine
password <password_str>	Enter the password for the system quarantine administrator account. Surround the password with single quotes. The password may be entered either literally, or as a pre-encoded string prefixed with "Enc ". For example, you might enter either: • systemquarantine • 'Enc XXmkN/Q7euFe+yfBweeuLXgnv7SiSfsBsOZ6pffiYZ4dQvrxkKJvk5rNCiq7TwUEg7HUhCVGFOvyYNQ7MJhjk8ZCB94pIqdrjFv5ub/WMLDuF4Z5'	forti12356net
forward-address <recipient_str>	Enter an email address to which all messages diverted to the system quarantine will be copied. Surround the email address with single quotes.	
quota <quota_int>	Enter the amount of disk space, in gigabytes, the system quarantine may use. The maximum permitted disk quota depends on available disk capacity.	5
quotafull {overwrite | noquarantine}	Enter the action the FortiMail unit should take when the system quarantine reaches its quota size and an additional quarantined email message arrives, either: • overwrite: Delete the oldest quarantined email message to make space in the quarantine and store the new email message. • noquarantine: Discard additional email.	overwrite
rotatesize <size_int>	Enter the maximum size of the current system quarantine folder ("Inbox"). When the folder reaches this size, the FortiMail unit renames the current folder based upon its creation date and rename date, and creates a new "Inbox" folder. Alternatively or additionally configure rotatetime <time_int>.	100
rotatetime <time_int>	Enter the maximum amount of time that the current system quarantine folder ("Inbox") will be used. When the folder reaches this size, the FortiMail unit renames the current folder based upon its creation date and rename date, and creates a new "Inbox" folder. Alternatively or additionally configure rotatesize <size_int>. The valid range is from 1 to 365 days.	1

History

FortiMail v4.0 New.

Related topics

- config mailsetting proxy-smtp
- config mailsetting relayserver
- config mailsetting storage config
- config mailsetting storage central-quarantine

policy access-control receive

Use this command to configure access control rules that apply to SMTP sessions being ***received*** by the FortiMail unit.

Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages for SMTP sessions that are initiated by SMTP clients.

When an SMTP client attempts to deliver email through the FortiMail unit, the FortiMail unit compares each access control rule to the commands used by the SMTP client during the SMTP session, such as the envelope's sender email address (`MAIL FROM:`), recipient email address (`RCPT TO:`), authentication (`AUTH`), and TLS (`STARTTLS`). Rules are evaluated for a match in the order of their list sequence, from top to bottom. If all the attributes of a rule match, the FortiMail unit applies the action selected in the matching rule to the SMTP session, and no subsequent access control rules are applied.

Only one access control rule is ever applied to any given SMTP session.

Note: If no access control rules are configured, or no matching access control rules exist, ***and*** if the SMTP client is not configured to authenticate, the FortiMail unit will perform the default action, which varies by whether or not the recipient email address in the envelope (`RCPT TO:`) is a member of a protected domain.

- For protected domains, the default action is *RELAY*.
- For ***un***protected domains, the default action is *REJECT*.

Without any configured access control rules, the FortiMail unit's access control prevents SMTP clients from using your protected server or FortiMail unit as an open relay: senders can deliver email incoming to protected domains, but cannot deliver email outgoing to unprotected domains.

If you want to allow SMTP clients such as your email users or email servers to send email to unprotected domains, you must configure at least one access control rule.

You may need to configure additional access control rules if, for example, you want to:

- discard or reject email from or to some email addresses, such as email addresses that no longer exist in your protected domain
- discard or reject email from some SMTP clients, such as a spammer that is not yet known to blacklists

Like IP-based policies, access control rules can reject connections based upon 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 upon the IP address of the SMTP server. (By the nature of how the ACL controls access to or through the FortiMail unit, the SMTP server is always the FortiMail unit itself, ***unless*** the FortiMail unit is operating in transparent mode.) For more information on IP-based policies, see the *FortiMail Administration Guide*.

Syntax

```
config policy access-control receive
  edit <rule_id>
    set action {bypass | discard | reject | relay}
    set authenticated {any | authenticated | not-authenticated}
    set recipient-pattern <pattern_str>
    set recipient-pattern-regexp {yes | no}
    set reverse-dns-pattern <pattern_str>
    set reverse-dns-pattern-regexp {yes | no}
    set sender-ip-mask <ip&netmask_str>
    set sender-pattern <pattern_str>
```

```
    set sender-pattern-regexp {yes | no}
    set status {enable | disable}
    set tls-profile <profile_str>
end
```

Variable	Description	Default
<rule_id>	Enter the number identifying the rule.	
action {bypass | discard | reject | relay}	Enter the action the FortiMail unit will perform for SMTP sessions matching this access control rule. • bypass:Relay or proxy and deliver the email, ***but***, if the sender or recipient belongs to a protected domain, bypass all antispam profile processing. Antivirus, content and other scans will still occur. • discard: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client. • reject: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (Relaying denied). • relay: Relay or proxy, process, and deliver the email normally if it passes all configured scans.	relay
authenticated {any | authenticated | not-authenticated}	Enter a value to indicate whether this rule applies only to messages delivered by clients that have authenticated with the FortiMail unit. • any: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit. • authenticated: Match this access control rule only for clients that have authenticated with the FortiMail unit. • not-authenticated: Match this access control rule only for clients that have ***not*** authenticated with the FortiMail unit.	authenti_ cated
recipient-pattern <pattern_str>	Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as \'*\').	*
recipient-pattern-regexp {yes | no}	Enter yes to use regular expression syntax instead of wildcards to specify the recipient pattern.	no
reverse-dns-pattern <pattern_str>	Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message. Because domain names in the SMTP session are self-reported by the connecting SMTP server and easy to fake, the FortiMail unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail does a DNS lookup using the SMTP server's IP address. The resulting domain name is compared to the reverse DNS pattern for a match. If the reverse DNS query fails, the access control rule match will also fail. If no other access control rule matches, the connection will be rejected with SMTP reply code 550 (Relaying denied). Wildcard characters allow you to enter partial patterns that can match multiple reverse DNS lookup results. An asterisk (*) represents one or more characters; a question mark (?) represents any single character. For example, the recipient pattern mail*.com will match messages delivered by an SMTP server whose domain name starts with "mail" and ends with ".com". **Note:** Reverse DNS queries for access control rules require that the domain name be a valid top level domain (TLD). For example, ".lab" is not a valid top level domain name, and thus the FortiMail unit cannot successfully perform a reverse DNS query for it.	*
reverse-dns-pattern-regexp {yes | no}	Enter yes to use regular expression syntax instead of wildcards to specify the reverse DNS pattern.	no

Variable	Description	Default
`sender-ip-mask <ip&netmask_str>`	Enter the IP address and netmask of the SMTP client attempting to deliver the email message. Use the netmask, the portion after the slash (`/`), to specify the matching subnet. For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as *10.10.10.0/24* in the access control rule table, with the `0` indicating that any value is matched in that position of the address. Similarly, `10.10.10.10/32` will appear as 10.10.10.10/32 and match only the 10.10.10.10 address. To match any address, enter `0.0.0.0/0`.	`0.0.0.0` `0.0.0.0`
`sender-pattern <pattern_str>`	Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*\'`).	`*`
`sender-pattern-regexp {yes | no}`	Enter `yes` to use regular expression syntax instead of wildcards to specify the sender pattern.	`no`
`status {enable | disable}`	Enter `enable` to activate this rule.	`enable`
`tls-profile <profile_str>`	Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile. • If the attributes match, the access control action is executed. • If the attributes do ***not*** match, the FortiMail unit performs the *Failure* action configured in the TLS profile. For more information on TLS profiles, see the *FortiMail Administration Guide*.	

History

FortiMail v4.0 New.

Related topics

- config policy access-control delivery
- config policy ip
- config policy recipient

policy access-control delivery

Use this command to configure delivery rules that apply to SMTP sessions being ***initiated*** by the FortiMail unit in order to deliver email.

Delivery rules enable you to require TLS for the SMTP sessions the FortiMail unit initiates when sending email to other email servers. They also enable you to apply identity-based encryption (IBE) in the form of secure MIME (S/MIME).

When initiating an SMTP session, the FortiMail unit compares each delivery rule to the domain name portion of the envelope recipient address (`RCPT TO:`), and to the IP address of the SMTP server receiving the connection. Rules are evaluated for a match in the order of their list sequence, from top to bottom. If a matching delivery rule does not exist, the email message is delivered. If a match is found, the FortiMail unit compares the TLS profile settings to the connection attributes and the email message is sent or the connection is not allowed, depending on the result; if an encryption profile is selected, its settings are applied. No subsequent delivery rules are applied. Only one delivery rule is ever applied to any given SMTP session.

Syntax

```
config policy access-control delivery
  edit <rule_id>
    set destination <ip&netmask_str>
    set encryption-profile <profile_str>
    set recipient-pattern <pattern_str>
    set sender-pattern <pattern_str>
    set status {enable | disable}
    set tls-profile <profile_str>
end
```

Variable	Description	Default
`<rule_id>`	Enter the number identifying the rule.	
`destination <ip&netmask_str>`	Enter the IP address and netmask of the system to which the FortiMail unit is sending the email message. Use the netmask, the portion after the slash (`/`) to specify the matching subnet. For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as *10.10.10.0/24* in the access control rule table, with the `0` indicating that any value is matched in that position of the address. Similarly, `10.10.10.10/32` will appear as *10.10.10.10/32* and match only the 10.10.10.10 address. To match any address, enter `0.0.0.0/0`.	`0.0.0.0` `0.0.0.0`
`encryption-profile <profile_str>`	Enter an encryption profile to apply identity-based encryption, if a corresponding sender identity exists in the certificate bindings. For more information on encryption profiles, see the *FortiMail Administration Guide*.	
`recipient-pattern <pattern_str>`	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 and 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.	

Variable	Description	Default
`sender-pattern <pattern_str>`	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 and 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.	
`status {enable | disable}`	Enter `enable` to activate this rule.	`disable`
`tls-profile <profile_str>`	Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile. • If the attributes match, the access control action is executed. • If the attributes do ***not*** match, the FortiMail unit performs the *Failure* action configured in the TLS profile. For more information on TLS profiles, see the *FortiMail Administration Guide*.	

History

FortiMail v4.0 New.

Related topics

- config policy access-control receive
- config policy ip
- config policy recipient

policy ip

Use this command to create policies that apply profiles to SMTP connections based upon the IP addresses of SMTP clients and/or servers.

Syntax

```
config policy ip
  edit <policy_int>
    set action {reject | scan | temp-fail}
    set client <client_ipv4mask>
    set exclusive {enable | disable}
    set profile-antispam <antispam-profile_name>
    set profile-antivirus <antivirus-profile_name>
    set profile-auth-type {imap | ldap | none | pop3 | radius | smtp}
    set profile-content <content-profile_name>
    set profile-ip-pool <ip-pool_name>
    set profile-session <session-profile_name>
    set server <smtp-server_ipv4mask>
    set server-ip-pool <ip-pool_str>
    set server-type {ip-address | ip-pool}
    set smtp-diff-identity {enable | disable}
    set status {enable | disable}
    set use-for-smtp-auth {enable | disable}
end
```

Variable	Description	Default
<policy_int>	Enter the index number of the IP-based policy.	
action {reject | scan | temp-fail}	Enter an action for this policy: • 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 indicate a temporary failure.	scan
client <client_ipv4mask>	Enter the IP address and subnet mask of the SMTP client to whose connections this policy will apply. To match all clients, enter 0.0.0.0/0.	192.168.224.15 255.255.255.255
exclusive {enable | disable}	Enable to omit evaluation of matches with recipient-based policies, causing the FortiMail unit to disregard applicable recipient-based policies and apply only the IP-based policy. Disable to apply any matching recipient-based policy in addition to the IP-based policy. Any profiles selected in the recipient-based policy will override those selected in the IP-based policy.	disable
profile-antispam <antispam-profile_name>	Enter the name of an outgoing antispam profile, if any, that this policy will apply.	
profile-antivirus <antivirus-profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-type {imap | ldap | none | pop3 | radius | smtp}	Enter the type of the authentication profile that this policy will apply. The command profile-auth-<auth_type> appears for the type chosen. Enter the name of an authentication profile for the type.	

Variable	Description	Default
profile-content <content-profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	
profile-ip-pool <ip-pool_name>	Enter the name of the IP pool profile that you want to apply to connections matching the policy.	
profile-session <session-profile_name>	Enter the name of the session profile that you want to apply to connections matching the policy.	
server <smtp-server_ipv4mask>	Enter the IP address and subnet mask of the SMTP server to whose connections this policy will apply. To match all servers, enter 0.0.0.0/0. This option applies only for FortiMail units operating in transparent mode. For other modes, the FortiMail unit receives the SMTP connection, and therefore acts as the server.	0.0.0.0 0.0.0.0
server-ip-pool <ip-pool_str>	Enter the name of the ip pool to whose connections this policy will apply. This option is only available when the server-type is ip-pool.	
server-type {ip-address | ip-pool}	If the FortiMail unit runs in transparent mode, enter the IP address and subnet mask of the SMTP server to whose connections this policy will apply. To match all servers, enter 0.0.0.0/0. If the FortiMail unit runs in gateway or server mode, the destination will be the FortiMail unit itself. But if you use virtual hosts on the FortiMail unit, you can specify which virtual host (IP/subnet or IP pool) the email is destined to. Otherwise, you do not have to specify the destination address. If you use virtual hosts, you must also configure the MX record to direct email to the virtual host IP addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well.	
smtp-diff-identity {enable | disable}	Enable to allow the SMTP client to send email using a different sender email address (MAIL FROM:) than the user name that they used to authenticate. Disable to require that the sender email address in the SMTP envelope match the authenticated user name.	disable
status {enable | disable}	Enable to apply this policy.	enable
use-for-smtp-auth {enable | disable}	Enable to authenticate SMTP connections using the authentication profile configured in profile-auth-type {imap | ldap | none | pop3 | radius | smtp}.	disable

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 New variables server-type and server-ip-pool.

Related topics

- config policy access-control receive
- config policy access-control delivery
- config policy recipient

policy recipient

Use this command to create recipient-based policies based on the incoming or outgoing directionality of an email message with respect to the protected domain.

Syntax

```
config policy recipient
  edit <policy_int>
    set auth-access-options {pop3 | smtp-auth | smtp-diff-identity | web}
    set certificate-required {yes | no}
    set pkiauth {enable | disable}
    set pkiuser <user_str>
    set profile-antispam <antispam-profile_name>
    set profile-antivirus <antivirus-profile_name>
    set profile-auth-type {imap | ldap | none | pop3 | radius | smtp}
    set profile-content <content-profile_name>
    set profile-ldap <profile_name>
    set recipient-domain <domain_str>
    set recipient-name <local-part_str>
    set recipient-type {ldap-group | local group| user}
    set sender-domain <domain_str>
    set sender-name <local-part_str>
    set sender-type {ldap-group | local group| user}
    set status {enable | disable}
end
```

Variable	Description	Default
<policy_int>	Enter the index number of the recipient-based policy.	
auth-access-options {pop3 | smtp-auth | smtp-diff-identity | web}	Enter the method that email users matching this policy use to retrieve the contents of their per-recipient spam quarantine. • pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine. • smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. • smtp-diff-identity: Allow email when the SMTP client authenticates with a different user name than the one that appears in the envelope's sender email address. You must also enter smtp-auth for this option to have any effect. • web: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine. **Note:** Entering 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.	
certificate-required {yes | no}	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter yes.	no
pkiauth {enable | disable}	Enable if you want to allow email users to log in to their per-recipient spam quarantine by presenting a certificate rather than a user name and password.	disable
pkiuser <user_str>	If pkiauth is enable, enter the name of a PKI user, such as 'user1'. For information on configuring PKI users, see "config user pki" on page 206.	

Variable	Description	Default
profile-antispam <antispam-profile_name>	Enter the name of an antispam profile, if any, that this policy will apply.	
profile-antivirus <antivirus-profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-type {imap | ldap | none | pop3 | radius | smtp}	Enter the type of the authentication profile that this policy will apply. The command profile-auth-<auth_type> appears for the type chosen. Enter the name of an authentication profile for the type.	none
profile-content <content-profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	
ldap_profile <ldap-profile_name>	If recipient-type or sender-type is ldap-group, enter the name of an LDAP profile in which the group owner query has been enabled and configured.	
recipient-domain <domain_str>	Enter the domain part of recipient email address to define recipient (RCPT TO:) email addresses that match this policy.	
recipient-name <local-part_str>	Enter the local part of recipient email address to define recipient (RCPT TO:) email addresses that match this policy.	
recipient-type {ldap-group | local group| user}	Enter one of the following ways to define recipient (RCPT TO:) email addresses that match this policy. If you enter ldap-group, also configure profile-ldap by entering an LDAP profile in which you have enabled and configured a group query.	user
sender-domain <domain_str>	Enter the domain part of sender email address to define sender (MAIL FROM:) email addresses that match this policy.	
sender-name <local-part_str>	Enter the local part of sender email address to define sender (MAIL FROM:) email addresses that match this policy.	
sender-type {ldap-group | local group| user}	Enter one of the following ways to define sender (MAIL FROM:) email addresses that match this policy. If you enter ldap-group, also configure profile-ldap profile-ldap by entering an LDAP profile in which you have enabled and configured a group query.	user
status {enable | disable}	Enable to apply this policy.	enable

History

FortiMail v4.0 New.

Related topics

- config policy access-control receive
- config policy access-control delivery
- config policy ip

profile antispam

Use this command to configure system-wide antispam profiles. To configure a domain-wide antispam profile, use “config profile antispam” on page 63.

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.

Antispam profiles are created and applied separately based upon the incoming or outgoing directionality of the SMTP connection or email message. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config profile antispam
  edit <profile_name>
    config bannedwords
      edit <word_str>
        set subject {enable | disable}
        set body {enable | disable}
    config dnsbl-server
      edit <server_name>
    config surbl-server
      edit <server_name>
    config whitelistwords
      edit <word_str>
        set subject {enable | disable}
        set body {enable | disable}
    set action-banned-word <action_profile>
    set action-bayesian <action-profile_name>
    set action-deep-header <action-profile_name>
    set action-default <action-profile_name>
    set action-dictionary <action-profile_name>
    set action-forged-ip <action-profile_name>
    set action-fortiguard <action-profile_name>
    set action-fortiguard-blackip <action-profile-name>
    set action-grey-list <action-profile_name>
    set action-heuristic <action-profile_name>
    set action-image-spam <action-profile_name>
    set action-rbl <action-profile_name>
    set action-spf-checking <action-profile_name>
    set action-surbl <action-profile_name>
    set action-virus <action-profile_name>
    set aggressive {enable | disable}
    set banned-word {enable | disable}
    set bayesian {enable | disable}
    set bayesian-autotraining {enable | disable}
    set bayesian-user-db {enable | disable}
    set bayesian-usertraining {enable | disable}
    set deepheader {enable | disable}
    set deepheader-analysis {enable | disable}
    set deepheader-check-ip {enable | disable}
    set dict-score <score_int>
    set dictionary {enable | disable}
```

```
    set direction {incoming | outgoing}
    set dnsbl {enable | disable}
    set forged-ip {enable | disable}
    set fortiguard-antispam {enable | disable}
    set fortiguard-check-ip {enable | disable}
    set greylist {enable | disable}
    set heuristic {enable | disable}
    set heuristic-lower <threshold_int>
    set heuristic-rules-percent <percentage_int>
    set heuristic-upper {threshold_int}
    set image-spam {enable | disable}
    set scan-bypass-on-auth {enable | disable}
    set maxsize <bytes_int>
    set scan-pdf {enable | disable}
    set spf-checking {enable | disable}
    set surbl {enable | disable}
    set virus {enable | disable}
    set whitelist-enable {enable | disable}
    set whitelist-word {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of an antispam profile.	
<word_str>	Enter the banned word to configure. Wild cards are not supported.	
subject {enable | disable}	Enable to check the subject line for the banned word.	disable
body {enable | disable}	Enable to check the message body for the banned word.	disable
<server_name>	Enter a DNSBL server name to perform a DNSBL scan. The FortiMail unit will query DNS blacklist servers.	
<server_name>	Enter a SURBL server name to perform a SURBL scan. The FortiMail unit will query SURBL servers.	
<word_str>	Enter the whitelisted word to configure. Wild cards are not supported.	
subject {enable | disable}	Enable to check the subject line for the whitelisted word.	disable
body {enable | disable}	Enable to check the message body for the whitelisted word.	disable
action-banned-word <action_profile>	Enter the action profile that you want the FortiMail unit to use if the banned word scan determines that the email is spam.	
action-bayesian <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the Bayesian scan determines that the email is spam.	
action-deep-header <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the deep header scan determines that the email is spam.	
action-default <action-profile_name>	Enter the default action profile that you want all scanners of the FortiMail unit to use. However, if you choose an action profile other than “default" for a scanner, this scanner will use the chose profile.	
action-dictionary <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam.	

Variable	Description	Default
`action-forged-ip <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the forged IP scan determines that the email is spam.	`default`
`action-fortiguard <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the FortiGuard Antispam scan determines that the email is spam.	
`action-fortiguard-blackip <action-profile-name>`	Enter the action profile that you want the FortiMail unit to use if the FortiGuard black IP scan determines that the email is spam.	
`action-grey-list <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the grey list scan determines that the email is spam.	
`action-heuristic <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam.	
`action-image-spam <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the banned word scan determines that the email is spam.	
`action-rbl <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the RBL scan determines that the email is spam.	
`action-spf-checking <action-profile_name>`	Enter the action profile you want the FortiMail unit to use if the SPF scan determines that the email is spam.	
`action-surbl <action-profile_name>`	Enter the action profile that you want the FortiMail unit to use if the SURBL scan determines that the email is spam.	
`action-virus <action-profile_name>`	Enter the action profile that requires the FortiMail unit to treat messages with viruses as spam.	
`aggressive {enable | disable}`	Enable this option to examine file attachments in addition to embedded images. To improve performance, enable this option only if you do not have a satisfactory spam detection rate.	`disable`
`banned-word {enable | disable}`	Enable this option to scan banned words for this antispam profile.	`disable`
`bayesian {enable | disable}`	Enable this option to activate Bayesian scan for this antispam profile.	`disable`
`bayesian-autotraining {enable | disable}`	Enable to use FortiGuard Antispam and SURBL scan results to train per-user Bayesian databases that are not yet mature (that is, they have not yet been trained with 200 legitimate email and 100 spam in order to recognize spam).	`enable`
`bayesian-user-db {enable | disable}`	Enable to use per-user Bayesian databases. If disabled, the Bayesian scan will use either the global or the per-domain Bayesian database, whichever is selected for the protected domain.	`disable`
`bayesian-usertraining {enable | disable}`	Enable to accept email forwarded from email users to the Bayesian control email addresses in order to train the Bayesian databases to recognize spam and legitimate email.	`enable`
`deepheader {enable | disable}`	Enable to perform extensive inspection of message headers.	`disable`

Variable	Description	Default
deepheader-analysis {enable | disable}	Enable to inspect all message headers for known spam characteristics. If the FortiGuard Antispam scan is enabled, this option uses results from that scan, providing up-to-date header analysis.	disable
deepheader-check-ip {enable | disable}	Enable to query for the blacklist status of the IP addresses of all SMTP servers appearing in the Received: lines of header lines. If this option is disabled, the FortiMail unit checks only the IP address of the current SMTP client. This option applies only if you have also configured either or both FortiGuard Antispam scan and DNSBL scan.	disable
dict-score <score_int>	Enter the number of dictionary term matches above which the email will be considered to be spam.	
dictionary {enable | disable}	Enable to perform a dictionary scan for this profile.	disable
direction {incoming | outgoing}	Enter Incoming for a profile that can be used by an incoming policy, or Outgoing for a profile that can be used by an outgoing policy. This option is not available when configuring an antispam profile for a domain.	incoming
dnsbl {enable | disable}	Enable to perform a DNSBL scan for this profile.	disable
forged-ip {enable | disable}	Enable to perform a forged IP address scan. This scan converts the SMTP client's IP address to a fully qualified domain name (FQDN) and compare the IP addresses returned from a reverse DNS lookup of the FQDN to the SMTP client's IP address. If the reverse DNS lookup results do not contain the SMTP client's IP address, the FortiMail unit treats the email message as spam.	disable
fortiguard-antispam {enable | disable}	Enable to let the FortiMail unit query the FortiGuard Antispam service to determine if any of the uniform resource identifiers (URI) in the message body are associated with spam. If any URI is blacklisted, the FortiMail unit considers the email to be spam, and you can select the action that the FortiMail unit will perform.	disable
fortiguard-check-ip {enable | disable}	Enable to include whether or not the IP address of the SMTP client is blacklisted in the FortiGuard Antispam query.	disable
greylist {enable | disable}	Enable to perform a greylist scan.	disable
heuristic {enable | disable}	Enable to perform a heuristic scan.	disable
heuristic-lower <threshold_int>	Enter the score equal to or below which the FortiMail unit considers an email to ***not*** be spam.	-20.000000
heuristic-rules-percent <percentage_int>	Enter the percentage of the total number of heuristic rules that will be used to calculate the heuristic score for an email message. The FortiMail unit compares this total score to the upper and lower level threshold to determine if an email is: • spam • not spam • indeterminable (score is between the upper and lower level thresholds) To improve system performance and resource efficiency, enter the lowest percentage of heuristic rules that results in a satisfactory spam detection rate.	100
heuristic-upper {threshold_int}	Enter the score equal to or above which the FortiMail unit considers an email to be spam.	10.000000
image-spam {enable | disable}	Enable to perform an image spam scan.	disable

Variable	Description	Default
`scan-bypass-on-auth {enable | disable}`	Enable to omit antispam scans when an SMTP sender is authenticated.	`disable`
`maxsize <bytes_int>`	Enter the maximum size, in bytes, that the FortiMail unit will scan for spam. Messages exceeding the limit will not be scanned for spam. To scan all email regardless of size, enter `0`.	`0`
`scan-pdf {enable | disable}`	Enable to scan the first page of PDF attachments using heuristic, banned word, and image spam scans, if they are enabled.	`disable`
`spf-checking {enable | disable}`	Enable to have the FortiMail unit perform the action configured in this antispam profile, instead of the action configured in the session profile. See "spf-validation {enable | disable}" on page 154.	`disable`
`surbl {enable | disable}`	Enable to perform a SURBL scan.	`disable`
`virus {enable | disable}`	Enable to treat email with viruses as spam. When enabled, instead of performing the action configured in the antivirus profile, the FortiMail unit will instead perform either the general or individualized action in the antispam profile.	`disable`
`whitelist-enable {enable | disable}`	Enable to automatically update personal whitelist database from sent email.	`disable`
`whitelist-word {enable | disable}`	Enable to perform a white list word scan.	`disable`

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 New options `set spf-checking` and `set action-spf-checking`.

Related topics

- config profile antispam-action
- config profile antivirus

profile antispam-action

Use this command to configure antispam action profiles.

Syntax

```
config profile antispam-action
  edit <profile_name>
    set action {discard | none | quarantine | quarantine-review | reject |
       rewrite-rcpt}
    set alternate-host {<relay_fqdn> | <relay_ipv4>}
    set alternate-host-status {enable | disable}
    set bcc-addr <recipient_email>
    set bcc-status {enable | disable}
    set direction {incoming | outgoing}
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set subject-tagging-status {enable | disable}
    set subject-tagging-text <tag_str>
    set quarantine-report {enable | disable}
    set quarantine-days <days_int>
    set release-through-email {enable | disable}
    set release-through-web {enable | disable}
    set release-auto-whitelist {enable | disable}
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
end
```

Variable	Description	Default
<profile_name>	Enter the name of an antispam action profile.	
action {discard | none | quarantine | quarantine-review | reject | rewrite-rcpt}	Enter an action for the profile. • discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • none: Apply any configured header or subject line tags, if any. • quarantine: Enter to redirect spam to the per-recipient quarantine. For more information, see the *FortiMail Administration Guide*. This option is available only for incoming profiles. If you enter this option, also configure quarantine-report {enable | disable}, quarantine-days <days_int>, release-through-email {enable | disable}, release-through-web {enable | disable}, and release-auto-whitelist {enable | disable}. • quarantine-review: Enter to redirect spam to the system quarantine. For more information, see the *FortiMail Administration Guide*. • reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • rewrite-rcpt: Enter 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). If you enter this option, also configure rewrite-rcpt-local-type {none | prefix | replace | suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix | replace | suffix}, and rewrite-rcpt-domain-value <value_str>.	none

Variable	Description	Default
direction {incoming | outgoing}	Enter incoming for a profile that can be used by an incoming antispam profile, or outgoing for a profile that can be used by an outgoing antispam profile.	outgoing
alternate-host {<relay_fqdn> | <relay_ipv4>}	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if alternate-host-status is enable.	No default.
alternate-host-status {enable | disable}	Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> | <relay_ipv4>}. **Note:** If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore config mailsetting relayserver and the protected domain's tp-use-domain-mta {yes | no}.	disable
bcc-addr <recipient_email>	Type the BCC recipient email address. This field applies only if bcc-status is enable.	No default.
bcc-status {enable | disable}	Enable to send a blind carbon copy (BCC) of the email. Also configure bcc-addr <recipient_email>.	disable
header-insertion-name <name_str>	Enter the message header key. The FortiMail unit will add 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. See header-insertion-value <header_str>.	
header-insertion-status {enable | disable}	Enable to add a message header to detected spam. See header-insertion-value <header_str>.	disable
header-insertion-value <header_str>	Enter the message header value. 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. See header-insertion-name <name_str>.	
subject-tagging-status {enable | disable}	Enable to prepend text defined using subject-tagging-text <tag_str> ("tag") to the subject line on detected spam.	disable
subject-tagging-text <tag_str>	Enter the text that will appear 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.	
quarantine-report {enable | disable}	Enable to send a quarantine report if the quarantine report is scheduled.	disable
quarantine-days <days_int>	Enter the number of days you want to keep the quarantined email. Enter a small enough value that will prevent the size of the quarantine from exceeding the available disk space. If you enter 0 to prevent automatic deletion of quarantined files, you must periodically manually remove old files.	14

Variable	Description	Default
release-through-email {enable | disable}	Enable to allow email users to remotely release email from the quarantine by sending email to quarantine control account email addresses. For more information, see the *FortiMail Administration Guide*.	disable
release-through-web {enable | disable}	Enable to allow email users to remotely release email from the quarantine by selecting the *Release* link in a quarantine report. For more information, see the *FortiMail Administration Guide*.	disable
release-auto-whitelist {enable | disable}	Enable to, when an email user releases an email from the quarantine, automatically add the sender email address of the quarantined email to the email user's personal white list ***if*** the option is also enabled in the email user's preferences. Email users' preferences can be configured from both the *Preferences* tab of FortiMail webmail and from the web-based manager. For more information, see the *FortiMail Administration Guide*.	disable
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
rewrite-rcpt-domain-type {none-prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.	none
rewrite-rcpt-domain-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix | replace | suffix}.	

History

FortiMail v4.0 New.

Related topics

- config profile antispam

profile antivirus

Use this command to create antivirus profiles that you can select in a policy in order to scan email for viruses.

If the FortiMail unit detects a virus, it replaces the infected file with a replacement message that notifies the email user the infected file has been removed. You can customize replacement messages. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config profile antivirus
  edit <profile_name>
    set discard {enable | disable}
    set heuristic {enable | disable}
    set heuristic-discard {enable | disable}
    set heuristic-reject {enable | disable}
    set reject {enable | disable}
    set scanner {enable | disable}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the profile. To view a list of existing entries, enter a question mark (`?`).	
`discard {enable | disable}`	Enable to accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client.	`disable`
`heuristic {enable | disable}`	Enable to use heuristics when performing antivirus scanning.	`disable`
`heuristic-discard {enable | disable}`	Enable to accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client.	`disable`
`heuristic-reject {enable | disable}`	Enable to reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550.	`disable`
`reject {enable | disable}`	Enable to reject infected email and reply to the SMTP client with SMTP reply code 550.	`disable`
`scanner {enable | disable}`	Enable to perform antivirus scanning for this profile.	`disable`

History

FortiMail v4.0 New.

Related topics

- config profile antispam

profile authentication

Use this command to configure the FortiMail unit to connect to an external SMTP server in order to authenticate email users.

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS

When the FortiMail unit is operating in server mode, only local and RADIUS authentication are available.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine.

Depending on the mode in which your FortiMail unit is operating, you may be able to apply authentication profiles through incoming recipient-based policies, IP-based policies, and email user accounts.

For more information, see the *FortiMail Administration Guide*.

Syntax

```
config profile authentication imap
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication pop3
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication radius
  edit <profile_name>
    set port <port_int>
    set secret <password_str>
    set send-domain {enable | disable}
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication smtp
  edit <profile_name>
    set option {ssl secure tls senddomain}\
    set server {<fqdn_str> | <host_ipv4>}
    set port <port_int>
    set try-ldap-mailhost {enable | disable}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the profile. To view a list of existing entries, enter a question mark (`?`).	
`option {ssl secure tls senddomain}`	Enter one or more of the following in a space-delimited list: • `senddomain`: Enable if the IMAP server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application	
`port <port_int>`	Enter the TCP port number of the IMAP server. The standard port number for IMAP is 143; for SSL-secured IMAP, it is 993.	
`server {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the IMAP server.	
`option {ssl secure tls senddomain}`	If you want to enable any of the following options, enter them in a space-delimited list: • `domain`: Enable if the POP3 server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application	
`port <port_int>`	Enter the TCP port number of the POP3 server. The standard port number for POP3 is 110; for SSL-secured POP3, it is 995.	
`server {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the POP3 server.	
`port <port_int>`	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server. The standard port number for RADIUS is 1812.	`1812`
`secret <password_str>`	Enter the password for the RADIUS server.	
`send-domain {enable | disable}`	Enable if the RADIUS server requires both the user name and the domain when authenticating.	
`server {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the RADIUS server.	
`option {ssl secure tls senddomain}`	If you want to enable any of the following options, enter them in a space-delimited list: • `senddomain`: Enable if the SMTP server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application	
`server {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	

Variable	Description	Default
`port <port_int>`	Enter the TCP port number of the SMTP server. The standard port number for SMTP is 25; for SSL-secured SMTP, it is 465.	
`try-ldap-mailhost {enable | disable}`	Enable if your LDAP server has a mail host entry for the generic user If you select this option, the FortiMail unit will querry the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will querry the server you entered in the server field.	`disable`

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 New variable `try-ldap-mailhost` for `config profile authentication smtp`.

Related topics

- config profile certificate-binding
- config profile encryption

profile certificate-binding

Use this command to create certificate binding profiles, which establish the relationship between an email address and the certificate that:

- proves an individual's identity
- provides their public (and, for protected domains, private) keys for use with encryption profiles

This relationship and that information can then be used for secure MIME (S/MIME).

If an email is ***incoming*** to a protected domain and it uses S/MIME encryption, the FortiMail unit compares the sender's identity with the list of certificate bindings to determine if it has a key that can decrypt the email. If it has a matching public key, it will decrypt the email before forwarding it. If it does ***not***, it forwards the still-encrypted email to the recipient; the recipient's MUA in that case must support S/MIME and possess the sender's public key.

If an email is ***outgoing*** from a protected domain, and you have selected an encryption profile in the message delivery rule that applies to the session, the FortiMail unit compares the sender's identity with the list of certificate bindings to determine if it has a certificate and private key. If it has a matching private key, it will encrypt the email using the algorithm specified in the encryption profile. If it does ***not***, it performs the failure action indicated in the encryption profile.

Syntax

```
config profile certificate-binding
  edit <profile_id>
    set address-pattern <pattern_str>
    set key-private <key_str>
    set key-public <key_str>
    set password <pwd_str>
    set type {internal | external}
end
```

Variable	Description	Default
`<profile_id>`	Enter the ID number of the certificate binding profile.	
`address-pattern <pattern_str>`	Enter the email address or domain associated with the identity represented by the personal or server certificate.	
`key-private <key_str>`	Enter the private key associated with the identity, used to encrypt and sign email from that identity.	
`key-public <key_str>`	Enter the public key associated with the identity, used to encrypt and sign email from that identity.	
`password <pwd_str>`	Enter the password for the personal certificate files.	
`type {internal | external}`	Enter `internal` to sign and encrypt outgoing email, or `external` to validate the signature of and decrypt incoming email, using the key(s) and certificate.	`internal`

History

FortiMail v4.0 New.

Related topics

- config profile authentication
- config profile encryption

profile content

Use this command to 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.

Content profiles can be used to apply content-based encryption to email. They can also be used to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. As such, content profiles can be used both for email that you want to protect, and for email that you want to prevent.

Content profile options vary by whether the profile matches incoming or outgoing email.

Syntax

```
config profile content
  edit <profile_name>
    config attachment-name
      edit attachment-name-pattern <pattern_str>
        set status {enable | disable}
    config attachment-type
      edit attachment-type <MIME-type_str>
        set status {enable | disable}
    config monitor
      edit monitor <index_int>
        set action <profile_name>
        set dict-score <score_int>
        set dictionary-group <dictionary-group_name>
        set dictionary-profile <dictionary-profile_name>
        set dictionary-type {group | profile}
        set scan-msoffice {enable | disable}
        set scan-pdf {enable | disable}
        set status {enable | disable}
    set action-default <action_profile>
    set action-encrypted <action-profile>
    set action-image <action_profile>
    set archive-block-on-failure-to-decompress {enable | disable}
    set archive-block-password-protected {enable | disable}
    set archive-block-recursive {enable | disable}
    set archive-content-check {enable | disable}
    set archive-max-recursive-level <depth_int>
    set attachment-name-disposition {block | pass}
    set attachment-type-disposition {block | pass}
    set block-msg-fragmented {enable | disable}
    set block-msg-without-attachment {enable | disable}
    set bypass-on-auth {enable | disable}
    set defersize <threshold_int>
    set direction {incoming | outgoing}
    set filetype-<file_type> {enable | disable}
    set remove-hidden-html-content {enable | disable}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the profile. To view a list of existing entries, enter a question mark (`?`).	No default.
`attachment-name-pattern <pattern_str>`	Enter a pattern, such as `'*.bat'`, that matches the email attachment names that you want the content profile to match. The patterns include: • *.bat • *.com • *.dll • *.doc • *.exe • *.gz • *.hta • *.ppt • *.rar • *.scr • *.tar • *.tgz • *.vb? • *.wps • *.xl? • *.zip • *.pif	No default.
`status {enable | disable}`	Enable or disable a pattern that matches the email attachment names that you want the content profile to match.	`disable`

Variable	Description	Default
attachment-type <MIME-type_str>	Enter one of the following MIME types or subtypes: • video • audio • image • image-gif • image-jpeg • image-tiff • image-png • image-other: This option includes all images not specified by the other image types. • executable • executable-activex • executable-java • executable-javascript • executable-vbs • executable-vba • executable-other: This option includes all executables not specified by the other executable types. • document • document-msoffice • document-msoffice-embedded-check • document-msoffice-vba-check • document-visio • document-visio-vba-check • document-openoffice • document-openoffice-embedded-check • document-pdf • document-other: This option includes all documents not specified by the other document types. • archive • application-other: This option includes all applications not specified by the other application types. • text • text-7bit • text-html • text-xml • text-other: This option includes all text documents not specified by the other text types. • encrypted: This option includes both the S/MIME type and PGP-encrypted email.	No default.
status {enable | disable}	Enter either: • enable: Perform the action configured in"config profile content-action" on page 127. • disable: Pass the file type filter. The email will still be subject to other content profile scans that you have configured, if any. **Note:** Unlike other MIME types, archive may receive the opposite of this action, or perform an action regardless of this setting.	disable
monitor <index_int>	Enter the index number of the monitor profile. If the monitor profile does not currently exist, it will be created.	No default.
action <profile_name>	Enter the action profile for this monitor profile. The FortiMail unit will perform the actions if the content of the email message matches words or patterns from the dictionary profile that the monitor profile uses.	No default.
dict-score <score_int>	Enter the number of times that an email must match the content monitor profile before it will receive the action configured in action <profile_name>.	1

Variable	Description	Default
`dictionary-group <dictionary-group_name>`	Enter the dictionary profile group that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profiles. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in `action <profile_name>`. For information on dictionary profiles, see the *FortiMail Administration Guide*.	No default.
`dictionary-profile <dictionary-profile_name>`	Enter the dictionary profile that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profile. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in `action <profile_name>`. For information on dictionary profiles, see the *FortiMail Administration Guide*.	No default.
`dictionary-type {group | profile}`	Enter `profile` to detect content based upon a dictionary profile, or `group` to detect content based upon a group of dictionary profiles. Depending on your selection, also configure either `dictionary-group <dictionary-group_name>` or `dictionary-profile <dictionary-profile_name>`.	`group`
`scan-msoffice {enable | disable}`	Enable or disable MS Word document scanning for this profile.	`disable`
`scan-pdf {enable | disable}`	Enable or disable PDF document scanning for this profile.	`disable`
`status {enable | disable}`	Enable or disable this monitor profile.	`disable`
`action-default <action_profile>`	Enter a content action profile to be used by all the content filters except for the encrypted email, which can have its own action. See below for details.	
`action-encrypted <action-profile>`	For the encrypted email file type, you can use a content action profile to overwrite the default action profile used in the content profile. For example, if you want to redirect encrypted email to a third party box (such as a PGP Universal Server) for decryption, in the content action profile that will be used for the encrypted email, you can enable the option to deliver email to the PGP server as an alternate host.	
`action-image <action_profile>`	For the image email file type, you can use a content action profile to overwrite the default action profile used in the content profile.	
`archive-block-on-failure-to-decompress {enable | disable}`	Enter to apply the action configured in "config profile content-action" on page 127 if an attached archive cannot be successfully decompressed in order to scan its contents.	`disable`
`archive-block-password-protected {enable | disable}`	Enter to apply the action configured in"config profile content-action" on page 127 if an attached archive is password-protected.	`disable`
`archive-block-recursive {enable | disable}`	Enable to block archive attachments whose depth of nested archives exceeds `archive-max-recursive-level <depth_int>`.	`enabled`
`archive-content-check {enable | disable}`	Enter to enable consideration of the nesting depth threshold, password protection, and successful decompression when scanning attachments that are archives.	`enabled`

Variable	Description	Default
archive-max-recursive-level <depth_int>	Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email. • archive-max-recursive-level **is** 0**, or attachment's depth of nesting equals or is less than** archive-max-recursive-level: If the attachment contains a file that matches one of the other MIME file types, perform the action configured for that file type, either block or pass. • **Attachment's depth of nesting is greater than** archive-max-recursive-level: Apply the block action, unless you have disabled archive-block-recursive {enable | disable}, in which case it will pass the MIME file type content filter. Block actions are specified in the "config profile content-action" on page 127. This option applies only if archive-content-check {enable | disable} is enabled.	0
attachment-name-disposition {block | pass}	Pass or block email if a file attachment matches the file name patterns enabled in attachment-name-pattern <pattern_str>. If an attachment matches a pattern not enabled, the FortiMail unit will perform the ***opposite*** action of whatever you selected, either block or pass. For example, if you enter block and have enabled the name pattern *.exe, files whose names end in .exe will be blocked. All other file names will pass attachment filtering, but will still be subject to any other filters or antispam scans that you have configured. Conversely, if you select pass and enabled *.doc, all file names other than those ending in .doc will be blocked.	block
attachment-type-disposition {block | pass}	Block or pass email if a file attachment matches the file types enabled in attachment-type <MIME-type_str>. File types that you have not enabled will receive the action opposite of your block/pass selection. Passed file types will pass attachment file type filtering only, and will still be subject to any other content filters or antispam scans that you have configured.	block
block-msg-fragmented {enable | disable}	Enable to detect and block fragmented email. Some mail user agents, such as Outlook, are able to fragment big emails into multiple sub-messages. This is used to bypass oversize limits/scanning	disable
block-msg-without-attachment {enable | disable}	Enable to apply the block action configured in the content action profile if an email does not have any attachments.	disable
bypass-on-auth {enable | disable}	Enable to omit antispam scans when an SMTP sender is authenticated.	disable
defersize <threshold_int>	Enter the size threshold in kilobytes. Delivery of email messages greater than this size will be deferred until the period configured for oversize email. To disable deferred delivery, enter 0.	0
direction {incoming | outgoing}	Enter either incoming for a profile that can be used by an incoming policy, or outgoing for a profile that can be used by an outgoing policy.	incoming

Variable	Description	Default
`filetype-<file_type> {enable | disable}`	Enable or disable content filtering for the specified file type. If enabled, the specified action profile in the content profile will be applied against the file type. If disabled, no content action profile will be applied. But other actions in other profiles will not be bypassed.	

`remove-hidden-html-content {enable | disable}`	Enable to detect hypertext markup language (HTML) tags and, if found:
	• apply the action profile
	• add `X-FEAS-ATTACHMENT-FILTER: Contains HTML tags.` to the message headers
	This option can be used to mitigate potentially harmful HTML content such as corrupted images or files, or phishing URLs that have been specially crafted for a targeted attack, and therefore not yet identified by the FortiGuard Antispam service.
	Depending on the action profile, for example, you could warn email users by tagging email that contains potentially dangerous HTML content, or, if you have removed the HTML tags, allow users to safely read the email to decide whether or not it is legitimate first, ***without*** automatically displaying and executing potentially dangerous scripts, images, or other files. (Automatic display of HTML content is a risk on some email clients.)
	Caution: *Unless* you also select `replace` for the action in the content action profile, HTML will ***not*** be removed, and the email will ***not*** be converted to plain text. Instead, the FortiMail unit will only apply whichever other action profile "block" action you have selected.
	To actually remove HTML tags, you must also select replace.
	If you select *Replace*, all HTML tags will be removed, except for the minimum required by the HTML document type definition (DTD):
	• `<html>`
	• `<head>`
	• `<body>`
	Stripped body text will be surrounded by `<pre>` tags, which is typically rendered in a monospace font, causing the appearance to mimic plain text.
	For linked files, which are hosted on an external web site for subsequent download rather than directly attached to the email, the FortiMail unit will download and attach the file to the email ***before*** removing the `<img>` or `<embed>` tag. In this way, while the format is converted to plain text, attachments and linked files which may be relevant to the content are still preserved.
	For example, in an email that is a mixture of HTML and plain text (`Content-Type: multipart/alternative`), and if the action profile's "block" action is `replace`, the FortiMail unit would remove hyperlink, font, and other HTML tags in the sections labeled with `Content-Type: text/html`. Linked images would be converted to attachments. (The MIME `Content-Type: text/html` label itself, however, would ***not*** be modified.)
		`disable`

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	New option `set action-image`. New options `set action`, `set scan-pdf`, `set scan-msoffice` for `config monitor`.

Related topics

- config profile content-action

profile content-action

Use this command to define content action profiles.

Content action profiles can be used 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, you would 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`.

Syntax

```
config profile content-action
  edit <profile_name>
    set action {discard | encryption | none | quarantine | quarantine-
       review | reject | replace | rewrite-rcpt | treat-as-spam}
    set alternate-host {<relay_fqdn> | <relay_ipv4>}
    set alternate-host-status {enable | disable}
    set bcc-addr <recipient_email>
    set bcc-status {enable | disable}
    set encryption-profile <encryption-profile_name>
    set rewrite-rcpt-domain-type {none | prefix | replace | suffix}
    set rewrite-rcpt-domain-value <case_str>
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set direction {incoming | outgoing}
    set header-insertion-name <text_str>
    set header-insertion-value <value_str>
    set subject-tagging-text <text_str>
    set tagging type {insert-header | tag-subject}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
action {discard | encryption | none | quarantine | quarantine-review | reject | replace | rewrite-rcpt | treat-as-spam}	Enter the action that the FortiMail unit will perform if the content profile determines that an email contains prohibited words or phrases, file names, or file types. • discard: Accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • encryption: Apply an encryption profile. Also configure encryption-profile <encryption-profile_name>. • none: Apply any configured header or subject line tags, if any. • quarantine: Divert the email to the per-recipient quarantine. • quarantine-review: Divert the email to the system quarantine. • reject: Reject the email, replying with an SMTP error code to the SMTP client. • replace: Accept the email, but replace the content matching this profile with a replacement message, and, if you have enabled remove-hidden-html-content {enable | disable}, strip HTML tags. • rewrite-rcpt: Enter to change the recipient address of any email that matches the content profile. Also configure rewrite-rcpt-domain-type {none | prefix | replace | suffix}, rewrite-rcpt-domain-value <case_str>, rewrite-rcpt-local-type {none | prefix | replace | suffix}, and rewrite-rcpt-local-value <value_str>. • treat-as-spam: Apply the action selected in the incoming antispam profile.	replace
alternate-host {<relay_fqdn> | <relay_ipv4>}	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if alternate-host-status is enable.	No default.
alternate-host-status {enable | disable}	Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> | <relay_ipv4>}. **Note:** If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore config mailsetting relayserver and the protected domain's tp-use-domain-mta {yes | no}.	disable
bcc-addr <recipient_email>	Type the BCC recipient email address. This field applies only if bcc-status is enable.	No default.
bcc-status {enable | disable}	Enable to send a blind carbon copy (BCC) of the email. Also configure bcc-addr <recipient_email>.	disable
encryption-profile <encryption-profile_name>	Enter the name of an encryption profile to use.	No default.
rewrite-rcpt-domain-type {none | prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email that matches the content profile. • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <case_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <case_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <case_str>.	none
rewrite-rcpt-domain-value <case_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none | prefix | replace | suffix}.	

Variable	Description	Default
`rewrite-rcpt-local-type {none | prefix | replace | suffix}`	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email that matches the content profile. • `none`: No change. • `prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • `suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	`none`
`rewrite-rcpt-local-value <value_str>`	Enter the text for the option (except `none`) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
`direction {incoming | outgoing}`	Enter either `incoming` for a profile that can be used by an incoming antispam profile, or `outgoing` for a profile that can be used by an outgoing antispam profile.	`incoming`
`header-insertion-name <text_str>`	Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Content-Filter: Contains banned word.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. Also configure tagging type {insert-header | tag-subject}.	
`header-insertion-value <value_str>`	Enter the message header value. The FortiMail unit will add this value to the message header of the email before forwarding it to the recipient. See header-insertion-name <text_str>. Also configure tagging type {insert-header | tag-subject}.	
`subject-tagging-text <text_str>`	Enter the text that will appear in the subject line of the email, such as "`[PROHIBITED-CONTENT]`". The FortiMail unit will prepend 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. Also configure tagging type {insert-header | tag-subject}.	
`tagging type {insert-header | tag-subject}`	Enter the type of tagging for this profile. Enter `insert-header` enables header-insertion-name <text_str> and header-insertion-value <value_str>. Enter `tag-subject` enables subject-tagging-text <text_str>.	

History

FortiMail v4.0 New.

Related topics

- config profile content

profile dictionary

Use this command to 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.

Syntax

```
config profile dictionary
  edit <profile_name>
    config item
      edit <item_int>
        set pattern <pattern_str>
        set pattern-comments <comment_str>
        set pattern-type {ABAROUTING | CANSIN | CUSIP | CreditCard | ISIN |
           USSSN | regex | wildcard}
        set pattern-weight <weight_int>
        set pattern-scan-area {header | body}
        set pattern-status {enable | disable}
        set pattern-max-weight <weight_int>
        set pattern-max-limit {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
<item_int>	Enter the index number for the pattern entry where you can add a word or phrase to the dictionary.	

pattern <pattern_str>	For a predefined pattern, enter a value to change the predefined pattern name.
	For a use-defined pattern, enter a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression.
	Regular expressions do not require slash (/) boundaries. For example, enter:
	`v[i1]agr?a`
	Matches are case ***in***sensitive and can occur over multiple lines as if the word were on a single line. (That is, Perl-style match modifier options `i` and `s` are in effect.)
	The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, not the originally encoded string. For example, if the original encoded string is:
	`=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=`
	the pattern must match:
	`Se trata del spam.`
	Entering the pattern `*iso-8859-1*` would ***not*** match.	

pattern-comments <comment_str>	Enter any description for the pattern.	

Variable	Description	Default
pattern-type {ABAROUTING | CANSIN | CUSIP | CreditCard | ISIN | USSSN | regex | wildcard}	Enter ABAROUTING, CANSIN, CUSIP, CreditCard, ISIN, or USSSN for predefined patterns. • ABAROUTING: 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. • CANSIN: Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666. • 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. • CreditCard: Major credit card number formats. • 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. • USSSN: United States Social Security number. The format is a nine digit number, such as 078051111. For user-defined patterns, enter either: • wildcard: Pattern is verbatim or uses only simple wild cards (? or *). • regex: Pattern is a Perl-style regular expression.	regex
pattern-weight <weight_int>	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 to determine whether or not to apply the content action.	1
pattern-scan-area {header | body}	Enter header to match occurrences of the pattern when it is located in an email's message headers, including the subject line, or body to match occurrences of the pattern when it is located in an email's message body.	
pattern-status {enable | disable}	Enable or disable a pattern in a profile.	disable
pattern-max-weight <weight_int>	Enter the maximum by which matches of this pattern can contribute to an email's dictionary match score.	1
pattern-max-limit {enable | disable}	Enable if the pattern must not be able to increase an email's dictionary match score more than the amount configured in pattern-max-weight <weight_int>.	disable

History

FortiMail v4.0 New.

FortiMail v4.0 MR1 The pattern-type variable has new options, CANSIN, USSSN, CreditCard, ABAROUTING, CUSIP, and ISIN. New variables pattern-status and pattern-comments

Related topics

- config profile dictionary-group

profile dictionary-group

Use this command to 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 "config profile dictionary" on page 130.

Syntax

```
config domain
  edit <group_name>
    config dictionaries
      edit <dictionary_name>
end
```

Variable	Description	Default
<group_name>	Enter the name of the dictionary group.	
<dictionary_name>	Enter the dictionary that you want to include in the dictionary group.	

History

FortiMail v4.0 New.

Related topics

- config profile dictionary

profile encryption

Use this command to create encryption profiles, which contain encryption settings for secure MIME (S/MIME).

Encryption profiles, unlike other types of profiles, are applied through message delivery rules, not policies.

Syntax

```
config profile encryption
  edit <profile_name>
    set encryption-algorithm {aes128 | aes192 | aes256 | cast5 | tripledes}
    set action-on-failure {drop | send | tls}
    set max-push-size <size_int>
    set protocol {smime | ibe}
    set retrieve-action {push | pull}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the encryption profile.	
encryption-algorithm {aes128 | aes192 | aes256 | cast5 | tripledes}	Enter the encryption algorithm that will be used with the sender's private key in order to encrypt the email.	aes128
action-on-failure {drop | send | tls}	Enter the action the FortiMail unit takes when identity-based encryption cannot be used, either: • drop: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable. • send: Deliver the email without encryption.	drop
max-push-size <size_int>	The maximum message size (in KB) of the secure mail delivered (or pushed) to the recipient. Messages that exceed this size are delivered via pull. The size cannot exceed 10240KB. This option applies to the IBE protocol only.	2048
protocol {smime | ibe}	The protocol used for this profile, S/MIME or IBE.	smime
retrieve-action {push | pull}	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. This option applies to the IBE protocol only.	push

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	New ibe option added to protocol, new retrieve-action and max-push-size options.

Related topics

- config profile authentication

profile ip-pool

Use this command to define a range of IP addresses. IP pools can be used in multiple ways:

- To define destination IP addresses of multiple protected SMTP servers if you want to load balance ***incoming*** email between them
- To define source IP addresses used by the FortiMail unit if you want ***outgoing*** email to originate from a range of IP addresses.

Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.

For more information, see the *FortiMail Administration Guide*.

Syntax

```
config profile ip-pool
  edit <profile_name>
    set iprange {enable | disable}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the IP pool profile.	
`iprange {enable | disable}`	Enter the first and last IP address in each contiguous range included in the profile.	

History

FortiMail v4.0 New.

profile ldap

Use this command to configure LDAP profiles which can query LDAP servers for authentication, email address mappings, and more.

Caution: Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server. When LDAP queries do not match with the server's schema and/or contents, unintended mail processing behaviors can result, including bypassing antivirus scans. For details on preparing an LDAP directory for use with FortiMail LDAP profiles, see the *FortiMail Administration Guide*.

LDAP profiles each contain one or more queries that retrieve specific configuration data, such as user groups, from an LDAP server.

Syntax

```
config profile ldap
  edit <profile_name>
    set address-map-state {enable | disable}
    set alias-base-dn <dn_str>
    set alias-bind-dn <bind_dn_str>
    set alias-bind-password <bindpw_str>
    set alias-dereferencing {never | always | search | find}
    set alias-expansion-level <limit_int>
    set alias-group-expansion-state {enable | disable}
    set alias-group-member-attribute <attribute_str>
    set alias-group-query <query_str>
    set alias-member-mail-attribute <attribute_str>
    set alias-member-query <query_str>
    set alias-schema {activedirectory | dominoperson | inetlocalmailrcpt |
       inetorgperson | userdefined}
    set alias-scope {base one | sub}
    set alias-state {enable | disable}
    set antispam <attribute_str>
    set anti-virus <attribute_str>
    set asav-state {enable | disable}
    set auth-bind-dn {cnid | none | searchuser | upn}
    set authstate {enable | disable}
    set base-dn <basedn_str>
    set bind-dn <binddn_str>
    set bind-password <bindpw_str>
    set cache-state {enable | disable}
    set cache-ttl <ttl_int>
    set cnid-name <cnid_str>
    set dereferencing {never | always | search | find}
    set domain-antispam-attr <attribute_str>
    set domain-antivirus-attr <attribute_str>
    set domain-parent-attr <attribute_str>
    set domain-query <query_str>
    set domain-routing-mail-host-attr <attribute_str>
    set domain-state {enable | disable}
    set external-address <attribute_str>
    set fallback-port <port_int>
    set fallback-server {<fqdn_str> | <server_ipv4>}
    set group-base-dn <basedn_str>
```

```
    set group-membership-attribute <attribute_str>
    set group-name-attribute <attribute_str>
    set group-owner {enable | disable}
    set group-owner-address-attribute <attribute_str>
    set group-owner-attribute <attribute_str>
    set group-relative-name {enable | disable}
    set group-virtual {enable | disable}
    set groupstate {enable | disable}
    set internal-address <attribute_str>
    set port <port_int>
    set query <query_str>
    set rcpt-vrfy-bypass {enable | disable}
    set routing-mail-host <attribute_str>
    set routing-mail-addr <attribute_str>
    set routing-state {enable | disable}
    set schema {activedirectory | dominoperson | inetlocalmailrcpt |
       inetorgperson | userdefined}
    set scope {base | one | sub}
    set secure {none | ssl}
    set server <name_str>
    set timeout <timeout_int>
    set unauth-bind {enable | disable}
    set upn-suffix <upns_str>
    set version {ver2 | ver3}
    set webmail-password-change {enable | disable}
    set webmailschema {openldap | activedirectory}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the LDAP profile.	
`address-map-state {enable | disable}`	Enable to query the LDAP server defined in the LDAP profile for user objects' mappings between email addresses.	`disable`
`alias-base-dn <dn_str>`	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for either alias or user objects. User or alias objects should be child nodes of this location. Whether you should specify the base DN of either user objects or alias objects varies by your LDAP schema style. Schema may resolve alias email addresses directly or indirectly (using references). • **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. • **Indirect resolution**: Alias objects do ***not*** directly contain an email address attribute that can resolve the alias; instead, in the style of LDAP group-like objects, the alias objects contain only references to user objects that are "members" of the alias "group." User objects' email address attribute values, such as `user@example.com`, actually resolve the alias. Alias objects refer to user objects by possessing one or more "member" attributes whose value is the DN of a user object, such as `uid=user,ou=People,dc=example,dc=com`. The FortiMail unit performs a first query to retrieve the distinguished names of "member" user objects, then performs a second query using those distinguished names to retrieve email addresses from each user object. The Base DN, such as `ou=People,dc=example,dc=com`, should contain user objects.	

Variable	Description	Default
alias-bind-dn <bind_dn_str>	Enter the bind DN, such as cn=FortiMailA,dc=example,dc=com, of an LDAP user account with permissions to query the basedn. This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled unauth-bind {enable | disable}.	
alias-bind-password <bindpw_str>	Enter the password of alias-bind-dn <bind_dn_str>.	
alias-dereferencing {never | always | search | find}	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.	never
alias-expansion-level <limit_int>	Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand.	0
alias-group-expansion-state {enable | disable}	Enable if your LDAP schema resolves email aliases indirectly. For more information on direct vs. indirect resolution, see alias-base-dn <dn_str>. When this option is ***disabled***, alias resolution occurs using ***one*** query. The FortiMail unit queries the LDAP directory using the basedn and the alias-member-query, and then uses the value of each alias-member-mail-attribute to resolve the alias. When this option is ***enabled***, alias resolution occurs using ***two*** queries: 1 The FortiMail unit first performs a preliminary query using the basedn and alias-group-query, and uses the value of each alias-group-member-attribute as the base DN for the second query. 2 The FortiMail unit performs a second query using the distinguished names from the preliminary query (instead of the basedn) and the alias-member-query, and then uses the value of each alias-member-mail-attribute to resolve the alias. The two-query approach is appropriate if, in your schema, alias objects are structured like group objects and contain references in the form of distinguished names of member user objects, rather than directly containing email addresses to which the alias resolves. In this case, the FortiMail unit must first “expand" the alias object into its constituent user objects before it can resolve the alias email address.	disable
alias-group-member-attribute <attribute_str>	Enter the name of the attribute for the group member, 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-mail-attribute <attribute_str>.	
alias-group-query <query_str>	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 filter string filters the result set, and should be based upon any attributes that are common to all alias objects but also exclude non-alias objects. For example, if alias objects in your directory have two distinguishing characteristics, their objectClass and proxyAddresses attributes, the query filter might be: (&(objectClass=group) (proxyAddresses=smtp:$m)) where $m is the FortiMail variable for an email address.	

Variable	Description	Default
alias-member-mail-attribute <attribute_str>	Enter the name of the attribute for the alias member's mail address, 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.	
alias-member-query <query_str>	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-mail-attribute <attribute_str>, from the LDAP directory. The query filter string filters the result set, and should be based upon any attributes that are common to all user/alias objects but also exclude non-user/alias objects. For example, if user objects in your directory have two distinguishing characteristics, their objectClass and mail attributes, the query filter might be: (& (objectClass=alias) (mail=$m)) where $m is the FortiMail variable for a user's email address.	
alias-schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}	Enter either the name of the LDAP directory's schema, or enter userdefined to indicate a custom schema.	inetorgperson
alias-scope {base one | sub}	Enter which level of depth to query: • base: Query the basedn level. • one: Query only the one level directly below the basedn in the LDAP directory tree. • sub: Query recursively all levels below the basedn in the LDAP directory tree.	sub
alias-state {enable | disable}	Enable to query user objects for email address aliases.	disable
antispam <attribute_str>	Enter the name of the attribute, such as antispam, whose value indicates whether or not to perform antispam processing for that user.	
anti-virus <attribute_str>	Enter the name of the attribute, such as antivirus, whose value indicates whether or not to perform antivirus processing for that user.	
asav-state {enable | disable}	Enable to query user objects for mappings between internal and external email addresses.	disable
auth-bind-dn {cnid | none | searchuser | upn}	Enter either none to not define a user authentication query, or one of the following to define a user authentication query: • cnid: Enter the name of the user objects' common name attribute, such as cn or uid. • searchuser: Enter to form the user's bind DN by using the DN retrieved for that user. • upn: Enter to form the user's bind DN by prepending the user name portion of the email address ($u) to the User Principle Name (UPN, such as example.com). By default, the FortiMail unit will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, also configure upn-suffix <upns_str>.	searchuser
authstate {enable | disable}	Enable to perform user authentication queries.	disable
base-dn <basedn_str>	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail unit will search for user objects, such as ou=People,dc=example,dc=com. User objects should be child nodes of this location.	

Variable	Description	Default
bind-dn <binddn_str>	Enter the bind DN, such as cn=FortiMailA,dc=example,dc=com, of an LDAP user account with permissions to query the basedn. This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled unauth-bind {enable | disable}.	
bind-password <bindpw_str>	Enter the password of bind-dn <binddn_str>.	
cache-state {enable | disable}	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiMail unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.	disable
cache-ttl <ttl_int>	Enter the amount of time, in minutes, that the FortiMail unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail unit to query the LDAP server, refreshing the cache. The default TTL value is 1,440 minutes (one day). The maximum value is 10,080 minutes (one week). Entering a value of 0 effectively disables caching.	1440
cnid-name <cnid_str>	Enter the name of the user objects' common name attribute, such as cn or uid.	
dereferencing {never | always | search | find}	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.	never
domain-antispam-attr <attribute_str>	Enter the name of the antispam profile attribute, such as businessCategory, 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.	
domain-antivirus-attr <attribute_str>	Enter the name of the antivirus profile attribute, such as preferredLanguage, 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.	
domain-parent-attr <attribute_str>	Enter the name of the parent domain attribute, such as description, whose value is the name of the parent domain from which a domain inheritate the specific RCPT check settings and quarantine report settings. The name of this attribute may vary by the schema of your LDAP directory.	

Variable	Description	Default
domain-query <query_str>	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. For details on query syntax, refer to any standard LDAP query filter reference manual. For this option to work, your LDAP directory should contain a single generic user for each domain. The user entry should be configured with attributes to represent the following: • parent domain from which a domain inheritate the specific RCPT check settings and quarantine report settings. For example, description=parent.com • IP address of the backend mail server hosting the mailboxes of the domain. For example, mailHost=192.168.1.105 • antispam profile assigned to the domain. For example, businessCategory=parentAntispam • antivirus profile assigned to the domain. For example, preferredLanguage=parentAntivirus	
domain-routing-mail-host-attr <attribute_str>	Enter the name of the mail host attribute, such as mailHost, whose value is the name of 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.	
domain-state {enable | disable}	Enable or disable the domain lookup option. For more information about domain lookup, see “domain-query <query_str>” on page 140.	disable
external-address <attribute_str>	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 into the value of internal-address <attribute_str> according to the match conditions and effects described in Table 9 on page 144. The name of this attribute may vary by the schema of your LDAP directory.	extAddress
fallback-port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number. The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636. The FortiMail unit will use SSL-secured LDAP to connect to the server if secure is ssl.	389
fallback-server {<fqdn_str> | <server_ipv4>}	Enter either the fully qualified domain name (FQDN) or IP address of the backup LDAP server. If there is no fallback server, enter an empty string ('').	
group-base-dn <basedn_str>	Enter the base DN portion of the group’s full DN, such as ou=Groups,dc=example,dc=com. This command applies only if group-relative-name is enable.	
group-membership-attribute <attribute_str>	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.	
group-name-attribute <attribute_str>	Enter the name of the attribute, such as cn, whose value is the group name of a group to which the user belongs. This command applies only if group-relative-name is enable.	

Variable	Description	Default
group-owner {enable | disable}	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 spam reports. Using that user's DN, the FortiMail unit will then perform a second query to retrieve that user's email address, where the spam report will be sent.For more information on sending spam reports to the group owner, see "config domain-setting" on page 51.	disable
group-owner-address-attribute <attribute_str>	Enter the name of the attribute, such as mail, whose value is the group owner's email address. If group-owner is enable, this attribute must be present in user objects.	
group-owner-attribute <attribute_str>	Enter the name of the attribute, such as groupOwner, whose value is the distinguished name of a user object. You can configure the FortiMail unit to allow that user to be responsible for handling the group's spam report. If group-owner is enable, this attribute must be present in group objects.	
group-relative-name {enable | disable}	Enable to specify the base distinguished name (DN) portion of the group's full distinguished name (DN) in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query. For example, you might find it more convenient in each recipient-based policy to type only the group name, admins, rather than typing the full DN, cn=admins,ou=Groups,dc=example,dc=com. In this case, you could enable this option, then basedn (ou=Groups,dc=example,dc=com) and groupnameattribute (cn). When performing the query, the FortiMail unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the groupnameattribute and the basedn 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.	disable
group-virtual {enable | disable}	Enable to use objects within the base DN of base-dn <basedn_str> 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 the user object query as if they were members of such a group.	disable
groupstate {enable | disable}	Enable to perform LDAP group queries.	disable
internal-address <attribute_str>	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 into the value of external-address <attribute_str> according to the match conditions and effects described in Table 9 on page 144. The name of this attribute may vary by the schema of your LDAP directory.	intAddress
port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number. The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.	389

Variable	Description	Default
query <query_str>	Enter an LDAP query filter, enclosed in single quotes ('), that selects a set of user objects from the LDAP directory. The query filter 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 example, if user objects in your directory have two distinguishing characteristics, their objectClass and mail attributes, the query filter might be: (& (objectClass=inetOrgPerson) (mail=$m)) where $m is the FortiMail variable for a user's email address. If the email address ($m) as it appears in the message header is different from the user's email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the user by the email address ($m) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract "-spam" from the ***end*** of the user name portion of the recipient email address, you could use the query filter: (& (objectClass=inetOrgPerson) (mail=m{-spam})) where ${-spam} is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract "spam-" from the ***beginning*** of the user name portion of the recipient email address, you could use the query filter: (& (objectClass=inetOrgPerson) (mail=m{^spam-})) where ${^spam-} is the FortiMail variable for the tag to remove before performing the query. For some schemas, such as Microsoft Active Directory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure an alias query to resolve aliases. For details on query syntax, refer to any standard LDAP query filter reference manual. This command applies only if schema is userdefined.	(&(objectClass=inetOrgPerson)(mail=$m))
rcpt-vrfy-bypass {enable | disable}	If you have selected using LDAP server to verify recipient address and your LDAP server is down, enabling this option abandons recipient address verification and the FortiMail unit will continue relaying email.	disable
routing-mail-host <attribute_str>	Enter the name of the LDAP 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.	mailHost
routing-mail-addr <attribute_str>	Enter the name of the LDAP attribute, such as mailRoutingAddress, whose value is the email address of a deliverable user on the email server, also known as the mail host. For example, a user may have many aliases and external email addresses that are not necessarily known to the email server. These addresses would all map to a real email account (mail routing address) on the email server (mail host) where the user's email is actually stored. A user's recipient email address located in the envelope or header portion of each email will be rewritten to this address.	mailRoutingAddress
routing-state {enable | disable}	Enable to perform LDAP queries for mail routing.	disable
schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}	Enter either the name of the LDAP directory's schema, or enter userdefined to indicate a custom schema. If you enter userdefined, you must configure query.	inetorgperson

Variable	Description	Default
scope {base | one | sub}	Enter which level of depth to query: • base: Query the basedn level. • one: Query only the one level directly below the basedn in the LDAP directory tree. • sub: Query recursively all levels below the basedn in the LDAP directory tree.	sub
secure {none | ssl}	Enter a value to indicate whether or not to connect to the LDAP server(s) using an encrypted connection. • none: Use a non-secure connection. • SSL: Use an SSL-secured (LDAPS) connection. **Note:** If your FortiMail unit is deployed in server mode, and you want to enable webmail-password-change {enable | disable} using an LDAP server that uses a Microsoft ActiveDirectory-style schema, you must select *SSL*. ActiveDirectory servers require a secure connection for queries that change user passwords.	none
server <name_str>	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.	
timeout <timeout_int>	Enter the maximum amount of time in seconds that the FortiMail unit will wait for query responses from the LDAP server.	10
unauth-bind {enable | disable}	Enable to perform queries in this profile without supplying a bind DN and password for the directory search. Many LDAP servers require LDAP queries to be authenticated using a bind DN and password. However, if your LDAP server does not require the FortiMail unit to authenticate before performing queries, you may enable this option. If this option is disabled, you must configure bind-dn <binddn_str> and bind-password <bindpw_str>.	disable
upn-suffix <upns_str>	If you want to use a UPN other than the mail domain, enter that UPN. This can be useful if users authenticate with a domain other than the mail server's principal domain name.	
version {ver2 | ver3}	Enter the version of the protocol used to communicate with the LDAP server.	ver3
webmail-password-change {enable | disable}	Enable to perform password change queries for FortiMail webmail users.	disable
webmailschema {openldap | activedirectory}	Enter one of the following to indicate the schema of your LDAP directory: • openldap: The LDAP directory uses an OpenLDAP-style schema. • activedirectory: The LDAP directory uses a Microsoft Active Directory-style schema. **Note:** Microsoft Active Directory requires that password changes occur over an SSL-secured connection.	openldap

Email address mapping

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

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

Like aliases, address mappings translate email addresses. They do not translate many email addresses into a single email address. However, ***unlike*** aliases:

- Mappings cannot translate one email address into many.

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

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

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

Table 9: 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 others**: user1@marketing.example.net in both the message envelope (`MAIL FROM:`) and many message headers (`From:`, etc.) would then be replaced with sales@example.com. Recipients would only be aware of the email address sales@example.com.
- **For email to sales@example.com from others**: The recipient address in the message envelope (`RCPT TO:`), but ***not*** the message header (`To:`), would be replaced with user1@marketing.example.net. user1@marketing.example.net would be aware that the sender had originally sent the email to the mapped address, sales@example.com.

Alternatively, you can configure an LDAP profile to query for email address mappings.

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	New variables `domain-state`, `domain-query`, `domain-parent-attr`, `domain-parent-attr`, `domain-routing-mail-host-attr`, `domain-antispam-attr`, `domain-antivirus-attr`, and `rcpt-vrfy-bypass`.

Related topics

- config profile authentication

profile session

Use this command to create session profiles.

While, like antispam profiles, session profiles protect against spam, session profiles focus on the connection and envelope portion of the SMTP session, rather than the message header, body, or attachments.

Similar to access control rules or delivery rules, session profiles control aspects of sessions in an SMTP connection.

Syntax

```
config profile session
  edit <profile_name>
    set block_encrypted {enable | disable}
    set bypass-bounce-verification {enable | disable}
    set conn-blacklisted {enable | disable}
    set conn-concurrent <connections_int>
    set conn-hiden {enable | disable}
    set idle_timeout <timeout_int>
    set conn-rate-minutes <connections_int> <time_int>
    set conn-rate-number <connections_int>
    set conn-total <connections_int>
    set dkim-signing {enable | disable}
    set dkim-signing-authenticated-only {enable | disable}
    set dkim-validation {enable | disable}
    set domain-key-validation {enable | disable}
    set endpoint-reputation {enable | disable}
    set endpoint-reputation-action {reject | monitor}
    set endpoint-reputation-blacklist-duration <duration_int>
    set endpoint-reputation-blacklist-trigger <trigger_int>
    set eom-ack {enable | disable}
    set error-drop-after <errors_int>
    set error-penalty-increment <penalty-increment_int>
    set error-penalty-initial <penalty-initial_int>
    set error-penalty-threshold <threshold_int>
    set limit-NOOPs <limit_int>
    set limit-RSETs <limit_int>
    set limit-email <limit_int>
    set limit-helo <limit_int>
    set limit-max-header-size <limit_int>
    set limit-max-message-size <limit_int>
    set limit-recipient <limit_int>
    set recipient-blacklist-status {enable | disable}
    set recipient-whitelist-status {enable | disable}
    set remove-header {enable | disable}
    set remove-received-headers {enable | disable}
    set sender-blacklist-status {enable | disable}
    set sender-reputation-reject-score <threshold_int>
    set sender-reputation-status {enable | disable}
    set sender-reputation-tempfail-score <threshold_int>
    set sender-reputation-throttle-number <rate_int>
    set sender-reputation-throttle-percentage <percentage_int>
    set sender-reputation-throttle-score <threshold_int>
```

```
    set sender-whitelist-status {enable | disable}
    set session-3way-check {enable | disable}
    set session-allow-pipelining {no | loose | strict}
    set session-command-checking {enable | disable}
    set session-disallow-encrypted {enable | disable}
    set session-helo-char-validation {enable | disable}
    set session-helo-domain-check {enable | disable}
    set session-helo-rewrite-clientip {enable | disable}
    set session-helo-rewrite-custom {enable | disable}
    set session-helo-rewrite-custom-string <helo_str>
    set session-prevent-open-relay {enable | disable}
    set session-recipient-domain-check {enable | disable}
    set session-reject-empty-domain {enable | disable}
    set session-sender-domain-check {enable | disable}
    set spf-validation {enable | disable}
    set splice-status {enable | disable}
    set splice-threshold
    set splice-unit {seconds | kilobytes}
    config header-removal-list
      edit <key_str>
    config recipient-blacklist
      edit <recipient_address_str>
    config recipient-whitelist
      edit <recipient_address_str>
    config sender-blacklist
      edit <sender_address_str>
    config sender-whitelist
      edit <sender_address_str>
  next
end
```

Variable	Description	Default
<profile_name>	Enter the name of the session profile.	
<key_str>	Enter a header key to remove it from email messages.	
<recipient_address_str>	Enter a blacklisted recipient email address to which this profile is applied.	
<recipient_address_str>	Enter a whitelisted recipient email address to which this profile is applied.	
<sender_address_str>	Enter a blacklisted sender email address to which this profile is applied.	
<sender_address_str>	Enter a whitelisted sender email address to which this profile is applied.	
block_encrypted {enable | disable}	Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam. Disable to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam. This option applies only if the FortiMail unit is operating in transparent mode.	disable

Variable	Description	Default
bypass-bounce-verification {enable | disable}	Select to, if bounce verification is enabled, omit verification of bounce address tags on incoming bounce messages. This bypass does not omit bounce address tagging of outgoing email. Alternatively, you can omit bounce verification according to the protected domain. For details, see "config domain-setting" on page 51. For information on enabling bounce address tagging and verification (BATV), see "config antispam bounce-verification key" on page 35.	disable
conn-blacklisted {enable | disable}	Enable to prevent clients from using SMTP servers that have been blacklisted in antispam profiles or, if enabled, the FortiGuard AntiSpam service. This option applies only if the FortiMail unit is operating in transparent mode.	disable
conn-concurrent <connections_int>	Enter a limit to the number of concurrent connections per SMTP client. Additional connections are rejected. To disable limiting of concurrent connections, enter 0.	0
conn-hiden {enable | disable}	Enter either of the following transparency behaviors: • enable: Be transparent. Preserve the IP address or domain name in: the SMTP greeting (HELO/EHLO) in the envelope, the Received: message headers of email messages, and the IP addresses in the IP header This masks the existence of the FortiMail unit. • disable: Do not be transparent. Replace the IP addresses or domain names with that of the FortiMail unit. This option applies only if the FortiMail unit is operating in transparent mode. For more information about the proxies and built-in MTA transparency, see the *FortiMail Administration Guide*. **Note:** Unless you have enabled exclusive {enable | disable} in "config policy ip" on page 104, the hide (tp-hidden {no | yes}) option in "config domain-setting" on page 51 has precedence over this option, and may prevent it from applying to incoming email messages. **Note:** For full transparency, also set the hide (tp-hidden {no | yes}) option in "config domain-setting" on page 51 to yes.	disable
idle_timeout <timeout_int>	Enter a limit to the number of seconds a client may be inactive before the FortiMail unit drops the connection. To disable idle timeouts, enter 0.	0
conn-rate-minutes <connections_int> <time_int>	This is a rate limit to the number of connections per client IP address. Enter the number of minutes that defines the time interval of the limit. To disable the connection rate limit, enter 0.	0
conn-rate-number <connections_int>	This is a rate limit to the number of message sent per client IP address. Enter the number of minutes that defines the time interval of the limit.	0
conn-total <connections_int>	Enter a limit to the total number of concurrent connections from all sources. To disable the limit of total connections, enter 0.	0
dkim-signing {enable | disable}	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 will not be able to validate your DKIM signature. For details on generating domain key pairs and publishing the public key, see the *FortiMail Administration Guide*.	disable
dkim-signing-authenticated-only {enable | disable}	Enable to sign outgoing email with a DKIM signature only if the sender is authenticated. This option is available only if dkim-signing is enable.	disable

Variable	Description	Default
`dkim-validation {enable | disable}`	Enable to, if a DKIM signature is present, 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 affect the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DKIM information or the message is not signed, the FortiMail unit omits the DKIM signature validation.	`disable`
`domain-key-validation {enable | disable}`	Enable to, if the DNS record for the domain name of the sender lists DomainKeys authorized IP addresses, compare the client IP address to the IP addresses of authorized senders. 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 DomainKeys information, the FortiMail unit omits the DomainKeys client IP address validation.	`disable`
`endpoint-reputation {enable | disable}`	Enable to accept, monitor, or reject email based upon endpoint reputation scores. This option requires that your RADIUS server provide mappings between dynamic IP addresses and MSISDNs/subscriber IDs to the FortiMail unit. If this profile governs sessions of SMTP clients with static IP addresses, instead consider sender-reputation-status {enable | disable}.	`disable`
`endpoint-reputation-action {reject | monitor}`	Enter either: • `reject`: Reject email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed *Auto blacklist score trigger value*. • `monitor`: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed `endpoint-reputation-blacklist-trigger` value. Log entries appear in the history log.	`reject`
`endpoint-reputation-blacklist-duration <duration_int>`	Enter the number of minutes that an MSISDN/subscriber ID will be prevented from sending email or MMS messages after they have been automatically blacklisted.	`0`
`endpoint-reputation-blacklist-trigger <trigger_int>`	Enter the MSISDN reputation score over which the FortiMail unit will add the MSISDN/subscriber ID to the automatic blacklist. The trigger score is relative to the period of time configured as the automatic blacklist window.	`5`
`eom-ack {enable | disable}`	Enable to acknowledge the end of message (EOM) signal immediately after receiving the carriage return and line feed (CRLF) characters that indicate the EOM, rather than waiting for antispam scanning to complete. If the FortiMail unit has not yet completed antispam scanning by the time that four (4) minutes has elapsed, it will return SMTP reply code 451(`Try again later`), resulting in no permanent problems, as according to RFC 2281, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail unit to acknowledge the EOM command. Enabling this option prevents those rare cases.	`disable`
`error-drop-after <errors_int>`	Enter the total number of errors the FortiMail unit will accept before dropping the connection.	`5`
`error-penalty-increment <penalty-increment_int>`	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.	`1`

Variable	Description	Default
`error-penalty-initial <penalty-initial_int>`	Enter the delay penalty in seconds for the first error after the number of “free" errors is reached.	`1`
`error-penalty-threshold <threshold_int>`	Enter the number of number of errors permitted before the FortiMail unit will penalize the SMTP client by imposing a delay.	`1`
`limit-NOOPs <limit_int>`	Enter the limit of NOOP commands that are permitted per SMTP session. Some spammers use NOOP commands to keep a long session alive. Legitimate sessions usually require few NOOPs.	`10`
`limit-RSETs <limit_int>`	Enter the limit of RSET commands that are permitted per SMTP session. Some spammers use RSET commands to try again after receiving error messages such as unknown recipient. Legitimate sessions should require few RSETs.	`20`
`limit-email <limit_int>`	Enter the limit of email messages per session to prevent mass mailing.	`10`
`limit-helo <limit_int>`	Enter the limit of SMTP greetings that a connecting SMTP server or client can perform before the FortiMail unit terminates the connection. Restricting the number of SMTP greetings allowed per session makes it more difficult for spammers to probe the email server for vulnerabilities, as a greater number of attempts results in a greater number of terminated connections, which must then be re-initiated.	`3`
`limit-max-header-size <limit_int>`	Enter the limit of the message header size. If enabled, messages with headers over the threshold size are rejected.	`32`
`limit-max-message-size <limit_int>`	Enter the limit of message size. If enabled, messages over the threshold size are rejected. **Note:** If both this option and `max-message-size <limit_int>` in the protected domain are enabled, email size will be limited to whichever size is smaller.	`10240`
`limit-recipient <limit_int>`	Enter the limit of recipients to prevent mass mailing.	`500`
`recipient-blacklist-status {enable | disable}`	Enable to use an envelope recipient (`RCPT TO:`) black list in SMTP sessions to which this profile is applied, then define blacklisted email addresses using <recipient_address_str>.	`disable`
`recipient-whitelist-status {enable | disable}`	Enable to use an envelope recipient (`RCPT TO:`) white list in SMTP sessions to which this profile is applied, then define whitelisted email addresses using <recipient_address_str>.	`disable`
`remove-header {enable | disable}`	Enable to remove other configured headers from email messages.	`disable`
`remove-received-headers {enable | disable}`	Enable to remove all `Received:` message headers from email messages.	`disable`
`sender-blacklist-status {enable | disable}`	Enable to use an envelope sender (`MAIL FROM:`) black list in SMTP sessions to which this profile is applied, then define the blacklisted email addresses using config <sender_address_str>.	`disable`
`sender-reputation-reject-score <threshold_int>`	Enter a sender reputation score over which the FortiMail unit will return a rejection error code when the SMTP client attempts to initiate a connection. This option applies only if sender-reputation-status {enable | disable} is `enable`.	`80`
`sender-reputation-status {enable | disable}`	Enable to reject email based upon sender reputation scores.	`disable`

Variable	Description	Default
sender-reputation-tempfail-score <threshold_int>	Enter a sender reputation score over which the FortiMail unit will return a temporary failure error code when the SMTP attempts to initiate a connection. This option applies only if sender-reputation-status {enable | disable} is enable.	55
sender-reputation-throttle-number <rate_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client.	5
sender-reputation-throttle-percentage <percentage_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client, as a percentage of the number of email messages that the sender sent during the previous hour.	1
sender-reputation-throttle-score <threshold_int>	Enter the sender reputation score over which the FortiMail unit will rate limit the number of email messages that can be sent by this SMTP client. The enforced rate limit is either sender-reputation-throttle-number <rate_int> or sender-reputation-throttle-percentage <percentage_int>, whichever value is greater. This option applies only if sender-reputation-status {enable | disable} is enable.	15
sender-whitelist-status {enable | disable}	Enable to use an envelope recipient (RCPT TO:) white list in SMTP sessions to which this profile is applied, then define whitelisted email addresses using <sender_address_str>.	disable
session-3way-check {enable | disable}	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. This check only affects unauthenticated sessions.	disable
session-allow-pipelining {no | loose | strict}	Select one of the following behaviors for ESMTP command pipelining, which causes some SMTP commands to be accepted and processed as a batch, increasing performance over high-latency connections. • no: Disabled. The FortiMail unit accepts only one command at a time during an SMTP session and will not accept the next command until it completes processing of the previous command. • loose: Enabled, and does not require strict compliance with RFC2920. • strict: Enabled, but requires strict compliance with RFC 2920. This option applies only if the FortiMail unit is operating in transparent mode.	no
session-command-checking {enable | disable}	Enable to return SMTP reply code 503, rejecting the 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, NOOP commands can arrive at any time. Other commands, or commands in an unacceptable order, return a syntax error. In the following example, the invalid commands are highlighted in bold: 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	disable

Variable	Description	Default
session-disallow-encrypted {enable | disable}	Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam. Clear to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam. This option applies only if the FortiMail unit is operating in transparent mode.	disable

session-helo-char-validation {enable | disable}	Enable to return SMTP reply code 501, rejecting 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 genuine, valid domain name. If this option is enabled, such connections are rejected.
	In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT`
	`EHLO ^^&^&^#$`
	`501 5.0.0 Invalid domain name`
	Valid characters for domain names include:
	• alphanumerics (A to Z and 0 to 9)
	• brackets ([and])
	• periods (.)
	• dashes (-)
	• underscores (_)
	• number symbols(#)
	• colons (:)
		disable

session-helo-domain-check {enable | disable}	Enable to return SMTP reply code 501, rejecting 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 genuine, valid domain name. If this option is enabled, such connections are rejected.
	In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT`
	`EHLO ^^&^&^#$`
	`501 5.0.0 Invalid domain name`
	Valid domain characters include:
	• alphanumerics (A to Z and 0 to 9)
	• brackets ([and])
	• periods (.)
	• dashes (-)
	• underscores (_)
	• number symbols(#)
	• colons (:)
		disable

session-helo-rewrite-clientip {enable | disable}	Enable to rewrite the HELO/EHLO domain to the IP address of the SMTP client to prevent domain name spoofing. This option applies only if the FortiMail unit is operating in transparent mode.	disable
session-helo-rewrite-custom {enable | disable}	Enable to rewrite the HELO/EHLO domain, then enter the replacement text using session-helo-rewrite-custom-string <helo_str>. This option applies only if the FortiMail unit is operating in transparent mode.	disable
session-helo-rewrite-custom-string <helo_str>	Enter the replacement text for the the HELO/EHLO domain.	

Variable	Description	Default
session-prevent-open-relay {enable | disable}	Enable to block unauthenticated outgoing connections to unprotected mail servers in order to prevent clients from using open relays to send email. If clients from your protected domains are permitted to use open relays to send email, email from your domain could be blacklisted by other SMTP servers. This feature: • applies only if the FortiMail unit is operating in transparent mode • only affects unauthenticated sessions, and • is applicable only if you allow clients to use an unprotected SMTP server for outgoing connections. For details, see "config mailsetting proxy-smtp" on page 88.	disable
session-recipient-domain-check {enable | disable}	Enable to return SMTP reply code 550, rejecting 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. In the following example, the invalid command is highlighted in bold: 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] This check only affects unauthenticated sessions.	disable
session-reject-empty-domain {enable | disable}	Enable to return SMTP reply code 553, rejecting the SMTP command, if a domain name does not follow the "@" symbol in the sender email address. Because the sender address is invalid and therefore cannot receive delivery status notifications (DSN), you may want to disable this feature. In the following example, the invalid command is highlighted in bold: 220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2007 14:48:32 GMT EHLO example.com 250-FortiMail-400.localdomain Hello [192.168.171.217], pleased to meet you ***MAIL FROM:<john@>*** 553 5.1.3 <john@>... Hostname required This check only affects unauthenticated sessions.	disable
session-sender-domain-check {enable | disable}	Enable o return SMTP reply code 421, rejecting 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. 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 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.	disable

Variable	Description	Default
`spf-validation {enable | disable}`	Enable to, if the sender domain DNS record lists SPF authorized IP addresses, compare the client IP address to the IP addresses of authorized senders in the DNS record. An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score. If the DNS record for the domain name of the sender does not publish SPF information, the FortiMail unit omits the SPF client IP address validation.	`disable`
`splice-status {enable | disable}`	Enable to permit splicing. Splicing enables the FortiMail unit to simultaneously scan an email and relay it to the SMTP server. This increases throughput and reduces the risk of a server timeout. If the FortiMail unit 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. This option applies only if the FortiMail unit is operating in transparent mode.	`disable`
`splice-threshold <integer>`	Enter a threshold value to switch to splice mode based on time (seconds) or data size (kilobytes) using splice-unit {seconds | kilobytes}.	`0`
`splice-unit {seconds | kilobytes}`	Enter the time (seconds) or data size (kilobytes) for the `splice threshold`.	`seconds`

History

FortiMail v4.0 New.

Related topics

- config profile content

profile tls

Use this command to configure TLS profiles that can be used by receive rules (also called access control rules) and delivery rules.

Syntax

```
config profile tls
  edit <profile_name>
    set level {encrypt | none | secure | preferred}
    set action {fail | tempfail}
end
```

Variable	Description	Default
`<profile_name>`	Enter the name of the tls profile.	
`level {encrypt | none | secure | preferred}`	Enter the security level of the TLS connection. • `encrypt`: Requires a basic TLS connection. Failure to negotiate a TLS connection results in the connection being rejected according to the `action` setting. • `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 unit before they can be used for secure TLS connections. For information on installing CA certificates, see the *FortiMail Administration Guide*.	`preferred`
`action {fail | tempfail}`	Select the action the FortiMail unit takes when a TLS connection cannot be established. • `fail` • `tempfail` This option does not apply for profiles whose `level` is `preferred`.	`tempfail`

History

FortiMail v4.0 New.

Related topics

- config policy access-control receive
- diagnose debug application starttls

report

Use this command to configure report profiles that define what information will appear in generated reports.

In addition to log files, FortiMail units require a report profile to be able to generate a report. A report profile is a group of settings that contains the report name, file format, subject matter, and other aspects that the FortiMail unit considers when generating the report.

Syntax

```
config report
  edit <profile_name>
    set direction {both | incoming | outgoing}
    set domains {all | <protected-domain_str>}
    set file-format {html | pdf}
    set period-absolute-from <start_str>
    set period-absolute-to <end_str>
    set period-relative {last-2-weeks | last-7-days | last-14-days | last-
       30-days | last-N-days | last-N-hours | last-N-weeks | last-month |
       last-quarter | last-week | not-used | this-month | this-quarter |
       this-week | this-year | today | yesterday}
    set period-relative-value <n_int>
    set query-status <query_str>
    set recipients <recipient_str>
    set schedule {daily | dates | none | weekdays}
    set schedule-dates <dates_str>
    set schedule-hour <time_int>
    set schedule-weekdays <days_str>
end
```

Variable	Description	Default
<profile_name>	Enter the name of the report profile.	
direction {both | incoming | outgoing}	Enter one of the following: • both: Report on both incoming and outgoing email. • incoming: Report only on email whose recipient is a member of a protected domain. • outgoing: Report only on email whose recipient is ***not*** a member of a protected domain.	both
domains {all | <protected-domain_str>}	Enter either ALL to include all protected domains in the report, or enter a list of one or more protected domains. Separate each protected domain with a comma (,).	all
file-format {html | pdf}	Enter the file format of the generated report.	pdf
period-absolute-from <start_str>	Enter the beginning of the time range in the format yyyy-mm-dd-hh, where yyyy is the year, mm is the month, dd is the day, and hh is the hour in 24-hour clock format. For example, entering 2008-10-24-09 includes log messages as early as 9 AM on October 24, 2008.	
period-absolute-to <end_str>	Enter the end of the time range in the format yyyy-mm-dd-hh, where yyyy is the year, mm is the month, dd is the day, and hh is the hour in 24-hour clock format. For example, entering 2009-10-24-17 includes log messages as late as 5 PM on October 24, 2009.	

Variable	Description	Default
period-relative {last-2-weeks | last-7-days | last-14-days | last-30-days | last-N-days | last-N-hours | last-N-weeks | last-month | last-quarter | last-week | not-used | this-month | this-quarter | this-week | this-year | today | yesterday}	Enter the time span of log messages from which to generate the report. If you entered last-N-days, last-N-hours, or last-N-weeks also configure period-relative-value <n_int>.	
period-relative-value <n_int>	If you entered last-N-days, last-N-hours, or last-N-weeks as the value for period-relative, enter the value of n.	
query-status <query_str>	Enter the name of a query whose result you want to include in the report, such as Mail_Stat_Viruses. To display a list of available query names, enter a question mark (?)	
recipients <recipient_str>	Enter a list of one or more recipient email addresses that will receive the report generated from the report profile. Separate each recipient with a comma (,).	
schedule {daily | dates | none | weekdays}	Enter a value to schedule when the report is automatically generated, or to disable generating reports on schedule if you want to initiate them only manually. • daily: Generate the report every day. • dates: Generate the report on certain dates in the month. Also configure schedule-dates <dates_str>. • none: If you do not want to automatically generate the report according to a schedule, enter none. You can still manually initiate the FortiMail unit to generate a report at any time. • weekdays: Generate the report on certain days of the week. Also configure schedule-weekdays <days_str>.	
schedule-dates <dates_str>	Enter the dates to generate the reports. Separate each date with a comma (,). For example, to generate a report on the first and fourteenth of each month, you would enter 1,14.	
schedule-hour <time_int>	If you want to automatically generate the report according to a schedule, enter the hour of the day, according to a 24-hour clock, at which you want to generate the report. Also configure the days on which you want to generate the report. For example, to generate reports at 5 PM, you would enter 17.	
schedule-weekdays <days_str>	Enter the days to generate the reports. Separate each day with a comma (,). For example, to generate a report on Friday and Wednesday, you would enter wednesday,friday.	

History

FortiMail v4.0 New.

Related topics

- config log alertemail setting

system accprofile

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

Syntax

```
config system accprofile
  edit <profile_name>
    set black-white-list {none | read | read-write}
    set others {none | read | read-write}
    set policy {none | read | read-write}
    set quarantine {none | read | read-write}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the access profile.	
black-white-list {none | read | read-write}	For the black and white list configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	read-write
others {none | read | read-write}	For the rest of the configurations except policy, black-white-list, and quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile.	read-write
policy {none | read | read-write}	For the policy configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	read-write
quarantine {none | read | read-write}	For the quarantine configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	read-write

History

FortiMail v4.0 New.

Related topics

- config system admin

system admin

Use this command to configure FortiMail administrator accounts.

By default, FortiMail units have a single administrator account, `admin`. For more granular control over administrative access, you can create additional administrator accounts that are restricted to being able to configure a specific protected domain and/or with restricted permissions. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config system admin
  edit <name_str>
    set access-profile <profile_name>
    set auth-strategy {local | local-plus-radius | pki | radius}
    set domain <admin_domain_str>
    set is-system-domain {no | yes}
    set language <lang_str>
    set password <password_str>
    set pkiuser <pkiuser_str>
    set radius-permission-check {enable | disable}
    set radius-profile <profile_int>
    set radius-subtype-id <subtype_int>]
    set radius-vendor-id <vendor_int>
    set sshkey <key_str>
    set theme <theme_str>
    set trusthosts <host_ipv4mask>
    set webmode (basic | advanced)
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the administrator account.	
`access-profile <profile_name>`	Enter the name of an access profile that determines which functional areas the administrator account may view or affect.	
`auth-strategy {local | local-plus-radius | pki | radius}`	Select the local or remote type of authentication that the administrator will be able to use: • `local` • `radius` • `radius-plus-local` • `pki`	`local`
`domain <admin_domain_str>`	Enter the name of a protected domain to restrict the administrator account to settings for that protected domain.	
`is-system-domain {no | yes}`	Enter `yes` to indicate that the administrator account may view all settings on the FortiMail unit.	`yes`
`language <lang_str>`	Enter this administrator account's preference for the display language of the web-based manager. Available languages vary by whether or not you have installed additional language resource files. To view a list of languages, enter a question mark (`?`).	`english`
`password <password_str>`	If `auth-strategy` is `local` or `radius-plus-local`, enter the password for the administrator account. **Caution:** Do not enter a FortiMail administrator password less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiMail unit.	

Variable	Description	Default
pkiuser <pkiuser_str>	If auth-strategy is pki, enter the name of a PKI user. Whether the administrator is required to log in only with a valid personal certificate or password-style authentication fallback is allowed varies by your configuration of pkimode {enable | disable}.	
radius-permission-check {enable | disable}	If auth-strategy is local or radius-plus-local, enable to query the RADIUS server for the permissions attribute.	disable
radius-profile <profile_int>	If auth-strategy is local or radius-plus-local, enter the index number of a RADIUS authentication profile.	
radius-subtype-id <subtype_int>]	If auth-strategy is local or radius-plus-local, and radius-permission-check is enable, enter the RADIUS subtype identifier.	0
radius-vendor-id <vendor_int>	If auth-strategy is local or radius-plus-local, and radius-permission-check is enable, enter the RADIUS vendor identifier.	0
sshkey <key_str>	Enter the SSH key string surrounded in single straight quotes ('). When connecting from an SSH client that presents this key, the administrator will not need to provide their account name and password in order to log in to the CLI.	
theme <theme_str>	Enter this administrator account's preference for the display theme when logging in.	
trusthosts <host_ipv4mask>	Enter one to three IP addresses and netmasks from which the administrator can log in to the FortiMail unit. Separate each IP address and netmask pair with a comma (,). To allow the administrator to authenticate from any IP address, enter 0.0.0.0/0.0.0.0.	0.0.0.0/0.0.0.0
webmode (basic | advanced)	Enter which display mode will initially appear when the administrator logs in to the web-based manager. The administrator may switch the display mode during their session; this affects only the initial state of the display.	basic

History

FortiMail v4.0 New.

Related topics

- config system accprofile

system appearance

Use this command to customize the appearance of the web-based manager, FortiMail webmail, and per-recipient quarantine of the FortiMail unit.

Syntax

```
config system appearance
  set login-page-language <lang_str>
  set product <product-name_str>
  set webmail-lang <language_str>
end
```

Variable	Description	Default
`login-page-language <lang_str>`	Enter the default language for the display of the login page of the web-based manager. To view a list of languages, enter a question mark (`?`). Note that the setting only affect the login page, not the entire web-based manager.	
`product <product-name_str>`	Enter the text that will precede 'Administrator Login' on the login page of the web-based manager.	`FortiMail`
`webmail-lang <language_str>`	Enter the name of the language in English, such as `'French'`, that will be used when an email user initially logs in to FortiMail webmail/per-recipient quarantine. The email user may switch the display language in their preferences; this affects only the initial state of the display. Available languages vary by whether or not you have installed additional language resource files.	`English`

History

v4.0 New.

Related topics

- config system global

system backup-restore-mail

Use this command to configure backup and restoration of email user's mailboxes.

For the initial backup, whether manually or automatically initiated, the FortiMail unit will make a full backup. For subsequent backups, the FortiMail unit will make the number of incremental backups that you selected in `incremental <incremental-backups_int>`, then make another full backup, and repeat this until it reaches the maximum number of full backups to keep on the backup media, which you selected in `full <full-backups_int>`. At that point, it will overwrite the oldest full backup.

For example, if `full <full-backups_int>` is 3 and `incremental <incremental-backups_int>` is 4, the FortiMail unit would make a full backup, then 4 incremental backups. It would repeat this two more times for a total of 3 backup sets, and then overwrite the oldest full backup when creating the next backup.

Syntax

```
config system backup-restore-mail
  set day-of-week <day_str>
  set folder <path_str>
  set full <full-backups_int>
  set host <fortimail-fqdn_str>
  set hour-of-day <hours_int>
  set incremental <incremental-backups_int>
  set port <port_int>
  set protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver
    | ssh}
  set status {enable | disable}
end
```

Variable	Description	Default
`day-of-week <day_str>`	Enter which day of the week to schedule backups on that day. **Note:** Scheduled backups do not occur if the backup media is an automatically-detected USB disk.	`sunday`
`folder <path_str>`	Enter the path of the folder on the backup server where the FortiMail unit will store the mailbox backups, such as: `/home/fortimail/mailboxbackups` This field appears only if the backup media is an NFS server or SSH server.	`FortiMail-mail-data-backup`
`full <full-backups_int>`	Enter the total number of full backups to keep on the backup media. Valid values are between 1 and 10.	`3`
`host <fortimail-fqdn_str>`	If you want to restore all mailboxes from a backup labeled with the fully qualified domain name (FQDN) of a previous FQDN, or that of another FortiMail unit, enter the FQDN of the backup that you want to restore. For example, to restore the most recent backup made by a FortiMail unit named fortimail.example.com, enter `fortimail.example.com`.	
`hour-of-day <hours_int>`	Enter the hour of the day, according to a 24-hour clock, on the days of the week at which to make backups. For example, to make backups at 9 PM, enter `21`.	`23`
`incremental <incremental-backups_int>`	Enter the number of incremental backups to make between each full backup. Valid values are between 0 and 20. Incremental backups can reduce the amount of time and disk space required for each backup, but may increase the amount of time required to restore the backup, and depend on a previous full backup, because incremental backups only contain the differences since the previous full backup.	`4`

Variable	Description	Default
`port <port_int>`	Enter the TCP port number on which the backup server listens for connections. This field does not appear if the backup media is a USB disk.	`22`
`protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver | ssh}`	Enter one of the following types of backup media: • `ext-usb`: An external hard drive connected to the FortiMail unit's USB port. • `ext-usb-auto`: An external disk connected to the FortiMail unit's USB port. Unlike the previous option, this option only creates a backup when you connect the USB disk, or when you manually initiate a backup rather than according to a schedule. • `iscsi_server`: An Internet SCSI (Small Computer System Interface), also called iSCSI, server. • `nfs`: A network file system (NFS) server. • `smb/winserver`: A Windows-style file share. • `ssh`: A server that supports secure shell (SSH) connections. Other available options vary by your choice of backup media.	`nfs`
`status {enable | disable}`	Enable to allow backups and restoration to occur, whether manually initiated or automatically performed on schedule. Also configure the backup media in `protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver | ssh}` and, if applicable to the type of the media, configure a schedule in `day-of-week <day_str>` and `hour-of-day <hours_int>`. **Note:** You should enable backups/restoration ***after*** configuring the other options if a scheduled backup will occur before you configure `protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver | ssh}`. Failure to do so would result in a failed backup attempt, requiring you to wait for the failed attempt to terminate before you can continue to configure this feature.	`disable`

History

FortiMail v4.0 New.

Related topics

- config system mailserver

system central-management

Use this command to enable FortiManager support.

Note: Latest FortiManager releases support centralized management of FortiMail v3.0 MR4 and MR5 releases. For FortiMail v4.0 releases, centralized management is supported in FortiManager v4.2 and later releases. Refer to FortiManager release notes for details about supported FortiMail versions. For information on configuring a FortiManager unit to manage or provide services to your other Fortinet brand devices, see the *FortiManager Administration Guide*.

In addition to configuration backup and remote administration, enabling FortiManager support allows your FortiMail unit to retrieve firmware image files.

In addition to enabling FortiManager support on the FortiMail unit, you must also register the device with the FortiManager unit's device list in order to indicate that it has permission to connect. For details, see the *FortiMail Administration Guide*.

Syntax

```
config system central-management
  set allow-push-configuration {enable | disable}
  set auto-backup {enable | disable}
  set ip <fortimanager_ipv4>
  set status {enable | disable}
end
```

Variable	Description	Default
`allow-push-configuration {enable | disable}`	Enable to accept configuration changes from the FortiManager unit. This command applies only if `status` is `enable` and `ip` is configured.	`disable`
`auto-backup {enable | disable}`	Enable to automatically send a configuration revision to the FortiManager unit when a FortiMail administrator logs out, if the configuration has changed. When configuration revisions are stored on a FortiManager unit, you can revert to any previous revision by using the command "restore config" on page 290. This command applies only if `central-management` is `enable` and `ip` is configured.	`disable`
`ip <fortimanager_ipv4>`	Enter the IP address of the FortiManager unit. This command applies only if `central-management` is `enable`.	0.0.0.0
`status {enable | disable}`	Enable to enable FortiManager support. Also configure `ip <fortimanager_ipv4>`, `auto-backup {enable | disable}`, and `allow-push-configuration {enable | disable}`. **Caution:** On the FortiManager unit, verify that the FortiMail unit has been registered with its device list. Failure to register the FortiMail unit may cause inability of the FortiMail unit to connect to the FortiManager unit.	`disable`

History

FortiMail v4.0 New.

Related topics

- execute central-mgmt

system certificate ca

Use this command to import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

CA certificates are required by connections that use transport layer security (TLS). For more information, see the *FortiMail Administration Guide*.

Syntax

```
config system certificate ca
  edit <name_str>
    set certificate <cert_str>
end
```

Variable	Description	Default
<name_str>	Enter a name for this certificate.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	

History

FortiMail v4.0 New.

Related topics

- config system certificate crl
- config system certificate local
- config system certificate remote

system certificate crl

Use this command to import certificate revocation lists.

To ensure that your FortiMail unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config system certificate crl
  edit <name_str>
    set crl <cert_str>
end
```

Variable	Description	Default
<name_str>	Enter a name for this certificate revocation list.	
crl <cert_str>	Enter or paste the certificate in PEM format to import it.	

History

FortiMail v4.0 New.

Related topics

- config system certificate ca
- config system certificate local
- config system certificate remote

system certificate local

Use this command to import signed certificates and certificate requests in order to install them for local use by the FortiMail unit.

FortiMail units require a local server certificate that it can present when clients request secure connections, including:

- the web-based manager (HTTPS connections only)
- webmail (HTTPS connections only)
- secure email, such as SMTPS, IMAPS, and POP3S

Caution: When using this command to import a local certificate, you must enter the commands in the order described in the following syntax. This is because the "set privatekey...." will need the password to decrypt the private key if it was encrypted and "set certificate ...." will try to find a matched private key file.

Syntax

```
config system certificate local
  edit <name_str>
    set password
    set private-key
    set certificate <cert_str>
    set csr <csr_str>
    set comments <comment_str>
end
```

Variable	Description	Default
<name_str>	Enter a name for the certificate to be imported.	
password	Enter a password for the certificate.	
private-key	Enter a private key for the certificate.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	
csr <csr_str>	Enter or paste the certificate signing request in PEM format to import it.	
comments <comment_str>	Enter any comments for this certificate.	

History

FortiMail v4.0 New.

Related topics

- config system certificate ca
- config system certificate crl
- config system certificate remote
- diagnose debug application starttls

system certificate remote

Use this command to import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA).

OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).

Remote certificates are required if you enable OCSP for PKI users.

Syntax

```
config system certificate remote
  edit <name_str>
    set certificate <cert_str>
end
```

Variable	Description	Default
<name_str>	Enter a name for the certificate to be imported.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	

History

FortiMail v4.0 New.

Related topics

- config system certificate ca
- config system certificate crl
- config system certificate local

system ddns

Use this command to configure the FortiMail unit to update a dynamic DNS (DDNS) service with its current public IP address.

Syntax

```
config system ddns
  edit <ddns-service_str>
    config domain
      edit domain <domain_str>\
        set ipmode {auto | bind | static}
        set interface <interface_str>
        set ip <host_ipv4>
        set status {enable | disable}
        set type {custom | dynamic | static}
    set password <password_str>
    set timeout <time_int>
    set username <username_str>
end
```

Variable	Description	Default
<ddns-service_str>	Enter one of the following DDNS update servers: • members.dhs.org • dipdnsserver.dipdns.com • www.dnsart.com • members.dyndns.org • www.dyns.net • ip.todayisp.com • ods.org • rh.tzo.com • ph001.oray.net **Note:** You must have an account with this DDNS service provider.	
domain <domain_str>	Enter the domain name that is tied to this username and server.	
ipmode {auto | bind | static}	Select the method of determining the IP address: • auto: Automatically detect the public IP address of the FortiMail unit and use that as the IP address to which domain <domain_str> will resolve. • bind: Use the IP address of a specific network interface as the IP address to which domain <domain_str> will resolve. Also configure interface <interface_str>. • static: Use the public IP address to which domain <domain_str> will resolve. Also configure ip <host_ipv4>.	auto
interface <interface_str>	Enter the specific network interface of which the IP address is used as the IP address to which domain <domain_str> will resolve.	
ip <host_ipv4>	Enter the public IP address to which domain <domain_str> will resolve.	
status {enable | disable}	Enable to notify a DDNS service provider to update public DNS records when the public IP address of the FortiMail unit changes.	disable
type {custom | dynamic | static}	Enter a service type for this domain.	
password <password_str>	Enter the password of the DDNS account.	

Variable	Description	Default
`timeout <time_int>`	Enter the amount of time in hours after which your FortiMail unit will contact the DDNS server to reaffirm its current IP address.	
`username <username_str>`	Enter the user name of your account with the DDNS service provider.	

History

FortiMail v4.0 New.

Related topics

- config system dns

system disclaimer

Use this command to 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. 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. For information on determining the directionality of an email message, see the *FortiMail Administration Guide*.

Syntax

```
config system disclaimer
  set incoming-body-content <disclaimer_str>
  set incoming-body-status {enable | disable}
  set incoming-header-content <disclaimer_str>
  set incoming-header-status {enable | disable}
  set outgoing-body-content <disclaimer_str>
  set outgoing-body-status {enable | disable}
  set outgoing-header-content <disclaimer_str>
  set outgoing-header-status {enable | disable}
end
```

Variable	Description	Default
`incoming-body-content <disclaimer_str>`	Enter the text that comprises the disclaimer message that appends to the message body of each incoming email.	
`incoming-body-status {enable | disable}`	Enable to append a disclaimer to the message body of each incoming email. Also configure incoming-body-content <disclaimer_str>.	`disable`
`incoming-header-content <disclaimer_str>`	Enter the text that comprises the disclaimer message that is inserted into the message header of each incoming email.	
`incoming-header-status {enable | disable}`	Enable to insert a disclaimer to the message header of each incoming email. Also configure incoming-header-content <disclaimer_str>.	`disable`
`outgoing-body-content <disclaimer_str>`	Enter the text that comprises the disclaimer message that appends to the message body of each outgoing email.	
`outgoing-body-status {enable | disable}`	Enable to append a disclaimer to the message body of each outgoing email. Also configure outgoing-body-content <disclaimer_str>.	`disable`
`outgoing-header-content <disclaimer_str>`	Enter the text that comprises the disclaimer message that is inserted into the message header of each outgoing email.	
`outgoing-header-status {enable | disable}`	Enable to insert a disclaimer to the message header of each outgoing email. Also configure outgoing-body-content <disclaimer_str>.	`disable`

History

FortiMail v4.0 New.

Related topics

- config system appearance

system dns

Use this command to configure the IP addresses of the primary and secondary DNS servers that the FortiMail unit will query to resolve domain names into IP addresses.

Syntax

```
config system dns
  set cache {enable | disable}
  set primary <dns_ipv4>
  set private_ip_query {enable | disable}
  set secondary <dns_ipv4>
end
```

Variable	Description	Default
`cache {enable | disable}`	Enable to cache DNS query results, improving performance. Disable the DNS cache to free memory if you are low on memory.	`enable`
`primary <dns_ipv4>`	Enter the IP address of the primary DNS server.	`0.0.0.0`
`private_ip_query {enable | disable}`	Enable to perform reverse DNS lookups on private network IP addresses, as defined in RFC 1918. The DNS server must have PTR records for your private network's IP addresses. Failure to contain records for those IP addresses may increase DNS query time and cause query results to be 'Host not found'.	`disable`
`secondary <dns_ipv4>`	Enter the IP address of the secondary DNS serve.	`0.0.0.0`

History

FortiMail v4.0 New.

Related topics

- config system ddns

system encryption ibe

Use this command to configure, enable, or disable Identity-Based Encryption (IBE) services, which control how secured mail recipients use the FortiMail IBE function.

Syntax

```
config system encryption ibe
  set expire-emails <days_int>
  set expire-inactivity <days_int>
  set expire-passwd-reset <hours_int>
  set expire-registration <days_int>
  set secure-compose {enable | disable}
  set secure-reply {enable | disable}
  set secure-forward {enable | disable}
  set service-name <name_str>
  set status {enable | disable}
  set url-about <url_str>
  set url-base <url_str>
  set url-help <url_str>
end
```

Variable	Description	Default
`expire-emails <days_int>`	Enter the number of days that the secured mail will be saved on the FortiMail unit.	`180`
`expire-inactivity <days_int>`	Enter the number of days the secured 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 he/she registers on the unit, the recipient will need to register again if another secured mail is sent to him/her. If the recipient accessed the FortiMail unit on the 15th days, the 30-day limit will be recalculated from the 15th day onwards.	`90`
`expire-passwd-reset <hours_int>`	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 his/her password within this time limit to access the FortiMail unit.	`24`
`expire-registration <days_int>`	Enter the number of days that the secured 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.	`30`
`secure-compose {enable | disable}`	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.	`disable`
`secure-reply {enable | disable}`	Allow the secured mail recipient to reply to the email with encryption.	`disable`
`secure-forward {enable | disable}`	Allow the secured mail recipient to forward the email with encryption	`disable`
`service-name <name_str>`	Enter the name for the IBE service. This is the name the secured mail recipients will see once they access the FortiMail unit to view the mail.	
`status {enable | disable}`	Enable the IBE service you have configured.	`disable`

Variable	Description	Default
`url-about <url_str>`	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 option empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification.	
`url-base <url_str>`	Enter the FortiMail unit URL, for example, https://192.168.100.20, where a mail recipient can register or authenticate to access the secured mail.	
`url-help <url_str>`	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 option empty, a default help file link will be added to the secure mail notification.	

History

FortiMail v4.0 MR1 New.

Related topics

- profile encryption
- profile content-action
- policy access-control delivery

system fortiguard antivirus

Use this command to configure how the FortiMail unit will retrieve the most recent updates to FortiGuard Antivirus engines and definitions.

Syntax

```
config system fortiguard antivirus
  set override-server-address <virtual-ip_ipv4>
  set override-server-status {enable | disable}
  set push-update-override-address <virtual-ip_ipv4>
  set push-update-override-port <port_int>
  set push-update-override-status {enable | disable}
  set push-update-status {enable | disable}
  set scheduled-update-day <day_int>
  set scheduled-update-frequency {daily | every | weekly}
  set scheduled-update-status {enable | disable}
  set scheduled-update-time <time_str>
  set tunneling-address <host_ipv4>
  set tunneling-password <password_str>
  set tunneling-port <port_int>
  set tunneling-status {enable | disable}
  set tunneling-username <username_str>
end
```

Variable	Description	Default
`override-server-address <virtual-ip_ipv4>`	If `override-server-status` is `enable`, enter the IP address of the public or private FortiGuard Distribution Server (FDS) that overrides the default FDS to which the FortiMail unit connects for updates.	
`override-server-status {enable | disable}`	Enable to override the default FDS to which the FortiMail unit connects for updates.	`disable`
`push-update-override-address <virtual-ip_ipv4>`	If `push-update-override-status` is `enable`, enter the public IP address that will forward push updates to the FortiMail unit. Usually, this is a virtual IP address on the external interface of a NAT device such as a firewall or router.	
`push-update-override-port <port_int>`	If `push-update-override-status` is `enable`, enter the port number that will forward push updates to UDP port 9443 the FortiMail unit. Usually, this is a port forward on the external interface of a NAT device such as a firewall or router.	
`push-update-override-status {enable | disable}`	Enable to override the default IP.	`disable`
`push-update-status {enable | disable}`	Enable to allow the FortiMail unit to receive notifications of available updates, which trigger it to download FortiGuard Antivirus packages from the Fortinet Distribution Network (FDN).	`disable`
`scheduled-update-day <day_int>`	Enter the day of the week at which the FortiMail unit will request updates where the range is from 0-6 and 0 means Sunday and 6 means Saturday.	
`scheduled-update-frequency {daily | every | weekly}`	Enter the frequency at which the FortiMail unit will request updates. Also configure scheduled-update-day <day_int> and scheduled-update-time <time_str>.	`weekly`
`scheduled-update-status {enable | disable}`	Enable to perform updates according to a schedule.	`enable`

Variable	Description	Default
`scheduled-update-time <time_str>`	Enter the time of the day at which the FortiMail unit will request updates, in the format hh:mm, where hh is the number of hours and mm is the number of minutes after the hour in 15 minute intervals.	`01:00`
`tunneling-address <host_ipv4>`	If `tunneling-status` is `enable`, enter the IP address of the web proxy.	
`tunneling-password <password_str>`	If `tunneling-status` is `enable`, enter the password of the account on the web proxy.	
`tunneling-port <port_int>`	If `tunneling-status` is `enable`, enter the TCP port number on which the web proxy listens.	
`tunneling-status {enable | disable}`	Enable to tunnel update requests through a web proxy.	`disable`
`tunneling-username <username_str>`	If `tunneling-status` is `enable`, enter the user name of the FortiMail unit's account on the web proxy.	

History

FortiMail v4.0 New.

Related topics

- config system fortiguard antispam
- execute update-now
- diagnose debug application updated

system fortiguard antispam

Use this command to configure how the FortiMail unit will retrieve the most recent updates to FortiGuard Antispam engines and definitions.

Syntax

```
config system fortiguard antispam
  set cache-mpercent <percentage_int>
  set cache-status {enable | disable}
  set cache ttl <ttl_int>
  set hostname {<fqdn_str> | <host_ipv4>}
  set port {53 | 8888 | 8889}
  set query-timeout <timeout_int>
  set server-override-ip <ipv4>
  set server-override-status {enable | disable}
  set status {enable | disable}
end
```

Variable	Description	Default
`cache-mpercent <percentage_int>`	Enter the percentage of memory the antispam cache is allowed to use in percentage. The range is 1-15%.	2
`cache-status {enable | disable}`	Enable to query to the FortiGuard Distribution Network (FDN) for FortiGuard Antispam ratings. This option must be enabled for antispam profiles where the FortiGuard Antispam scan is enabled to have an effect.	`enable`
`cache ttl <ttl_int>`	Enter the time to live (TTL) in seconds for cache entries.	`300`
`hostname {<fqdn_str> | <host_ipv4>}`	Enter an IP address or a fully qualified domain name (FQDN) to override the default FortiGuard Antispam query server.	`antispam.fortigate.com`
`port {53 | 8888 | 8889}`	Enter the port number used to communicate with the FortiGuard Antispam query servers.	`53`
`query-timeout <timeout_int>`	Enter the timeout value for the FortiMail unit to query the FortiGuard Antispam query server.	`7`
`server-override-ip <ipv4>`	If `server-override-status` is `enable`, enter the IP address of the public or private FortiGuard Antispam query server that overrides the default query server to which the FortiMail unit connects for updates.	
`server-override-status {enable | disable}`	Enable to override the default FortiGuard Antispam query server to which the FortiMail unit connects for updates.	`disable`
`status {enable | disable}`	Enable to allow the FortiMail unit to retrieve the most recent updates to FortiGuard Antispam engines and definitions.	`enable`

History

FortiMail v4.0 New.

Related topics

- config system fortiguard antivirus
- execute update-now
- diagnose debug application updated

system global

Use this command to configure many FortiMail system-wide configurations.

Syntax

```
config system global
  set access-banner {admin | webmail | ibe}
  set admin-idle-timeout <timeout_int>
  set default-certificate <name_str>
  set disclaimer-per-domain {enable | disable}
  set disk-monitor {enable | disable}
  set hostname <host_str>
  set lcdpin <pin_int>
  set lcdprotection {enable | disable}
  set ldap-conn-monitor {enable | disable}
  set ldap-sess-cache-size <session_int>
  set ldap-sess-cache-state {enable | disable}
  set operation mode {gateway | server | transparent}
  set pki-certificate-req {yes | no}
  set pkimode {enable | disable}
  set strong-crypto {enable | disable}
end
```

Variable	Description	Default
`access-banner {admin | webmail | ibe}`	Enable or disable the legal disclaimer. • `admin`: Select to display the disclaimer message when the administrator logs into the FortiMail unit web-based manager. • `webmail`: Select to display the disclaimer message when the user logs into the FortiMail Webmail. • `ibe`: Select to display the disclaimer message when the user logs into the FortiMail unit to view IBE encrypted email.	
`admin-idle-timeout <timeout_int>`	Enter the amount of time in minutes after which an idle administrative session will be automatically logged out. The maximum idle time out is 480 minutes (8 hours). To improve security, do not increase the idle timeout.	5
`default-certificate <name_str>`	Enter the name of a local certificate to use it as the “default" (that is, currently chosen for use) certificate. FortiMail units require a local server certificate that it can present when clients request secure connections.	
`disclaimer-per-domain {enable | disable}`	Enable to allow individualized disclaimers to be configured for each protected domain.	
`disk-monitor {enable | disable}`	Enable to monitor the hard disk status of the FortiMail unit. If a problem is found, an alert email is sent to the administrator.	`disable`
`hostname <host_str>`	Enter the host name of the FortiMail unit.	Varies by model.
`lcdpin <pin_int>`	Enter the 6-digit personal identification number (PIN) that administrators must enter in order to access the FortiMail LCD panel. The PIN is used only when `lcdprotection` is `enable`.	Encoded value varies.
`lcdprotection {enable | disable}`	Enable to require that administrators enter a PIN in order to use the buttons on the front LCD panel. Also configure `lcdpin`.	`disable`

Variable	Description	Default
`ldap-conn-monitor {enable | disable}`	Enable to monitor the connection status to LDAP server. If FortiMail's connection to the LDAP server is not healthy, the FortiMail LDAP daemon may not do off-box query all the time; instead, the LDAP daemon will return TEMPFAIL to the LDAP query right away. This is intended to reduce the burden on the alreay heavily loaded LDAP server. This feature is enabled by default. In some cases, this feature may not be desired.	`enable`
`ldap-sess-cache-size <session_int>`	Enter the number of connection sessions allowed from the FortiMail unit to the LDAP server. This option applies when `ldap-sess-cache-state` is `enable`.	`10`
`ldap-sess-cache-state {enable | disable}`	Enable to keep the continuity of the connection sessions to the LDAP server. Repeated session connections waste network resources. Also configure ldap-sess-cache-size.	`enable`
`operation mode {gateway | server | transparent}`	Enter one of the following operation modes: • `gateway`: The FortiMail unit acts as an email gateway or MTA, but does not host email accounts. • `server`: The FortiMail unit acts as a standalone email server that hosts email accounts and acts as an MTA. • `transparent`: The FortiMail unit acts as an email proxy.	`gateway`
`pki-certificate-req {yes | no}`	If the administrator's web browser does not provide a valid personal certificate for PKI authentication, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter `yes`. To allow password-style fallback, enter `no`.	`no`
`pkimode {enable | disable}`	Enable to allow PKI authentication for FortiMail administrators. For more information, see "config user pki" on page 206 and "config system admin" on page 159. Also configure `pki-certificate-req {yes | no}`. **Caution:** Before disabling PKI authentication, select another mode of authentication for FortiMail administrators and email users that are currently using PKI authentication. Failure to first select another authentication method before disabling PKI authentication will prevent them from being able to log in.	`disable`
`strong-crypto {enable | disable}`	Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta) and higher. Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.	`disable`

History

FortiMail v4.0	New.
FortiMail v4.0 MR1	Added `strong-crypto {enable | disable}` and `acccess-banner`.
v4.0 Patch 5 **v4.0 MR1 Patch 1**	Added `ldap-conn-monitor {enable | disable}`.

Related topics

- config config domain-setting

system ha

Use this command to configure the FortiMail unit to act as a member of a high availability (HA) cluster in order to increase processing capacity or availability. It also enables you to monitor the HA cluster.

Syntax

```
config system ha
  set failover <interface_str> {add | bridge | ignore |
     set}<address_ipv4mask>
  set hard-drives-check {enable | disable}
  set hb-base-port <interface_int>
  set hb-lost-threshold
  set heartbeat-1-interface <interface_int>
  set heartbeat-1-ip <local_ipv4mask>
  set heartbeat-1-peer <primary-peer_ipv4>
  set heartbeat-2-interface <interface_str>
  set heartbeat-2-ip <secondary-local_ipv4mask>
  set heartbeat-2-peer <secondary-peer_ipv4>
  set http-check {enable | disable}
  set imap-check {enable | disable}
  set local-service {ports | hd} <interval_int> <retries_int>
  set mail-data-sync {enable | disable}
  set mailqueue-data-sync {enable | disable}
  set mode {config-master | config-slave | master | off | slave}
  set network-intf-check {enable | disable}
  set on-failure {off | restore-role | become-slave}
  set password <password_str>
  set pop-check {enable | disable}
  set port-monitor {enable | disable}
  set remote-service {smtp | pop | imap | http} <interface_ipv4> <port_int>
     <interval_int> <wait_int> <retries_int>
  set remote-services-as-heartbeat {enable | disable}
  set smtp-check {enable | disable}
end
```

Variable	Description	Default
failover <interface_str> {add | bridge | ignore | set}<address_ipv4mask>	Use this option to configure whether and how to configure the IP addresses and netmasks of the FortiMail unit whose effective operating mode is currently MASTER. For example, a primary unit might be configured to receive email traffic through port1 and receive heartbeat and synchronization traffic through port5 and port6. In that case, you would configure the primary unit to set the IP addresses or add virtual IP addresses for port1 of the backup unit upon failover in order to mimic that of the primary unit. This option applies only for FortiMail units operating in the active-passive HA mode, as a primary unit. (The configuration of this command is synchronized to the backup unit for use when it assumes the role of the primary unit.) Enter the name of a network interface, such as port6, or enter mgmt to configure the management IP address (transparent mode only), then enter one of the following behaviors of the network interface when this FortiMail unit is acting as the primary unit: • ignore: Do not change the network interface configuration upon failover, and do not monitor. For details on service monitoring for network interfaces, see local-service {ports | hd} <interval_int> <retries_int>. Primary and secondary heartbeat network interfaces must use this option. • set: Change the network interface to use the specified IP address and netmask upon failover. • add: Add the specified virtual IP address and netmask to the network interface upon failover. Normally, you will configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. Both originating and reply traffic uses the virtual IP address. Unlike set, this option results in the network interface having two IP Addresses: the actual and the virtual. • bridge: Include the network interface in the Layer 2 bridge. While the effective operating mode is SLAVE, the interface is deactivated and cannot process traffic, preventing Layer 2 loops. Then, when the effective operating mode becomes MASTER, the interface is activated again and can process traffic. This option applies only if the FortiMail unit is operating in transparent mode, and for FortiMail interfaces that are already members of the bridge. For information on configuring bridging network interfaces, see "config system interface" on page 187. Network interface(s) configured as the primary heartbeat and secondary heartbeat network interface are required to maintain their IP addresses for heartbeat and synchronization purposes, and cannot be configured with the type set or bridge. After entering a network interface behavior, enter the IP address and netmask. If you have entered bridge or ignore for the previous keyword, because those behaviors do not use IP addresses, you may enter 0.0.0.0 0.0.0.0.	
hard-drives-check {enable | disable}	Enable to test the responsiveness of the hard drives.	disable
hb-base-port <interface_int>	Enter the first of four total TCP port numbers that will be used for: • the heartbeat signal • synchronization control • data synchronization • configuration synchronization **Note:** For active-passive groups, in addition to configuring the heartbeat, you can configure service monitoring. For details, see local-service {ports | hd} <interval_int> <retries_int>.	20000

Variable	Description	Default
hb-lost-threshold	Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the backup unit assumes the role of the primary unit. The heartbeat will continue to check for availability once per second. To prevent premature failover when the primary unit is simply experiencing very heavy load, configure a total threshold of three (3) seconds or more to allow the backup unit enough time to confirm unresponsiveness by sending additional heartbeat signals. This option appears only for active-passive groups. **Note:** If the failure detection time is too short, the backup unit may falsely detect a failure when during periods of high load. **Caution:** If the failure detection time is too long the primary unit could fail and a delay in detecting the failure could mean that email is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover.	15
heartbeat-1-interface <interface_int>	Enter the name of the network interface that will be used for the primary heartbeat, and that is connected directly or through a switch to the primary heartbeat interface of the other FortiMail unit(s) in the HA group.	Varies by model. (The network interface with the highest number.)
heartbeat-1-ip <local_ipv4mask>	Enter the IP address and netmask of the primary network interface, separated by a space. Use this IP address as the value of the peer IP address when configuring heartbeat-1-peer <primary-peer_ipv4> for the other FortiMail units in the HA group.	10.0.0.1 255.255.255.0
heartbeat-1-peer <primary-peer_ipv4>	Enter the IP address of the primary heartbeat network interface on the other FortiMail unit in the HA group. For example, if the primary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.1, enter 10.0.0.1.	10.0.0.2
heartbeat-2-interface <interface_str>	Enter the name of a network interface: Use this network interface as the secondary heartbeat network interface. It must be connected to the secondary heartbeat network interface on the other FortiMail unit in the HA group. Also configure config heartbeat-2-ip <secondary-local_ipv4mask>.	Varies by model. (The network interface with the highest number.)
heartbeat-2-ip <secondary-local_ipv4mask>	Enter the IP address and netmask of the secondary network interface, separated by a space. Use this IP address as the value of the peer IP address when configuring heartbeat-2-peer <secondary-peer_ipv4> for the other FortiMail units in the HA group.	0.0.0.0 0.0.0.0
heartbeat-2-peer <secondary-peer_ipv4>	Enter the IP address of the secondary heartbeat network interface on the other FortiMail unit in the HA group. For example, if the secondary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.3, enter 10.0.0.3.	0.0.0.0
http-check {enable | disable}	Enable to test the connection responsiveness of HTTP.	disable
imap-check {enable | disable}	Enable to test the connection responsiveness of IMAP.	disable

Variable	Description	Default
`local-service {ports | hd} <interval_int> <retries_int>`	Enter a local service to monitor. If you enter `ports`, continue entering: • `<interval_int>`: Enter the amount of time in seconds between each network interface check. The valid range is between 1 and 60 seconds, or 0 to disable checking. The default value is 0. • `<retries_int>`: Enter the number of times a network interface must consecutively fail to respond in order to trigger a failover. The valid range is 1 to a very high number. The default value is 0. If you enter `hd`, continue entering: • `<interval_int>`: Enter the amount of time in seconds between each hard drive check. The valid range is between 1 and 60 seconds, or 0 to disable checking. The default value is 0. • `<retries_int>`: Enter the number of times a hard drive must consecutively fail to respond in order to trigger a failover. The valid range is 1 to a very high number. The default value is 0. During local service monitoring, the primary unit in an active-passive HA group monitors its own network interfaces and hard drives. If service monitoring detects a failure, the effective operating mode of the primary unit switches to OFF or FAILED (depending on the “On failure" setting) and, if configured, the FortiMail units send HA event alert email, record HA event log messages, and send HA event SNMP traps.A failover then occurs, and the effective operating mode of the backup unit switches to MASTER. This command applies only if the FortiMail unit is operating in an active-passive HA group, as the primary unit.	`PORTS 10 3` `HD 10 3`
`mail-data-sync {enable | disable}`	Enable to synchronize system quarantine, email archives, email users’ mailboxes (server mode only), preferences, and per-recipient quarantines. Unless the HA cluster stores its mail data on a NAS server, you should configure the HA cluster to synchronize mail directories. This option applies only for active-passive groups.	`enable`
`mailqueue-data-sync {enable | disable}`	Enable to synchronize the mail queue of the FortiMail unit. This option applies only for active-passive groups. **Caution:** If the primary unit experiences a hardware failure and you cannot restart it, if this option is disabled, MTA spool directory data could be lost. **Note:** Enabling this option is not recommended. Periodic synchronization can be processor and bandwidth-intensive. Additionally, because the content of the MTA spool directories is very dynamic, periodically synchronizing MTA spool directories between FortiMail units may not guarantee against loss of all email in those directories. Even if MTA spool directory synchronization is disabled, after a failover, a separate synchronization mechanism may successfully prevent loss of MTA spool data.	`disable`
`mode {config-master | config-slave | master | off | slave}`	Enter one of the following HA operating modes: • `config-master`: Enable HA and operate as the primary unit in a config-only HA group. • `config-slave`: Enable HA and operate as the backup unit in a config-only HA group. • `master`: Enable HA and operate as the primary unit in an active-passive HA group. • `off`: Disable HA. Each FortiMail unit operates independently. • `slave`: Enable HA and operate as the backup unit in an active-passive HA group. **Caution:** For config-only HA, if the FortiMail unit is operating in server mode, you must store mail data externally, on a NAS server. Failure to store mail data externally could result in mailboxes and other data scattered over multiple FortiMail units. For details on configuring NAS, see the *FortiMail Administration Guide*.	`off`

Variable	Description	Default
network-intf-check {enable | disable}	Enable to test the responsiveness of network interfaces. Network interface monitoring tests all active network interfaces whose: • failover <interface_str> {add | bridge | ignore | set}<address_ipv4mask>setting is ***not*** ignore • port-monitor {enable | disable} setting is enable.	enable
on-failure {off | restore-role | become-slave}	Enter one of the following behaviors of the primary unit when it detects a failure. • off: Do not process email or join the HA group until you manually select the effective operating mode. • restore-role: On recovery, the failed primary unit's effective operating mode resumes its configured operating mode. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent. • become-slave: On recovery, the failed primary unit's effective operating mode becomes SLAVE (backup), and it then synchronizes the content of its MTA spool directories with the current primary unit. The new primary unit can then deliver email that existed in the former primary unit's MTA spool at the time of the failover. In most cases, you should enter become-slave. For details on the effects of this option on the effective operating mode, see the *FortiMail Administration Guide*. For information on configuring service/interface monitoring, see local-service {ports | hd} <interval_int> <retries_int>, remote-service {smtp | pop | imap | http} <interface_ipv4> <port_int> <interval_int> <wait_int> <retries_int> and remote-services-as-heartbeat {enable | disable}. This option applies only if the FortiMail unit is operating in an active-passive HA group, as a primary unit.	
password <password_str>	Enter a password for the HA group. The password must be the same on the primary and backup FortiMail unit(s). The password must be a least 1 character.	change_me
pop-check {enable | disable}	Enable to test the connection responsiveness of POP service.	disable
port-monitor {enable | disable}	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover. This option applies only if local network interface monitoring is enabled. For details, see local-service {ports | hd} <interval_int> <retries_int>.	
remote-service {smtp | pop | imap | http} <interface_ipv4> <port_int> <interval_int> <wait_int> <retries_int>	Enter a remote service to monitor. Then enter the subsequent values in order: • <interface_ipv4>: Enter the IP address to contact when testing the availability of the service. The default value is 0.0.0.0. • <port_int>: Enter the TCP port number on which the remote FortiMail unit listens for connections of that service type. The default value is 0. For example, if you have configured the primary FortiMail unit to listen for SMTP connections on TCP port 25, you would enter 25. • <interval_int>: Enter the interval in minutes between each remote service availability test. The valid range is 1 to 60 minutes. The default value is 0. • <wait_int>: Enter the amount of time in seconds to wait for the primary unit to respond to the remote service availability test. The valid range is 1 to a very high number of seconds, or 0 to disable remote service monitoring. The default value is 0. • <retries_int>: Enter the number of consecutive availability test failures after which the primary unit is deemed unresponsive and a failover occurs. The valid range is 1 to a very high number. The default value is 0. This option applies only if the FortiMail unit is operating in an active-passive HA group, as a backup unit.	

Variable	Description	Default
`remote-services-as-heartbeat {enable | disable}`	Enable to use remote service monitoring as a tertiary heartbeat signal. This option applies only for FortiMail units operating in the active-passive HA mode, and requires that you also configure remote service monitoring using remote-service {smtp | pop | imap | http} <interface_ipv4> <port_int> <interval_int> <wait_int> <retries_int>.	
`<wait_int>`	Enter the amount of time in seconds to wait for the primary unit to respond to the remote service availability test. The valid range is 1 to a very high number of seconds, or 0 to disable remote service monitoring.	`0`
`<retries_int>`	Enter the number of consecutive availability test failures after which the primary unit is deemed unresponsive and a failover occurs. The valid range is 1 to a very high number.	`0`
`smtp-check {enable | disable}`	Enable to test the connection responsiveness of SMTP.	`disable`

History

FortiMail v4.0 New.

Related topics

- config system global
- diagnose debug application hahbd
- diagnose debug application hasyncd
- diagnose system ha failover
- diagnose system ha restore
- diagnose system ha showcsum
- diagnose system ha sync

system interface

Use this command to configure allowed and denied administrative access protocols, maximum transportation unit (MTU) size, and up or down administrative status for the network interfaces of a FortiMail unit.

Syntax

```
config system interface
  edit interface <interface_str>
    set allowaccess {ping http https snmp ssh telnet}
    set ip <ipv4mask>
    set mac-addr <xx.xx.xx.xx.xx.xx>
    set mode {static | dhcp}
    set mtu <mtu_int>
    set speed {auto | 10full | 10half | 100full | 100half | 1000full}
    set status {down | up}
end
```

Variable	Description	Default
`interface <interface_str>`	Enter the name of the network interface.	
`allowaccess {ping http https snmp ssh telnet}`	Enter one or more of the following protocols to add them to the list of protocols permitted to administratively access the FortiMail unit through this network interface: • `ping`: Allow ICMP ping responses from this network interface. • `http`: Allow HTTP access to the web-based manager, webmail, and per-recipient quarantines. **Caution:** HTTP connections are ***not*** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. • `https`: Allow secure HTTP (HTTPS) access to the web-based manager, webmail, and per-recipient quarantines. • `snmp`: Allow SNMP v2 access. For more information, see "system snmp community" on page 195, "system snmp sysinfo" on page 197, and "system snmp threshold" on page 198. • `ssh`: Allow SSH access to the CLI. • `telnet`: Allow Telnet access to the CLI. **Caution:** Telnet connections are ***not*** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. To control SMTP access, configure access control rules and session profiles. For details, see "config policy access-control receive" on page 99 and "config profile session" on page 146.	Varies by the network interface.
`ip <ipv4mask>`	Enter the IP address and netmask of the network interface. If the FortiMail unit is in transparent mode, *IP*/*Netmask* may alternatively display *bridging*. This means that the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, *IP* and *Netmask* may alternatively display *bridged (isolated)* while the effective operating mode is *slave* and therefore the network interface is currently disconnected from the network, or *bridging (waiting for recovery)* while the effective operating mode is *failed* and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity.	
`mac-addr <xx.xx.xx.xx.xx.xx>`	Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx.	Factory set

Variable	Description	Default
`mode {static | dhcp}`	Enter the interface mode. DHCP mode applies only if the FortiMail unit is operating in gateway mode or server mode.	`static`
`mtu <mtu_int>`	Enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The valid range is from 576 to 1500 bytes.	`1500`
`speed {auto | 10full | 10half | 100full | 100half | 1000full}`	Enter the speed of the network interface. **Note:** Some network interfaces may not support all speeds.	`auto`
`status {down | up}`	Enter either `up` to enable the network interface to send and receive traffic, or `down` to disable the network interface.	`up`

History

FortiMail v4.0 New.

Related topics

- config system accprofile
- config system admin

system mailserver

Use this command to configure the system-wide mail settings.

Syntax

```
config system mailserver
  set deadmail-expiry <time_int>
  set defer-delivery-starttime <time_str>
  set defer-delivery-stoptime <time_str>
  set delivery-esmtp {no | yes}
  set dsn-sender-address <email_str>
  set dsn-sender-displayname <name_str>
  set dsn-status {enable | disable}
  set ldap-domaincheck {enable | disable}
  set ldap-domaincheck-auto-associate {enable | disable}
  set ldap-domaincheck-internal-domain <domain_str>
  set ldap-domaincheck-profile <profile_str>
  set local-domain-name <local-domain_str>
  set pops-port <port_int>
  set queue-dsn-timeout <timeout_int>
  set queue-retry <interval_int>
  set queue-timeout <timeout_int>
  set queue-warning <first-dsn_int>
  set smtp-auth {enable | disable}
  set smtp-auth-over-tls {enable | disable}
  set smtp-auth-smtps {enable | disable}
  set smtp-max-connections <connection_int>
  set smtp-msa {enable | disable}
  set smtp-msa-port <port_int>
  set smtp-port <port_int>
  set smtps-port <port_int
  set smtps-tls-status {enable | disable}
  set timeout-connect <seconds_int>
  set timeout-greeting <seconds_int>
end
```

Variable	Description	Default
`deadmail-expiry <time_int>`	Enter the number of days to keep permanently undeliverable email in the dead mail folder. Dead mail has both incorrect recipient and sender email addresses, and can neither be delivered nor the sender notified. The valid range is from 1 to 365 days.	1
`defer-delivery-starttime <time_str>`	Enter the time that the FortiMail unit will begin to process deferred oversized email, using the format hh:mm, where hh is the hour according to a 24-hour clock, and mm is the minutes.	`00:00`
`defer-delivery-stoptime <time_str>`	Enter the time that the FortiMail unit will stop processing deferred oversized email, using the format hh:mm, where hh is the hour according to a 24-hour clock, and mm is the minutes.	`00:00`
`delivery-esmtp {no | yes}`	Enter either: • `yes`: Disable the FortiMail unit from delivering email using ESMTP, and use standard SMTP instead. • `no`: Enable the FortiMail unit to deliver email using ESMTP if the SMTP server to which it is connecting supports the protocol.	`no`

Variable	Description	Default
dsn-sender-address <email_str>	Enter the sender email address in delivery status notification (DSN) email messages sent by the FortiMail unit to notify email users of delivery failure. If this string is empty, the FortiMail unit sends DSN from the default sender email address of “postmaster@example.com", where “example.com" is the domain name of the FortiMail unit.	
dsn-sender-displayname <name_str>	Enter the display name of the sender email address for DSN. If this string is empty, the FortiMail unit uses the display name “postmaster".	
dsn-status {enable | disable}	Enable to allow DSN email generation.	disable
ldap-domaincheck {enable | disable}	Enable to verify the existence of domains that have not been configured as protected domains. Also configure ldap-domaincheck-profile <profile_str> and ldap-domaincheck-auto-associate {enable | disable}. To verify the existence of unknown domains, the FortiMail unit queries an LDAP server for a user object that contains the email address. If the user object exists, the verification is successful, the action varies by configuration of ldap-domaincheck-auto-associate {enable | disable}.	disable
ldap-domaincheck-auto-associate {enable | disable}	If ldap-domaincheck is enable, select whether to enable or disable automatic creation of domain associations. • enable: The FortiMail unit automatically adds the unknown domain as a domain associated of the protected domain selected in ldap-domaincheck-internal-domain <domain_str>. • disable: If the DNS lookup of the unknown domain name is successful, the FortiMail unit routes the email to the IP address resolved for the domain name during the DNS lookup. Because the domain is not formally defined as a protected domain, the email is considered to be outgoing, and outgoing recipient-based policies are used to scan the email. For more information, see “config policy recipient” on page 106.	disable
ldap-domaincheck-internal-domain <domain_str>	If ldap-domaincheck is enable, and ldap-domaincheck-auto-associate is enable, enter name of the protected domain with which successfully verified domains will become associated.	
ldap-domaincheck-profile <profile_str>	If ldap-domaincheck is enable, enter the name of the LDAP profile to use when verifying unknown domains.	
local-domain-name <local-domain_str>	Enter the name of the domain to which the FortiMail unit belongs, such as example.com. This option applies only if the FortiMail unit is operating in server mode.	
pops-port <port_int>	Enter the port number on which the FortiMail unit’s POP3 server will listen for POP3 connections. The default port number is 110. This option applies only if the FortiMail unit is operating in server mode.	110
queue-dsn-timeout <timeout_int>	Enter the maximum number of days a delivery status notification (DSN) message can remain in the mail queues. If the maximum time is set to zero (0) days, the FortiMail unit attempts to deliver the DSN only once. After the maximum time has been reached, the DSN email is moved to the dead mail folder. The valid range is from zero to ten days.	5
queue-retry <interval_int>	Enter the number of minutes between delivery retries for email messages in the deferred and spam mail queues. The valid range is from 10 to 120 minutes.	27

Variable	Description	Default
`queue-timeout <timeout_int>`	Enter the maximum number of hours that deferred email messages can remain in the deferred or spam mail queue, during which the FortiMail unit periodically retries to send the message. After the maximum time has been reached, the FortiMail unit will send a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable. The valid range is from 1 to 240 hours.	`120`
`queue-warning <first-dsn_int>`	Enter the number of hours after an initial failure to deliver an email message before the FortiMail unit sends the first delivery status notification (DSN) email message to notify the sender that the email message has been deferred. After sending this initial DSN, the FortiMail unit will continue to retry sending the email until reaching the limit configured in `timeout`. The valid range is from 1 to 24 hours.	`4`
`smtp-auth {enable | disable}`	Enable to accept the `AUTH` command to authenticate email users for connections using SMTP.	`enable`
`smtp-auth-over-tls {enable | disable}`	Enable to accept the `AUTH` command to authenticate email users for connections using SMTP over TLS.	`enable`
`smtp-auth-smtps {enable | disable}`	Enable to accept the `AUTH` command to authenticate email users for connections using SMTPS (SMTP with SSL).	`enable`
`smtp-max-connections <connection_int>`	Enter the maximum number of concurrent smtp connections.	`256`
`smtp-msa {enable | disable}`	Enable to allow your email clients to use SMTP for message submission on a separate TCP port number from deliveries or mail relay by MTAs. For details on message submission by email clients as distinct from SMTP used by MTAs, see RFC 2476.	`disable`
`smtp-msa-port <port_int>`	Enter the TCP port number on which the FortiMail unit listens for email clients to submit email for delivery.	`587`
`smtp-port <port_int>`	Enter the port number on which the FortiMail unit's SMTP server will listen for SMTP connections.	`25`
`smtps-port <port_int`	Enter the port number on which the FortiMail unit's built-in MTA listens for secure SMTP connections.	`465`
`smtps-tls-status {enable | disable}`	Enable to allow SSL- and TLS-secured connections from SMTP clients that request SSL/TLS. When disabled, SMTP connections with the FortiMail unit's built-in MTA must occur as clear text, unencrypted.	`disable`
`timeout-connect <seconds_int>`	Enter the maximum amount of time to wait, after the FortiMail unit initiates it, for the receiving SMTP server to establish the network connection. The valid range is 10 to 120. **Note:** This timeout applies to all SMTP connections, regardless of whether it is the first connection to that SMTP server or not.	`30`
`timeout-greeting <seconds_int>`	Enter the maximum amount of time to wait for an SMTP server to send SMTP reply code 220 to the FortiMail unit. The valid range is 10 to 360. **Note:** RFC 2821 recommends a timeout value of 5 minutes (300 seconds). For performance reasons, you may prefer to have a smaller timeout value, which reduces the amount of time spent waiting for sluggish SMTP servers. However, if this causes your FortiMail unit to be unable to successfully initiate an SMTP session with some SMTP servers, consider increasing the timeout.	`60`

History

FortiMail v4.0	New.

Related topics

- config system route

system password-policy

Use this command to configure password policy for administrators, FortiMail Webmail users, and IBE encrypted email users..

Syntax

```
config system password-policy
  set status {enable | disable}
  set apply-to {admin-user | ibe-user | local-mail-user}
  set minimum-length <minimum_int>
  set must-contain {upper-case-letter | lower-case-letter | number | non-
     alphanumeric}

end
```

Variable	Description	Default
`status {enable | disable}`	Select to enable the password policy.	
`apply-to {admin-user | ibe-user | local-mail-user}`	Select where to apply the password policy: `admin_user` — Apply to administrator passwords. If any password does not conform to the policy, require that administrator to change the password at the next login. `local-mail-user` — Apply to FortiMail webmail users' passwords. If any password does not conform to the policy, require that user to change the password at the next login. `ibe-user` — Apply to the passwords of the users who access the FortiMail unit to view IBE encrypted email. If any password does not conform to the policy, require that user to change the password at the next login.	
`minimum-length <minimum_int>`	Set the minimum acceptable length for passwords.	`8`
`must-contain {upper-case-letter | lower-case-letter | number | non-alphanumeric}`	Select any of the following special character types to require in a password. Each selected type must occur at least once in the password. • `upper-case-letter` — A, B, C, ... Z • `lower-case-letter` — a, b, c, ... z • `number` — 0, 1, 2, 3, 4, 5, 6, 7 8, 9 • `non-alphanumeric` — punctuation marks, @,#, ... %	

History

FortiMail v4.0 MR1 New.

Related topics

- config system mailserver

system route

Use this command to configure static routes.

Syntax

```
config system route
  edit <route_int>
    set destination <destination_ipv4mask>
    set gateway <gateway_ipv4>
end
```

Variable	Description	Default
<route_int>	Enter the index number of the route in the routing table.	
destination <destination_ipv4mask>	Enter the destination IP address and netmask of traffic that will be subject to this route, separated with a space. To indicate all traffic regardless of IP address and netmask, enter 0.0.0.0 0.0.0.0.	0.0.0.0 0.0.0.0
gateway <gateway_ipv4>	Enter the IP address of the gateway router.	0.0.0.0

History

FortiMail v4.0 New.

Related topics

- config system mailserver

system snmp community

Use this command to configure simple network management protocol (SNMP) settings.

These commands apply only if the SNMP agent is enabled. For details, see status {enable | disable}.

Syntax

```
config system snmp community
  edit <index_int>
    config host
      edit <index_int>
        set ip <address_ipv4>
    set name <name_str>
    set queryportv1 <port_int>
    set queryportv2c <port_int>
    set queryv1-status {enable | disable}
    set queryv2c-status {enable | disable}
    set status {enable | disable}
    set trapevent {archive | cpu | deferred-queue | ha | ip-change |
       logdisk | maildisk | mem | power | raid | spam | system | virus}
    set trapportv1_local <port_int>
    set trapportv1_remote <port_int>
    set trapportv2c_local <port_int>
    set trapportv2c_remote <port_int>
    set trapv1_status {enable | disable}
    set trapv2c_status {enable | disable}
end
```

Variable	Description	Default
<index_int>	Enter the index number of the SNMP community.	
<index_int>	Enter the index number of the SNMP monitor.	
ip <address_ipv4>	Enter the IP address of the SNMP monitor. The FortiMail unit will, if traps are enabled, send traps to this IP address, and, if queries are enabled, receive queries from this IP address.	
name <name_str>	Enter the name of the SNMP community	
queryportv1 <port_int>	Enter the TCP port on which to listen for SNMPv1 queries from the SNMP monitor.	161
queryportv2c <port_int>	Enter the TCP port on which to listen for SNMPv2c queries from the SNMP monitor.	161
queryv1-status {enable | disable}	Enable to allow the FortiMail unit to receive SNMPv1 queries from the SNMP monitor.	enable
queryv2c-status {enable | disable}	Enable to allow the FortiMail unit to receive SNMPv2c queries from the SNMP monitor.	enable
status {enable | disable}	Enable to activate the SNMP community.	disable

Variable	Description	Default
`trapevent {archive | cpu | deferred-queue | ha | ip-change | logdisk | maildisk | mem | power | raid | spam | system | virus}`	Enter one or more of the following events that will generate a trap when the event occurs or when its threshold is reached: • `cpu`: CPU usage threshold • `mem`: Memory low threshold • `logdisk`: Log disk space low threshold • `maildisk`: Mail disk space low threshold • `deferred-queue`: Deferred queue threshold • `virus`: Virus threshold • `spam`: Spam threshold • `system`: System event, such as a change in the state of hardware • `raid`: RAID event • `ha`: High availability (HA) event • `archive`: Remote archive server event • `ip-change`: Interface IP address change • `psu`: Power supply unit (PSU) monitor event **Note:** `psu` will have no effect for those models that do not have monitored power supplies. Consult the hardware specifications for your FortiMail model to determine whether your FortiMail model contains a monitored PSU. To set SNMP trap thresholds for the event types that use them, see "config system snmp threshold" on page 198.	`archive deferred-queue cpu ha logdisk maildisk mem raid spam system virus`
`trapportv1_local <port_int>`	Enter the TCP port that the FortiMail unit will use to send SNMP v1 traps to SNMP monitors.	`162`
`trapportv1_remote <port_int>`	Enter the TCP port that the FortiMail unit will use to send SNMP v1 traps to SNMP monitors.	`162`
`trapportv2c_local <port_int>`	Enter the TCP port that the FortiMail unit will use to send SNMP v2c traps to SNMP monitors.	`162`
`trapportv2c_remote <port_int>`	Enter the TCP port that the FortiMail unit will use to send SNMP v2c traps to SNMP monitors.	`162`
`trapv1_status {enable | disable}`	Enable to activate sending SNMP v1 traps to the SNMP monitor.	`enable`
`trapv2c_status {enable | disable}`	Enable to activate sending SNMP v2c traps to the SNMP monitor.	`enable`

History

FortiMail v4.0 New.

Related topics

- config system snmp sysinfo
- config system snmp threshold

system snmp sysinfo

Use this command to enable or disable the SNMP agent on the FortiMail unit, and to configure the location, description, and contact information.

Syntax

```
config system snmp sysinfo
  set contact <contact_str>
  set description <description_str>
  set location <location_str>
  set status {enable | disable}
end
```

Variable	Description	Default
`contact <contact_str>`	Enter the contact information for the administrator of this FortiMail unit, such as '`admin@example.com`'.	
`description <description_str>`	Enter a description for the FortiMail unit that will uniquely identify it to the SNMP monitor, such as '`FortiMail-400 Rack 1`'.	
`location <location_str>`	Enter the location of this FortiMail unit, such as '`NOC_Floor2`'.	
`status {enable | disable}`	Enable to activate the SNMP agent.	`enable`

History

FortiMail v4.0 New.

Related topics

- config system snmp community
- config system snmp threshold

system snmp threshold

Use this command to configure the event types that trigger an SNMP trap.

Enter a number above which an SNMP trap will be sent for an event type. The valid range varies by the nature of the threshold: the valid range for percentages is from 1 to 99; the valid range for counts of event instances is from 1 to a very high number.

For example, if you enter:

```
set system snmp maildisk 75
```

the FortiMail unit will send an SNMP trap to the SNMP monitor when the mail disk is 75% full.

Syntax

```
config system snmp threshold
  set cpu <threshold_int>
  set deferred-queue <threshold_int>
  set logdisk <threshold_int>
  set maildisk <threshold_int>
  set mem <threshold_int>
  set spam <threshold_int>
  set virus <threshold_int>
end
```

Variable	Description	Default
`cpu <threshold_int>`	Enter the percentage of CPU used.	80
`deferred-queue <threshold_int>`	Enter the disk space used for the deferred mail queue.	`1000`
`logdisk <threshold_int>`	Enter the percentage of log disk space consumed.	`90`
`maildisk <threshold_int>`	Enter the percentage of mail disk space consumed.	`90`
`mem <threshold_int>`	Enter the percentage of memory used.	`80`
`spam <threshold_int>`	Enter the number of spam detections.	`1`
`virus <threshold_int>`	Enter the number of virus detections.	`1`

History

FortiMail v4.0 New.

Related topics

- config system snmp community
- config system snmp sysinfo

system time manual

Use this command to manually configure the system time of the FortiMail unit.

Accurate system time is required by many features of the FortiMail unit, including but not limited to log messages and SSL-secured connections.

This command applies only if NTP is disabled. Alternatively, you can configure the FortiMail unit to synchronize its system time with an NTP server. For details, see “system time ntp” on page 200.

Syntax

```
config system time manual
  set daylight-saving-time {disable | enable}
  set zone <zone_int>
end
```

Variable	Description	Default
`daylight-saving-time {disable | enable}`	Enable to automatically adjust the system time for daylight savings time (DST).	`enable`
`zone <zone_int>`	Enter the number that indicates the time zone in which the FortiMail unit is located.	`12`

History

FortiMail v4.0 New.

Related topics

- config system time ntp

system time ntp

Use this command to configure the FortiMail unit to synchronize its system time with a network time protocol (NTP) server.

Accurate system time is required by many features of the FortiMail unit, including but not limited to log messages and SSL-secured connections.

Alternatively, you can manually configure the system time of the FortiMail unit. For details, see “config system time manual” on page 199.

Syntax

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

Variable	Description	Default
`ntpserver {<address_ipv4> | <fqdn_str>}`	Enter either the IP address or fully qualified domain name (FQDN) of an NTP server. You can add a maximum of 10 NTP servers. The FortiMail unit uses the first NTP server based on the selection mechanism of the NTP protocol. To locate a public NTP server, visit http://www.ntp.org/.	`pool.ntp.org`
`ntpsync {enable | disable}`	Enable to synchronize the FortiMail unit with an NTP server, instead of manually configuring the system time.	`enable`
`syncinterval <interval_int>`	Enter the interval in minutes between synchronizations of the system time with the NTP server. The valid range is from 1 to 1440 minutes.	`60`

History

FortiMail v4.0 New.

Related topics

- config system time manual

system webmail-language

Use this command to create or rename a webmail language.

When you create a webmail language, it is initialized using by copying the English language file. For example, the location in webmail whose resource ID is `mail_box` contains the value `Mail Box`. To finish creation of your webmail language, you must replace the English values with your translation or customized term by either:

- editing the resource values for each resource ID in the web-based manager
- downloading, editing, then uploading the language resource file

For information on how to edit a webmail language, see the *FortiMail Administration Guide*.

Syntax

```
config system webmail-language
  edit en_name <language-name-en_str>
    set name <language-name_str>
    set file_name <file_str>
end
```

Variable	Description	Default
`en_name <language-name-en_str>`	Enter the name of the language in English, such as `'French'`. Available languages vary by whether or not you have installed additional language resource files.	No default.
`name <language-name_str>`	Enter the name of the language, such as `'Français'`.	No default.
`file_name <file_str>`	Enter the name of the language resource file, such as `'custom_french1'`.	No default.

History

FortiMail v4.0 New.

Related topics

- config config user mail

user alias

Use this command to configure email address aliases.

Aliases are sometimes also called distribution lists, and may translate one email address to the email addresses of several recipients, also called members, or may be simply a literal alias — that 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.

Alternatively, you can configure an LDAP profile in which the alias query is enabled. For details, see "config profile ldap" on page 135.

Syntax

```
config user alias
  edit name <email-alias_str>
    set member <recipient_str>
end
```

Variable	Description	Default
`name <email-alias_str>`	Enter the email address that is the alias, such as `alias1@example.com`.	No default.
`member <recipient_str>`	Enter a recipient email addresses to which the alias will translate or expand.	No default.

History

FortiMail v4.0 New.

Related topics

- config user map
- config user pki

user map

Use this command to configure email address mappings.

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

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

Like aliases, address mappings translate email addresses. They do not translate many email addresses into a single email address. However, ***unlike*** aliases:

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

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

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

Table 10: 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 others**: user1@marketing.example.net in both the message envelope (`MAIL FROM:`) and many message headers (`From:`, etc.) would then be replaced with sales@example.com. Recipients would only be aware of the email address sales@example.com.

- **For email to sales@example.com from others**: The recipient address in the message envelope (`RCPT TO:`), but ***not*** the message header (`To:`), would be replaced with user1@marketing.example.net. user1@marketing.example.net would be aware that the sender had originally sent the email to the mapped address, sales@example.com.

Alternatively, you can configure an LDAP profile to query for email address mappings. For details, see "config profile ldap" on page 135.

Syntax

```
config user map
  edit internal-name <pattern_str>
    set external-name <pattern_str>
end
```

Variable	Description	Default
`internal-name <pattern_str>`	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 will be rewritten into `external-name <pattern_str>` according to the match conditions and effects described in Table 10 on page 203. **Note:** If you enter a pattern with a wild card (`*` or `?`): • You must enter a pattern using the same wild card in `external-name <pattern_str>`. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the external address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, `*` mapped to `?` or vice versa), this substitution will fail. • `external-name <pattern_str>` must not be within the same protected domain. This could 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.	No default.
`external-name <pattern_str>`	Enter either an email address, such as `user2@example.com`, or an email address pattern, such as `*@example.net`, that exists in a protected domain. This email address will be rewritten into `internal-name <pattern_str>` according to the match conditions and effects described in Table 10 on page 203. **Note:** If you enter a pattern with a wild card (`*` or `?`): • You must enter a pattern using the same wild card in `internal-name <pattern_str>`. 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 internal address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, `*` mapped to `?` or vice versa), this substitution will fail. • `internal-name <pattern_str>` must not be within the same protected domain. This could 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.	No default.

History

FortiMail v4.0 New.

Related topics

- config user alias
- config user pki

user pki

Use this command to configure public key infrastructure (PKI) users.

A PKI user can be either an email user or a FortiMail administrator. PKI users can authenticate by presenting a valid client certificate, rather than by entering a user name and password.

When the PKI user connects to the FortiMail unit with his or her web browser, the web browser presents the PKI user's certificate to the FortiMail unit. If the certificate is valid, the FortiMail unit then authenticates the PKI user. To be valid, a client certificate must:

- Not be expired
- Not be revoked by either certificate revocation list (CRL) or, if enabled, online certificate status protocol (OCSP)
- Be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail unit
- Contain a "ca" field whose value matches the CA certificate
- Contain a "issuer" field whose value matches the "subject" field in the CA certificate
- Contain a "subject" field whose value contains the subject, or is empty
- If `ldap-query` is `enable`, contain a common name (CN) or Subject Alternative field whose value matches the email address of a user object retrieved using the user query of the LDAP profile

If the client certificate is ***not*** valid, depending on whether you have configured the FortiMail unit to require valid certificates"config system global" on page 179, authentication will either fail absolutely, or fail over to a user name and password mode of authentication.

If the certificate is valid and authentication succeeds, the PKI user's web browser is redirected to either the web-based manager (for PKI users that are FortiMail administrators) or the mailbox folder that contains quarantined spam (for PKI users that are email users).

After using this command to configure a PKI user, you must also configure the following aspects of the FortiMail unit and the PKI user's computer:

- Import each PKI user's client certificate into the web browser of each computer from which the PKI user will access the FortiMail unit. For details on installing certificates, see the documentation for your web browser.

Caution: Control access to each PKI user's computer. Certificate-based PKI authentication controls access to the FortiMail unit based upon PKI certificates, which are installed on each email user or administrator's computer. If anyone can access the computers where those PKI certificates are installed, they can gain access to the FortiMail unit, which can compromise the security of your FortiMail unit.

- Import the CA certificate into the FortiMail unit. For information on uploading a CA certificate, see the *FortiMail Administration Guide*.
- For PKI users that are FortiMail administrators, select the PKI authentication type and select a PKI user to which the administrator account corresponds. For more information, see "config system admin" on page 159.
- For PKI users that are email users, enable PKI user authentication for the recipient-based policies which match those email users.

This command takes effect only if PKI authentication is enabled by `pkimode {enable | disable}` in the command "config system global" on page 179.

Syntax

```
config user pki
  edit name <name_str>
```

```
    set ca <certificate_str>
    set domain <protected-domain_str>
    set ldap-field {cn | subjectalternative}
    set ldap-profile <profile_str>
    set ldap-query {enable | disable}
    set ocsp-ca <remote-certificate_str>
    set ocsp-check {enable | disable}
    set ocsp-unavailable-action {revoke | ignore}
    set ocsp-url <url_str>
    set subject <subject_str>
end
```

Variable	Description	Default
`name <name_str>`	Enter the name of the PKI user.	
`ca <certificate_str>`	Enter the name of the CA certificate used when verifying the CA's signature of the client certificate. For information on uploading a CA certificate, see the *FortiMail Administration Guide*.	
`domain <protected-domain_str>`	Enter the name of the protected domain to which the PKI user is assigned, or enter `system` if the PKI user is a FortiMail administrator and belongs to all domains configured on the FortiMail unit. For more information on protected domains, see "config domain" on page 51.	
`ldap-field {cn | subjectalternative}`	Enter the name of the field in the client certificate (either CN or Subject Alternative) which contains the email address of the PKI user, either `subjectalternative` (if the field is a Subject Alternative) or `cn` (if the field is a common name). This email address will be compared with the value of the email address attribute for each user object queried from the LDAP directory to determine if the PKI user exists in the LDAP directory. This variable is used only if `ldap-query` is `enable`.	`subject`
`ldap-profile <profile_str>`	Enter the LDAP profile to use when querying the LDAP server for the PKI user's existence. For more information on LDAP profiles, see "profile ldap" on page 135. This variable is used only if `ldap-query` is `enable`.	
`ldap-query {enable | disable}`	Enable to query an LDAP directory, such as Microsoft Active Directory, to determine the existence of the PKI user who is attempting to authenticate. Also configure `ldap-profile <profile_str>` and `ldap-field {cn | subjectalternative}`.	`disable`
`ocsp-ca <remote-certificate_str>`	Enter the name of the remote certificate that is used to verify the identity of the OCSP server. For information on uploading a remote (OCSP) certificate, see the *FortiMail Administration Guide*. This option applies only if `oscpverify` is `enable`.	
`ocsp-check {enable | disable}`	Enable to use an Online Certificate Status Protocol (OCSP) server to query whether the client certificate has been revoked. Also configure `ocsp-url <url_str>`, `[ocsp-ca <remote-certificate_str>`, and `ocsp-unavailable-action {revoke | ignore}`.	`disable`
`ocsp-unavailable-action {revoke | ignore}`	Enter the action to take if the OCSP server is unavailable. If set to ignore, the FortiMail unit allows the user to authenticate. If set to revoke, the FortiMail unit behaves as if the certificate is currently revoked, and authentication fails. This option applies only if `oscp-check` is `enable`.	`ignore`

Variable	Description	Default
`ocsp-url <url_str>`	Enter the URL of the OCSP server. This option applies only if `oscp-check` is `enable`.	
`subject <subject_str>`	Enter the value which must match the “subject" field of the client certificate. If empty, matching values are not considered when validating the client certificate presented by the PKI user’s web browser.	

History

FortiMail v4.0 New.

Related topics

- config user alias
- config user map

diagnose

`diagnose` commands display diagnostic information that help you to troubleshoot problems.

This chapter describes the following commands:

debug application burstd

Use this command to set the level of verbosity in debugging messages for mailbox backup and restoration events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application burstd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose system top`
- `execute backup-restore`

debug application cmdb_event

Use this command to set the level of verbosity in debugging messages for configuration database events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application cmdb_event {0 | 1 | 2}
```

Variable	Description	Default
{0 | 1 | 2}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- diagnose debug enable
- diagnose system top
- execute backup
- execute factoryreset
- execute reload
- execute restore config

debug application expiremail

Syntax

```
diagnose debug application expiremail {check | purge} <email_pattern> {0 |
   1 | 2}
```

Variable	Description	Default
{check | purge}	Type whether to examine bulk, inbox, and other user mailboxes for email that should be deleted due to age that exceeds the configured limit, or to actually delete those expired email messages.	No default.
<email_pattern>	Type the email address of an email user account on the FortiMail unit, such as user1@example.com, or a wildcard pattern matching multiple accounts, such as user*.	No default.
{0 | 1 | 2}	Type the number indicating the amount of status messages to include in the CLI display while executing the command. 0 displays no status messages; 2 displays detailed status messages.	No default.

Example

```
FortiMail# diag debug application expiremail user* 1
3076474544 User bulk mail folder purge task started at 2010-01-14 05:23:05 -
   0600

3076474544 Server mode user mailbox purge task started at 2010-01-14
   05:23:05 -0600
```

History

FortiMail v4.0 New.

Related topics

- diagnose debug enable

debug application fdsmgmtd

Use this command to set the level of verbosity in debug-level messages for centralized management by a FortiManager unit.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application fsmgmtd {0 | 1 | 2}
```

Variable	Description	Default
{0 | 1 | 2}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

Example

The following example displays brief debug messages about the activities of the centralized management daemon. Centralized management was enabled, its configuration changed, and then disabled.

```
FortiMail# diag debug application fdsmgmtd 2
daemon: create_daemons, daemon_list_cnt = 1

 daemon: initialize daemon

 daemon: enter event loop

 daemon: detected cmdb config change

 daemon: cleanup daemon

 daemon: exits event loop
```

History

FortiMail v4.0 New.

Related topics

- config system central-management
- diagnose debug enable
- diagnose system top
- execute central-mgmt

debug application hahbd

Use this command to set the level of verbosity in debugging messages for high availability (HA) heartbeat events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application hahbd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- config system ha
- `diagnose debug enable`
- `diagnose debug application hasyncd`
- `diagnose system ha failover`
- `diagnose system top`

debug application hasyncd

Use this command to set the level of verbosity in debugging messages for high availability (HA) synchronization events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application hasyncd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- config system ha
- `diagnose debug enable`
- `diagnose debug application hahbd`
- `diagnose system ha sync`
- `diagnose system top`

debug application httpd

Use this command to set the level of verbosity in debugging messages for HTTP daemon (FortiMail webmail and web-based manager display) events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application httpd access-log {enable | disable}
diagnose debug application httpd trace-log {enable | disable}
```

Variable	Description	Default
`access-log {enable | disable}`		No default.
`trace-log {enable | disable}`		No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose system top`
- `execute reload`

debug application mailfilterd display

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application mailfilterd display
```

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose system top`

debug application mailfilterd trace

Syntax

```
diagnose debug application mailfilterd trace {0 | 1 | 2}
```

Variable	Description	Default
{0 | 1 | 2}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- diagnose debug enable
- diagnose system top

debug application mailfilterd trap-email

Syntax

```
diagnose debug application mailfilterd trap-email trap-email {enable |
   disable}
```

Variable	Description	Default
`trap-email {enable | disable}`		No default.

History

FortiMail v4.0 New.

Related topics

- diagnose debug enable
- diagnose system top

debug application miglogd

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application miglogd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose system top`

Related topics

debug application netd

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application netd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose netlink ip list`
- `diagnose system top`

debug application nasd

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application nasd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.1 New.

Related topics

- `diagnose debug enable`
- `diagnose netlink ip list`
- `diagnose system top`

debug application ntpd

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application nasd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose netlink ip list`
- `diagnose system top`

debug application radius-accounting

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application nasd {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.1 New.

Related topics

- `diagnose debug enable`
- `diagnose netlink ip list`
- `diagnose system top`

debug application smtpproxy

Use this command to set the level of verbosity in debugging messages for transparent mode proxy events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application smtpproxy {0 | 1 | 2}
```

Variable	Description	Default
{0 | 1 | 2}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- config mailsetting proxy-smtp
- diagnose debug enable
- diagnose debug application smtpproxy-children
- diagnose system top

debug application smtpproxy-children

Use this command to set the level of verbosity in debugging messages for transparent mode proxy children's events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application smtpproxy-children {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose debug application smtpproxy`

debug application sshd

Use this command to set the level of verbosity in debugging messages for SSH logins and logouts.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application sshd {0 | 1 | 2}
```

Variable	Description	Default
{0 | 1 | 2}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

Example

```
FortiMail# diag debug application sshd 1
SSH: debug1: Received SIGCHLD.
SSH: debug1: session_by_pid: pid 1027
SSH: debug1: session_exit_message: session 0 channel 0 pid 1027
SSH: debug1: session_exit_message: release channel 0
SSH: debug1: session_close: session 0 pid 1027
SSH: debug1: session_pty_cleanup: session 0 release /dev/pts/3
SSH: syslogin_perform_logout: logout() returned an error
SSH: debug3: channel 0: will not send data after close
SSH: debug3: channel 0: will not send data after close
SSH: debug1: channel 0: free: server-session, nchannels 1
SSH: debug3: channel 0: status: The following connections are open:
  #0 server-session (t4 r256 i3/0 o3/0 fd -1/-1)

SSH: debug3: channel 0: close_fds r -1 w -1 e -1
```

History

FortiMail v4.0 New.

Related topics

- Connecting to the CLI
- `diagnose debug enable`
- `diagnose system top`

debug application starttls

Use this command to set the level of verbosity in debugging messages for STARTTLS daemon events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application starttls {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • 1: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- config config domain-setting
- config system certificate local
- config profile tls
- `diagnose debug enable`

debug application updated

Use these commands to set the level of verbosity in debugging messages for FortiGuard update daemon events.

Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application updated {0 | 1 | 2}
```

Variable	Description	Default
`{0 | 1 | 2}`	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • `0`: Do not display messages. • `1`: Display verbose messages in the CLI. • `2`: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- config system fortiguard antivirus
- config system fortiguard antispam
- `diagnose debug enable`
- `diagnose system top`
- `execute update-now`

debug application urlfilterd

Use this command to Before using this command, first enable debug output (`diagnose debug enable`). This command produces output only while the daemon is active. Output is printed to your CLI display until you stop it by pressing Ctrl + C.

Syntax

```
diagnose debug application urlfilterd {stop | <server_ipv4>}
```

Variable	Description	Default
`{stop | <server_ipv4>}`	Type either the	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose debug enable`
- `diagnose system top`

debug cli

Use this command to set the level of verbosity in debugging messages for command line interface (CLI) events.

Syntax

```
diagnose debug cli {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}
```

Variable	Description	Default
{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- Connecting to the CLI
- diagnose debug enable

debug disable

Use this command to disable debugging messages to the CLI display.

Syntax

```
diagnose debug disable
```

History

FortiMail v4.0 New.

Related topics

- diagnose debug enable

debug enable

Use this command to enable debugging messages to the CLI display.

Syntax

```
diagnose debug enable
```

History

FortiMail v4.0 New.

Related topics

- diagnose debug disable

debug kernel

Use this command to set the level of verbosity in debugging messages for kernel events.

Syntax

```
diagnose debug kernel {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}
```

Variable	Description	Default
{0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}	Type the number indicating the amount of debugging messages to output to the CLI display while executing the command. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	No default.

History

FortiMail v4.0 New.

Related topics

- execute ping
- execute traceroute

fortiguard rating

Use this command to query the FortiGuard Antispam service in order to determine whether or not an IP address is known to produce spam.

To use this command, the FortiMail unit must be able to contact the FortiGuard Distribution Network (FDN). To verify this, you can use the commands `execute ping` and `execute traceroute`. For more information on troubleshooting connections to the FDN, see the *FortiMail Administration Guide*.

Syntax

```
diagnose fortiguard rating <server_ipv4>
```

Variable	Description	Default
`<server_ipv4>`	Type the IP address of an SMTP server. **Tip:** If you know the name of the mail domain, but are unsure of the IP address of its SMTP server, you can use the command `execute nslookup` to determine the IP address.	No default.

Example

```
FortiMail# diagnose fortiguard rating 208.85.225.147
ip: 208.85.225.147, score=-1
```

History

FortiMail v4.0 New.

Related topics

- `execute ping`
- `execute traceroute`

netlink ip list

Use this command to display all of the physical and virtual IP addresses associated with the network interfaces of the FortiMail unit.

Syntax

```
diagnose netlink ip list
```

Example

The following example shows that there are IP addresses associated with these four network interfaces:

- port1 (`index=4`)
- port2 (`index=5`)
- port3 (`index=6`)
- the loopback interface (`index=1`)

```
FortiMail# diagnose netlink ip list
IP=127.0.0.1 MASK=255.0.0.0 index=1 devname=lo
IP=172.20.120.167 MASK=255.255.255.0 index=4 devname=port1
IP=10.0.0.2 MASK=255.255.255.0 index=5 devname=port2
IP=10.1.1.1 MASK=255.255.255.0 index=6 devname=port3
```

History

FortiMail v4.0 New.

Related topics

- `diagnose debug application netd`

sniffer packet

Use this command to perform a packet trace on one or more network interfaces.

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

FortiMail units have a built-in sniffer. Packet capture on FortiMail units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing Ctrl + C, or until it reaches the number of packets that you have specified to capture.

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

Syntax

```
diagnose sniffer packet <interface_name> '<filter_str>' {1 | 2 | 3 | 4 | 5 |
    6} [<count_int>] [a]
```

Variable	Description	Default
`<interface_name>`	Type the name of a network interface whose packets you want to capture, such as `port1`, or type `any` to capture packets on all network interfaces.	No default.

`'<filter_str>'`	Type either `none` to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as `'tcp port 25'`. Surround the filter string in quotes.
	The filter uses the following syntax:
	`'[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or] [[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]'`
	To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source, and which is the destination.
	For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:
	`'udp and port 1812 and src host 1.example.com and dst \( 2.example.com or 2.example.com \)'`
		`none`

`{1 | 2 | 3 | 4 | 5 | 6}`	Type one of the following integers indicating the depth of packet headers and payloads to capture: • `1` for header only • `2` for IP header and payload • `3` for Ethernet header and payload • `4` for the output from `1`, plus the name of the network interface • `5` for the output from `2`, plus the name of the network interface • `6` for the output from `3`, plus the name of the network interface For troubleshooting purposes, Fortinet Technical Support may request a verbose level (`3`).	No default

Variable	Description	Default
[<count_int>]	Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press Ctrl + C.	No default
[a]	Type a to use a timestamp in the absolute, universal coordinated time (UTC) format yyyy-mm-dd hh:mm:ss.ms, where: • yyyy is the year • mm is the month • dd is the date • hh is the hour • mm is the minute • ss is the second • ms is the millisecond Omit the a, or type any other value, to use a timestamp that is relative to the start of the packet capture (ss.ms).	No default.

Example

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of none), that passes through the network interface named port1. The capture uses a low level of verbosity (indicated by 1).

```
FortiMail# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by 1). Because the filter does not specify either host as the source or destination in the IP header (src or dst), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded.

```
FortiMail# diag sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1
   and tcp port 80' 1

192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265

5 packets received by filter
0 packets dropped by kernel
```

Example

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by `3`).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the FortiMail unit are not bolded.

```
FortiMail # diag sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000   0009 0f09 0001 0009 0f89 2914 0800 4500        ..........)...E.
0x0010   003c 73d1 4000 4006 3bc6 d157 fede ac16        .<s.@.@.;..W....
0x0020   0ed8 c442 01bb 2d66 d8d2 0000 0000 a002        ...B..-f........
0x0030   16d0 4f72 0000 0204 05b4 0402 080a 03ab        ..Or............
0x0040   86bb 0000 0000 0103 0303                       ..........
```

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

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

To view sniffer output using HyperTerminal and Wireshark

1 Type the sniffer CLI command, such as:

```
diag sniffer port1 'tcp port 80' verbose 3
```

2 After you type the sniffer command but ***before*** you press Enter, go to *Transfer* > *Capture Text...*.

3 Select the name and location of the output file, such as `C:\Documents and Settings\username\FortiMail_sniff.txt`.

4 Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.

5 When you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.

6 Go to *Transfer* > *Capture Text* > *Stop* to stop and save the file.

7 Convert this plain text file to a format recognizable by your network protocol analyzer application.

You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethereal) using the fgt2eth.pl Perl script. To download fgt2eth.pl, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

Note: The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system, such as ActivePerl (http://www.activestate.com/Products/activeperl/index.mhtml).

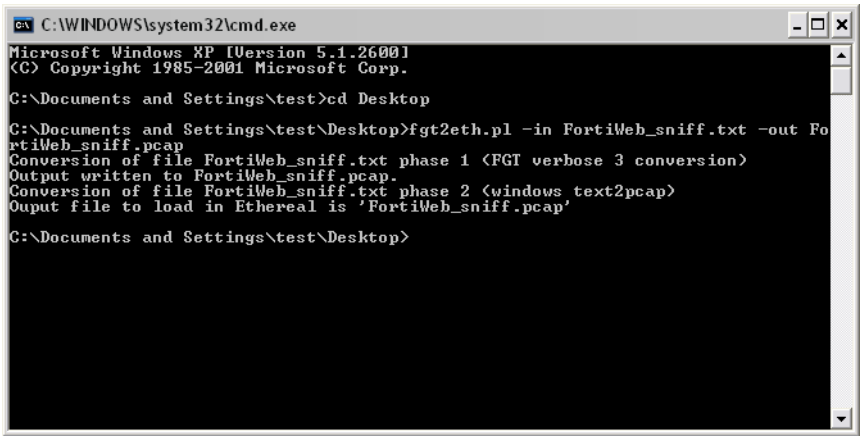
To use fgt2eth.pl on Windows XP, go to *Start* > *Run* and enter `cmd` to open a command prompt, then enter a command such as the following:

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

where:

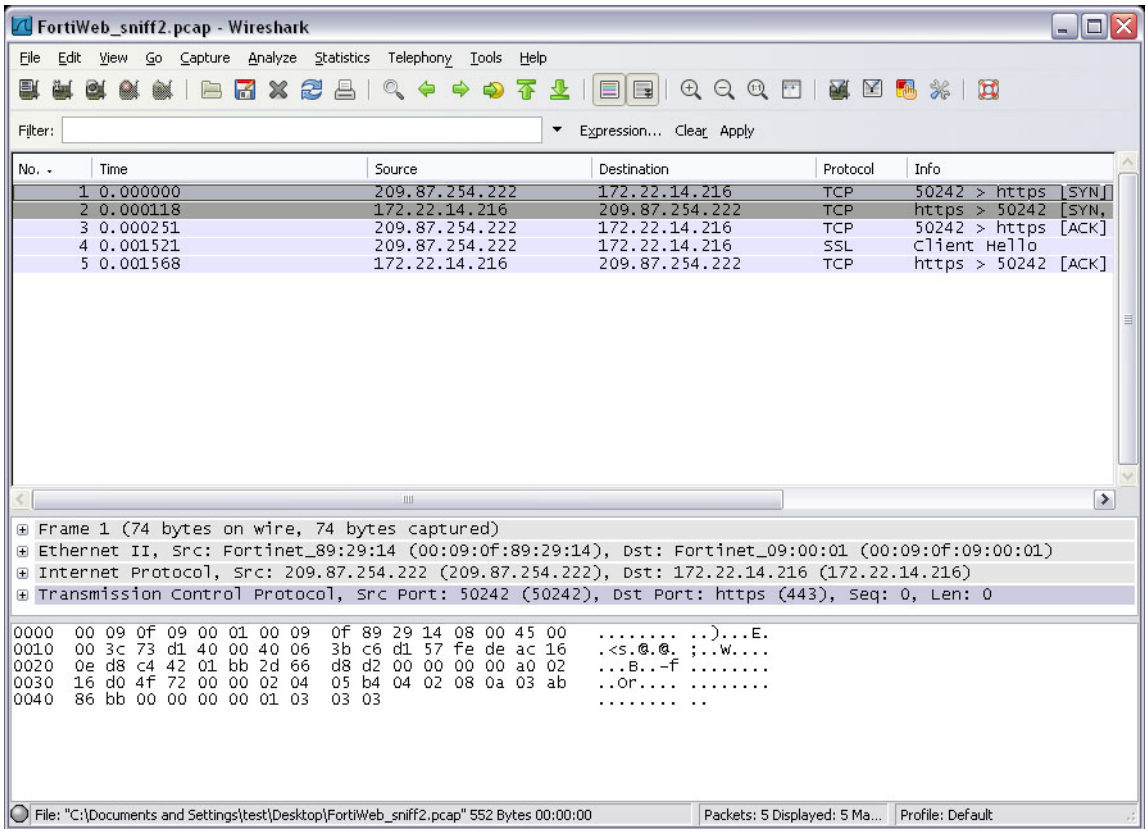
- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `FortiMail_sniff.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `FortiMail_sniff.pcap`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

Figure 2: Converting sniffer output to .pcap format



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

Figure 3: Viewing sniffer output in Wireshark



For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

History

FortiMail v4.0 New.

statistics clear

Use this command to delete the current set of antispam and antivirus statistics.

These statistics are the ones which populate the charts and graphs in the *Statistics History* and *Statistics Summary* widgets of the web-based manager's dashboard, and in *Monitor* > *Mail Statistics*.

For more information on the web-based manager, see the *FortiMail Administration Guide*.

Caution: Back up statistics that you want to keep using `diagnose statistics save` before entering this command. This command cannot be undone.

Syntax

```
diagnose statistics clear
```

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics get`
- `diagnose statistics load`

statistics get

Use this command to display the current set of antispam and antivirus statistics.

These statistics are the ones which populate the charts and graphs in the *Statistics History* and *Statistics Summary* widgets of the web-based manager's dashboard, and in *Monitor* > *Mail Statistics*.

For more information on the web-based manager, see the *FortiMail Administration Guide*.

Tip: CLI output for this command can be very long. To ensure that output is not truncated, you may need to increase the memory buffer size of your CLI client, or save the output to a text file for subsequent viewing in a plain text editor. Available methods vary. For details, see your CLI client's documentation.

Syntax

```
diagnose statistics get {minute | hour | day | month | year | total | all}
```

Variable	Description	Default
`get {minute | hour | day | month | year | total | all}`	Type the interval of time whose email statistics you want to display.	No default.

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics save`

statistics load

Use this command to load a set of antispam and antivirus statistics from a file.

Syntax

```
diagnose statistics load [<file-name_str>]
```

Variable	Description	Default
`load [<file-name_str>]`	Type the path and file name of a previously saved statistics file that you want to load.	`/var/spool/etc/mailstatistics/mailstats`

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics save`

statistics save

Use this command to save the current set of antispam and antivirus statistics to a file.

These statistics are the ones which populate the charts and graphs in the *Statistics History* and *Statistics Summary* widgets of the web-based manager's dashboard, and in *Monitor* > *Mail Statistics*.

For more information on the web-based manager, see the *FortiMail Administration Guide*.

Tip: Before running a simulation or generating a set of sample statistics, you may find it useful to save your actual statistics to a file using `diagnose statistics save`, so that you can reload them later, after testing is complete, using `diagnose statistics load`.

Syntax

```
diagnose statistics save [<file-name_str>]
```

Variable	Description	Default
`[<file-name_str>]`	Type the path and file name to use when saving the current email statistics.	`/var/spool/etc/mailstatistics/mailstats`

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics get`
- `diagnose statistics load`
- `diagnose statistics set flat`
- `diagnose statistics set random`

statistics set autoupdate

Use this command to toggle whether or not to display up-to-the-moment statistics.

Syntax

```
diagnose statistics set autoupdate {on | off}
```

Variable	Description	Default
`autoupdate {on | off}`	Enable to display up-to-the-moment statistics.	`on`

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics save`
- `diagnose statistics clear`

statistics set flat

Use this command to generate a linearly increasing set of sample spam and virus detection statistics. These statistics will be used to populate the charts and graphs in the *Statistics History* and *Statistics Summary* widgets of the web-based manager's dashboard, and in *Monitor* > *Mail Statistics*.

Unlike `diagnose statistics set random`, this command instantly produces a set of statistics for each unit of time (year, month, hour, minute) that can appear on a graph, including times prior to when the command was entered. It does not simulate realtime throughput over a duration.

For more information on the web-based manager, see the *FortiMail Administration Guide*.

Tip: Before running a simulation or generating a set of sample statistics, you may find it useful to save your actual statistics to a file using `diagnose statistics save`, so that you can reload them later, after testing is complete, using `diagnose statistics load`.

Syntax

```
diagnose statistics set flat
```

Example

The following example instantly generates linearly increasing sample statistics for all periods of time possible, beginning with the first possible date and time on the system clock (in this case, 7:00 PM EST on December 31, 1969), up to the present (11:12 AM EST on January 19, 2010).

```
FortiMail# diagnose statistics set flat
First update at 1969-12-31 19:00:01 -0500(1)
Latest update at 2010-01-19 11:12:13 -0500(1263917533)
Latest dump at 1969-12-31 19:00:00 -0500(0)
```

History

FortiMail v4.0 New.

Related topics

- `diagnose statistics set random`
- `diagnose statistics save`
- `diagnose statistics clear`

statistics set random

Use this command to simulate email throughput and generate a random set of sample spam and virus detection statistics. These statistics will be used to populate the charts and graphs in the *Statistics History* and *Statistics Summary* widgets of the web-based manager's dashboard, and in *Monitor* > *Mail Statistics*.

Unlike `diagnose statistics set flat`, this command produces statistics only for the duration of the simulation (`random <samples_int>` x `<interval_int>` seconds), from the moment that the command is entered. While the simulation is running, you may refresh the graphs and charts to observe the increases in each kind of statistic. No statistics are generated for the period of time before the simulation was initiated.

For more information on the web-based manager, see the *FortiMail Administration Guide*.

Note: This command can take several seconds or more, depending on your configuration of `<interval_int>`. If you do not want to wait for the command to complete in order to continue administration tasks, you can initiate a second CLI connection while this command is running. Alternatively, you can press Ctrl + C to return to the command prompt. The command will complete in the background, and will notify you via CLI output when finished.

Tip: Before running a simulation or generating a set of sample statistics, you may find it useful to save your actual statistics to a file using `diagnose statistics save`, so that you can reload them later, after testing is complete, using `diagnose statistics load`.

Syntax

```
diagnose statistics set random <samples_int> <interval_int>
```

Variable	Description	Default
`random <samples_int>`	Type the number of email to simulate passing through the FortiMail unit. Each one will be categorized by a randomly determined simulated antivirus and antispam scan status. For example, some of the simulated email will be categorized as if they had been detected as spam by a DNSBL scan, and will appear in that category in the graphs or charts.	No default.
`<interval_int>`	Type the approximate interval in seconds between each email in the simulation. The actual interval will vary slightly by a randomly determined amount of time.	No default.

Example

The following example generates sample statistics for 20 email. Simulated email pass through the FortiMail unit at approximately 10 seconds apart. As a result, the command takes approximately 200 seconds (3 minutes 20 seconds) to complete, starting from the time that the command was entered (4:48 PM EST on January 10, 2010).

```
FortiMail# diagnose statistics set random 20 10

Start testing 20 samples with interval 10 seconds at local time 2010-01-15
   16:48:39 -0500(1263592119)

Finished testing with 20 samples and average interval 8.1 seconds at local
   time 2010-01-15 16:51:21 -0500(1263592281)
```

History

FortiMail v4.0 New.

Related topics

- diagnose statistics set flat
- diagnose statistics save
- diagnose statistics clear

system ha failover

Use this command to manually trigger failover in a FortiMail high availability (HA) group.

This command is applicable only for active-passive style HA groups. For details on HA failover, see the *FortiMail Administration Guide*.

Syntax

```
diagnose statistics system ha failover
```

History

FortiMail v4.0 New.

Related topics

- config system ha
- diagnose system ha restore

system ha restore

Use this command to revert a member of a FortiMail high availability (HA) group to its configured role (either master/primary or slave/backup) after a failover.

This command is applicable only for active-passive style HA groups. For details on HA failover, see the *FortiMail Administration Guide*.

Syntax

```
diagnose statistics system ha restore
```

History

FortiMail v4.0 New.

Related topics

- config system ha
- diagnose system ha failover

system ha showcsum

Syntax

```
diagnose system ha showcsum
```

Example

```
FortiMail# diagnose system ha showcsum
debugzone
global: 7d b4 d3 29 5a f8 0c a8 e4 a9 8b f5 29 07 bb 8d
all: 49 30 f4 89 dc b9 1d b6 e2 9c 5b fa e9 8d 1b bc

checksum
global: 7d b4 d3 29 5a f8 0c a8 e4 a9 8b f5 29 07 bb 8d
all: 49 30 f4 89 dc b9 1d b6 e2 9c 5b fa e9 8d 1b bc
```

History

FortiMail v4.0 New.

Related topics

- config system ha

system ha sync

Use this command to synchronize members of a FortiMail high availability (HA) group.

For details on HA synchronization, see the *FortiMail Administration Guide*.

Syntax

```
diagnose statistics system ha sync
```

History

FortiMail v4.0 New.

Related topics

- config system ha
- diagnose debug application hasyncd

system smartctl

Use this command to use SMART (self-monitoring, analysis, and reporting technology) to test the health of a hard drive.

Syntax

Syntax varies by FortiMail model.

FortiMail-100:

```
diagnose sys smartctl ata /dev/hdc
```

FortiMail-400:

```
diagnose sys smartctl ata /dev/hda
diagnose sys smartctl ata /dev/hdb
```

FortiMail-400B:

```
diagnose system smartctl ata /dev/sda
diagnose system smartctl ata /dev/sdb
```

FortiMail-2000A:

```
diag system smartctl 3ware,<hard-drive_int> /dev/twa0
```

FortiMail-4000A:

```
diag system smartctl 3ware,<hard-drive_int> /dev/twa0
```

Variable	Description	Default
<hard-drive_int>	Type the index number of the hard drive that you want to test. For FortiMail-2000A, the valid range is 0 to 5. For FortiMail-4000A, the valid range is 0 to 11.	No default.

History

FortiMail v4.0 New.

Related topics

- execute checklogdisk
- execute checkmaildisk

system top

Use this command to display:

- up time (`Run Time`)
- current total processor and memory usage
- current free memory
- a list of the top most resource-intense currently running system processes and daemons, with respect to their memory (RAM) and processor (CPU) usage

The first two lines of the display indicate the up time, and the processor and memory usage. Processor and memory usages on the second line have abbreviated labels, highlighted below in bold.

```
Run Time:  0 days, 21 hours and 3 minutes
0U, 4S, 95I; 1035792T, 646920F
```

Table 11: Abbreviations for processor and memory usage

Letter	Description
U	User CPU usage (%)
S	System CPU usage (%)
I	Idle CPU usage (%)
T	Total memory (KB)
F	Free memory (KB)

The remaining lines contain the process list, which has the following columns.

Table 12: Process list columns

Column 1	Column 2	Column 3	Column 4	Column 5
Process name, such as `sshd`	Process ID (PID) number, such as `731`	Status • **S**: sleeping (idle) • **R**: running • **Z**: zombie (crashed) • **<**: high priority • **N**: low priority **Note:** You may be able to restart a zombie process ***without*** rebooting. See `execute reload`.	CPU usage (%)	Memory usage (%)

While the command is running, you can sort the process list. By default, it is sorted by CPU usage.

- **Shift + P**: Sort by CPU usage.
- **Shift + M**: Sort by memory usage.

Process list output is printed to your CLI display until you stop it by pressing either `q` or Ctrl + C.

Syntax

```
diagnose system top <refresh_int>
```

Variable	Description	Default
`<refresh_int>`	Type the interval in seconds between each refresh of the process list. For example, to refresh the process list every 5 seconds, type `5`.	No default.

Example

The following example refreshes the display of the top 19 most system-intensive processes every 5 seconds. The output indicates that the FortiMail unit is mostly idle, except for some processor resources used by a connection to the web-based manager (`admin.fe`), and to the CLI.

```
FortiMail# diagnose system top 5
Run Time:  0 days, 21 hours and 3 minutes
0U, 4S, 95I; 1035792T, 646920F
  admin.fe      987      S       6.0     0.0
  admin.fe      979      S       1.4     0.0
       cli      984      R       0.2     0.0
   miglogd      755      S       0.2     0.0
 dbmanager      731      S       0.0     0.0
mailfilter      767      S       0.0     0.0
     httpd      972      S       0.0     0.0
     smtpd      793      S       0.0     0.0
     smtpd      796      S       0.0     0.0
  dbdaemon      766      S       0.0     0.0
     smtpd      829      S       0.0     0.0
     smtpd      830      S       0.0     0.0
     smtpd      831      S       0.0     0.0
     smtpd      828      S       0.0     0.0
 smtpproxy      780      S       0.0     0.0
spamreport      790      S       0.0     0.0
fmlmonitor      799      S       0.0     0.0
   cmdbsvr      745      S       0.0     0.0
      netd      756      S       0.0     0.0
```

History

FortiMail v4.0 New.

Related topics

- diagnose debug cli
- diagnose debug application httpd
- diagnose debug application mailfilterd trace
- diagnose debug application smtpproxy
- diagnose debug application sshd
- execute reload

execute

`execute` commands perform immediate operations on the FortiMail unit.

This chapter describes the following `execute` commands:

backup

Use this command to back up the configuration file to a TFTP server or management station.

Caution: This command does not produce a complete backup. For information on how to back up other configuration files such as Bayesian databases, see the *FortiMail Administration Guide*.

Syntax

```
execute backup {config | full-config | mail-queue | user-config}
  tftp <filename_str> <tftp_ipv4> <password_str>
  management-station <comments>
```

Variable	Description	Default
`{config | full-config | mail-queue | user-config}`	Type either: • `config`: Back up configuration changes only. The default settings will not be backed up. • `full-config`: Back up the entire configuration file, including the default settings. • `mail-queue`: Back up the mail queues. • `user-config`: Enable updating user-specific configurations, such as user preferences, personal black/white lists, and secondary addresses, to the user configuration file. To update the configurations, see "execute userconfig" on page 299.	
`<filename_str>`	Type the file name that will be used for the backup file, such as `FortiMail_backup.txt`.	
`<tftp_ipv4>`	Type the IP address of the TFTP server.	
`<password_str>`	Type a password that will be used to encrypt the backup file, and which must be provided when restoring the backup file. If you do not provide a password, the backup file is stored as clear text.	
`<comments>`	Back up the system configuration to a configured management station. If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (" ") or any other punctuation marks. For example, uploadedthetransparentmodeconfigfortheaccountingdepartmentwilluploadonadailybasis.	

History

FortiMail v4.0 New.

Related topics

- `execute restore config`
- `execute factoryreset`
- `execute userconfig`

backup-restore

Use this command to back up or restore email users' mailboxes. Before using this command, you must specify the backup destination or the restore location first. For details, see "config system backup-restore-mail" on page 162.

Syntax

```
execute backup-restore check-device
execute backup-restore format-device
execute backup-restore old-restore <full_int> <increments_int> domain
   <domain_str> user <user_str>
execute backup-restore restore {domain <domain> user <user> | host <host>}
execute backup-restore start
execute backup-restore stop
```

Variable	Description	Default
check-device	Performs file system check on the backup device.	
format-device	Format the backup device as a preparation step before backup.	
old-restore <full_int> <increments_int> domain <domain_str> user <user_str>	<full_int> is the full backup version you specify when you configure the backup settings. <increments_int> is the number of incremental backups to make between each full backup. <domain_str>: optionally specify which domain's mailbox will be restored. <user_str>: optionally specify which user's mailbox will be restored. For details, see "config system backup-restore-mail" on page 162.	
restore {domain <domain> user <user> | host <host>}	Restores mailboxes, or optionally, for the specified domain or user. If you want to restore mailboxes from backups identified by another FQDN, such as a previous FQDN or the FQDN of another FortiMail unit, specify the <host>, which is the FQDN. Usually, you should enter an FQDN of this FortiMail unit, but you may enter the FQDN of another FortiMail unit if you want to import that FortiMail unit's mailbox backup. For example, you may be upgrading to a FortiMail-2000 from a FortiMail-400. Previously, you have used a USB disk to store a backup of the mailboxes of the FortiMail-400, whose fully qualified domain name (FQDN) was fortimail.example.com. You have then configured the FortiMail-2000 to also use the USB disk as its backup media. You could then import the FortiMail-400's mailbox backup to the FortiMail-2000 by entering fortimail.example.com in this field on the FortiMail-2000's web-based manager.	
start	Initiate an immediate backup. Note that all data on the backup device will be erased.	
stop	Stops any currently running backups.	

History

FortiMail v4.0 New.

Related topics

- execute restore config
- execute backup
- diagnose debug application burstd

central-mgmt

Use this command to manage the communication ID with the FortiManager central management unit and get firmware update information from the FortiManager unit.

Syntax

```
execute central-mgmt get-mgmt-id
execute central-mgmt set-mgmt-id <id>
execute central-mgmt update
```

Variable	Description	Default
`get-mgmt-id`	The FortiMail unit and the FortiManager central management unit use a unique ID to communicate with each other. This ID is assigned by the FortiManager unit. Use this command to display the ID number.	Factory set
`set-mgmt-id <id>`	Use this command to overwrite the ID.	Factory set
`update`	Use this command to display the firmware that is available for the FortiMail unit on the FortiManager unit.	

History

FortiMail v4.0 New.

Related topics

- config system central-management

certificate

Use this command to upload and download certificates, and to generate certificate signing requests (CSR).

Syntax

```
execute certificate ca import tftp <file_name> <tftp_ip>
execute certificate ca export tftp <cert_name> <file_name> <tftp_ip>
execute certificate crl import tftp <file_name> <tftp_ip>
execute certificate local export tftp <cert_name> <file_name> <tftp_ip>
execute certificate local generate <cert_name> <key_size> <subject>
   <country> <state> <organization> <unit> <email>
execute certificate local import tftp <file_name> <tftp_ip>
execute certificate remote import tftp <file_name> <tftp_ip>
execute certificate remote export tftp <cert_name> <file_name> <tftp_ip>
```

Variable	Description	Default
`ca import tftp <file_name> <tftp_ip>`	Imports the certificate authority (CA) certificate from a TFTP server. Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.	
`ca export tftp <cert_name> <file_name> <tftp_ip>`	Exports the CA certificate to a TFTP server.	
`crl import tftp <file_name> <tftp_ip>`	Imports the Certificate Revocation List. To ensure that your FortiMail unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses.	
`local export tftp <cert_name> <file_name> <tftp_ip>`	Exports a certificate signing request or a local certificate to a TFTP server. Note that this command does not support exporting a certificate in PKCS#12 format. To do this, you must go to the web-based manager.	
`local generate <cert_name> <key_size> <subject> <country> <state> <organization> <unit> <email>`	Enter the information required to generate a certificate signing request. Certificate signing request files can then be submitted for verification and signing by a certificate authority (CA).	
`local import tftp <file_name> <tftp_ip>`	Imports a local certificate from a TFTP server. Note that this command does not support importing a certificate that is in PKCS#12 format. To do this, you must go to the web-based manager. FortiMail units require a local server certificate that it can present when clients request secure connections, including: • the web-based manager (HTTPS connections only) • webmail (HTTPS connections only) • secure email, such as SMTPS, IMAPS, and POP3S	

Variable	Description	Default
`remote import tftp <file_name> <tftp_ip>`	Imports the certificate of the online certificate status protocol (OCSP) servers of your certificate authority (CA). OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).	
`remote export tftp <cert_name> <file_name> <tftp_ip>`	Exports the OCSP certificate to a TFTP server.	

History

FortiMail v4.0 New.

Related topics

- config profile certificate-binding

checklogdisk

Use this command to find and correct errors on the log disk.

Caution: Use this command only when recommended by Fortinet Technical Support. Logging is suspended while this command is executing.

Syntax

```
execute checklogdisk
```

History

FortiMail v3.0 New.

Related topics

- execute checkmaildisk
- diagnose system smartctl

checkmaildisk

Use this command to find and correct errors on the mail disk. Actions are displayed at the command prompt. If the command cannot fix an error automatically, it displays a list of manual correction options from which you must select.

Caution: Use this command only when recommended by Fortinet Technical Support. Email-related functions are suspended while this command is executing.

Syntax

```
execute checkmaildisk
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Renamed from `checkspooldisk`.

Related topics

- `execute checklogdisk`
- `diagnose system smartctl`

clearqueue

Select to remove all messages from the deferred queue.

Syntax

```
execute clearqueue
```

History

FortiMail v3.0 MR3 New.

Related topics

- execute maintain

create

Use this command to create various system-wide, domain-wide, and user-wide antispam settings, such as black/white lists and custom messages.

Syntax

```
execute create blacklist <domain> <blacklist_content>
execute create custom-message <domain> <message_content>
execute create disclaimer <domain> enable {inheader | inbody | outheader |
   outbody} <content>
execute create system-blacklist <content>
execute create system-custom-message <contents>
execute create system-whitelist <content>
execute create user-blacklist <user_name> <content>
execute create user-preference <user_name> <content>
execute create user-secondaryaddr <user_name> <content>
execute create user-whitelist <user_name> <content>
execute create whitelist <domain> <content>
```

Variable	Description	Default
`blacklist <domain> <blacklist_content>`	Creates domain-wide blacklists. For information about valid formats of the black and white lists, see the *FortiMail Administration Guide*.	
`custom-message <domain> <message_content>`	Creates domain-wide custom messages.	
`disclaimer <domain> enable {inheader | inbody | outheader | outbody} <content>`	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. Enter a domain name and enable it to use domain-wide disclaimers; if you want to input a system-wide disclaimer, do not enter a domain name. The disclaimer can be appended to the incoming email header (inheader), incoming email body (inbody), outgoing email header (outheader), and/or outgoing email body (outbody).	
`system-blacklist <content>`	Creates system-wide blacklists.	
`system-custom-message <contents>`	Creates system-wide custom messages.	
`system-whitelist <content>`	Creates system-wide white lists.	
`user-blacklist <user_name> <content>`	Creates blacklists for a specific user.	
`user-preference <user_name> <content>`	Configures the user preference settings. For details, see the User chapter in the *FortiMail Administration Guide*.	
`user-secondaryaddr <user_name> <content>`	Configures the secondary email address for the user.	

Variable	Description	Default
`user-whitelist <user_name> <content>`	Creates personal whitelists.	
`whitelist <domain> <content>`	Creates domain-wide whitelists.	

History

FortiMail v4.0 New.

Related topics

- `execute backup`

date

Use this command to set the system date.

Syntax

```
execute date <date_str>
```

Variable	Description	Default
<date_str>	Enter the system date in the format of mm/dd/yyyy.	

History

FortiMail v4.0 New.

Related topics

- config system time manual
- config system time ntp

db

Use this command to repair, rebuild, or reset the following FortiMail databases:

- Bayesian database
- Certificate database
- Dictionary database
- DKIM key database
- End point database
- End point sender reputation database
- Greylist database
- Greylist exempt database
- IBE deatabase
- Radius accounting database
- Sender reputation database
- User alias database
- User address mapping database

Syntax

```
execute db force-recover
execute db rebuild
execute db reset <database>
```

Variable	Description	Default
`force-recover`	Try to repair all of the databases using force recovery.	
`rebuild`	Clean and rebuild all of the databases.	
`reset <database>`	Clean and rebuild one of the FortiMail databases. <database> is one of the above-listed databases.	

History

FortiMail v4.0 New.

FortiMail v4.0 Patch 1 Added the reset commands.

Related topics

- `execute maintain`

factoryreset

Use this command to reset the FortiMail unit to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

Caution: Back up your configuration before entering this command. This procedure resets all changes that you have made to the FortiMail unit's configuration file and reverts the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the *FortiMail Administration Guide*.

Syntax

```
execute factoryreset
```

Example

The following example resets the FortiMail unit to default settings for the currently installed firmware version.

```
execute factoryreset
```

The CLI displays the following:

```
This operation will change all settings to
factory default! Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
System is resetting to factory default...
```

History

FortiMail v3.0 New.

Related topics

- `execute restore config`
- `execute backup`

fips

Use this command to enable Federal Information Processing Standards-Common Criteria (FIPS-CC) mode.

This enhanced security mode is required by some organizations, but may not be appropriate for others. It is valid only if you have installed a FIPS-certified firmware build. For more information on FIPS, or to obtain a certified build, contact Fortinet Technical Support.

When switching to FIPS mode, you will be prompted to confirm, and must log in again.

To disable FIPS mode, restore the firmware default configuration using `execute factoryreset`.

Caution: Back up the configuration before enabling FIPS mode. When you enable or disable FIPS-CC mode, all of the existing configuration is lost. For more information on making a complete backup, see the *FortiMail Administration Guide*.

Syntax

```
execute fips
```

History

FortiMail v4.0 New.

Related topics

- `execute factoryreset`
- `execute restore image`

formatlogdisk

Use this command to reformat the local hard disk that contains log data.

Note: Regularly format the hard disk to improve performance.

Caution: Back up all data on the disk before entering this command. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatlogdisk
```

Example

The following example formats the log disk.

```
execute formatlogdisk
```

The CLI displays the following:

```
This operation will erase all data on the log disk!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk,  Please wait a few seconds!
```

History

FortiMail v3.0 New.

Related topics

- execute partitionlogdisk
- execute formatmaildisk
- execute formatmaildisk_backup

formatmaildisk

Use this command to reformat the local hard disk that contains email data, ***without*** first performing a backup.

You can alternatively perform a backup before formatting the mail disk. For details, see "execute formatmaildisk_backup" on page 274.

Note: Regularly format the hard disk to improve performance.

Caution: Back up all data on the disk before beginning this procedure. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatmaildisk
```

Example

The following example formats the log disk.

```
execute formatmaildisk
```

The CLI displays the following:

```
This operation will erase all data on the mail disk!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk,  Please wait a few seconds!
```

History

FortiMail v3.0 New.

Related topics

- `execute formatmaildisk_backup`
- `execute formatlogdisk`

formatmaildisk_backup

Use this command to back up data contained on the mail disk to the log disk, and then format the local mail disk.

You can alternatively format the mail disk without performing a backup. For details, see “execute formatmaildisk” on page 273.

Note: Regularly format the hard disk to improve performance.

Syntax

```
execute formatmaildisk_backup
```

History

FortiMail v3.0 New.

Related topics

- execute formatmaildisk
- execute formatlogdisk

ha commands

Use this command to help debugging FortiMail HA issues.

Note: Type the full command names (such as `ha commands ...`), instead of the abbreviated names (such as `ha com ...`).

Syntax

```
execute ha commands age <time_str>
```

Variable	Description	Default
`config-sync-start`	Start synchronizing the HA cluster configuration.	
`config-sync-stop`	Stop the cluster from completing synchronizing its configuration.	
`failover-start`	Allow HA failover to happen.	
`failover-stop`	Prevent HA failover form happening.	

History

FortiMail v4.0 Patch 2 New.

Related topics

- `execute clearqueue`

ibe-data

Use this command to generate and view an IBE data file.

Syntax

```
execute ibe-data execute generate
execute ibe-data execute getinfo
```

Variable	Description	Default
generate	Generate an IBE data file.	
getinfo	Get current IBE data file information.	

History

FortiMail v4.0 New.

Related topics

- execute db

maintain

Use this command to perform maintenance on mail queues by deleting out-of-date messages.

Syntax

```
execute maintain mailqueue clear age <time_str>
```

Variable	Description	Default
`age <time_str>`	Enter an age between 1 hour and 10 years. The FortiMail unit deletes mail messages in the mail queues greater than this age. The age consists of an integer appended to a letter that indicates the unit of time: `h` (hours), `d` (days), `m` (months), or `y` (years).	`24h`

Example

This example will clear messages that are 23 days old and older.

```
execute maintain mailqueue clear age 23d
```

The CLI would display the following message:

```
Clearing messages in mail queues at least 23 days old.
```

History

FortiMail v3.0 MR3 New.

Related topics

- `execute clearqueue`

nslookup

Use this command to query the DNS server for a host name (A) or MX record. The FortiMail unit queries the DNS server configured in "config system dns" on page 173.

Syntax

```
execute nslookup host {<fqdn_str> | <host_ipv4>}
execute nslookup mx <domainname_str>
```

Variable	Description	Default
`host {<fqdn_str> | <host_ipv4>}`	Enter either an IP address or a fully qualified domain name (FQDN) of a host.	
`mx <domainname_str>`	Enter a domain name for a mail domain. For example, to determine the host that is the mail gateway for example.com, you would enter `example.com`.	

Example

You could use this command to determine the DNS resolution for the fully qualified domain name mail.example.com

```
execute nslookup host mail.example.com
```

The CLI would display the following:

```
Name:    example.com
Address: 192.168.1.15
```

Similarly, you could use this command to determine the domain name hosted on the IP address 192.168.1.15:

```
execute nslookup host 192.168.1.15
```

The CLI would display the following:

```
Address: 192.168.1.15
Name:    mail.example.com
```

You could also use this command to determine the host that is mail exchanger (MX) for the domain example.com:

```
execute nslookup mx example.com
```

The CLI would display the following:

```
example.com    mail exchanger = 10 mail.example.com.
```

History

FortiMail v3.0 New.

Related topics

- `diagnose fortiguard rating`
- `execute ping`
- `execute traceroute`
- config system dns

partitionlogdisk

Use this command to adjust the size ratio of the hard disk partitions for log and mail data.

Caution: Back up all data on the disks before beginning this procedure. Partitioning the hard disks deletes all files on those disks.

Syntax

```
execute partitionlogdisk <logpercentage_str>
```

Variable	Description	Default
`partitionlogdisk <logpercentage_str>`	Enter an integer between 10 and 90 to create a partition for log files using that percentage of the total hard disk space. The remaining partition (by default, 75% of the hard disk space) will be used for mail data.	`25`

History

FortiMail v3.0 MR4 New.

Related topics

- `execute formatlogdisk`

ping

Use this command to perform an ICMP ECHO request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by “execute ping-option” on page 282.

Pings are often used to test connectivity.

Syntax

```
execute ping {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`ping {<fqdn_str> | <host_ipv4>}`	Enter either the IP address or fully qualified domain name (FQDN) of the host.	

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms

--- 172.16.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between the FortiWeb unit and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds (ms).

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output has been displayed. The administrator halts the ping by pressing Ctrl + C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host may be down, or that there is no route between the FortiMail unit and 10.0.0.1. To determine the cause, further diagnostic tests are required, such as “execute traceroute” on page 296.

History

FortiMail v3.0 New.

Related topics

- `execute ping-option`
- `execute smtptest`
- `execute telnettest`
- `execute traceroute`
- config system dns

ping-option

Use this command to configure behavior of "execute ping" on page 280.

Syntax

```
execute ping-option data-size <bytes_int>
execute ping-option df-bit {yes | no}
execute ping-option pattern <bufferpattern_hex>
execute ping-option repeat-count <repeat_int>
execute ping-option source {auto | <interface_ipv4>}
execute ping-option timeout <seconds_int>
execute ping-option tos {default | lowcost | lowdelay | reliability |
   throughput}
execute ping-option ttl <hops_int>
execute ping-option validate-reply {yes | no}
execute ping-option view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes.This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure pattern <bufferpattern_hex>.	56
df-bit {yes | no}	Enter either yes to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter no to allow the ICMP packet to be fragmented.	no
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as 00ffaabb, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by data-size <bytes_int>.	
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto | <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either auto or a FortiMail network interface's IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2
tos {default | lowcost | lowdelay | reliability | throughput}	Enter the IP type-of-service option value, either: • default: Do not indicate. (That is, set the TOS byte to 0.) • lowcost: Minimize cost. • lowdelay: Minimize delay. • reliability: Maximize reliability. • throughput: Maximize throughput.	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes | no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	

Example

This example sets the number of pings to three and the source IP address to that of the port2 network interface, 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
        Repeat Count: 3
        Data Size: 56
        Timeout: 2
        TTL: 64
        TOS: 0
        DF bit: unset
        Source Address: 10.10.10.1
        Pattern:
        Pattern Size in Bytes: 0
        Validate Reply: no
```

History

FortiMail v3.0 New.

Related topics

- execute ping
- execute traceroute

radius-accounting

Use this command to back up or delete a Radius accounting database.

Syntax

```
execute radius-accounting execute backup
execute radius-accounting execute delete
```

Variable	Description	Default
backup	Back up the Radius accounting database.	
delete	Delete the Radius accounting database.	

History

FortiMail v4.1 New.

Related topics

- execute db

raid-add-disk

Use this command to find and add a hard disk to the array unit after you insert a second hard disk into the drive bay of a FortiMail-400B unit.

Note: This command is for FortiMail-400B models only.

Syntax

```
execute raid-add-disk
```

Example

You could notify the RAID controller to add the hard disk to the array unit after inserting a new hard disk.

```
execute raid-add-disk
```

The CLI displays the following:

```
This operation will scan for new hard drives and add them into the RAID array
Do you want to continue? (y/n)
```

After you enter `y` (yes), if all hard disks have already been added to an array, the CLI displays the following:

```
existing raid disk at 12 is 120034123776
existing raid disk at 13 is 120034123776
no NEW disks in the system
```

History

FortiMail v3.0 MR4 Patch 4 New.

Related topics

- `get system status`

reboot

Use this command to restart the FortiMail unit.

Syntax

```
execute reboot
```

Example

The following example reboots the FortiMail unit.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

History

FortiMail v3.0 New.

Related topics

- `execute shutdown`

reload

If you set your console to batch mode, use this command to flush the current configuration from system memory (RAM) and reload the configuration from a previously saved configuration file.

In addition, you can also use this command to reload individual daemons that have crashed. In this case, the command is as following:

```
exec reload [{httpd | ...}]
```

where [{httpd | ...}] indicates the name of a specific daemon that you want to restart, if you want to limit the reload to a specific daemon.

For example, if HTTP and HTTPS access are enabled, but you cannot get a connection response on webmail or the GUI, although you can still connect via SSH and ping. Thus you know that the FortiMail unit has not crashed entirely. If you do not want to reboot because this would interrupt SMTP, you can choose to restart the HTTP daemon only.

```
FortiMail-400 # exec reload httpd
Restart httpd?
Do you want to continue? (y/n)y

Reloading httpd....done
```

Note that the command does not check whether your indicated daemon actually exists. It simply indicates whether the command is executed. If the command does not take a few seconds to execute, it is possible that the daemon does not really exist.

Syntax

```
execute reload [<daemon_name>]
```

History

FortiMail v3.0 New.

Related topics

- execute reboot
- execute restore config
- execute restore image
- diagnose debug application cmdb_event
- diagnose system top

restore as

use this command to restore an antispam configuration file from a TFTP server.

Syntax

```
execute restore as tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

History

FortiMail v4.0 New.

Related topics

- execute restore av

restore av

use this command to restore an antivirus configuration file from a TFTP server.

Syntax

```
execute restore av tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

History

FortiMail v4.0 New.

Related topics

- execute restore as

restore config

Use this command to restore a primary configuration file from a TFTP server.

Caution: Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the *FortiMail Administration Guide*.

Note: Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiMail unit to its firmware/factory default configuration. For information on installing firmware via TFTP boot interrupt, see the *FortiMail Administration Guide*.

Syntax

```
execute restore config {tftp <filename_str> <server_ipv4> |
   management-station {normal | template} <revision_int>}
```

Variable	Description	Default
`<filename_str>`	If you want to restore a configuration file stored on a TFTP server, enter the name of the configuration file.	
`<server_ipv4>`	If you want to restore a configuration file stored on a TFTP server, enter the IP address of the TFTP server.	
`management-station {normal | template}`	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the `management-station` keyword then enter either: • `normal`: Restore a configuration revision number. • `template`: Apply a template revision number.	
`<revision_int>`	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the revision number of the configuration file or template.	

Example

This example restores configuration file revision 2, which is stored on the FortiManager unit.

```
execute restore config management-station normal 2
```

The CLI displays the following:

```
This operation will overwrite the current settings!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
Connect to FortiManager ...
Please wait...
```

Example

This example restores a configuration file from a TFTP server at 172.16.1.5.

```
execute restore config tftp fml.cfg 172.16.1.5
```

The CLI displays the following:

```
This operation will overwrite the current settings!
(The current admin password will be preserved.)
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following, then terminates the SSH connection and reboots with the restored configuration:

```
Connect to tftp server 172.16.1.5 ...
Please wait...

Get config file from tftp server OK.
File check OK.
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR4	Added keyword `management-station` for restoring files from the FortiManager unit.

Related topics

- `execute backup`
- `execute factoryreset`
- config system central-management

restore image

Use this command to restore a firmware file from a TFTP server or FortiManager unit.

Caution: Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the *FortiMail Administration Guide*.

Syntax

```
execute restore image {tftp <filename_str> <server_ipv4> |
   management-station <image_id>}
```

Variable	Description	Default
`<filename_str>`	If you want to restore a firmware file stored on a TFTP server, enter the name of the firmware file backup file.	
`<server_ipv4>`	If you want to restore a firmware file stored on a TFTP server, enter the IP address of the TFTP server.	
`management-station <image_id>`	If you want to restore a firmware file stored on a FortiManager unit, enter the `management-station` keyword then enter the ID number of the firmware file.	

Example

This example restores firmware file FE_2000A-v300-build397-FORTINET.out, which is stored on the TFTP server 192.168.1.20.

```
execute restore image tftp FE_2000A-v300-build397-FORTINET.out 192.168.1.20
```

The CLI displays the following:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
Connect to tftp server 192.168.1.20 ...
Please wait...
#######################
Get image from tftp server OK.
Check image OK.
```

History

FortiMail v3.0 New.

FortiMail v3.0 MR4 Added `management-station` for restoring files from the FortiManager unit.

Related topics

- `execute restore config`
- config system central-management

shutdown

Use this command to prepare the FortiMail unit to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Caution: Power off the FortiMail unit only after issuing this command. Unplugging or switching off the FortiMail unit without issuing this command could result in data loss.

Syntax

```
execute shutdown
```

Example

The following example halts the FortiMail unit.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

History

FortiMail v3.0 New.

Related topics

- `execute reboot`

smtptest

Use this command to test SMTP connectivity to a specified host.

Syntax

```
execute smtptest {<fqdn_str> | <host_ipv4>}[:<port_int>] [domain
   <domain_str>]
```

Variable	Description	Default
{<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	No default.
[:<port_int>]	If the SMTP server listens on a port number other than port 25, enter a colon (:) followed by the port number.	:25
[domain <domain_str>]	If you want to test the connection from an IP address in the protected domain's IP pool, enter the name of the protected domain.	No default.

Example

This example tests the connection to an SMTP server at 192.168.1.10 on port 2525. For the outgoing connection, the FortiMail unit uses the source IP address 192.168.1.20 from the IP pool selected in the protected domain example.com.

```
execute smtptest 192.168.1.10:2525 domain example.com
```

The CLI displays the following:

```
(using 192.168.1.20 to connect)
Remote Output:
    220 fortimail.example.com ESMTP Smtpd; Mon, 19 Jan 2009
 13:27:35 -0500
Connection Status:
    Connecting to remote host succeeded.
```

History

FortiMail v3.0 New.

Related topics

- execute telnettest
- execute traceroute
- execute ping
- config system dns

telnettest

Use this command to test Telnet connectivity to a specified host.

Syntax

```
execute telnettest {<fqdn_str> | <host_ipv4>}[:<port_int>]
```

Variable	Description	Default
{<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the Telnet server.	No default.
[:<port_int>]	If the Telnet server listens on a port number other than port 23, enter a colon (:) followed by the port number.	:23

Example

This example tests the connection to an Telnet server at 192.168.1.10 on port 2323.

```
execute telnettest 192.168.1.10:2323
```

The CLI displays the following:

```
(using 192.168.1.20 to connect)
Remote Output(hex):
    FF FD 18 FF FD 20 FF FD
    23 FF FD 27
Connection Status:
    Connecting to remote host succeeded.
```

History

FortiMail v3.0 New.

Related topics

- execute smtptest
- execute traceroute
- execute ping
- config system dns

traceroute

Use this command to use ICMP to test the connection between the FortiMail unit and another network device, and display information about the time required for network hops between the device and the FortiMail unit.

Syntax

```
execute traceroute {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`traceroute {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example tests connectivity between the FortiMail unit and http://docs.fortinet.com. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiMail# execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte
  packets
 1  172.16.1.200 (172.16.1.200)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
 1 172.16.1.2   0 ms  0 ms  0 ms
 2  10.10.10.1  <static.isp.example.net>  2 ms  1 ms  2 ms
 3  10.20.20.1   1 ms   5 ms   1 ms
 4  10.10.10.2  <core.isp.example.net>  171 ms  186 ms  14 ms
 5  10.30.30.1  <isp2.example.net>  10 ms  11 ms  10 ms
 6  10.40.40.1  73 ms  74 ms  75 ms
 7 192.168.1.1  79 ms  77 ms  79 ms
 8 192.168.1.2  73 ms  73 ms  79 ms
 9 192.168.1.10 73 ms  73 ms  79 ms
10 192.168.1.10 73 ms  73 ms  79 ms
```

Example

This example attempts to test connectivity between the FortiMail unit and example.com. However, the FortiMail unit could not trace the route, because the primary or secondary DNS server that the FortiMail unit is configured to query could not resolve the FQDN `example.com` into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiMail# execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiMail unit with the IP addresses of DNS servers that are able to resolve the FQDN `example.com`. For details, see “system dns” on page 173.

History

FortiMail v3.0 New.

Related topics

- `execute smtptest`
- `execute telnettest`
- `execute ping`
- `execute ping-option`
- config system dns

update-now

Use this command to manually request updates to the FortiGuard Antivirus and FortiGuard Antispam engine and definitions from the FortiGuard Distribution Network (FDN).

You can alternatively or additionally configure scheduled updates and push updates. For details, see “config system fortiguard antivirus” on page 176 and “config system fortiguard antispam” on page 178.

Syntax

```
execute updatenow
```

History

FortiMail v3.0 New.

Related topics

- config system fortiguard antivirus
- config system fortiguard antispam
- `diagnose debug application updated`

userconfig

Use this command to generate a file with the latest user-specific configurations, such as user preferences, personal black/white lists, and secondary addresses, to the user configuration file, so that you will have the latest configuration when you make a configuration backup using `execute backup`.

Syntax

```
execute userconfig generate
execute userconfig getinfo
```

Variable	Description	Default
`generate`	Updates the user configuration file with the latest user-specific configuration.	
`getinfo`	Displays the timestamp when the last configuration file update was performed.	

History

FortiMail v4.0 New.

Related topics

- `execute backup`

get

`get` commands display a part of your FortiMail unit's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays ***all*** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
FortiMail# get system dns

primary             : 172.16.95.19
secondary           : 0.0.0.0
private-ip-query    : enable
cache               : enable
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has been reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
FortiMail# get system dns
```

and this command would not:

```
FortiMail# get
```

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding config commands in the `config` chapter.

Other `get` commands, such as `get system performance`, are used to display system information that is ***not*** configurable. This chapter describes this type of `get` command.

This chapter describes the following commands.

`get system performance`

`get system status`

Note: Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show and show full-configuration` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see "config" on page 33.

system performance

Displays the FortiMail unit's CPU usage, memory usage, system load, and up time.

Syntax

```
get system performance
```

Example

```
FortiMail# get system performance
CPU usage:     0% used, 100% idle
Memory usage:  17% used
System Load:   5
Uptime:        0 days,  8 hours,  24 minutes.
```

History

FortiMail v4.0 New.

Related topics

- get system status

system status

Use this command to display FortiMail system status information including:

- firmware version, build number and date
- antivirus definition version and release date and time
- FortiMail unit serial number and BIOS version
- log hard disk availability
- mailbox disk availability
- host name
- operation mode
- distribution scope
- branching point (same as firmware build number)
- release version
- system time

Syntax

```
get system status
```

Example

```
FortiMail-400 # get system status
Version: FortiMail-400 v4.0.0,build0087,091105
Virus-DB: 11.23(11/05/2009 01:20)
Serial-Number: FE-4002905500226
BIOS version: 04000000
Log disk: Capacity 20 GB, Used 1 GB ( 8.27%), Free 18 GB
Mailbox disk: Capacity 89 GB, Used 278 MB ( 0.31%) , Free 89 GB
Hostname: FortiMail-400
Operation Mode: Transparent
Distribution: International
Branch point: 087
Release Version Information: v4.0.0
System time: Thu Nov  5 16:25:31 2009
```

History

FortiMail v4.0 New.

Related topics

- get system performance

show and show full-configuration

The `show` commands display a part of your FortiMail unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

Note: Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see "Command syntax" on page 19.

Unlike `get`, `show` does ***not*** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
FortiMail# show system dns
config system dns
  set primary 172.16.1.10
  set secondary 172.16.1.11
end
```

Notice that the command only displays the setting for the primary and secondary DNS server settings. This indicates that these settings have been configured.

On the contrary, the `show full-configuration` commands display the full configuration, including the default settings.

For example:

```
FortiMail# show full-configuration system dns
config system dns
  set primary 172.16.1.10
  set secondary 172.16.1.11
  set private-ip-query enable
  set cache enable
end
```

Notice that the command displays the default settings for private IP query and DNS query cache as well.

Index

Symbols

Numerics

A

B

C

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

www.fortinet.com

www.fortinet.com